555-7001-301

Meridian 1

Meridian Mail
System Administration Guide

Product release 12 Standard 1.0 January 1998

NORTEL
NORTHERN TELECOM

P0875914

Meridian 1

Meridian Mail
System Administration Guide

Publication number:	555-7001-301
Product release:	12
Document release:	Standard 1.0
Date:	January 1998

© 1993, 1994, 1995, 1996, 1997, 1998 Northern Telecom
All rights reserved

Printed in the United States of America

Information is subject to change without notice. Northern Telecom reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

Meridian 1, Meridian, and Nortel are trademarks of Northern Telecom.

Publication history

January 1998	Manual released as Standard 1.0. This version of the *Meridian Mail System Administration Guide* is intended for Meridian Mail Release 12 base software.
November 1996	Manual released as Standard 1.0. This version of the *Meridian Mail System Administration Guide* is intended for Meridian Mail Release 11 base software.
August 1995	Manual released as Standard 1.0. This version of the *Meridian Mail System Administration Guide* is intended for Meridian Mail Release 10 base software.
April 1995	Manual released as Standard 1.0. This version of the *Meridian Mail System Administration Guide* is intended for Meridian Mail Release 9.5 base software.
March 1994	Manual released as Standard 1.0. This version of the *Meridian Mail System Administration Guide* is intended for Meridian Mail Release 9 base software.
April 1993	Manual released as Standard 1.0. This version of the *Meridian Mail System Administration Guide* is intended for Meridian Mail Release 8 base software.

Contents

1 About this guide 1-1

Overview 1-2
What this guide is about 1-3
Who should use this guide 1-4
Systems supported by this guide 1-5
Structure of this guide 1-6
Typographic conventions 1-11
Referenced documents 1-14

2 Navigating through system administration 2-1

Overview 2-2

Section A: The administration menu hierarchy 2-3

The system administration menu hierarchy 2-4
The Main menu 2-6
User administration 2-7
General administration 2-8
Voice administration 2-10
Hardware administration 2-14
System status and maintenance 2-15
Operational measurements 2-18
Class of Service administration 2-20
Fax administration 2-21
Network administration 2-22
Hospitality administration 2-23

Section B: Understanding menus, screens, and keys 2-25

Overview 2-26
Keypad functions 2-27
Meridian Mail menus 2-28
Meridian Mail screens 2-31
Getting around in screens 2-33
Entering information in fields 2-34

Softkeys 2-39
Getting help 2-40
Error messages 2-41

Section C: Meridian Mail features and interfaces 2-43
The main administration terminal and multiple administration terminals (MATs) 2-44
Meridian Mail feature availability 2-46
Meridian Mail telset interfaces 2-48

3 Logging on 3-1
Overview 3-2
Types of consoles 3-3
Logon/Status screen 3-4
Setting the system administration password 3-6
Changing the system administration password 3-8
Recovering a system administration password 3-10
Logging on from the main administration terminal 3-11
Logging on from a MAT 3-13
Logging on from a remote terminal (non-EC system) 3-15
Logging on from a remote terminal (EC system) 3-18
Using a single terminal to access the M1 and Meridian Mail 3-23

4 Setting up the system 4-1
Overview 4-2

Section A: Basic setup procedures 4-3
Overview 4-4
Changing the system administration password 4-5
Checking the hardware configuration 4-6
Checking the system status 4-7
Checking the Channel Allocation Table 4-8
Configuring general system options 4-9
Setting up dialing translations 4-10
Setting up restriction and permission lists 4-11
Customizing voice messaging options 4-12
Adding networking information to a network database . . . 4-13
Adding DNs to the VSDN table 4-14

Defining classes of service 4-15
Configuring operational measurement options 4-16
Adding users to the system 4-17
Creating system distribution lists 4-18
Configuring optional features and other services 4-19
Setting up system security 4-20
Backing up the system 4-21

Section B: Setting up optional features 4-23
Overview 4-24
Setting up the Outcalling feature 4-25
Setting up the Voice Menus feature 4-26
Setting up the Voice Forms feature 4-27
Setting up the Fax on Demand feature 4-28
Setting up the Meridian Networking feature 4-29
Setting up the AMIS Networking feature 4-30
Setting up the Virtual Node AMIS Networking feature . . . 4-31
Setting up the Enterprise Networking feature 4-32
Setting up the Network Message Service feature 4-33
Setting up the Hospitality feature 4-34
Setting up the Meridian Mail Reporter feature 4-35
Setting up the Meridian Mail AutoAdmin feature 4-36
Setting up the ACCESS feature 4-37

5 Making voice recordings 5-1
Overview 5-2
Types of recordings 5-4
How Call Answering uses personal greetings and personal verifications 5-7
Voice recording tips 5-11

Section A: Making recordings 5-13
Overview 5-14
Logging in to Meridian Mail 5-15
Recording a call answering greeting 5-18
Recording personal greetings 5-24
Recording a personal verification 5-26
Recording a personal verification for a system distribution list 5-31

Identifying remote site names 5-34
Recording a personal verification for the broadcast mailbox 5-37
Recording and sending broadcast messages 5-39
Making Voice Services recordings 5-43

Section B: VMUIF recordings 5-47
Overview 5-48
VMUIF introductory tutorials and the VMUIF login greeting. 5-49
Recording the VMUIF login greeting 5-52

6 Setting up Meridian Mail security 6-1
Overview 6-2

Section A: Telecommunication criminals and the problems they pose 6-3
Overview 6-4
Designing a security system 6-7
Ongoing security measures 6-8

Section B: Using Basic Access Restrictions features 6-9
Overview 6-10
Trunk Group Access Restrictions 6-11
Class of Service 6-13
TGAR/TARG and CLS interaction 6-17
Transfer feature on modems 6-19

Section C: Features that modify access restrictions 6-21
Overview 6-22
System Speed Call. 6-23
Authorization Codes 6-24
Station Specific Authorization Codes 6-25
Forced Charge Account. 6-27
Controlled Class of Service 6-29
Enhanced Controlled Class of Service 6-32
Flexible Feature Codes—Electronic Lock 6-33
Code Restriction 6-34
New Flexible Code Restriction 6-36

Section D: Controlling remote access to calling privilege 6-39
Overview 6-40
Call Forward All Calls 6-41
Call Forward External Deny 6-42
Call Forward to Trunk Access Code—DID Calls 6-43
Internal Call Forward 6-44
Flexible Feature Codes—Remote Call Forward 6-45
User Selectable Call Redirection 6-46

Section E: Controlling access through Least Cost Routing (BARS/NARS) 6-47
Overview 6-48
Supplemental Digit Recognition 6-50
Supplemental Digit Restriction 6-52
Network Class of Service—Facility Restriction Level 6-55
Network Speed Call 6-58
Network Authorization Code 6-60
Authorization Code Conditionally Last 6-61
Time-of-Day Routing 6-64
Routing Control 6-67
Incoming Trunk Group Exclusion 6-70

Section F: Controlling access to PBX administration programs 6-73
Overview 6-74
Password control 6-75
Limited access to overlays 6-77
Limited access password—user name 6-78
Single Terminal Access 6-79
Multi-user login 6-80
Input/Output port recovery 6-81
History file 6-82

Section G: Controlling Direct Inward System Access 6-83
Overview 6-84
DISA and security codes 6-85
DISA and Class of Service 6-86
DISA and authorization codes 6-87

Section H: Restriction/Permission lists 6-89
Overview 6-90
What are restriction/permission lists and codes? 6-91
Defaults 6-93
Understanding how restriction/permission codes work . . . 6-94
Recommendations for using the first four restriction/ permission lists 6-97
Defining and applying restriction/permission lists 6-99

Section I: Controlling access to Meridian Mail services and features 6-103
Overview 6-104
Custom Revert 6-106
Thru-Dial 6-109
Call Answering or Express Messaging 6-110
Extension dialing (mailbox thru-dial) 6-112
Fax on Demand 6-115
Remote Notification 6-116
Delivery to Non-User 6-118
External Call sender 6-120
AMIS Networking 6-121

Section J: Controlling access to Meridian Mail mailboxes 6-123
Overview 6-124
Using the Voice Security Options screen 6-125
Default security settings 6-131
Initial password change 6-133
Password display suppression 6-135
Password prefix 6-136
Password length 6-138
Forced regular password changes 6-139
Invalid logon attempts 6-142
Modifying mailbox security settings 6-146
Restricting off-site access to mailboxes 6-147
Disabling unused mailboxes 6-148

Section K: Monitoring access to Meridian Mail mailboxes and features **6-149**
Overview 6-150
Hacker Monitor 6-151
Mailbox Login Monitoring 6-152
Thru-Dial Monitoring 6-154
CLID Monitoring 6-157
The Services Summary Traffic report 6-160

Section L: Equipment security **6-161**
Overview 6-162
Switchroom access 6-163
Administration terminals 6-164
Meridian Mail and switch printouts 6-165

7 User administration—an overview 7-1

Section A: Introduction to User Administration **7-3**
The User Administration menu 7-4
Types of users 7-7
Distribution lists 7-10
Limitations and guidelines 7-11
Support for multiple appearance DNs 7-12

Section B: New user planning **7-15**
Overview 7-16
Class of service planning 7-17
Distributing local voice users evenly over volumes 7-19
Guidelines for adding users to a system that has disk shadowing 7-21
Guidelines for adding a large number of users 7-22
How user models in pre-Release 9 systems are converted to classes of service 7-23

8 Local voice users 8-1

Section A: Adding local voice users **8-3**
Integrated mailbox administration 8-4
Before you begin adding local voice users 8-5
Adding a local voice user 8-6

Setting the default administration context for NMS 8-8
Accessing the Add Local Voice User screen 8-10
The Add Local Voice User screen 8-13
Entering user information 8-15
Assigning a user to a class of service 8-20
Primary DN and extension DNs 8-24
The revert DN 8-26
The message waiting indication DN 8-29
Specifying the primary DN, extension DNs,
the revert DN, and message waiting indication DN 8-31
Recording a personal verification for a user 8-34
Creating a remote notification schedule for a user 8-36
Setting other local voice user characteristics 8-39

Section B: Finding local voice users 8-45
Overview 8-46
Wildcard characters 8-47
Accessing the Find Local Voice Users screen 8-49
The Find Local Voice Users screen 8-50
Restrictions on how you can combine search criteria 8-67
Finding, listing, and printing local voice users 8-69
Reassigning a subset of local voice users to another
class of service 8-73

Section C: Modifying and deleting local voice users 8-79
Accessing the View/Modify Local Voice User screen 8-80
Viewing and modifying a local voice user 8-84
Checking a user's status 8-86
Enabling a disabled mailbox 8-91
Changing a user's password 8-93
Monitoring mailbox logins for suspected hacker activity . . 8-94
Reassigning a mailbox to another user 8-96
Deleting a local voice user 8-97

9 Remote voice users 9-1

Section A: Introduction 9-3
What is a remote voice user?. 9-4
Remote voice user changes and enhancements 9-6
Permanent remote voice users 9-8
Temporary remote voice users 9-9

Section B: Adding remote voice users 9-11
The Add Remote Voice User screen 9-12
Adding remote voice users through User Administration . . 9-17
Recording a personal verification for a remote voice user . 9-19
Adding temporary remote voice users using RVU Propagation via Enterprise Networking 9-21
Adding remote voice users using RVU Propagation via Bulk Provisioning 9-24

Section C: Finding remote voice users 9-27
Accessing the Find Remote Voice Users screen 9-28
The Find Remote Voice Users screen 9-29
Wildcard characters 9-32
Finding, listing, and printing remote voice users 9-34

Section D: Modifying and deleting remote voice users 9-39
Viewing and modifying remote voice users 9-40
Manually deleting remote voice users 9-45
How temporary remote voice users are automatically deleted from the system 9-49

10 Directory entry users 10-1
Overview 10-2
What is a directory entry user? 10-3
The Add Directory Entry User screen 10-4
Adding directory entry users 10-7
Recording a personal verification 10-8
The Find Directory Entry Users screen 10-10
Finding directory entry users 10-12
The List of Directory Entry Users screen 10-13
Printing directory entry users 10-15
Viewing or modifying directory entry users 10-16
Deleting directory entry users 10-18

11 Distribution lists 11-1
Overview 11-2
Understanding distribution lists 11-3
Limitations on distribution lists 11-4
Accessing the Distribution Lists softkeys screen 11-7

Adding a system distribution list 11-9
Finding and viewing a system distribution list 11-17
Modifying a system distribution list 11-22
Printing a system distribution list 11-24
Deleting a system distribution list 11-26

12 General administration–an overview 12-1
General Administration 12-2

13 General options 13-1
Overview 13-2
Accessing the General Options screen 13-3
Modifying the system name and system number 13-5
Defining the system addressing length and the supervised transfer delay 13-8
Verifying installed features 13-11
Assigning classes of service to the system 13-13
Setting the attendant DN 13-15
Setting the date format for reports 13-18
Setting printer port names 13-20

14 Volume administration 14-1
Overview 14-2
Volume names 14-3
Volume contents 14-5
Volume distribution on single- and multi-node systems . . . 14-7
Voice storage capacity in single- and multi-node systems . 14-8
Checking volume capacity and usage levels for your system 14-10

15 Back up and restore Meridian Mail data 15-1
Overview 15-2

Section A: Preparing for backups 15-3
Overview 15-4
The three types of backups 15-5
Selective backup 15-6
Partial backup 15-8
Full backup 15-9
Volumes to back up 15-10
How often to do backups 15-11
Disk backup or tape backup 15-13
Before you perform a backup 15-14

Section B: Full and partial backups to tape 15-15
Overview 15-16
Performing a full backup to tape 15-18
Performing a partial backup to tape 15-20

Section C: Selective backup of users and services 15-23
Overview 15-24
Backing up all users 15-25
Backing up individual users 15-27
Backing up all users in a specified volume 15-29
Backing up all users assigned to a particular class of service 15-31
Backing up all users in a specific department 15-33
Backing up all multimedia services 15-35
Backing up selected individual multimedia services 15-37

Section D: Partial backups to disk 15-39
Performing a partial backup to disk 15-40

Section E: Scheduled backups 15-41
Scheduling the backup for a later time 15-42
Deleting a scheduled backup 15-45

Section F: Backup maintenance 15-47
Checking the status of a backup 15-48
Cleaning/maintaining the tape drive 15-52

Section G: Restoring information from a Selective backup 15-53
Overview 15-54
Restore from Selective backup 15-56

16 Password and system time changes 16-1
Overview 16-2
Changing the system administrator password 16-3
Changing the customer administrator password for MATs and Meridian Mail AutoAdmin 16-5
Setting the minimum password length for all administrator passwords 16-7
The AdminPlus Download password 16-8
Changing the system time 16-10

17 Dialing translations 17-1
Overview 17-2

Section A: Introduction to dialing translations 17-3
Overview 17-4
Dialing translations 17-5
Default dialing prefixes and local system defaults 17-7
When default dialing translations defaults are required . . 17-10
Translation tables 17-12
When translation tables are required 17-14

Section B: How dialing translations work 17-17
Overview 17-18
How Meridian Mail collects digits 17-19
How dialing translations translate numbers 17-22
How Meridian Mail uses the dialable number 17-27

Section C: Setting up network dialing prefixes and local defaults 17-29
Overview 17-30
Worksheet for default dialing prefixes and local system defaults 17-31
Dialing translation defaults screen 17-33
Configuring the default dialing prefixes and local system defaults 17-37
Sample datafills for dialing translation defaults 17-40

Section D: Setting up translation tables 17-43
Overview 17-44
Identifying translation table requirements. 17-45
Identifying translation tables required on your system . . . 17-48
Local dialing to a different area/city code (area/city code required) 17-52
Local dialing to a different area/city code (no area/city code required) 17-56
Long distance dialing to the same area/city code (area/city code required) 17-59
Long distance dialing to the same area/city code (area/city code not required) 17-61
The View/Modify Translation Table screen 17-62
Configuring translation tables 17-64
Deleting translation tables 17-67

Section E: Sample datafills 17-69
Overview 17-70
Datafill for countries without area/city codes 17-71
Datafill for a case where the switch handles dialing translation 17-72

Section F: Troubleshooting dialing translations 17-75
Overview 17-76
Diagnosing and tracing problems in a dialing translation . 17-77

18 Routine maintenance 18-1

Overview 18-2
Monitoring Meridian Mail operation 18-3
Monitoring Meridian Mail hardware. 18-5
Backing up the system. 18-7
Cleaning the tape drive 18-9

19 Voice administration—an overview 19-1

Voice Administration 19-2

20 Voice messaging options 20-1

Section A: Introduction 20-3
Overview 20-4
Accessing the Voice Messaging Options screen. 20-5
The Voice Messaging Options screen. 20-6
Defining voice messaging options 20-9

Section B: Languages on multilingual systems 20-11
Overview 20-12
The default language and the user's preferred language. . 20-13
Setting up languages on systems without dual language prompting 20-15
Setting up languages on systems with dual language prompting 20-19

Section C: Customizing recordings 20-27
Overview 20-28
Recording a customized call answering greeting 20-29
VMUIF introductory tutorials and the VMUIF login greeting. 20-32
Recording or disabling VMUIF tutorials and login greeting. 20-34

Section D: Defining operational characteristics for voice messaging 20-37
Overview 20-38
Enabling/disabling timed delivery and name dialing/name addressing 20-40
Defining the lockout revert DN and personal distribution list prefix 20-45
Setting up the broadcast mailbox 20-47
Defining the billing DN. 20-51
Specifying the message delivery priority for networked systems 20-53
Specifying the mailbox full warning threshold 20-55
Specifying the maximum read message retention 20-57
Enabling/disabling external call sender. 20-60
Enabling and configuring speed control 20-62

21 Display options 21-1
Overview 21-2
Different ways of sorting the VSDN table 21-3
Different ways of sorting the service definitions tables . . . 21-5
Different ways of sorting the Choice of Services and Menu Actions list 21-7
Changing the display options 21-9

22 Finding and printing VSDNs and service definitions 22-1
Overview 22-2
Wildcards 22-5
The Find Subset of VSDNs/Services screen 22-7
Finding and printing VSDNs. 22-9
Finding and printing service definitions 22-11

23 Configuring Meridian Mail services 23-1

Overview 23-2

Section A: Introduction 23-3

Automatic Call Distribution (ACD) 23-4
Meridian 1 – Meridian Mail connections 23-6
How Meridian Mail uses ACD 23-7
Types of queues. 23-9
Assigning DNs to services in the VSDN table 23-11

Section B: Planning your configuration 23-13

Overview 23-14
Types of Meridian Mail ports 23-15
Port requirements for Meridian Mail services. 23-18
Identifying the ports that are installed on your system . . . 23-20
Should you dedicate ports? 23-23
Dedicating ports because of mixed port types. 23-24
Dedicating ports to services 23-26
Determining how many ACD queues you need 23-28
Determining how many dummy queues you need 23-29

Section C: Configuring the Meridian 1 for Meridian Mail services 23-31

Overview 23-32
Creating ACD queues for a totally shared configuration . 23-33
Creating ACD queues for a combination (shared and dedicated) configuration 23-35
Partially dedicating ports – blocking inbound calls only . 23-40
Partially dedicating ports – blocking outbound calls only 23-43
Fully dedicating ports – blocking inbound and outbound calls 23-49
Creating an agent queue 23-52
Adding agents to a queue 23-55
Creating a dummy queue. 23-59
Moving agents from one queue to another 23-61
Removing agents from a queue. 23-63
Modifying the Channel Allocation Table after moving agents 23-64

24 The VSDN table 24-1

Section A: Introduction 24-3
Overview 24-4
When to create a VSDN 24-5
Network Message Service requirements 24-6
Accessing the VSDN table 24-7
The VSDN table 24-9

Section B: Adding messaging VSDNs 24-11
Overview 24-12
Adding a VSDN for Voice Messaging 24-13
Adding a VSDN for Express Messaging. 24-15
Adding a VSDN for Call Answering 24-17
Adding a VSDN for hospitality voice messaging 24-19
Adding a VSDN for the Post-Checkout Mailbox service . 24-22
Adding a VSDN for the Greetings Service 24-24

Section C: Adding networking and ACCESS VSDNs 24-27
Overview 24-28
Adding a VSDN for AMIS Networking 24-29
Adding a VSDN for Meridian Networking 24-31
Adding a VSDN for Enterprise Networking 24-33
Adding a VSDN for a Meridian ACCESS application . . . 24-36

Section D: Adding voice service and fax service DNs 24-39
Overview 24-40
Adding a VSDN for an announcement 24-41
Adding a VSDN for a thru-dial service. 24-43
Adding a VSDN for a voice menu 24-45
Adding a VSDN for a time-of-day controller 24-48
Adding a VSDN for Voice Prompt Maintenance 24-52
Adding a VSDN for Remote Activation 24-54
Adding a VSDN for a voice form 24-56
Adding a VSDN for the Transcription Service 24-58
Adding a VSDN for the Fax Information Service. 24-61
Adding a VSDN for the Fax Item Maintenance Service. . 24-64

Section E: Session profiles 24-67
What is a session profile? 24-68
How session profiles work when multiple services are invoked by one VSDN 24-70

How Meridian Mail 9/10 session profiles are converted to Meridian Mail 12 session profiles 24-72
Fax callback number formats 24-74
Determining how many VSDNs you need for a callback fax service 24-78
The basic service session profile 24-81
The full-service voice session profile 24-83
The full-service multimedia session profile 24-86
Customizing the session profile for Voice Menus, Fax Items, and Time-of-Day Controllers 24-90
Specifying the channel capability, session time limit, and maximum number of invalid selections 24-92
Specifying fax service options 24-96
Specifying callback delivery options 24-102
Creating a custom cover sheet 24-107
Customizing the session profile for the Fax Item Maintenance Service 24-109

Section F: Viewing, modifying, and deleting VSDNs 24-115
Viewing and modifying a VSDN or session profile, or both 24-116
Deleting a VSDN 24-119

25 Voice services profile 25-1
Overview 25-2
Timeouts 25-3
How timeouts work 25-4
Modifying the voice services profile 25-6

26 Class of Service administration 26-1
Overview 26-2

Section A: Introduction to Class of Service 26-3
What is a Class of Service? 26-4
System Class of Service versus Personal Class of Service . 26-6
How Class of Service is administered 26-7

Section B: Adding, changing, printing, and deleting System Classes of Service 26-9
Adding a Class of Service 26-10
The Add Class of Service screen (MMUI) 26-13
The Add Class of Service screen (VMUIF) 26-30
Assigning Classes of Service to the system 26-49
The Find Class of Service screen 26-50
Finding, listing, or printing a Class of Service 26-51
Modifying a Class of Service 26-54
Deleting a Class of Service 26-59

Section C: Assigning Classes of Service to users 26-63
Assigning a Class of Service to a user 26-64
Creating and Assigning a Personal Class of Service to a user 26-65
The Class of Service conversion utility for converted systems 26-66

27 Hardware administration 27-1
Overview 27-2
The Hardware Administration menu 27-3

Section A: Viewing the node configuration 27-5
Overview 27-6
The Node Configuration screen 27-7
The View Node screen 27-10

Section B: Viewing the data port configuration 27-17
Overview 27-18
The Data Port Configuration screen 27-23
Viewing data ports 27-25
View Terminal data ports 27-27
View Printer data port 27-30
View MMLink data port 27-32
View/Modify NWModem data port 27-34
View PMS data port 27-36
View AdminPlus data port 27-38
View Modem data port 27-40
View MSLink data port 27-42

Section C: Printing node and data port information 27-45
Overview 27-46
Printing node and data port information 27-47

28 System status and maintenance 28-1
Overview 28-2
What is system status and maintenance?. 28-3

Section A: System Status 28-5
Overview 28-6
The System Status screen 28-8
Disabling/activating the system (“Courtesy Down”) 28-15
Disabling/enabling nodes 28-17
Courtesy disabling/enabling ports 28-18

Section B: Card Status 28-19
Overview 28-20
The Card Status screen 28-21
Enabling/disabling cards 28-27
Running out-of-service diagnostics. 28-28

Section C: DSP Port Status 28-29
Overview 28-30
The DSP Port Status screen. 28-31
Detailed view of the DSP Port Status screen 28-38
Single mode and range mode 28-39
Disabling/enabling DSP ports in single mode. 28-40
Disabling/enabling DSP ports in range mode 28-42

Section D: Channel Allocation Table 28-45
Overview 28-46
The Channel Allocation Table 28-47
Should you dedicate ports? 28-56
Modifying the Channel Allocation Table 28-59

Section E: Disk Maintenance 28-61
Overview 28-62
Checking disk status 28-63
Disabling disk shadowing (unsynching) 28-68
Replacing a failed disk 28-69
Reenabling disk shadowing (synching a disk pair) 28-70
Running diagnostics on a disk or a disk pair. 28-72

Section F: Diagnostic Schedules 28-75
Overview 28-76
What are Voice Path Diagnostics? 28-77
Changing the parameters and schedule for diagnostics. . . 28-78
Analyzing the results of the diagnostics 28-82

29 SEERs and Meridian Mail Alarms 29-1
Overview 29-2

Section A: SEERs and Alarms 29-3
What is a SEER? 29-4
Retrieving SEERs 29-6
What is an alarm? 29-9
How to check alarm status 29-10
Silencing an alarm 29-12

Section B: Customizing SEER processing 29-15
Overview 29-16
Using SEER remapping 29-17
Using SEER throttling 29-20
Using SEER escalation 29-23

Section C: Notification options for SEERs and alarms 29-27
Overview 29-28
Notification options for SEERs and alarms 29-29
Using SEER filtering 29-31
Using SEER triggering 29-35
SEERs printing 29-38
Setting the SEER printer port name 29-40

30 Operational Measurements 30-1
Overview 30-2

Section A: Overview of Operational Measurements (OM) 30-3
Overview 30-4
What are Operational Measurements? 30-5
How Operational Measurements are useful 30-7

Section B: Setting up Operational Measurements 31-11
Overview 31-12
Using the Operational Measurements menu 31-13
Calculating disk space required for OM data storage 31-15
Operational Measurements Options screen 31-19
Fields in the Operational Measurement Options screen . . 31-21
Setting Meridian Mail to collect and receive data. 31-24

Section C: Interpreting Operational Measurements 30-25
Overview 30-26
Calculating centi-call seconds 30-27
Interpretation guidelines 30-28

31 Operational Measurements traffic reports 31-1
Overview 31-2

Section A: Generating traffic reports 31-3
Overview 31-4
Traffic Reports screen 31-5
Generating traffic reports 31-7

Section B: Traffic reports 31-9
Overview 31-11
Services Summary report 31-12
Fields in the Services Summary report 31-13
Analyzing the Services Summary report. 31-15
Voice Messaging Detail report 31-18
Fields in the Voice Messaging Detail report 31-19
Analyzing the Voice Messaging Detail report 31-21
Channel Usage Detail report 31-22
Fields in the Channel Usage Detail report 31-23
Analyzing the Channel Usage Detail report 31-25
Services Detail report 31-26
Fields in the Services Detail report 31-27
Analyzing the Services Detail report. 31-29
Networking Detail report 31-31
Fields in the Networking Detail report 31-32
Analyzing the Networking Detail report 31-35
AMIS Networking Detail report 31-37
Fields in the AMIS Networking Detail report. 31-38
Analyzing the AMIS Networking Detail report 31-40

Outcalling Detail report 31-41
Fields in the Outcalling Detail report 31-42
Analyzing the Outcalling Detail report 31-45
Fax Delivery Detail report 31-47
Fields in the Fax Delivery Detail report 31-48
Analyzing the Fax Delivery Detail report 31-50
Disk Usage Detail report 31-52
Fields in the Disk Usage Detail report 31-53
Analyzing the Disk Usage Detail report 31-54
Hospitality Statistics report 31-56
Fields in the Hospitality Statistics report 31-57
Analyzing the Hospitality Statistics report 31-58
Guest Console Statistics report 31-59
Fields in the Guest Console Statistics report 31-60
Analyzing the Guest Console Statistics report 31-61

32 User Usage reports 32-1
Overview 32-2
The User Usage Reports screen 32-3
Fields in the User Usage Reports screen 32-4
Generating User Usage reports 32-7
User Usage report 32-9
Fields in the User Usage report 32-11
Analyzing User Usage reports 32-14

33 Audit Trail reports 33-1
Overview 33-2

Section A: Collecting Audit Trail data 33-3
Overview 33-4
Enabling the collection of audit trail data 33-5

Section B: Outcalling Audit Trail reports 33-9
Overview 33-10
Generating an Outcalling Audit Trail report 33-11
The Summary Outcalling Audit Trail report 33-15
Fields in the Summary Outcalling Audit Trail report 33-16
Analyzing the Summary Outcalling Audit Trail report . . 33-18

The Detail Outcalling Audit Trail report 33-19
Fields in the Detail Outcalling Audit Trail report 33-20
Analyzing the Detail Outcalling Audit Trail report 33-28

Section C: Fax Audit Trail reports 33-29
Overview 33-30
The Fax Audit Trail Report screen 33-31
The Summary Fax Audit Trail report 33-35
Fields in the Summary Fax Audit Trail report screen 33-36
Analyzing the Summary Fax Audit Trail report 33-37
The Detail Fax Audit Trail report 33-38
Fields in the Detail Fax Audit Trail report screen 33-39
Analyzing the Detail Fax Audit Trail report 33-43

34 Bulk provisioning 34-1
Overview 34-2

Section A: Introduction to bulk provisioning 34-3
Overview 34-4
What is bulk provisioning? 34-5
Using bulk provisioning 34-6

Section B: Working with bulk provisioning data sets 34-9
Overview 34-10
Assembling bulk provisioning data sets 34-11
Creating and modifying bulk provisioning data sets 34-14
Viewing and printing bulk provisioning data sets 34-21
Deleting bulk provisioning data sets 34-25

Section C: Transferring bulk provisioning data onto tape 34-27
Overview 34-28
Copying provisioning data sets onto tape 34-29

Section D: Provisioning data into a Meridian Mail system 34-33
Overview 34-34
Before you start 34-35
Provisioning data 34-37
Viewing and printing data conflicts 34-43

A Integrated Mailbox Administration A-1

Overview A-2

Section A: Interaction between IMA and Meridian Mail A-3

Overview A-4
What is Integrated Mailbox Administration? A-5
IMA data translations A-6
Synchronizing IMA and Meridian Mail databases A-9
IMA and Meridian Mail processing differences and implementation issues A-10

Section B: System installation using VMBA A-15

Overview A-16
Installing at a new site without a preconfigured database on Meridian Mail or the Meridian 1 core A-17
Installing at a new site with sets and VMBs preconfigured on the Meridian 1 core but not on Meridian Mail A-18
Installing at an existing site with VMBs preconfigured on Meridian Mail but not the Meridian 1 core A-20

B Meridian Mail AutoAdmin Utility B-1

Overview B-2
Introduction B-3
Meridian Mail AutoAdmin installation B-5
AutoAdmin Configurator B-12
AutoAdmin Utility B-21
The AutoAdmin window B-25
Using Meridian Mail AutoAdmin B-34
Troubleshooting B-51

Index Index-1

List of Fields Fields-1

Chapter 1

About this guide

In this chapter

Overview	1-2
What this guide is about	1-3
Who should use this guide	1-4
Systems supported by this guide	1-5
Structure of this guide	1-6
Typographic conventions	1-11
Referenced documents	1-14

Overview

Introduction

This system administration guide provides the procedures and related information necessary to administer a Meridian Mail Release 12 system operating on a Meridian 1 platform. This guide includes the initial setup of your system, its daily operation, and its routine maintenance.

Before you begin

All your hardware, including the main administration terminal and optional printer, must already be installed.

What this guide is about

Introduction

This guide explains how to set up, operate, and maintain your Meridian Mail system.

Administrative tasks

This guide contains information and procedures for the following:

- setting up the initial system configuration (normally a once-only operation)
- logging on and navigating
- adding users and maintaining the user database
- making voice recordings, such as announcements and voice menus
- administering fax services on the system
- setting up system security
- backing up the system
- monitoring system status
- performing routine maintenance
- monitoring traffic reports and system usage reports
- troubleshooting
- configuring special features on your system

Where more detailed information is available in other manuals, this guide directs you to the appropriate resources.

Task frequency

Some of these tasks must be performed every day. Others are carried out frequently, while some need to be done only occasionally.

These tasks are performed either through menu-driven screens at your administration terminal or through your telephone.

Who should use this guide

Introduction

This guide is intended for users who are responsible for setting up, operating, and maintaining the Meridian Mail system.

Guide users

There are two main groups of users who refer to this guide:

- The guide's primary users rely on this documentation to do their job.
- The guide's secondary users may need to refer to the documentation to do their jobs.

Examples of users

The following table identifies the primary and secondary users of this guide.

Users	Example
Primary users	• database administrators located at customer sites who perform all Meridian Mail administration tasks • technical support personnel
Secondary users	• installation and maintenance technicians • database administrators located at customer sites who perform only basic Meridian Mail administration tasks • sales engineers • trainers and courseware developers • technical application specialists

Systems supported by this guide

Introduction

This administration guide is common to the following hardware platforms:

- Meridian Mail Modular Option
- Meridian Mail Modular Option EC
- Meridian Mail Option 11

All of these platforms are connected to a Meridian 1/SL-1 switch using an AML/CSL link.

Supported systems

Some of the features documented in this guide may not be installed on your system.

In addition, because certain features are hardware dependent, it may not be possible for you to install them.

To determine whether you can install a particular feature on your system, see “Meridian Mail feature availability” on page 2-46.

Structure of this guide

Introduction

This guide is organized to reflect the hierarchical set of procedures accessible from the Main Menu. Most items that appear in the Main Menu have a corresponding chapter describing the administrative tasks and the screens and fields required to complete the tasks.

Contents of this guide

This guide contains the following chapters.

Chapter number and title	Description
Chapter 1: About this guide	Identifies the purpose, scope, audience, and structure of this guide. Sets out the typographic conventions used in the guide. Explains the guide's structure. Lists the publications referred to in this guide.
Chapter 2: Navigating through system administration	Provides an overview of the functional areas presented in the System Administration menu. Describes basic screen navigation tools and techniques. Introduces the two Meridian Mail Release 12 user interfaces. Lists the features available for each Meridian Mail hardware platform and user interface.
Chapter 3: Logging on	Describes how to log on to Meridian Mail. Describes how to log on to the Meridian 1 switch through a Meridian Mail administration terminal.
Chapter 4: Setting up the system	Refers users to procedures for checking the provisioning of Meridian Mail Release 12. Provides an overview of a complete basic setup of Meridian Mail Release 12, with cross-references to relevant information and procedures in other chapters and guides.
Chapter 5: Making voice recordings	Describes how to make voice recordings for use by Meridian Mail.

Chapter number and title	Description
Chapter 6: Setting up Meridian Mail security	Identifies the high-risk areas of a Meridian Mail system and the types of abuse that can occur. Lists the measures that can be taken to set up and monitor system security. Describes the use of security features to prevent unauthorized mailbox access. Describes measures to prevent the use of Meridian Mail features for unauthorized long distance calling. Suggests procedures to prevent unauthorized use of the administration terminal. Describes the reporting features available to help administrators detect abuse.
Chapter 7: User administration — an overview	Introduces the concepts and issues concerning user administration. Cross-references appropriate chapters for routine user administration tasks of particular interest or concern.
Chapter 8: Local voice users	Describes procedures for administering local voice users.
Chapter 9: Remote voice users	Describes procedures for administering remote voice users.
Chapter 10: Directory entry users	Describes procedures for administering directory entry users.
Chapter 11: Distribution lists	Describes procedures for administering system distribution lists.
Chapter 12: General administration — an overview	Introduces the concepts and issues concerning general administration. Directs users to the appropriate chapters for routine general administration tasks.
Chapter 13: General options	Describes how to perform the tasks and locate the information available under the General Options screen.
Chapter 14: Volume administration	Describes the tasks that can be performed through the volume administration side of Volume and selective backups.

Chapter number and title	Description
Chapter 15: Back up and restore Meridian Mail data	Explains the importance of Meridian Mail system backups. Suggests which volumes to back up, and how frequently. Describes the two available backup media and how to perform a backup with either one. Describes the procedures for scheduling a backup to occur automatically at a later time and for checking on the status of a backup in progress.
Chapter 16: Password and system time changes	Describes how and how often to change the administration password and the AdminPlus password. Describes how to change Meridian Mail's system time setting.
Chapter 17: Dialing translations	Introduces the concept of dialing translations. Specifies the situations and features requiring dialing translations. Guides users through setting up dialing prefixes and translation tables appropriate to their system. Provides in-depth detail for those who wish to customize dialing translations.
Chapter 18: Routine maintenance	Lists the routine maintenance tasks recommended for optimum Meridian Mail operation.
Chapter 19: Voice administration—an overview	Provides an overview of voice administration. Describes the Voice Administration menu and its menu options. Directs users to the appropriate chapters for documentation of the menus and screens accessible from the Voice Administration menu.
Chapter 20: Voice messaging options	Describes the tasks that can be performed using the Voice Messaging Options screen.
Chapter 21: Display options	Describes how to change the display options for the Voice Services Administration screen using the Set Display Options screen.
Chapter 22: Finding and printing VSDNs and service definitions	Describes how to use the Find function to find and print VSDNs and service definitions.
Chapter 23: Configuring Meridian Mail services	Provides an overview of the configuration of Meridian Mail services: the setup of the Meridian 1 switch and Meridian Mail setup.

Chapter number and title	Description
Chapter 24: The VSDN table	Documents the procedures for configuring VSDNs for each Meridian Mail feature that potentially requires a DN.
Chapter 25: Voice services profile	Documents the tasks that can be performed using the Voice Services Profile screen. Provides information about the different kinds of timeouts and how they work.
Chapter 26: Class of Service administration	Introduces the concept of Class of Service and the types of Class of Service. Guides users through creating, assigning, changing, and deleting individual Classes of Service.
Chapter 27: Hardware administration	Describes the methods for viewing and printing out the configuration of Meridian Mail's dedicated nodes and data ports.
Chapter 28: System status and maintenance	Describes procedures for checking on system, card, and port status. Describes procedures for enabling and disabling certain system components as part of routine maintenance, troubleshooting, and replacement. Describes the use of the Channel Allocation Table during system expansion or reorganization.
Chapter 29: SEERs and Meridian Mail Alarms	Introduces the concepts of SEERs and Meridian Mail alarms. Describes how to customize a system's SEER processing protocols to control how certain SEER messages are categorized and reported.
Chapter 30: Operational Measurements	Provides an overview of the Operational Measurements feature and how it can be used to monitor Meridian Mail system activity. Describes how to generate, view, print, and analyze Operational Measurement reports.
Chapter 31: Operational Measurements traffic reports	Provides information and procedures for Operational Measurements traffic reports.
Chapter 32: User Usage reports	Provides information and procedures for Operational Measurements user usage reports.
Chapter 33: Audit Trail reports	Provides information and procedures for Operational Measurements audit trail reports.

Chapter number and title	Description
Chapter 34: Bulk provisioning	Introduces the concept of bulk provisioning. Offers examples of situations where bulk provisioning can be used. Describes procedures for transferring bulk provisioning data onto tape and into another Meridian Mail system.
Appendix A: Integrated Mailbox Administration	Presents information and procedures for avoiding data corruption or task conflicts when using the Integrated Mailbox Administration feature to administer mailboxes.
Appendix B: Meridian Mail AutoAdmin Utility	Presents information and procedures for using Meridian Mail AutoAdmin to administer mailboxes from a PC, and to use data files from other applications to supply user information for new mailboxes.

Typographic conventions

Introduction

This topic describes the typographic conventions used in this guide for the following:

- softkeys
- keyboard keys or hardkeys
- telephone keypad keys
- text input
- fields in a menu
- values in a field
- system responses
- spoken words
- recorded prompts

Conventions

The following table identifies, describes, and provides examples of the conventions used in this guide.

Convention for	Description	Example
softkey	Softkeys are displayed on the administration menus and screens. They indicate which keyboard function keys you press to carry out specific Meridian Mail tasks. A softkey is referred to by its label (as displayed in the menu or screen) enclosed in square brackets. It appears in the same typeface as the accompanying text.	[Exit] [Record]
keyboard key or hardkey	A keyboard key or hardkey is referred to by its label enclosed in angle brackets. When two key names appear together, you press them both at the same time. A keyboard key or hardkey appears in the same typeface as the accompanying text.	<1> <Prev Screen> <Help> <Return> <Ctrl> <r>

Convention for	Description	Example
telephone keypad key	The telephone keypad keys that you press appear in bold print in the same typeface as the accompanying text.	Press **829** on the telephone keypad.
text input	Text that you type appears in bold print. In a procedure, it appears in the same typeface as the accompanying text. In other text, it appears in a different typeface from the accompanying text.	Type **m.**
fields in a menu	The name of a field is capitalized and appears in the same typeface as the accompanying text.	the Last Name field the Invalid Logon Attempt field
values in a field	A value in a field is capitalized and appears in the same typeface as the accompanying text.	The default is No.
system responses	System responses appear in the same typeface as the accompanying text. They are often introduced with **Result:.**	**Result:** The system prompts you for a password.
spoken words	The suggested wording of a greeting or an announcement appears in italics enclosed in double quotation marks.	You might want to include the following statement in your voice menu: "*Please wait on the line. An Attendant will be with you shortly*."
recorded prompts	Prompts played by the system appear in italics enclosed in double quotation marks (the same as spoken words).	"*You have no new voice messages. One old message is still unsent*."

Cross-references

For a cross-reference to another part of this guide or to another manual, the following conventions are used.

Cross-reference	Convention	Example
to another topic in this guide	This cross-reference is enclosed in double quotation marks.	For more information, see "Logging in to Meridian Mail" on page 5-15.
to another manual	The title of the manual appears in italics. The applicable reference number is also presented.	Refer to the *Meridian Mail System Installation and Modification Guide* (NTP 555-7001-215).

Referenced documents

Introduction

You may find it useful to have a number of additional resources available as you are reading this manual.

Referenced documents

The following table identifies the documents that are referred to in this guide.

Note: An "x" in a Nortel (Northern Telecom) Publication (NTP) number indicates that this digit varies, depending on the Meridian Mail hardware platform:

- 7041 indicates Meridian Mail Modular Option
- 7061 indicates Meridian Mail Modular Option EC
- 7071 indicates Option 11

NTP number	Title	Description
555-7001-000	*NTP Contents Overview*	Lists the NTPs in the Meridian Mail suite and provides a brief description of their content.
555-7001-100	*Meridian Mail Messaging Overview*	Provides an overview of the Meridian Mail system and features.
555-70x1-200	*Meridian Mail Site Installation and Planning Guide*	Documents the steps necessary to engineer and plan a Meridian Mail system. This is available only for Meridian Mail Modular Option and Modular Option EC.
555-7001-215	*Meridian Mail System Installation and Modification Guide*	Documents software installation, port reconfiguration, and upgrades, among other topics.
555-7001-221	*Hospitality Voice Services Implementation Guide*	Documents the implementation of a hospitality system.
555-70x1-250	*Meridian Mail Installation and Maintenance Guide*	Documents the installation of Meridian Mail hardware. Also describes how to provision the Meridian 1 switch for Meridian Mail.

NTP number	Title	Description
555-7071-210	*Meridian Mail Installation and Maintenance Guide* (Card Option)	Documents the installation of Meridian Mail hardware.
555-7001-241	*Meridian Networking Planning Guide*	Provides descriptive information and instructions for choosing a networking service.
555-7001-242	*AMIS Networking Installation and Administration Guide*	Documents the implementation of AMIS Networking (networking with the AMIS protocol).
555-7001-243	*Meridian Mail Network Message Service Installation and Administration Guide*	Documents the implementation of Meridian Mail Network Message Service.
555-7001-244	*Meridian Networking Installation and Administration Guide*	Documents the implementation of Meridian Networking (networking with modems).
555-7001-245	*Virtual Node AMIS Installation and Administration Guide*	Documents the implementation of Virtual Node AMIS Networking (a combination of Meridian Networking and AMIS Networking).
555-7001-246	*Meridian Mail Enterprise Networking Installation and Administration Guide*	Documents the implementation of Meridian Mail Enterprise Networking (networking without modems).
555-7001-305	*Meridian Mail System Administration Tools*	Documents additional administrative tools and utilities that are available at the tools level.
555-7001-310	*Meridian Mail Reporter System Administration Guide*	Documents the Meridian Mail Reporter feature, which allows you to use a PC to download information from the Meridian Mail system.
555-7001-315	*Meridian ACCESS Configuration Guide*	Documents the Meridian Mail and PBX configuration required to support Meridian ACCESS.
555-7001-316	*Meridian ACCESS Developer's Guide*	Documents how to develop and maintain Meridian ACCESS applications.

NTP number	Title	Description
555-7001-318	*Meridian ACCESS Voice Prompt Editor User's Guide*	Documents how to use the voice prompt editor to create and maintain voice segment files and individual voice segments.
555-7001-320	*Meridian Mail Outcalling Application Guide*	Documents the implementation of the Remote Notification feature and Delivery to Non-User feature.
555-7001-325	*Meridian Mail Voice Services Application Guide*	Documents the planning, configuration, and implementation of voice services.
555-7001-327	*Meridian Mail Fax on Demand Application Guide*	Documents the planning, configuration, and implementation of the fax information service and fax item maintenance service.
555-7001-510	*Meridian Mail Maintenance Messages (SEERs)*	Lists System Event and Error Reports (SEERs) to help isolate and fix system problems.
553-3001-300	*Meridian 1 X11 System Management Overview, Applications, and Security*	Provides an introduction to the system management facilities provided with the Meridian 1 switch.

Chapter 2

Navigating through system administration

In this chapter

Overview	2-2
Section A: The administration menu hierarchy	2-3
Section B: Understanding menus, screens, and keys	2-25
Section C: Meridian Mail features and interfaces	2-43

Overview

Introduction

This chapter contains the following information:

- an overview of how the menus are arranged into a hierarchy
- an overview of the functional areas presented in the Main menu
- the layout of screens and menus
- navigation tools and techniques
- instructions on how to modify fields
- a list of the features available for each Meridian Mail hardware platform
- an introduction to the two Meridian Mail telset interfaces and the features available in each
  - Meridian Mail User Interface (MMUI)
  - Voice Messaging User Interface Forum (VMUIF)

Section A: The administration menu hierarchy

In this section

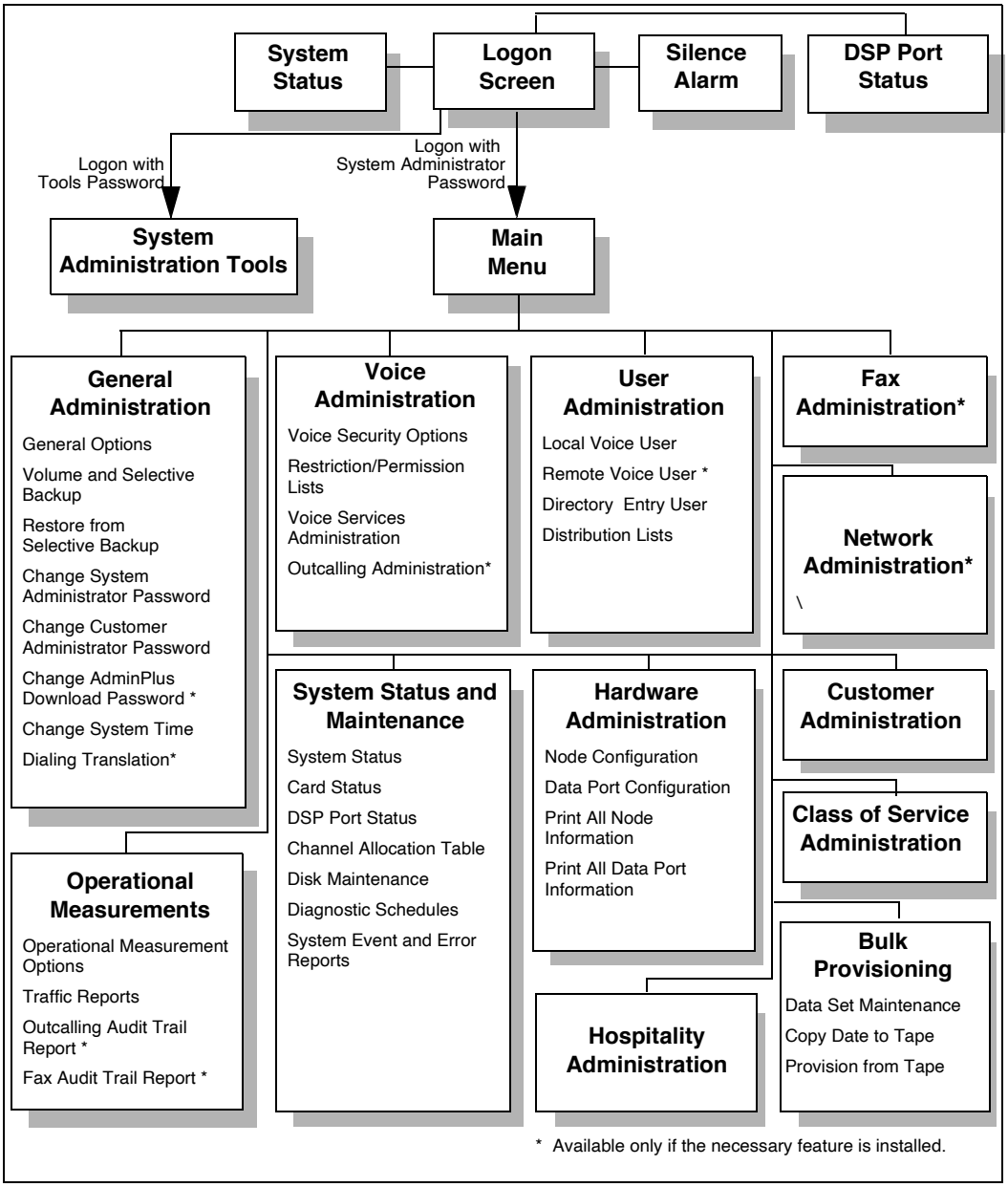
The system administration menu hierarchy	2-4
The Main menu	2-6
User administration	2-7
General administration	2-8
Voice administration	2-10
Hardware administration	2-14
System status and maintenance	2-15
Operational measurements	2-18
Class of Service administration	2-20
Fax administration	2-21
Network administration	2-22
Hospitality administration	2-23

The system administration menu hierarchy

Menu hierarchy

The following is an example of the system administration menu hierarchy.

The system administration menu hierarchy



The Main menu

Introduction

The Main menu is the first screen that is displayed after you log on. This menu is your starting point for performing Meridian Mail administration tasks.

The menu

Here is an example of the Main menu.

```
Main Menu

        1  User Administration
        2  General Administration
        3  Voice Administration
        4  Fax Administration
        5  Hardware Administration
        6  System Status and Maintenance
        7  Operational Measurements
        8  Class of Service Administration
        9  Bulk Provisioning

Select an item > 1

   Logoff
```

Feature-dependent items

The following menu items are displayed only if the appropriate feature is installed:

- Fax Administration is displayed if Fax on Demand is installed.
- Network Administration is displayed if Meridian Networking or AMIS Networking, or both, are installed.
- Hospitality Administration is displayed if Hospitality Voice Messaging is installed.

User administration

Description

User administration involves creating and maintaining a database of users.

Local voice users

Local voice users have mailboxes. You can add, modify, and delete local voice users in User Administration. You can also carry out other user-related functions such as recording personal verifications and setting up remote notification schedules.

Remote voice users

If Meridian Networking or Enterprise Networking, or both, are installed, you can add users at remote sites to your local user database. One way of adding and deleting remote voice users is through User Administration.

Remote voice users can be added to distribution lists at the local site. Local users can use name dialing and call sender to call remote voice users and name addressing to compose messages to them.

Directory entry users

Directory entry users do not have mailboxes. They are, however, in the user directory, and therefore can be accessed by features such as name dialing and Thru-Dial. These users are added, modified, and deleted from User Administration.

Distribution lists

Distribution lists contain a list of mailbox numbers. Whenever you send a message to a distribution list, it is sent to all of the mailboxes in the list.

Administering distribution lists involves

- assigning a number to each list
- adding mailbox numbers to each list
- keeping the lists up to date
- recording a personal verification for each list

General administration

Introduction

General Administration is divided into a number of administration areas from which you can perform a variety of tasks.

Defining general options

Defining general system options involves the following tasks:

- assigning classes of service to the system
- defining the attendant DN
- setting the date format for reports
- specifying the SEER printer and Reports printer port names

Backing up and restoring data

You can perform the following types of backups:

- full backups (of data and voice) to tape
- partial backups (of data only) to tape or disk (if the Disk to Disk Backup feature is installed)
- selective backups of users or services to tape

From Generation Administration, you can restore only users or services that were selectively backed up.

For information about restoring data from a full or partial backup, refer to the *System Installation and Modification Guide* [NTP 555-7001-215].

Changing passwords and the system time

You can change the following:

- the system administrator password
- the customer administrator password (for Multiple Administration Terminals and Meridian Mail AutoAdmin)
- the AdminPlus download password (if AdminPlus is installed)
- the system time

Setting up dialing translations

If Fax on Demand, or AMIS Networking, or both, are installed, you must set up translation tables. These tables tell Meridian Mail how to translate collected digits (from an AMIS message header or a fax callback number entered by a caller) into a number that Meridian Mail can dial.

Voice administration

Introduction

Voice Administration is divided into a number of administration areas from which you can perform a variety of tasks.

Defining voice messaging options

Defining voice messaging options involves the following tasks:

- If more than one language is installed, you must define the default language and whether it overrides users' preferred languages.
- If Dual Language Prompting is installed, you must define the secondary language in which prompts are played.
- You can record customized versions of the call answering greeting (MMUI) and VMUIF tutorials.
- You can enable or disable name dialing/name addressing and external call sender.
- You can define operational characteristics for voice messaging such as
  - the maximum delay for timed delivery
  - the broadcast mailbox number
  - the maximum number of days that read messages are retained
  - the playback speeds that mailbox users can apply to individual mailbox messages

Defining voice security options

Defining voice security options is extremely important in order to safeguard your system from unauthorized use and abuse by hackers and users. You can do the following to secure your Meridian Mail system:

- Make mailbox passwords more secure by
  - defining the password prefix
  - specifying the minimum password length
  - forcing users to change their passwords the first time they log on
  - suppressing the display of passwords on the telset
- Specify the maximum number of invalid logon attempts that are allowed before a mailbox is disabled or a session is terminated.
- Set up monitoring periods for
  - system accesses
  - thru-dials
  - specific internal or external calling line IDs (CLIDs), or both

Defining restriction/ permission lists

Restriction/permission lists are another very important part of ensuring system security. A restriction/permission list specifies which dialing codes are not allowed, thereby preventing users or callers from placing calls to unauthorized numbers such as domestic long distance numbers or international numbers.

You can define up to 80 different restriction/permission lists that can then be applied to different features that place outcalls such as call sender, Thru-Dial, Remote Notification, and AMIS networking.

Performing voice services administration

Voice Services Administration is divided into a number of administration areas:

- The VSDN Table is where you add voice service DNs (VSDNs) for each service that you want to make directly dialable by a unique number.
- The Voice Services Profile is where you define characteristics for voice services such as timeouts and holidays (used by time-of-day controllers).
- You can add, modify, and delete the following voice and fax services from Voice Services Administration:
  - announcement definitions
  - thru-dial definitions
  - time-of-day controller definitions
  - voice menu definitions
  - fax item definitions

Setting display options

Display options allow you to choose

- how you want information sorted in Voice Services Administration screens
- whether the Choice of Services and Menu Actions lists are displayed

Performing outcalling administration

Outcalling includes the Remote Notification (RN) and the Delivery to Non-User (DNU) features. If installed, you must check that the default settings are acceptable, or change them to suit your needs.

Remote Notification parameters include

- the maximum number of remote notification retry repeats
- the numeric pager data terminator

Delivery to Non-User parameters include

- allowed delivery times for weekdays and weekends
- retry limits and intervals for busy, unanswered, and answered conditions
- the number of times to play a DNU message

Defining voice forms

Creating voice forms involves setting operational characteristics for each voice form as a whole, recording all of the prompts (known as fields), and setting field-specific operational characteristics.

Hardware administration

Introduction

Almost all of the screens in Hardware Administration are read-only. They are for viewing purposes only.

To modify your hardware configuration, you must log on to the Tools level and access the Modify Hardware tool. For more information, refer to *Meridian Mail System Administration Tools* (NTP 555-7001-305).

Node configuration

You can view the number of nodes that are installed and the types of cards that have been configured for each node.

Data port configuration

You can view configurations for the following data ports:

- MMLink
- Terminal
- Printer
- PMS
- Modem
- MSLink (for Meridian Mail AutoAdmin)
- AdminPlus (if installed)
- NWModem

Note: You can modify the Network Modem DN from Hardware Administration.

Printing information

You can print all node and all data port information.

System status and maintenance

Introduction

System Status and Maintenance primarily involves viewing the status of the system and various hardware components to see if everything is operational.

When a hardware component needs servicing, it must first be disabled and then reenabled when the problem is fixed. This is done in System Status and Maintenance.

Viewing status and disabling components

For each of the following hardware components, you can view its status, disable (or courtesy disable) it for servicing, and reenable it:

- the entire system
- nodes
- cards
- DSP ports

Channel Allocation Table

The Channel Allocation Table shows how channels (ports) are allocated to services.

From the Channel Allocation Table, you can view the following:

- the channels that are on your system, their type, and whether they are shared by services or dedicated to a particular service for placing outbound calls
- the maximum number of each type of port, and how many of each port type have been allocated

If you disable ports, you can do the following:

- Modify the Primary DN.
- Modify Channel DN.
- Modify the port type and capability.
- Dedicate ports to a particular service (for outcalls only).

Disk maintenance

Shadowed systems

On shadowed systems, you can do the following from the Disk Maintenance screen:

- View the status of the prime and shadow disks in a disk pair.
- Disable and enable a disk.
- Perform diagnostics.

Unshadowed systems

On unshadowed systems, you can view the status of the prime disk and perform diagnostics.

Diagnostic schedules

You can schedule diagnostics to occur at a specific time on certain days. You can specify the following about the scheduled diagnostics:

- whether voice path diagnostics should be performed, and other related parameters

System event and error reports

You can perform the following tasks from the System Event and Error Reports menu.

SEER retrieval

If you do not want all SEERs to be retrieved, you can specify which SEERs should be retrieved according to SEER class, severity level, or SEER type.

SEER configuration

From the SEER Configuration screen, you can do the following:

- Specify the mailbox (the message trigger mailbox) to which you want messages to be sent when a SEER that meets a specific criteria is generated. This allows you to be notified immediately of SEERs that you consider to be critical.
- Set SEER throttling parameters which allow you to prevent SEERs that are duplicated a certain number of times from being sent to the printer or message trigger mailbox, or both.

- Set SEER escalation parameters which allow you to specify how many times a SEER needs to be duplicated before it is escalated to the next severity level.
- Set the SEER filtering levels which allow you to control which SEERs are sent to the printer and message trigger mailbox (according to type and severity level).

SEER remapping

SEER remapping allows you to remap the severity level of up to 60 SEERs to a different severity level and have that information stored on disk.

For example, a SEER that is classified as major in Meridian Mail may be critical to your particular system. You could, therefore, remap this SEER as critical.

Operational measurements

Introduction

There are three kinds of operational measurement reports: traffic reports, user usage reports, and audit trail reports.

Operational measurement options

Setting operational measurement options involves specifying

- whether to collect traffic, user usage, session trace, and audit trail data
- the start and end times for the traffic period
- the number of days traffic data, user usage data, and audit trail data are stored

Traffic reports

You can view or print a summary of traffic report services that shows the number of accesses, the average length, and voice mail usage.

You can view or print more detailed traffic reports for the following:

- Voice Messaging
- Channel Usage
- Services
- Networking
- AMIS Networking
- Outcalling
- Fax
- Disk Usage

You can view or print statistics for the following:

- Hospitality
- Guest Console

User usage reports

You can view or print user usage reports which provide local usage data, Meridian network usage data, and AMIS network usage data.

Audit trail reports

Outcalling audit trails

If Outcalling is installed, you can view or print summary reports that show the target DNs to which users are sending DNU messages and remote notifications as well as the status of each call.

You can also view or print more detailed reports that also show the channel DN that was used and how many retries there were.

Fax audit trails

If Fax on Demand is installed, you can view or print summary reports that show the called DN, billing DN, duration, and status of each fax call.

You can also view or print more detailed reports that show the channel DN that was used and how many retries there were.

Class of Service administration

Introduction

Before you can add local voice users, you must create your classes of service (COS). Each local voice user must be assigned to an already defined class of service.

COS-controlled features

Classes of service determine the feature capabilities of the local voice users assigned to them. Some examples of features and limits that are controlled by classes of service are

- the voice storage limit
- the maximum length of composed messages
- the maximum length of call answering messages
- the ability to send broadcast and network broadcast messages
- notification of busy line to callers
- delivery to non-user (DNU) capability and related DNU parameters
- remote notification (RN) capability and related RN parameters
- the ability to receive and send AMIS open network messages
- the restriction/permission lists that are applied to AMIS open networking, extension dialing, and custom revert

Maintaining classes of service

Maintaining classes of service involves modifying classes of service as needed. Whenever a change is made to a class of service, the change is propagated to all users belonging to that class of service.

It also involves deleting classes of service that are no longer needed (and reassigning users to another class of service before you delete).

Fax administration

Administration of the Fax on Demand service

Fax Administration is available only if Fax on Demand is installed. It involves configuring the following parameters for the Fax on Demand service:

- the maximum number of fax delivery channels
- the maximum resolution of fax reception (normal or fine)
- the maximum number of pages allowed per fax item
- fax delivery retry limits and intervals for cases where fax items cannot be delivered (due to transmission errors or no carrier availability)
- allowed times for delivery of fax items on weekdays and weekends
- the delivery time limit

Creating fax items

Fax items are not created in Fax Administration. You must access the Voice Services Administration menu at the Customer Administration level to add fax item definitions.

Network administration

Description

Network administration involves the administration of Meridian Networking, Enterprise Networking, and AMIS Networking.

Meridian Networking and Enterprise Networking

Administration of the Meridian Networking and Enterprise Networking features involves

- local site maintenance
- remote site maintenance, which involves adding remote sites, specifying the networking protocol and dialing plan for each site, and recording a spoken site name
- network configuration, which involves setting initiation times, holding times, stale times, the batch threshold, and wakeup interval
- performing a modem verification test
- checking the network status periodically

AMIS and Virtual Node AMIS Networking

Administration of AMIS Networking includes the following:

- enabling or disabling incoming and outgoing messages
- specifying the allowed delivery times for outgoing messages
- specifying the initiation time, holding times, stale times, batch threshold, and wakeup interval
- defining the AMIS compose prefix
- specifying the number of messages to transmit per session
- defining the system access number
- checking the status of the AMIS Networking service

Hospitality administration

Introduction

Hospitality Administration is available only if the Hospitality Voice Messaging feature is installed.

Hospitality profile

The Hospitality Profile screen is where you define parameters for all Guest Messaging services. Some examples are

- the initial guest password length
- whether the initial guest password is generated using the guest's last name or the check-in date
- Post Check-out Mailbox settings
- customizable greetings for
  - the guest logon greeting
  - unanswered and busy guest phones
  - vacant rooms
  - rooms that do not have voice messaging

Modifying mailboxes

You can view or modify a guest mailbox from Hospitality Administration. You can modify settings such as

- room number and status
- the guest's first and last name
- autologon
- the revert DN

Changing the GAC password

You should change the default GAC password after installation and continue to change it on a regular basis.

Hospitality system status

You can view the status of the Hospitality system, including the links from Meridian Mail to the PMS (if there is one) and the Meridian 1.

Hospitality install parameters

Modifying install parameters involves

- setting PMSI parameters
- setting SL-1 link parameters
- setting voice count parameters
- configuring the language identifier table
- providing international character mapping for the PMSI link

Section B: Understanding menus, screens, and keys

In this section

Overview	2-26
Keypad functions	2-27
Meridian Mail menus	2-28
Meridian Mail screens	2-31
Getting around in screens	2-33
Entering information in fields	2-34
Softkeys	2-39
Getting help	2-40
Error messages	2-41

Overview

Introduction

System administration menus and screens have a consistent format. The way in which items are selected and data is entered is the same for all menus and screens.

In this section

This section describes

- keypad functions
- the layout of menus
- the layout of screens
- types of fields
- how to select menu items
- how to select options and enter data in fields
- how to navigate through fields in screens
- how to scroll through multipage screens
- softkeys
- how to get help

Keypad functions

Application mode

When the keypad is in application mode, certain functions are available on the keypad when you press single keys or key combinations. Application mode is the default whenever the system is rebooted.

Supported terminals

Keypad functions are supported on VT220 terminals and the following VT200-compatible terminals: VT320, VT420, HP700/22, and HP700/32.

Numeric keypad

If you choose to work with a numeric keypad (where the numeric keys generate numbers when you press them), then only the F1, F2, F3, and F4 keys retain the functions indicated. The keypad is set to numeric mode through the terminal's setup function.

Keypad function key positions

The following illustration shows the functions available when the keypad is in application mode.

F1	F2	F3	F4
7	8	9	–
4	5	6	,
1	2	3	ENTER
0		.	

F1 - Softkey 1
F2 - Softkey 2
F3 - Softkey 3
F4 - Softkey 4
1 - Start of field
2 - Next word in field
3 - End of field
4 - Previous field
5 - Next field
7 - Previous page
8 - Next page
- - Delete field contents
. - HELP
ENTER - Softkey 5

(shading indicates that the key does not have a function)

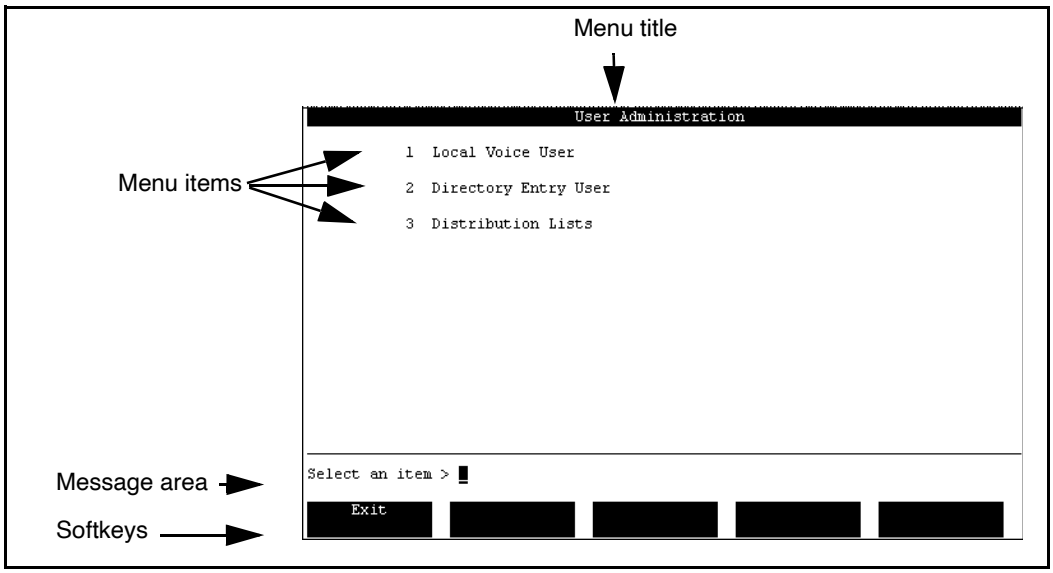
Meridian Mail menus

Description

A menu presents a list of items from which you can choose. When an item is selected, either another menu or a screen is displayed.

A typical menu

The following is an example of a menu.



Parts of a menu

This table describes the parts of a menu.

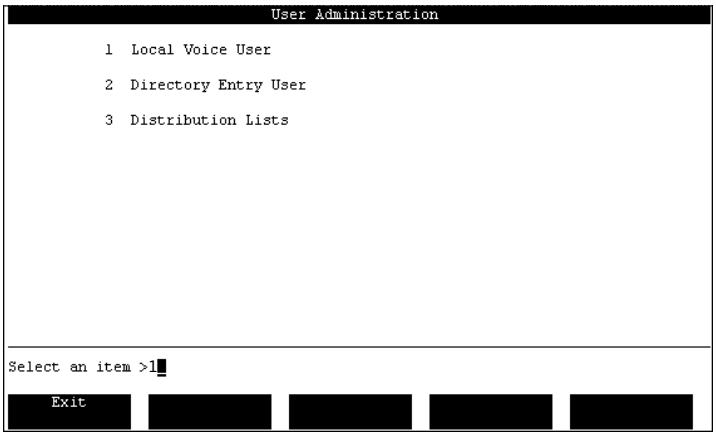
Part	Description
Menu title	Menu titles are always on the first line.
Menu items	Each menu has a list of choices that are preceded by numbers. These are menu items from which you can choose. Choosing a menu item causes either another menu or a screen to be displayed.
Message area	This is where system prompts, responses, and error messages are displayed.
Softkeys	The bottom line in a menu is a set of softkeys. Softkeys are used to carry out actions.

Choosing a menu item

Each item in a menu has a number. The system displays a prompt requesting you to make a selection from the items presented.

To select a menu item, follow these steps.

Starting Point: Any menu with the “Select an item” prompt displayed

Step	Action
1	Enter the number that corresponds to the item you want to choose and press <Return>. **Example:** You want to add local voice users to your system so you enter 1 and press <Return>.  **Result:** Another menu or a screen is displayed.

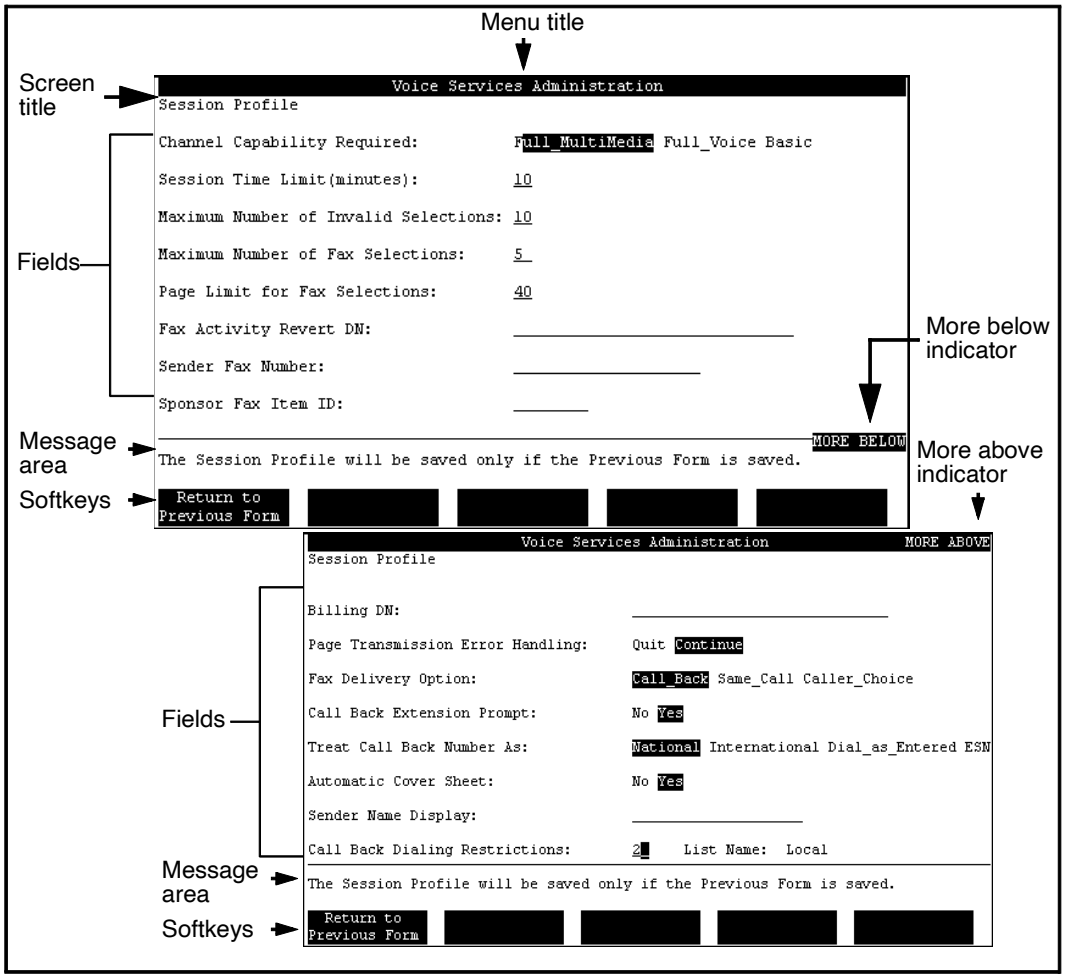
Meridian Mail screens

Description

Screens contain fields in which you can either make selections or enter data. It is by filling in fields that you customize Meridian Mail to meet your requirements and suit your needs.

A typical screen

The following is an example of a screen.



Parts of a screen

This table describes the parts of a screen.

Part	Description
Menu title	This is the name of the menu from which the screen was accessed.
Screen title	The name of the screen.
Fields	Fields in screens are much like fields in forms. You can either enter information in them, or select from a predetermined set of options. It is by filling in fields that you define how you want Meridian Mail to work and customize the system to meet your needs.
Message area	This is where system prompts, responses, and error messages are displayed.
Softkeys	The bottom line in a menu is a set of softkeys. Softkeys are used to carry out actions.
More below indicator	This indicator is displayed in multipage screens. It indicates that there are more fields below the last field that is currently displayed.
More above indicator	This indicator is displayed in multipage screens. It indicates that there are more fields above the first field that is currently displayed.

Getting around in screens

Navigating between fields

The following keys on the keyboard and on the application keypad (see “Keypad functions” on page 2-27) move the cursor between fields.

IF you want to	THEN press
move to the next field	• the Tab key • the down arrow key • the Return key, or • 5 on the application keypad.
move to the previous field	• the up arrow key, or • 4 on the application keypad.

Moving through multipage screens

Certain screens contain more fields than can be displayed at one time on the display terminal. You can view additional pages in one of two ways: by scrolling and by paging.

Scrolling

If you see “More Below” at the bottom of a screen or “More Above” at the top of a screen, you can use the following keys.

IF you want to	THEN press the
view the next page of a multipage screen	• Next Scrn hardkey.
view the previous page of a multipage screen	• Prev Scrn hardkey.

When the “More Below” prompt disappears, you are at the end of the screen. When the “More Above” prompt disappears, you are at the top of the screen.

Using the down arrow key

The down arrow key displays only the last input field, even if there is instructional text below it. To view any text that may appear at the end of a screen, use the Next Scrn hardkey.

Paging

In some screens, a [Next Page] softkey is displayed that can be used to move between the pages of a screen.

Entering information in fields

Introduction

Information is entered in the fields of Meridian Mail screens. There are two types of fields:

- selectable fields
- data entry fields

Example

This screen contains both types of fields.

Selectable fields

Data entry fields

Selectable fields

```
                          User Administration                    MORE ABOVE
View Class of Service

Receive Composed Messages:                 No Yes

Message Waiting Indication Options:        None Any Urgent

External Call-Sender
Restriction/Permission List:               2_  List Name:  Local

Read Message Retention (days):             0_
("0" implies that read messages
are retained until the user
deletes them manually.)

Send Messages to External Users:           No Yes

Retain Copy of Sent Messages:              No Yes
                                                                MORE BELOW
The Class of Service data will be saved only if the user is saved.

 Return to
 Basic Fields
```

Selectable fields

Selectable fields present a number of predefined options from which you can choose.

The option that is in reverse video (light text on a dark background) is the selected option.

After installation, selectable fields always have one of the options selected as the default.

Examples

Examples of selectable fields in the above screen example are Receive Composed Messages and Retain Copy of Sent Messages.

Choosing an option in a selectable field

To choose a predefined option in a selectable field, follow these steps.

Step	Action
1	Move the cursor to the field you want to modify.
2	Use the right (and left) arrow keys, or the spacebar, to select the option you desire. **Note:** The selected option appears in reverse video.

Data entry fields

You type information, such as titles and numbers, into data entry forms. There are often limitations placed on data entry fields, such as the types of characters you can enter or a range of numbers. Data entry fields are indicated by an underline next to the field name. This is where you enter information.

Some of these fields are prefilled with default values. These values can be changed as needed. Others are blank by default and require an entry.

Example

An example of a data entry field (on page 2-34) is the Read Message Retention (days) field.

Entering information in a data entry field

To enter information in a data entry field, follow these steps.

Step	Action
1	Move the cursor to the field you want to modify.
2	Is there currently any information in the field? • If yes, go to step 3. • If no, type the information in the field.
3	Delete the current content of the field.

IF you want to	THEN press
clear the current contents	the <Remove> key.
delete one character to the left of the cursor	the <x> key.
delete the character on which the cursor is positioned	the <Back Space> key.

4	Type the information in the field.

Selecting an entire line

In some screens, especially those that provide a list of things from which to choose, you need to select an entire line to indicate on which item you want to perform an action, and then press a softkey to indicate which action you want to perform.

To select an entire line in a screen, follow these steps.

Step	Action
1	Move the cursor to the line you want to select using the up and down arrow keys.
2	Press the spacebar. **Result:** The entire line is selected (as indicated by reverse video).

Prompt

Screens requiring this mode of selection often indicate this with the following prompt: “Move the cursor to the item and press the spacebar to select it.”

Example

You want to record a personal verification for all users assigned to class of service 2 that do not currently have personal verifications. After using Find, you get this list of users. You select the first user, Bob LePage, and then press [View/Modify] to modify the user.

```
                              User Administration
List of Local Voice Users
                                                                  Storage Personal
                                                            COS   Used    Verific.
 Name           Mailbox                        Department   Num.  (mins)  Recorded
 LePage,Bob     65551234                       9t23           0      0      No
 Rorty,Phillip  65558050                       9t23           0      0      No

Select a softkey >

 Exit   Toggle Cos Assignment   View/Modify   Delete   Voice
```

Mandatory fields

Certain data fields require you to insert values, whereas other fields are optional. Mandatory fields are identified in the field descriptions.

If you do not fill in a mandatory field and then try to save your settings, the system does not save the screen but, instead, prompts you to fill in the necessary field.

Softkeys

Description

Softkeys appear on the bottom two lines of menus and screens and are displayed in reverse video (light characters on a dark background).

They correspond to function keys F1 through F5 or F6 through F10 on the top row of the keyboard. The softkeys change according to the menu or screen. They may also change with the function you are performing.

Purpose

Softkeys are always actions. When you select a softkey, you are performing a function.

Common softkeys

The following softkeys occur frequently on the administration screens:

- [Exit]
- [Add]
- [View/Modify]
- [Delete]
- [Find]
- [Save]
- [Cancel]

Softkey positions

If any of these keys occur on a screen, they typically occur in the following positions.

```
Select a softkey >
Exit    Add    View/Modify    Delete    Find
```

```
Select a softkey >
Save    Cancel
```

Getting help

Introduction

Online help is available for most of the menus and screens, including the Main Menu.

Procedure

To get Help, follow these steps.

Step	Action
1	Press the Help key. **Result:** The system displays explanations of the fields on the menu or screen in which you are working.
2	Once you are done reading the Help information, press the [Exit] softkey to return to the menu or screen.

A typical Help screen

The following shows an example of a Help screen.

```
                                Main Menu

                            Meridian Mail Help
Using Help

When displaying help, the page up/down keys and cursor keys can
be used to scroll through the text.

Softkeys Available:

Exit          Returns user to the context for which help was
              originally displayed.

Using Help    Displays this screen.

Keypad Help   Displays the layout and supported functions of an
              NT220 or compatible application keypad.

   Exit                                          Keypad
                                                 Help
```

Error messages

Introduction

The system displays error messages, both general and screen-specific, on the line above the softkey display.

These messages remain on the screen until the next user input or until another error message appears.

Purpose

These messages provide feedback on administration actions. They should not be confused with System Event and Error Report (SEER) messages.

SEER messages

If SEER printing is disabled, SEER messages will print out on the administration screen.

Examples of error messages

The following are two examples of error messages:

- “The key entered is not valid at this time.”
- “Enter a number in the range of 1 to 6.”

Section C: Meridian Mail features and interfaces

In this section

The main administration terminal and multiple administration terminals (MATs) 2-44

Meridian Mail feature availability 2-46

Meridian Mail telset interfaces 2-48

The main administration terminal and multiple administration terminals (MATs)

Introduction

Meridian Mail is administered through a menu-driven administration interface available at a terminal or personal computer (PC) using terminal emulation software. Using the administration menus, you establish the initial configuration of your system, maintain the user information base, create voice applications such as announcements and voice menus, monitor system usage and performance, and perform routine system maintenance.

The main administration terminal

All of these tasks are performed from the main administration terminal or from a PC using terminal emulation software.

Multiple administration terminals

The Multiple Administration Terminals (MATs) feature enables you to configure your main administration terminal and up to three secondary terminals, or MATs, on your system.

Tasks performed on MATs

Only a limited number of administrative tasks can be performed from a MAT. These include the following:

- User Administration

  You can perform all User Administration tasks, such as adding, modifying, and deleting users and distribution lists.
- Class of Service administration

  You can only view existing classes of service from a MAT. You cannot add, modify, or delete them.
- Voice Administration

  You can add, view, modify, and delete
  - voice service DNs
  - announcement and voice menu definitions
  - thru-dial definitions
  - time-of-day control definitions
  - fax item definitions

See also

For more information about configuring MATs, refer to the *System Administration Tools Guide* (NTP 555-7001-305).

Meridian Mail feature availability

Available platforms

This system administration guide is common to the following hardware platforms:

- Meridian Mail Modular Option
- Meridian Mail Modular Option EC

Both of these platforms are connected to a Meridian 1/SL-1 switch using an AML/CSL link.

Feature availability

Use the following table to determine whether you can install a particular feature on your system.

Feature	Meridian Mail Modular Option	Meridian Mail Modular Option EC
ACCESS	yes	yes
AdminPlus	yes	yes
AMIS Networking	yes	yes
Calling Line ID (CLID)	yes	yes
Disk Shadowing	yes	yes
Disk to Disk backup	yes	yes
Dual Language Prompting	yes	yes
Enterprise Networking	yes	yes
Fax on Demand	yes	yes
Hospitality	yes	yes
Integrated Mailbox Administration	yes	yes
Maximum number of languages supported	4	4
Meridian Mail AutoAdmin	yes	yes
Meridian Networking	yes	yes
Multiple Administration	yes	yes

Feature	Meridian Mail Modular Option	Meridian Mail Modular Option EC
Network Message Service (NMS)	yes	yes
Outcalling	yes	yes
Password Display Suppression	yes	yes
Single Terminal Access	yes	yes
Virtual Node AMIS Networking	yes	yes
VMUIF Voice Messaging	yes	yes
Voice Forms	yes	yes
Voice Menus	yes	yes
9600 bps Meridian Mail Interface	yes	yes

Meridian Mail telset interfaces

Introduction

Through the Meridian Mail telset interfaces, users interact with the Meridian Mail system to log in to their mailboxes, listen to messages, and compose and send messages.

Two telset interfaces

There are two Meridian Mail interfaces:

- Meridian Mail User Interface (MMUI)
- Voice Messaging User Interface Forum (VMUIF)

Note: A Meridian Mail system can support only one of these interfaces. When the system is installed, it is defined as using either the MMUI interface or the VMUIF interface.

Definition: MMUI

The MMUI interface is a full-featured, command-driven Nortel proprietary voice mail interface. It is intended primarily for large business users.

Definition: VMUIF

VMUIF is a menu-driven interface. It is intended primarily for small business users, providing either full-featured voice messaging or only call answering and message retrieval.

VMUIF is also well suited to large campus environments such as universities or hospitals.

Terminology: users and subscribers

Users added to a system on which the MMUI interface is installed are referred to as *users*. Users added to a system on which the VMUIF interface is installed are referred to as *subscribers*, because they typically subscribe to a service through a central office.

Note: All of the Meridian Mail administration screens refer simply to users, even though user administration applies to both MMUI users and VMUIF subscribers.

Available features of MMUI and VMUIF

This table indicates which features are available for the two Meridian Mail user interfaces.

Feature	MMUI	VMUIF
handling of forwarded calls	yes	yes
personalized greetings	yes	yes
message waiting indication (MWI) support	yes	yes
remote notification (although user-changeable remote notification schedules from the telephone set are available only in the MMUI interface)	yes	yes
password-protected mailboxes	yes	yes
mailbox summaries and message playback	yes	yes
message reply, reply all, and message forward	yes	yes
personal distribution lists	yes	yes
message compose and send	yes	yes
AMIS Networking (if installed)	yes	yes
ability to assign a class of service (COS)	yes	yes
18-digit mailbox	yes	yes
mailbox Thru-Dial (A user can press **0** and dial a number while logged in to the mailbox.)	yes	
name addressing (A user can dial another user by name instead of by extension.)	yes	
Meridian Mail Networking (if installed)	yes	
Virtual Node AMIS Networking (if installed)	yes	
message tagging options (During message composition, a user can tag messages as urgent or for timed delivery.)	yes	
retention of sent or unsent messages	yes	
internal, external, and temporary greeting	yes	1 greeting
user-changeable personal verification	yes	yes
choice of identification (mailbox number or personal verification) to be played during call answering	yes	

Feature	MMUI	VMUIF
customizable customer greeting and customer attendant	yes	
custom operator revert	yes	
user-changeable remote notification schedules through the telephone set	yes	
express messaging	yes	
bilingual prompting (if more than one language is installed)	yes	
record, playback, and message tagging during call answering	yes	
speed control during message playback	yes	
adding to a recorded message	yes	
call answer only mailbox (Compose and Send must be disabled.)		yes
send only mailbox (Call Answering must be disabled.)		yes
rotary set interface (message retrieval with no DTMF input required)		yes
greeting change service (greeting change with no DTMF input required)		yes
introductory tutorial (special greeting on first access)		yes
volume control (DTMF control of default volume and volume setting)		yes
family mailboxes (Up to eight submailboxes can be administered through one telephone set.)		yes
“save as new” (Read messages can be reverted to “unread” or “new” status.)		yes
send on disconnect (implicit send command if a user hangs up after composing a message)		yes
mailbox resources (limiting receipt of messages based on mailbox resources)		yes
customizable login greeting		yes
disable reset (automated, timed reset of automated lockout resulting from password violation)		yes
editing capabilities for personal distribution lists	yes	
lockout revert (If locked out from the mailbox, a revert DN is possible.)		yes

Chapter 3

Logging on

In this chapter

Overview	3-2
Types of consoles	3-3
Logon/Status screen	3-4
Setting the system administration password	3-6
Changing the system administration password	3-8
Recovering a system administration password	3-10
Logging on from the main administration terminal	3-11
Logging on from a MAT	3-13
Logging on from a remote terminal (non-EC system)	3-15
Logging on from a remote terminal (EC system)	3-18
Using a single terminal to access the M1 and Meridian Mail	3-23

Overview

Introduction

This chapter explains how to set your administration password and log on to the Meridian Mail system from the following types of consoles:

- the main administration terminal
- a multiple administration terminal (MAT)
- a remote terminal (non-EC system)
- a remote terminal (EC system)

After you are logged on, you can begin to work with the system administration menus, which are the starting point for general administrative functions and for customizing your system.

The chapter also describes how to change or recover your administration password.

Types of consoles

Introduction

Administrative functions can be carried out from the main administrative console for your Meridian Mail system or from a remote terminal connected to the system through a modem.

Multiple administration terminals

If the Multiple Administration Terminal feature is installed, your Meridian Mail system can support up to four administration terminals: one main administration terminal and up to three secondary terminals, or MATs.

Console types

The following table lists the types of consoles and their available features.

Main administration terminal	Multiple administration terminal	Remote terminal
installed with your system	available feature	available feature
all functions	user administration: add, modify, and delete mailboxes COS administration: view and find (read-only) voice services administration: add, view, modify, delete voice service DNs, announcement definitions, Thru-Dial definitions, time-of-day control definitions, and voice menu definitions	generally used by off-site service personnel to troubleshoot a system

Logon/Status screen

Description

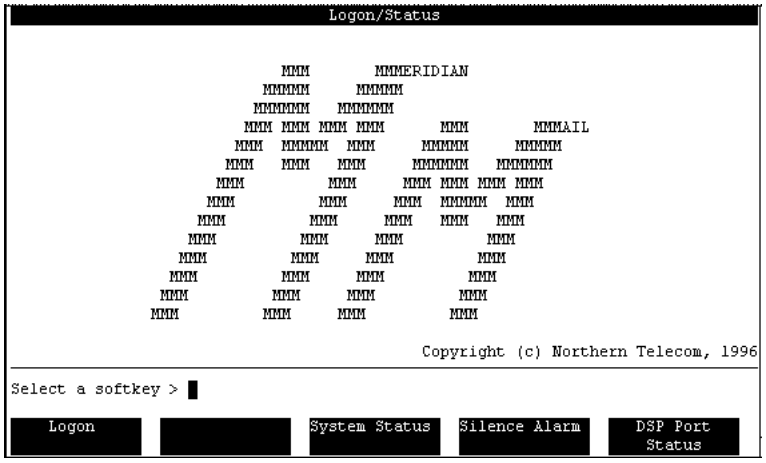
From this screen, you log on to the administration console to perform the following tasks:

- setting up and customizing your system
- carrying out administrative tasks on a system-wide basis, or a per-user basis
- configuring voice services
- viewing system status or DSP port status
- silencing alarms

The Logon/Status screen is displayed when the administration terminal is idle.

The Logon/Status screen

The following shows an example of the Logon/Status screen.



Note: When you log on at a MAT, only the [Logon] softkey is displayed.

> **ATTENTION**
>
> For security and memory usage reasons, do not leave the administration console unattended while you are logged on. Also, remember to log out at night. If you do not log out, critical audit and backup routines may not run because of insufficient memory.

Available softkeys

For information about the softkeys available from the Logon/ Status screen, see Chapter 28, “System status and maintenance”.

Redrawing the Logon/ Status screen

If you power down your terminal and then power it back up, the screen may be drawn incorrectly. If the screen is corrupted, you see a row of “q”s (qqqqqqqqqqqqq) instead of the line near the bottom of the screen above the softkeys.

To redraw a corrupted screen, follow these steps.

Step	Action
1	Press <Ctrl> <w>. **Result:** A small window opens.
2	Type **if**. **Note:** You do not have to press <Return>. The “i” means initialize, and the “f” means full screen.

Setting the system administration password

Overview

To log on to the Meridian Mail system from an administration terminal, you require a system administration password.

Your password can be any combination of letters and numerals. It can be between 6 and 16 characters long. (The minimum length can be increased by the System Administrator. See "Setting the minimum password length for all administrator passwords" on page 16-7.)

Passwords are not case sensitive; even if you use capital letters when you define your password, you do not need to use capital letters when you type it.

Password security

For greater system security, your password should be no fewer than seven characters in length. A longer password is more difficult to guess than a shorter password.

For more information about ensuring the security of your system, see Chapter 6, "Setting up Meridian Mail security".

Procedure

To set your system administration password for the first time, follow these steps.

Starting Point: The Logon/Status screen

Step	Action
1	Select the [Logon] softkey. **Result:** The system prompts you for a password.
2	Type the default password **adminpwd**. **Result:** The system prompts you for a new password. It does not allow you to log on until you change the default password.
3	Type a new password, and press <Return>. **Result:** The system prompts you to reenter the password for verification.
4	Type your new password a second time, and press <Return>. **Result:** The system records the new password and displays the Main Menu. **Note:** If you type a different password the second time, the system reports that the password has not changed because the new passwords did not match. If you receive this message, repeat step 1 to step 4.

Changing the system administration password

Introduction

To help ensure the security of your system, change the logon password regularly.

You can change the password only at the main administration terminal. The change is then automatically made to the configured MATs.

Your password can be any combination of letters and numerals. It can be between 6 and 16 characters long. (The minimum length can be increased by the System Administrator. See "Setting the minimum password length for all administrator passwords" on page 16-7.)

For more information about ensuring the security of your system, see Chapter 6, "Setting up Meridian Mail security".

Procedure

To change your system administration password, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration.
2	Select Change System Administrator Password. **Result:** The system prompts you to enter your existing administration password.
3	Type your existing password. **Note:** Your password is not displayed on the screen as you type it. **Result:** The system prompts you to enter a new password.
4	Type your new password, and press <Return>. **Result:** The system prompts you to reenter the password for verification.
5	Type your new password a second time, and press <Return>. **Result:** The system records the new password, and you are returned to the General Administration menu. **Note:** If you type a different password the second time, the system reports that the password has not changed because the new passwords did not match. If you receive this message, repeat steps 2 to 5.

Recovering a system administration password

Introduction

This topic describes how to restore a password that has been forgotten or lost to the system.

Procedure

To recover a system administration password, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Insert the install tape in the tape drive.
2	Reboot the system from the tape.
3	Select More Utilities from the menu.
4	Select Change to Default System Password. **Result:** You are prompted to enter Yes to continue, or No to stop.
5	Enter Yes to continue. **Result:** The system reports that the operation has been successfully completed.
6	Remove the install tape from the tape drive.
7	Reboot the system from the disk.
8	Select the [Logon] softkey. **Result:** The system prompts you for a password.
9	Type the default password **adminpwd**. **Result:** The system prompts you for a new password. It does not allow you to log on until you change the default password.
10	Type a new password, and press <Return>. **Result:** The system prompts you to reenter the password for verification.
11	Type your new password a second time, and press <Return>. **Note:** If you type a different password the second time, the system reports that the password has not changed because the new passwords did not match. If you receive this message, repeat step 8 to step 11.

Logging on from the main administration terminal

Introduction

This topic explains how to log on as the system administrator from the main administration terminal.

Note: If you are logging on from a multiple administration terminal, you cannot perform step 2.

Procedure

To log on from the main administration terminal, follow these steps.

Starting Point: The Logon/Status screen

Step	Action
1	Select the [Logon] softkey. **Result:** The system prompts you for a password.
2	Use the following table to determine the next step.

IF	THEN
you are logging on for the first time	see “Setting the system administration password” on page 3-6.
you have logged on before	go to step 3.

Step	Action
3	Type your system administration password, and press <Return>. **Result:** The system displays the Main Menu. **Note:** If an invalid password is entered, an error message appears. Repeat step 1 and step 3.

The Main Menu

The following shows an example of the Main Menu displayed at the main administration terminal.

```
                              Main Menu

          1  User Administration
          2  General Administration
          3  Voice Administration
          4  Fax Administration
          5  Hardware Administration
          6  System Status and Maintenance
          7  Operational Measurements
          8  Class of Service Administration
          9  Bulk Provisioning

Select an item >

   Logoff
```

Note: Some of these features may not be available on your system.

ATTENTION

An unsuccessful logon attempt is automatically recorded in the system log file. As a security precaution, after a third unsuccessful attempt to log on, the system forces a 10-minute delay before a further logon attempt is accepted. Only your Nortel representative has the required privileges to gain access to the system during the lockout period.

Logging on from a MAT

Introduction

If the Multiple Administration Terminal (MAT) feature is installed on your system, your Meridian Mail system can support up to four administration terminals (one main administration terminal and up to three MATs).

When you are logged on to a secondary terminal, you can perform a limited number of administrative tasks. For more information, see "Types of consoles" on page 3-3.

Your logon password is the same for both the main administration terminal and a MAT.

This topic explains how to log on from a MAT.

The default password

The default password for logging onto a MAT is custpwd.

Changing the default password

The system will prompt you to change the default password the first time you log on. This is for security reasons.

Once you have changed the password after initial logon, you can change the password at any time from the General Administration menu by selecting the Change Customer Administrator Password item.

Restriction

You cannot make the MAT password the same as the system administration password.

Before you begin

The Multiple Administration Terminal feature must be installed on your system.

Logging on from a MAT

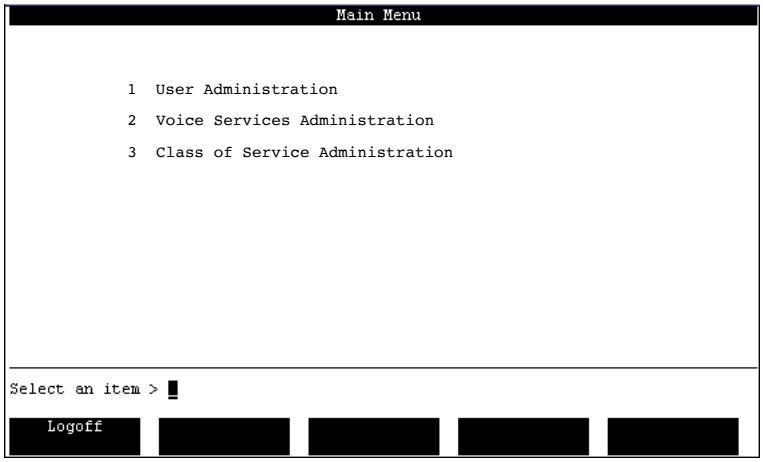
To log on from a MAT, follow these steps.

Starting Point: The Logon/Status screen

Step	Action
1	Select the [Logon] softkey.
2	Type the system administration password, and press <Return>. **Result:** The system displays the Main Menu. **Note:** If an invalid password is entered, an error message appears. Repeat step 1 and step 2.

The Main Menu at a MAT

The following shows an example of the Main Menu displayed at a MAT.



Logging on from a remote terminal (non-EC system)

Introduction

This topic explains how to log on to the system through a remote terminal from a system that is not a Modular Option EC system.

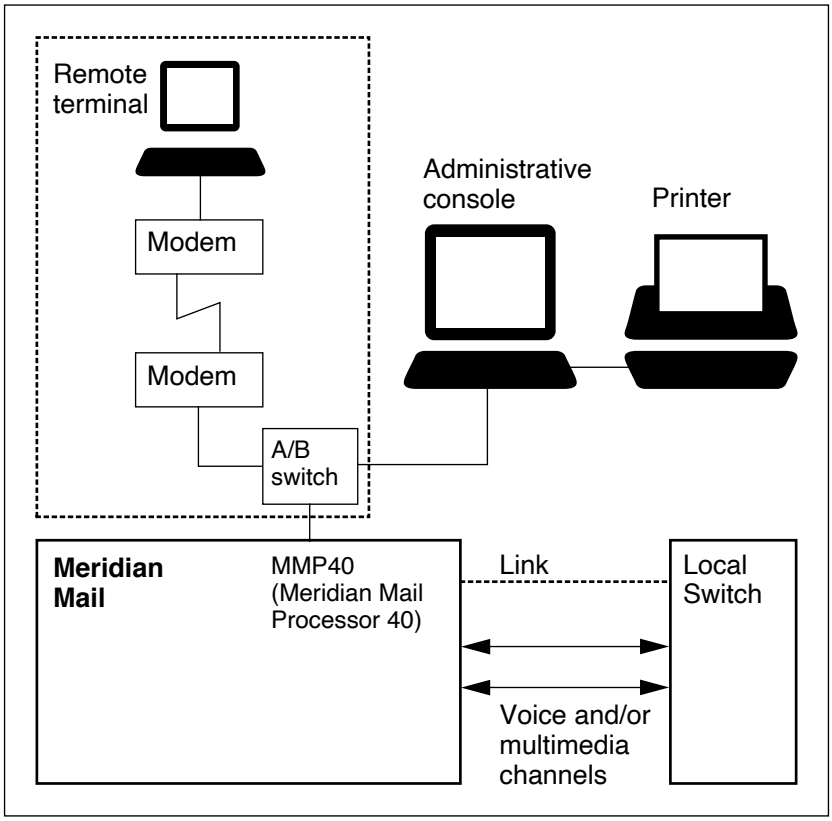
If your installation has a remote administration terminal installed for service personnel, administrative functions can be performed remotely.

Your logon password is the same for both the main administration terminal and the remote terminal.

The administrative functions described in this guide are identical whether viewed from the local administration terminal or from the remote terminal.

Typical remote terminal configuration (non-EC system)

The following diagram shows a typical remote terminal configuration for a system that is not a Modular Option EC system.



Coordinating a remote logon

Because no administrative functions can be carried out from the local console while a remote logon is in effect, a remote logon should be coordinated with the local administrator.

Logging on from a remote terminal (non-EC system)

To log on from a remote terminal on a non-EC system, follow these steps.

Starting Point: The Logon/Status screen at the local administration console

Step	Action
1	Change the A/B switch setting to remote.
2	Notify the user at the remote terminal. The user at the remote terminal does the following: a. Dial in to the modem. b. Press <Ctrl> <r> to display the Logon screen. c. Type the administration password. d. Carry out administrative tasks as required, and then log off.

Disabling remote terminal access (non-EC system)

To disable remote terminal access on a non-EC system, follow these steps.

Step	Action
1	At the local site, change the A/B switch back to the local setting. **Result:** Control is returned to the local console where the Logon/Status screen is again displayed.

Logging on from a remote terminal (EC system)

Introduction

This topic explains how to log on to the system through a remote terminal on a Modular Option EC system.

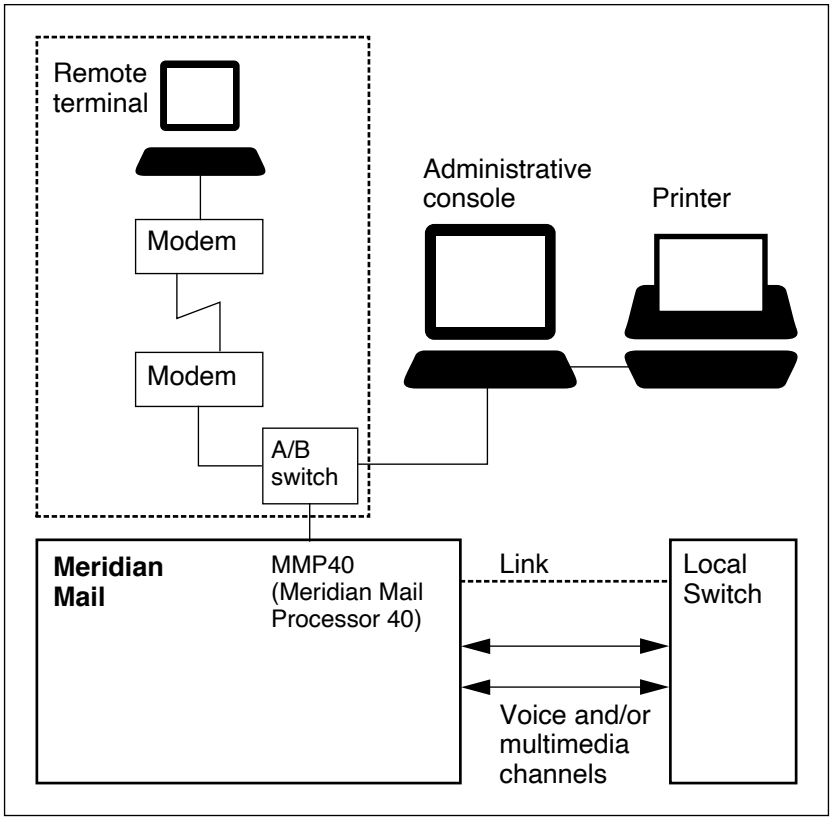
If your installation has a remote administration terminal installed for service personnel, administrative functions can be performed remotely.

Your logon password is the same for both the main administration terminal and the remote terminal.

The administrative functions described in this guide are identical whether viewed from the local administration terminal or from the remote terminal.

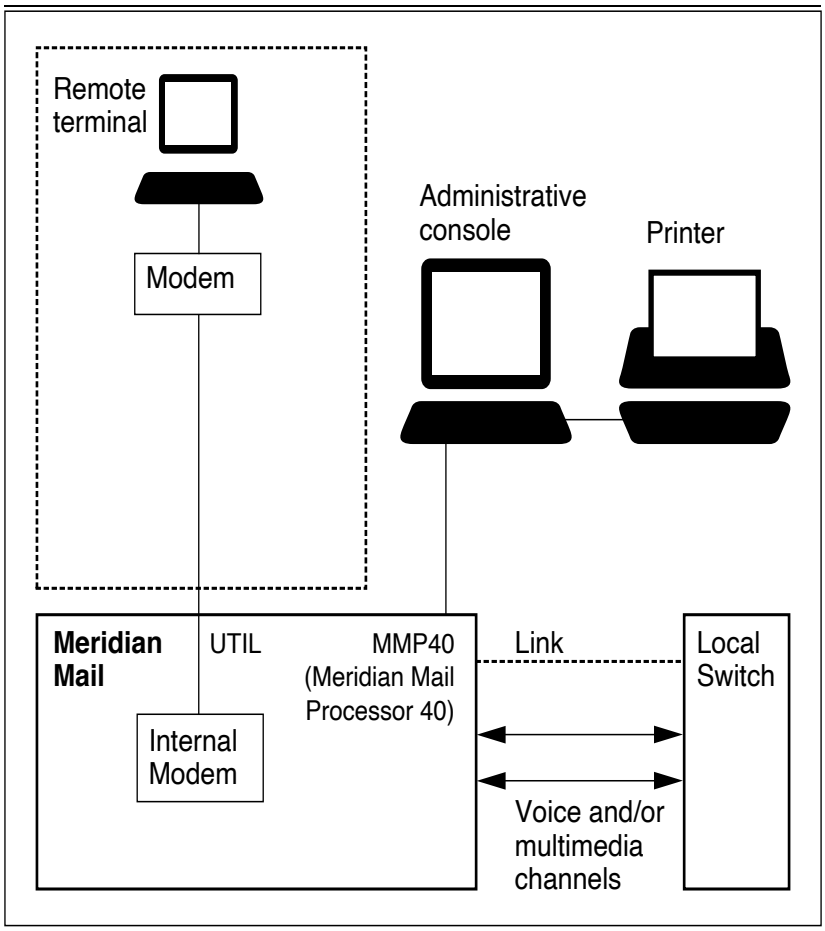
Typical remote terminal configuration (EC system)

The following diagram shows a typical remote terminal configuration for a Modular Option EC system.



Typical remote terminal configuration (EC system with internal modem)

The following diagram shows a typical remote administration configuration with an internal modem on the utility card for a Modular Option EC system.



Coordinating a remote logon

Because no administrative functions can be carried out from the local console while a remote logon is in effect, a remote logon should be coordinated with the local administrator.

Logging on from a remote terminal (EC system)

To log on from a remote terminal on an EC system, follow these steps.

Starting Point: The Logon/Status screen at the local administration console

Step	Action
1	To bring up the COBRAVT selection window, press <Ctrl> <w>. **Result:** The COBRAVT selection window is displayed. **Note:** For help using COBRAVT, type a question mark (?). A help screen is displayed.
2	Type **m** (case does not matter).
3	Notify the user at the remote terminal.
4	Dial in to the modem. The user at the remote terminal does the following: a. Press the <Break> key to gain control of the console. b. Type the administration password.

Disabling remote terminal access (EC system)

To disable remote terminal access, follow these steps.

Starting Point: The Logon/Status screen at the local administration console

Step	Action
1	To bring up the COBRAVT selection window, press <Ctrl> <w>. **Result:** The system displays the COBRAVT selection window.
2	Type **m** (case does not matter). **Result:** Control is returned to the local console where the system again displays the Logon/Status screen. **Note:** You can terminate a remote logon at any time if you press <Ctrl> <w> and type **m.**

CAUTION

Risk of data loss

If the remote administrator is in the process of changing system data and a save is not performed before a remote logon is terminated, data may be lost.

Using a single terminal to access the M1 and Meridian Mail

Introduction

If you are logging on at a site with only one terminal access, then you will need to toggle back and forth between the M1 and Meridian Mail.

Procedure

To toggle between the M1 and Meridian Mail, follow these steps.

Step	Action
1	Determine the steps you need to follow. **IF you want to toggle** — **THEN go to** from the M1 to MM — step 2. from MM to the M1 — step 7.
2	Flip the toggle switch to MM.
3	Press <Ctrl> <w> to clear the screen.
4	Press **i**, then **f**.
5	Is the screen displaying the MM interface? If yes, continue. If no, press <Ctrl> <r> to refresh the screen.
6	You can work at the terminal now.
7	Flip the toggle switch to the M1.
8	Press the Setup Key on the keyboard.
9	Use the up and down arrow keys to move to the Clear Display screen, and press <Return>. **Result:** If you are already logged on, the screen displays the M1 prompt: **>** **Result:** If you are not logged on to the M1, the screen displays the prompt:**.**
10	You can work at the terminal now.

Chapter 4

Setting up the system

In this chapter

Overview	4-2
Section A: Basic setup procedures	4-3
Section B: Setting up optional features	4-23

Overview

Introduction

This chapter contains the following information:

- It provides an overview of a complete basic setup of your system.
- It refers you to procedures for checking the provisioning of your Meridian Mail system.
- It lists and describes optional features and refers you to the procedures to set up these features.

Section A: Basic setup procedures

In this section

Overview	4-4
Changing the system administration password	4-5
Checking the hardware configuration	4-6
Checking the system status	4-7
Checking the Channel Allocation Table	4-8
Configuring general system options	4-9
Setting up dialing translations	4-10
Setting up restriction and permission lists	4-11
Customizing voice messaging options	4-12
Adding networking information to a network database	4-13
Adding DNs to the VSDN table	4-14
Defining classes of service	4-15
Configuring operational measurement options	4-16
Adding users to the system	4-17
Creating system distribution lists	4-18
Configuring optional features and other services	4-19
Setting up system security	4-20
Backing up the system	4-21

Overview

Introduction

This section provides general information and procedures for checking the provisioning of your Meridian Mail system. Wherever necessary, it refers you to more detailed information in other chapters of this guide and in other manuals.

It also provides an overview of a complete basic setup of your system.

Objective

This section is intended as a checklist for system setup.

Before you begin

To ensure that your Meridian Mail system is properly provisioned, refer to the procedures in the *Meridian Mail Installation and Maintenance Guide* (NTP 555-70x1-250).

Changing the system administration password

Introduction

This involves logging on to the main administration terminal using the current password, and then following the system instructions to change the password.

You can make password changes only at the main administration terminal. If you have MATs on your system, your changes are then automatically made to them.

Procedure

For information and procedures for changing the system administration password, see Chapter 3, “Logging on”.

Checking the hardware configuration

Introduction

This involves checking the node configuration and the data port configuration.

Check the data port configuration to verify the assignment of data devices, especially parameters such as the baud rate and parity for the administration console.

Procedure

To check the hardware configuration, refer to the procedures in the *Meridian Mail Installation and Maintenance Guide* (NTP 555-70x1-250).

Checking the system status

Introduction

This involves verifying the status of the system and enabling or disabling system nodes and DSP ports.

Procedure

For information and procedures for checking the system status, see Chapter 28, “System status and maintenance”.

Checking the Channel Allocation Table

Introduction

This involves configuring the primary DN and Channel DN for each agent/channel. It also involves configuring the service or services for which the channel will be used. In most cases, channels are shared by all services. If any channels are to be dedicated to a specific service, enter the service in the Channel Allocation Table.

You check the Channel Allocation Table to ensure consistency between the switch and the Meridian Mail system.

Note: This step should be carried out only by a qualified technician.

Procedure

To check the Channel Allocation Table, see "Channel Allocation Table" on page 28-45.

Configuring general system options

Introduction

This involves viewing the features that are installed on your system and configuring the attendant DN and date format for reports. The General Options screen is also where you assign classes of service to the system. You can also modify the SEER and Reports printer port names if different from the console port.

Procedure

For information and procedures for configuring general system options, see Chapter 13, “General options”.

Setting up dialing translations

Introduction

This involves defining network access prefixes for local off-switch, long distance, and international dialing, and for dialing translation tables.

Procedure

For information and procedures for setting up dialing translations, see Chapter 17, “Dialing translations”.

Setting up restriction and permission lists

Introduction

This involves modifying the restriction and permission codes to allow users to dial only the external phone numbers or internal extension numbers that you specify. Unless you are upgrading from an earlier release of Meridian Mail, features such as Mailbox Thru-Dial, Custom Revert DN, or Extension Dialing are initially restricted and do not work until you modify the restriction and permission codes.

You define restriction and permission codes to prevent external callers or internal users from placing local or long distance calls that you do not want billed to your system.

Note: This is a very important step.

Procedure

For information and procedures for setting up restriction and permission lists, see Chapter 6, “Setting up Meridian Mail security”.

Customizing voice messaging options

Introduction

This involves setting voice messaging parameters.

If the MMUI interface is installed, this includes such tasks as setting the broadcast mailbox number, the maximum allowed delay for timed delivery, and the name dialing prefix.

If VMUIF is installed, this includes such tasks as recording various greetings and setting the personal distribution list prefix, the lockout revert DN, and the maximum length of time that read messages are kept before they are deleted by the system.

Procedure

For information and procedures for customizing voice messaging options, see Chapter 20, “Voice messaging options”.

Adding networking information to a network database

Introduction

If the Network Message Service (NMS) feature is installed, you must configure the prime location and all satellite locations that are part of your network. This must be done before you add any service DNs and users.

Procedure

To add networking information to a network database, refer to the procedure in the *Network Message Service Installation and Administration Guide* (NTP 555-7001-243).

Adding DNs to the VSDN table

Introduction

The VSDN table lists the DNs associated with specific voice services. A DN is required for each voice service that you want users to be able to access directly by dialing a unique DN. The VSDN table maps voice services onto DNs so that when your Meridian Mail system receives an incoming call, it looks up the DN to determine which service is being requested and which prompts to play.

You define a DN in the VSDN table for each voice service that is to be directly dialable by internal users or external callers. This includes services such as voice messaging and express messaging.

Before you begin

For each service you plan to add to the VSDN table, an existing ACD queue must already be configured on the Meridian 1.

Procedure

For information and procedures for adding DNs to the VSDN table, see Chapter 24, “The VSDN table”.

Defining classes of service

Introduction

This involves identifying which of your users have similar needs and what those needs are, and then defining the operating parameters or Class of Service (COS) for each group of users.

When you change a parameter in a COS, all users belonging to that COS have the changes automatically updated.

> **ATTENTION**
>
> You must add classes of service before you add users. Each user must be assigned to a class of service.

Procedure

For information and procedures for defining classes of service, see Chapter 26, “Class of Service administration”.

Assigning COSs to the system

After you add classes of service you must assign them to the system. If you do not do this, the classes of service will not show up in the Add a Local Voice User screen and you will not be able to assign them to users.

Classes of service are assigned to the system in the General Options screen.

Configuring operational measurement options

Introduction

This involves defining how system and user statistics are collected. This includes, for example, the kinds of data to be collected, the time that traffic data collection begins and ends each day, and how often collected traffic statistics are written to disk.

You do not need to configure the operational measurement options right away. You may choose instead to use the default settings.

You can then modify these settings after your system has been in use for a time to provide a level of detail that is more appropriate for your needs.

Procedure

For information and procedures for configuring operational measurement options, see Chapter 30, “Operational Measurements”.

Adding users to the system

Introduction

This involves a number of tasks. Before you begin, you need to determine the capacity of your disk volume, survey users to establish the classes of services that will be necessary, estimate the average system usage of each class of user, and create classes of service to reflect your research.

You also identify users as local voice users, remote voice users, or directory entry users according to their needs.

Procedure

For information and procedures for adding users to the system, see the following chapters.

For information about	See
user administration in general	Chapter 7, “User administration—an overview”
local voice users	Chapter 8, “Local voice users”
remote voice users	Chapter 9, “Remote voice users”
directory entry users	Chapter 10, “Directory entry users”
distribution lists	Chapter 11, “Distribution lists”

Creating system distribution lists

Introduction

A distribution list is a collection of mailbox numbers. It allows you to send the same message to a number of people. Distribution lists are convenient if you frequently have to send messages to the same group or groups of people.

You do not need to create system distribution lists as part of the initial configuration. If you know which lists you need, then you can create them, but they can be created at any time.

Procedure

For information and procedures for creating system distribution lists, see Chapter 11, “Distribution lists”.

Configuring optional features and other services

Introduction

This involves configuring optional features that are installed on your system, such as Fax on Demand or AMIS Networking.

You can either continue with the configuration of these optional features or back up the system now and continue at a later time.

Procedure

For information and procedures for configuring optional features and other services, see “Setting up optional features” on page 4-23.

Setting up system security

Introduction

In today's telecommunications environment, every computerized system is potentially open to unauthorized access. It is necessary to take all possible precautions to prevent security breaches.

If your system is properly secured, it is difficult for a user connected to Meridian Mail (such as a user who is logged on to a mailbox or an external caller who has connected to Meridian Mail through a call answering session or a voice menu) to place unauthorized calls that will be billed to your system.

Procedure

For information and procedures for setting up system security, see Chapter 6, "Setting up Meridian Mail security".

Backing up the system

Introduction

After you have finished customizing your system configuration, back up the new data onto tape to ensure its safety. This involves making backup copies of some or all of the system's data.

In the event of disk failure, you will not need to reenter user and site-specific information, and you can bring your system back into service quickly.

Procedure

For information and procedures for backing up the system, see Chapter 15, "Back up and restore Meridian Mail data".

Section B: Setting up optional features

In this section

Overview	4-24
Setting up the Outcalling feature	4-25
Setting up the Voice Menus feature	4-26
Setting up the Voice Forms feature	4-27
Setting up the Fax on Demand feature	4-28
Setting up the Meridian Networking feature	4-29
Setting up the AMIS Networking feature	4-30
Setting up the Virtual Node AMIS Networking feature	4-31
Setting up the Enterprise Networking feature	4-32
Setting up the Network Message Service feature	4-33
Setting up the Hospitality feature	4-34
Setting up the Meridian Mail Reporter feature	4-35
Setting up the Meridian Mail AutoAdmin feature	4-36
Setting up the ACCESS feature	4-37

Overview

Introduction

This section introduces the following optional features:

- Outcalling
- Voice Menus
- Voice Forms
- Fax on Demand
- Meridian Mail Networking (includes Meridian and Enterprise Networking)
- AMIS Networking
- Network Message Service
- Hospitality
- Meridian Mail Reporter
- Meridian Mail AutoAdmin
- ACCESS

It also refers you to the procedures and information you require to set up these features.

Setting up the Outcalling feature

Introduction

The Outcalling feature refers to two functions: the Remote Notification feature and the Delivery to Non-User feature.

Remote Notification allows Meridian Mail users to be notified of new messages at remote phone or pager numbers. Delivery to Non-User allows users to compose and send messages to people outside the Meridian Mail system.

Procedure

For information and procedures for setting up the Outcalling feature, refer to *Meridian Mail Outcalling Application Guide* (NTP 555-7001-320).

Setting up the Voice Menus feature

Introduction

The Voice Menus feature enables you to create a number of custom call answering applications.

The Announcements service allows you to record messages that can be played back within a voice menu or as a stand-alone service that can be dialed directly.

Thru-Dial services access predefined DNs or user-prompted DNs that can be used either within a voice menu service or as a separate service with a directory number. Thru-Dial services can be set up to allow Name Dialing and can have restrictions barring users from dialing unauthorized numbers, such as long distance access codes.

The Time-of-Day Controllers service allows you to control the activation of voice services based on the date and time at which a call is received. This allows you to control the availability of voice services during off-hours and holidays.

The Voice Menus service enables you to create single-layered or multilayered menus that present callers with a series of choices about the action they can perform.

The Voice Prompt Maintenance service enables you to modify the prompts and greetings available in your voice menus and announcements using a telephone.

The Remote Activation service allows you to enable or disable voice services while you are offsite through a standard dual-tone multifrequency (touch tone) telephone set.

Procedure

For information and procedures for setting up the Voice Menus feature, refer to *Meridian Mail Voice Services Application Guide* (NTP 555-7001-325).

Setting up the Voice Forms feature

Introduction

The Voice Forms feature has two parts: Voice Forms administration and Voice Forms transcription.

Voice Forms administration involves the creation of applications that collect voice information from callers. An application consists of a series of questions, played in sequential order, to which callers give voice responses. It is as if callers are filling in a form over the phone.

Voice Forms transcription refers to the process of retrieving the information collected by a voice form application. Once retrieved, the data can be processed in a number of ways, depending on why you have collected the information.

Procedure

For information and procedures for setting up the Voice Forms feature, refer to *Meridian Mail Voice Services Application Guide* (NTP 555-7001-325).

Setting up the Fax on Demand feature

Introduction

Fax on Demand is a Meridian Mail feature that allows a caller to obtain information in the form of a fax. The fax information is stored in Meridian Mail and is sent on request to a fax device.

The configuration of the Fax on Demand application affects its available features. For example, fax documents may be stored either as stand-alone, directly dialed fax items, or as items selected from voice menus. Depending on how the Fax on Demand application is configured and on whether the caller is using a fax phone, fax information may be delivered as part of the call requesting the information, or later, by callback to the caller's fax device.

Procedure

For information and procedures for setting up the Fax on Demand feature, refer to *Meridian Mail Fax on Demand Application Guide* (NTP 555-7001-327).

Setting up the Meridian Networking feature

Introduction

Meridian Networking is a Meridian Mail networking protocol that permits one or more Meridian Mail systems to send messages to and receive messages from users at remote Meridian Mail sites.

It uses the following:

- a network database to define local and remote sites
- a hybrid analog and digital transmission scheme
- modems to transmit control passwords, message header information, and message delivery acknowledgments between sites

Procedure

For information and procedures for setting up the Meridian Networking feature, refer to *Networking Planning Guide* (NTP 555-7001-241) and *Meridian Networking Installation and Administration Guide* (NTP 555-7001-244).

Setting up the AMIS Networking feature

Introduction

AMIS Networking uses the Audio Messaging Interface Specification (AMIS) protocol. This protocol permits users to send messages to and receive messages from users at other voice messaging systems that also use the AMIS protocol (not necessarily Meridian Mail systems).

AMIS does not require special hardware or passwords. It does, however, require the ability to generate dual-tone multifrequency (DTMF) tones.

Procedure

For information and procedures for setting up the AMIS Networking feature, refer to *Networking Planning Guide* (NTP 555-7001-241) and *AMIS Networking Installation and Administration Guide* (NTP 555-7001-242).

Setting up the Virtual Node AMIS Networking feature

Introduction

Virtual Node AMIS Networking is a combination of Meridian Networking and AMIS Networking. Meridian Networking provide the ability to define local and remote sites as using the AMIS protocol. Sites that use the AMIS protocol are called virtual nodes. They may or may not have a Meridian Mail system installed.

Virtual Node AMIS uses the AMIS protocol to deliver messages. As a result, Virtual Node AMIS messages are restricted to the same functionality as the AMIS protocol.

Procedure

For information and procedures for setting up the Virtual Node AMIS Networking feature, refer to *Networking Planning Guide* (NTP 555-7001-241) and *Virtual Node AMIS Networking Installation and Administration Guide* (NTP 555-7001-245).

Setting up the Enterprise Networking feature

Introduction

Enterprise Networking is a Meridian Mail Networking protocol that permits one or more Meridian Mail systems to send messages to and receive messages from users at remote Meridian Mail sites. It uses the following:

- a network database to define local and remote sites
- DTMF signaling based on the AMIS protocol, instead of modems, to transmit messages between sites

Procedure

For information and procedures for setting up the Enterprise Networking feature, refer to *Networking Planning Guide* (NTP 555-7001-241) and *Enterprise Networking Installation and Administration Guide* (NTP 555-7001-246).

Setting up the Network Message Service feature

Introduction

Network Message Service (NMS) is a Meridian Mail feature that permits one Meridian Mail system to provide voice messaging services to users in a network of Meridian 1 switches that are interconnected by ISDN PRA trunks.

Procedure

For information and procedures for setting up the Network Message Service feature, refer to *Networking Planning Guide* (NTP 555-7001-241) and *Network Message Service Installation and Administration Guide* (NTP 555-7001-243).

Setting up the Hospitality feature

Introduction

The Meridian Hospitality Voice Service (MHVS) provides specialized functions for the hotel industry. The MHVS system consists of Meridian 1/SL-1 and Meridian Mail components connected to a Property Management System. MHVS provides voice messaging services to hotel staff and guests and automates the management of mailboxes for guest rooms.

When a guest checks in to the hotel, a mailbox is created for the room the guest will be occupying. Upon checkout, the mailbox is removed, and any read or unread messages that arrived for that guest prior to checkout are moved to a post-checkout mailbox for later retrieval.

Procedure

For information and procedures for setting up the Hospitality feature, refer to the *Hospitality Voice Services Implementation Guide* (NTP 555-7001-221).

Setting up the Meridian Mail Reporter feature

Introduction

Meridian Mail Reporter is an application that runs on a PC connected to Meridian Mail and enables you to download operational measurements data. Using this information, you can produce and print summary and detailed reports for use in managing Meridian Mail systems.

These reports support all areas of administrative responsibility, including general administration, troubleshooting, security, capacity analysis, and billing.

Procedure

For information and procedures for setting up the Meridian Mail Reporter feature, refer to the *Meridian Mail Reporter User's Guide* (P019082).

Setting up the Meridian Mail AutoAdmin feature

Introduction

Meridian Mail AutoAdmin is an application that runs on a PC connected to Meridian Mail; through it you can add, view, update, and delete user mailboxes. AutoAdmin allows large messaging customers such as universities, hospitals, government entities, and so on, to mass-create mailboxes with user data entered in another system and transferred to AutoAdmin, thereby reducing errors and data entry effort.

Procedure

For instructions on setting up and using AutoAdmin, see Appendix B, “Meridian Mail AutoAdmin Utility”, in this manual.

Setting up the ACCESS feature

Introduction

ACCESS uses a Unix interface to provide a development tool for creating specialized voice service applications for incoming or outgoing calls or for administrative purposes.

ACCESS applications can make use of the full range of voice and telephony functions that a digital voice processing system and a telephone switching system can offer. No special voice or telephone interface cards are needed, as the PBX and Meridian Mail together provide all of the necessary resources.

An ACCESS application can receive or place telephone calls, play prompts, receive "input" in the form of keypresses on a touch tone phone keypad (which can be interpreted as commands or data), transfer calls, record messages, and use Meridian Mail services.

Examples of ACCESS applications include banking-by-phone and order entry-by-phone, where the system places orders for callers based on the caller input on a touch tone telephone.

Procedure

For information and procedures for setting up the ACCESS feature, refer to the following publications:

- *Meridian ACCESS Configuration Guide* (NTP 555-7001-315)
- *Meridian ACCESS Developer's Guide* (NTP 555-7001-316)
- *Meridian ACCESS Voice Prompt Editor User's Guide* (NTP 555-7001-318)

Chapter 5

Making voice recordings

In this chapter

Overview	5-2
Types of recordings	5-4
How Call Answering uses personal greetings and personal verifications	5-7
Voice recording tips	5-11
Section A: Making recordings	5-13
Section B: VMUIF recordings	5-47

Overview

Introduction

As administrator, you make two types of voice recordings: those used only for administrative purposes, and those played to the public or other users. You make these recordings through the administration terminal (with a telephone nearby) or by using a telephone handset alone.

This chapter provides information and procedures for making different kinds of voice recordings or, where necessary, refers you to other chapters or manuals for this information.

The overview presents an introduction to the types of voice recordings you can make. It also offers some guidelines for making voice recordings.

Section A

Section A presents information and procedures for logging in to Meridian Mail and creating, playing back, editing, and deleting recordings.

These recordings include the following:

- the call answering greeting
- personal verifications (which can be recorded by you or the users on your system)
- system distribution list personal verifications
- remote site name verifications
- broadcast mailbox personal verifications
- Voice Services recordings (announcements, Thru-Dial services, Fax on Demand, voice menus, and Voice Prompt Maintenance)

For your reference, Section A also presents an overview of some of the voice recordings that users on your system make. These include the following:

- personal greetings
- broadcast messages

For more information about the recordings users can make, refer to the *Meridian Mail Voice Messaging User Guide* (P0875935).

Section B

Section B provides information and procedures for the greetings and introductory tutorials available for the VMUIF interface.

For information about making recordings for Hospitality systems, refer to the *Hospitality Voice Services Implementation Guide* (NTP 555-7001-221) and to the *Hospitality Voice Services Guest Administration Console Guide* (NTP 555-7001-222).

Types of recordings

Introduction

You can make different kinds of voice recordings from the administration terminal and a telephone or from a telephone handset alone. This overview presents an introduction to these recordings.

Call answering greeting

When MMUI is installed on your system, the call answering greeting identifies your organization to external callers. This greeting is not available if VMUIF is installed.

You record the call answering greeting from the administration terminal or from a telephone handset with administrator capabilities.

For information and procedures, see "Recording a call answering greeting" on page 5-18.

Personal greetings

If MMUI is installed on your system, users can record three kinds of personal greetings from their telephone handsets: external, internal, and temporary greetings.

If VMUIF is installed, users can record external and internal greetings.

For information and procedures, see "Recording personal greetings" on page 5-24. You may also wish to refer to the *Meridian Mail Voice Messaging User Guide* (P0875935). For information on how Meridian Mail decides which prompts, personal greetings, and personal verifications to play during an individual Call Answering session, see "How Call Answering uses personal greetings and personal verifications" on page 5-7.

Personal verification

The personal verification is used to identify local, remote, or directory entry users. Typically, it is recorded by the users themselves from their telephones, but you can also record it from the administration terminal as you add a user to the system or if you are logged into a mailbox as administrator.

For information and procedures, see "Recording a personal verification" on page 5-26. For information on how Meridian

Mail decides which prompts, personal greetings, and personal verifications to play during an individual Call Answering session, see "How Call Answering uses personal greetings and personal verifications" on page 5-7.

System distribution list personal verification

The system distribution list personal verification is an optional recording. This verification helps you to confirm you have selected the correct distribution list when you enter its number as you compose a message. The list title can describe who is included in the list or the purpose of the list.

For information and procedures, see "How Call Answering uses personal greetings and personal verifications" on page 5-7.

Remote site name verification

The site name verification is available if MMUI is installed on your system. It works like a personal verification for network sites. You record the site name verification from the administration terminal. It is used to confirm the site name when a message is addressed or when users receive a message from a network site.

For information and procedures, see "Identifying remote site names" on page 5-34, and refer to the *Meridian Networking Installation and Administration Guide* (NTP 555-7001-244).

Broadcast mailbox personal verification

Broadcast mailboxes can be set up for both the MMUI and VMUIF interface.

A broadcast message is a message that is sent to all Meridian Mail users.

You can record a personal verification for the broadcast mailbox so that when you enter the mailbox number during message composition, you get a verification that you have entered the correct number.

The personal verification for a broadcast mailbox can say something like: *"Broadcast mailbox 5555."*

For information and procedures, see "Recording a personal verification for the broadcast mailbox" on page 5-37.

Broadcast messages

A broadcast message is a message that is sent to all Meridian Mail users.

When you or the users on your system compose a message to the broadcast mailbox, the message is sent to all of the users on the system. If you have Meridian Mail Networking or NMS-MM, you can choose to send broadcast messages to all users at a particular Networking remote site, or at a particular NMS-MM location.

For more information and procedures, see "Recording and sending broadcast messages" on page 5-39.

Voice Services recordings

The Voice Services feature enables you to create custom call answering applications. Voice services recordings include announcement recordings, Thru-Dial greetings, fax item confirmation prompts, voice menu greetings, voice menu choices, and voice menu prompts.

For more information and procedures, see "Making Voice Services recordings" on page 5-43, and refer to the *Voice Services Application Guide* (NTP 555-7001-325).

How Call Answering uses personal greetings and personal verifications

Introduction

Call Answering is the collection of Meridian Mail features which deals with directing callers to a user's mailbox when

- the user does not answer his or her phone
- the call has been transferred directly to the mailbox by a Call Answering DN
- the DN is busy with another call

There is a variety of prompts Meridian Mail can play to a caller, depending on which prompts have been recorded, where the call originates, and the mailbox user's Class of Service settings. The charts below show how Meridian Mail decides which prompts to play during an MMUI Call Answering session.

VMUIF users

Call Answering is simpler for VMUIF mailbox users.

Call Answering - no answer/call transferred to mailbox

1. Is there a greeting recorded?

   If yes, play the greeting.

   If no, play the standard system "Nobody is available to take your call..." message.

Call Answering - user busy

1. Play the standard system "This line is busy..." message.
2. Is there a greeting recorded?

   If yes, play the greeting.

   If no, proceed to the next step.
3. Play the standard system "Please leave a message after the tone..." message.

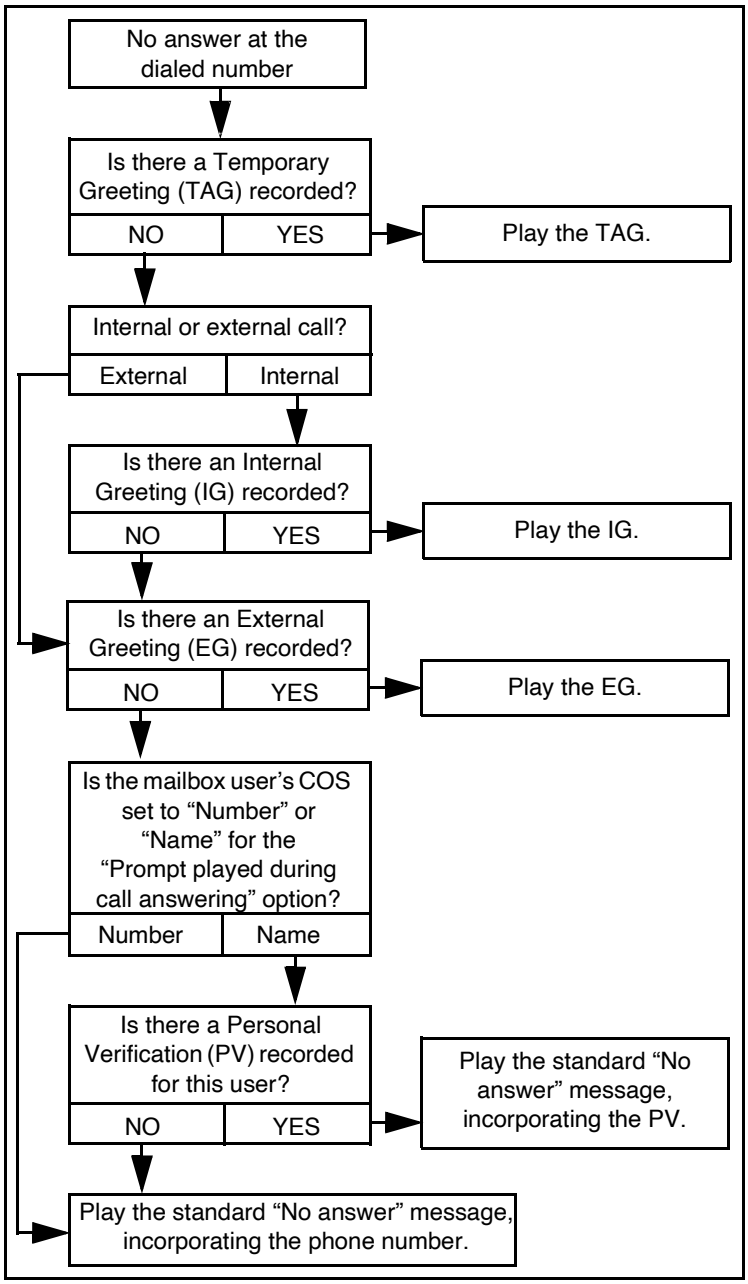
HVS Staff and Guest users

HVS Staff users are treated as MMUI mailbox users.

HVS Guest users behave as VMUIF mailbox users.

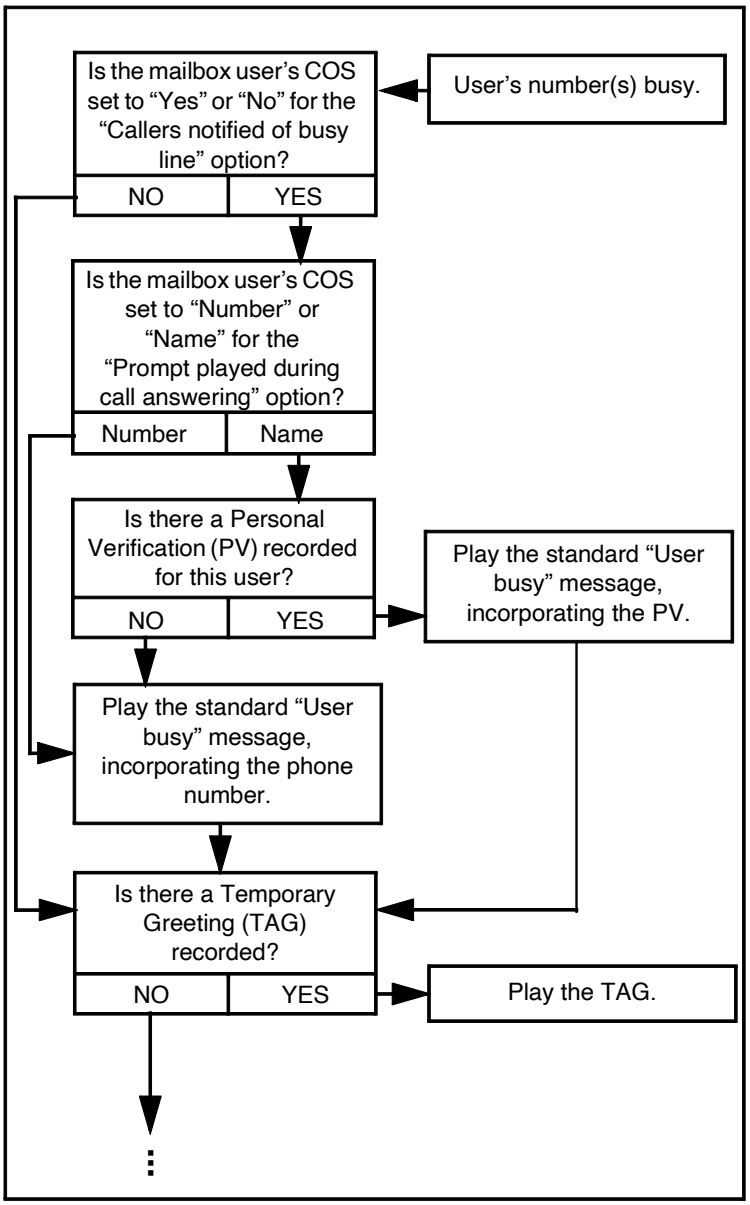
Call Answering - no answer/call transferred to mailbox

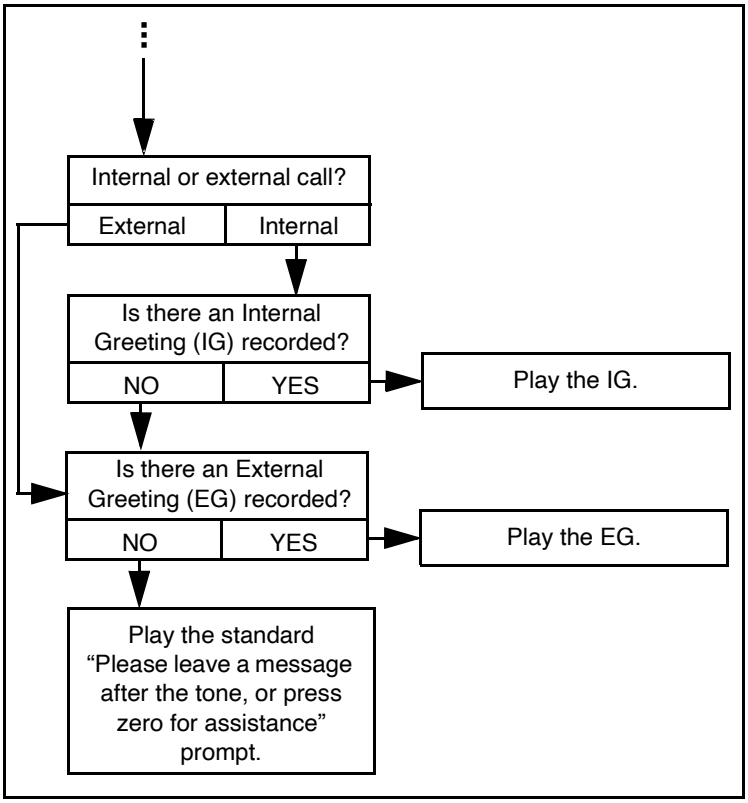
This is how Meridian Mail decides which prompt(s) to play to a caller when a mailbox user does not answer his or her phone, or when a Call Answering DN has sent the call directly to the mailbox.



Call Answering - user busy

This is how Meridian Mail decides which prompt(s) to play to a caller when a mailbox user's phone is already busy.




Internal or external call?
External
Internal
Is there an Internal Greeting (IG) recorded?
NO
YES
Play the IG.
Is there an External Greeting (EG) recorded?
NO
YES
Play the EG.
Play the standard "Please leave a message after the tone, or press zero for assistance" prompt.

Voice recording tips

Introduction

As administrator, you make two types of voice recordings:

- prompts that are used only for administrative purposes (such as broadcast mailbox personal verifications or system distribution list personal verifications)
- recordings played to the public or other users (such as the call answering greeting, personal verifications, remote site name verifications, and Voice Services recordings such as announcements, Thru-Dial services, Fax on Demand, or voice menus)

Prompts used only for administrative purposes require little preparation after you decide on their wording.

Voice menus or announcements played to the public or other users may require more formal preparation. For more information, you may wish to refer to the *Voice Services Application Guide* (NTP 555-7001-325).

Guidelines for voice recordings

The following are some suggestions for making voice recordings:

- Use only one voice for your voice recordings, so that callers are not distracted by changes in pitch, tone, intonation, or accent.
- To select a person to make your voice recordings, begin by auditioning a few candidates. Record their voices and then listen to the recordings over the telephone line. Low-pitched voices reproduce better than high-pitched voices over telephone lines. The voice used for the Meridian Mail prompts provides a good model.
- Print out complete, definitive copies of the script.
- Record in quiet surroundings.

  Start recording immediately after the tone, and stop the recording immediately after the last word. This prevents unnecessary pauses when system prompts and personal verifications are joined.

Guidelines for voice recordings (cont'd)

- To stop recording, press the number sign (#) if you are recording from a telephone handset, or the [Stop] softkey if you are recording from the administration terminal. Do not hang up the phone while you are recording as this may produce clicks in the recording.
- For applications that provide current information, have the person who knows the information monitor the prompts to ensure that the information is always up-to-date.

Section A: Making recordings

In this section

Overview 5-14
Logging in to Meridian Mail 5-15
Recording a call answering greeting 5-18
Recording personal greetings 5-24
Recording a personal verification 5-26
Recording a personal verification for a system distribution list 5-31
Identifying remote site names 5-34
Recording a personal verification for the broadcast mailbox 5-37
Recording and sending broadcast messages 5-39
Making Voice Services recordings 5-43

Overview

Introduction

This section presents information and procedures for logging in to Meridian Mail from the administration terminal or from a telephone on your system. It also explains how to create, play back, edit, and delete voice recordings.

Logging in to Meridian Mail

Introduction

Before you can create, play back, modify, or delete voice recordings, you need to log in to Meridian Mail. You do this either through a telephone set or through an administration terminal with a telephone nearby.

About using the telephone to make recordings

Using a telephone on your system, you or the users on your system log into Meridian Mail and access personal greetings. You can then make a number of kinds of voice recordings:

- external, internal, and temporary absence greetings
- personal verifications
- broadcast messages

About using a terminal to make recordings

Using the administration terminal or a telephone set with administrator capabilities, you can make certain kinds of recordings:

- the call answering greeting
- personal verifications
- system distribution list personal verifications
- site name verifications
- broadcast mailbox personal verifications
- Voice Services recordings

To make recordings through the system interface, the [Voice] softkey must be displayed.

Note: A telephone set is required to make recordings through the administration terminal. Ensure that a phone set is available near the administration terminal where you are working.

Screens with recording softkeys

Recording softkeys are available from some of the User Administration screens and Voice Services Administration screens.

Recording softkey positions

The following shows typical recording softkey positions.

```
Enter a phone number in Dialable format > _____________________
Return | Play | Record | Delete | Disconnect
```

Logging in using a telephone

To log in to Meridian Mail using a telephone set, follow these steps.

Step	Action
1	Dial the Meridian Mail access number.
2	Use the following table to determine the next step.

IF you are logging in from	THEN
your own telephone	press **#**.
another touch tone telephone	using the telephone keypad, enter your mailbox number, and press **#**.

Step	Action
3	Enter your password using the telephone keypad, and press **#**.
4	Use the following table to determine the next step.

IF you want to	THEN
create, play back, modify, or delete an internal greeting	see “Recording personal greetings” on page 5-24.
create, play back, modify, or delete an external greeting	see “Recording personal greetings” on page 5-24.
create, play back, modify, or delete a temporary absence greeting	see “Recording personal greetings” on page 5-24.
create, play back, or delete a personal verification	see “Recording a personal verification” on page 5-26.

Logging in from the administration terminal

To log in to Meridian Mail from the administration terminal, follow these steps.

Starting Point: The Logon/Status screen

Step	Action
1	Select [Logon]. **Result:** The system prompts you for a password.
2	Use the following table to determine the next step.

IF	THEN
you are logging in for the first time	see “Setting the system administration password” on page 3-6.
you have logged in before	go to step 3.

Step	Action
3	Type your system administration password, and press <Return>. **Result:** The system displays the Main Menu. **Note:** If an invalid password is entered, an error message appears. Return to step 1.
4	Use the following table to determine the next step.

IF you want to record	THEN
the call answering greeting	see “Recording personal greetings” on page 5-24.
a personal verification	see “Recording a personal verification” on page 5-26.
a personal verification for a system distribution list	see “How Call Answering uses personal greetings and personal verifications” on page 5-7.
a personal verification for a remote site name	see “Identifying remote site names” on page 5-34.
a broadcast mailbox personal verification	see “Recording a personal verification for the broadcast mailbox” on page 5-37.
make Voice Services recordings	see “Making Voice Services recordings” on page 5-43.

Recording a call answering greeting

Introduction

This topic provides information and procedures for recording a call answering greeting.

When you have MMUI installed, the call answering greeting identifies your organization to callers and users. Typically, this greeting consists of the spoken name of the organization.

The call answering greeting is played when

- an external caller is transferred to Meridian Mail to leave a message
- a user answers a remote notification call

Note: This greeting is available only if the MMUI interface is installed on your system. It is not available if VMUIF is installed.

You record the call answering greeting from the administration terminal or from a telephone set with administrator capability.

Using the call answering greeting

This greeting is optional. If you record the greeting, external callers hear it before they hear a user's personal greeting. If no greeting is recorded, callers hear only the user's personal greeting when they connect to a mailbox.

During remote notification calls, the following prompt is played to users if no call answering greeting is recorded: *"Hello. Meridian Mail has received a message for ...."*

When a call answering greeting exists, the following prompt is played: *"Hello. <Call Answering Greeting> has received a message for ...."*

Guidelines for composing

The following are some guidelines for composing a call answering greeting:

- Because this greeting is used in a variety of situations, consider how best to word it (or decide whether you want to record a greeting at all).
- If you do not record a call answering greeting, your organization's name is not announced at the beginning of a call answering session. If you feel that the user's personal greeting is sufficient, you may regard the call answering greeting as unnecessary.
- If you record only the organization's name (*"Myelin Incorporated"*), the greeting played during call answering may be too abrupt, but the prompt played during remote notification sounds quite natural.
- A friendlier greeting (*"Thank you for calling Myelin Incorporated"*) is ideal for call answering but is awkward when it is played for remote notification.

Multilingual systems

If more than one language is installed on your Meridian Mail system and you want to record a call answering greeting, you need to record one greeting for each language.

Recording the call answering greeting from a telephone set

To record, play back, modify, or delete the call answering greeting from a telephone set with administrator capabilities, follow these steps.

Step	Action
1	Press **82** on the telephone keypad.
2	Press **9** for the system greeting.
3	Use the following table to determine the next step.

IF you want to	THEN
review the greeting	go to step 4.
delete the greeting	go to step 5.
rerecord the greeting	go to step 5.
add to the greeting	go to step 6.

Step	Action
4	To review the greeting, press **2**.
5	To delete the greeting, press **76**. **Note:** If you do not delete the existing greeting, your new recording is appended to it.
6	To begin recording or add to the greeting, press **5**.
7	At the tone, record the call answering greeting.
8	To stop recording, press **#**. **Note:** Do not hang up the phone during recording as this may produce a click sound.
9	To review the greeting, press **2**.
10	To end your voice messaging session, press **83**, and then hang up.

Procedure

To create, play back, modify, or delete a call answering greeting through the administration terminal, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Messaging Options. **Result:** The system displays the Voice Messaging Options screen.

```
                          Voice Administration
Voice Messaging Options

Default Language:                                American_English
                                                 Canadian_French

Default Language Overrides User's
Preferred Language for Call Answering:           No Yes

Customized recording for American_English

  Call Answering Greeting (Voice):               No

Customized recording for Canadian_French

  Call Answering Greeting (Voice):               No

Maximum Delay for Timed Delivery (days):         31_
                                                                    MORE BELOW

   Save        Cancel                                              Voice
```

Step	Action
3	Move the cursor to the first Call Answering Greeting (Voice) field.
4	Select the [Voice] softkey. **Result:** The current screen remains displayed; the softkey display changes to [Cancel]. The system prompts for an extension number.
5	Type the extension number of the telephone set you will use to make the recording, and press <Return>. **Result:** The phone rings.
6	Pick up the telephone handset. **Result:** The system displays the recording softkeys.
7	Select the [Record] softkey. **Result:** The system displays the [Stop] softkey in place of the [Record] softkey. You hear a tone through the telephone receiver.

Step	Action
8	At the tone, begin speaking into the receiver. **Note:** Recording stops automatically if the greeting exceeds the Maximum Prompt Size or the Record Timeout set in the Voice Services Profile.
9	To stop recording, select the [Stop] softkey. **Result:** The recording stops automatically, and the system again displays the recording softkeys.
10	Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 11.
delete the recording	go to step 13.
record the greeting again	go to step 7.
save the recording	go to step 17.

11	Select the [Play] softkey. **Result:** If a recording is available, it is played. The system displays the [Stop] softkey. **Note:** If there is no current recording, the system displays a message on the console.
12	To stop the playback at any time, select the [Stop] softkey. **Result:** The system again displays the recording softkeys.
13	To delete the recording, select the [Delete] softkey. **Result:** The system displays the [OK to Delete] and [Cancel] softkeys. You are requested to confirm the deletion.
14	Use the following table to determine the next step.

IF you want to	THEN
cancel the deletion	go to step 15.
confirm the deletion	go to step 16.

15	To cancel the deletion, select the [Cancel] softkey. **Result:** The recording is not deleted. The system again displays the recording softkeys.

Step	Action
16	To delete the recording, select the [OK to Delete] softkey. **Result:** The system deletes the recording. The system again displays the recording softkeys.
17	To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone. **Result:** The system displays the original softkeys. **Note:** When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey. When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.
18	To update the screen and store the changes to the recording, use the [Save] softkey.

Recording personal greetings

Introduction

You and the users on your system record personal greetings—external, internal, and temporary greetings—from the telephone. These recordings are played when callers connect to a mailbox. The external greeting is played to external callers, the internal greeting is played to internal callers, and the temporary greeting, when one is recorded, preempts both internal and external greetings. The temporary greeting is commonly used for short-term messages to notify all callers that the mailbox user is away sick that day, or on vacation, or to otherwise alter the user's greeting on the short term.

This is an overview of personal greetings. For more information, refer to the *Meridian Mail Voice Messaging User Guide* (P0875935). For information on which personal greetings are used during a Call Answering session, see "How Call Answering uses personal greetings and personal verifications" on page 5-7.

Note: If VMUIF is installed on your system, users can record only external and internal greetings.

Recording personal greetings

To create, play back, modify, or delete a personal greeting, follow these steps.

Note: You must be logged in to a Meridian Mail mailbox. See "Logging in to Meridian Mail" on page 5-15.

Step	Action
1	Press **82** on the telephone keypad.
2	Select an external, internal, or temporary personal greeting. **IF you want to select** — **THEN** your external greeting — press **1**. your internal greeting — press **2**. your temporary greeting — press **3**. **Result:** The system confirms the greeting you select.
3	Use the following table to determine the next step. **IF you want to** — **THEN** review your greeting — go to step 4. delete your greeting — go to step 5. record your greeting again — go to step 5. add to your greeting — go to step 6. set an expiry date for your temporary greeting — go to step 9.
4	To review the greeting, press **2**.
5	To delete the greeting, press **76**. **Note:** If you do not delete your existing greeting, your new recording is appended to it.
6	To begin recording or add to the greeting, press **5**.
7	At the tone, record your greeting.
8	To stop recording, press **#**. **Note:** Do not hang up the phone during recording as this may produce a click sound.
9	To set the expiry date for your temporary greeting, press **9**. **Note:** Whenever you log in to your mailbox, the system prompts that you are using a temporary greeting.
10	To end your voice messaging session, press **83**, and then hang up.

Recording a personal verification

Introduction

This topic provides information and procedures for recording a personal verification using either a telephone handset alone or the administration terminal and a telephone.

The personal verification is a recording of a user's first and last names (and extension, if desired). It is used to identify the owner of a mailbox. Ideally, users should record personal verifications in their own voice. However, as administrator, you can record personal verifications for users either from the administration terminal or from a telephone set with administrator capabilities.

Using a personal verification

A personal verification is played in the following situations:

- Call Answering can be activated by a caller encountering a busy/unanswered DN, or by a caller calling a Call Answering service DN which directs the call to a particular mailbox.

  In Call Answering, the personal verification is played when the called number is busy. It is also played when the called number does not answer, and no personal greeting has been recorded. See "How Call Answering uses personal greetings and personal verifications" on page 5-7. for a complete explanation of the use of personal verifications in Call Answering.
- During message composition, the system plays the verification after a user enters a mailbox number to verify that the correct person is being addressed.
- When a user receives a message, the system plays the verification to identify who the message is from (such as the system administrator) or to advise all recipients that the message is a broadcast message.
- When messages are delivered to nonusers (using the Delivery to Non-Users feature), the system includes the verification. Recipients are more likely to listen to messages if they recognize who the messages are from.

- When callers use the Name Dialing feature, the system plays the personal verification. If a personal verification has not been recorded, the system spells out the name instead.
- During remote notification, the system plays the verification to identify who the message is intended for.

No personal verification recorded

If no verification is recorded, the system plays a recording of the user's extension number. Because it is easier for callers to confirm they have reached the correct person by hearing a name rather than by hearing an extension number, it is highly recommended that you or the users on your system record a personal verification for each mailbox.

Who can change personal verifications

Users can change their personal verifications only if this capability is enabled in the class of service to which they are assigned. For more information, see Chapter 26, "Class of Service administration".

Guidelines for composing

The following are some suggestions for recording personal verifications:

- Record a few names for personal verification, and listen to them before recording the remaining names.

  This ensures that the procedure is done correctly and the intonation is good. Test each of the following areas where personal verification applies:
  - call answering
  - message envelope playback
  - address playback in the compose command
  - name dialing
  - name addressing
  - express messaging
  - delivery to non-user
- When you are recording a personal verification for two or more people in your organization who have the same name (or very similar names), provide more information (their extension number or title, for example) to distinguish them.

Recording a personal verification using a telephone

To create, play back, or delete a personal verification using a telephone handset, follow these steps.

Note: You must be logged in to a Meridian Mail mailbox. See "Logging in to Meridian Mail" on page 5-15.

Step	Action
1	Press **89** on the telephone keypad. **Result:** The system plays the existing name for personal verification. If no name is recorded, the system reports this.
2	Use the following table to determine the next step.

IF you want to	THEN
hear the name for personal verification again	go to step 3.
record a new personal verification	go to step 4.
delete the existing personal verification	go to step 8.

Step	Action
3	To hear the name for personal verification again, press **2**.
4	To record a new personal verification, press **5**.
5	At the tone, record your greeting. **Note:** The maximum length is 20 seconds.
6	To stop recording, press **#**. **Result:** The system replays your recording.
7	To add to the recording, press **5**, and repeat step 5 and step 6.
8	To delete the existing personal verification, press **76**.
9	To end your voice messaging session, press **83**, and then hang up.

Recording a personal verification through the administration terminal

To create, play back, or delete a personal verification from the administration terminal, follow these steps.

Starting Point: The Main Menu

1. Select User Administration.
2. Select Local Voice User.
3. Select the [View/Modify] softkey, and type the mailbox number of the user whose personal verification you want to record.

   Result: The system displays the View/Modify Local Voice User screen.
4. Select the [Voice] softkey.

   Result: The current screen remains displayed; the softkey display changes to [Cancel].

   The system prompts for an extension number.
5. Type the extension number of the telephone set you will use to make the recording, and press <Return>.

   Result: The phone rings.
6. Pick up the telephone handset.

   Result: The system displays the recording softkeys.
7. Select the [Record] softkey.

   Result: The system displays the [Stop] softkey in place of the [Record] softkey.

   You hear a tone through the telephone receiver.
8. At the tone, begin speaking into the receiver.

   Note: Recording stops automatically if the recording exceeds the Maximum Prompt Size or the Record Timeout set in the Voice Services Profile.
9. To stop recording, select the [Stop] softkey.

   Result: The recording stops automatically, and the system again displays the recording softkeys.
10. Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 11.
delete the recording	go to step 14.
record the verification again	go to step 7.

11 To review your recording, select the [Play] softkey.

Result: The system plays the recording.

The system displays the [Stop] softkey.

12 To stop the playback at any time, select the [Stop] softkey.

Result: The system again displays the recording softkeys.

13 To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone.

Result: The system displays the original softkeys.

Note: When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey.

When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.

14 To delete a personal verification, use the arrow keys to select the entry, select the name using the spacebar, and press [Delete].

Result: The system displays the [OK to Delete] and [Cancel] softkeys.

15 Select [OK to Delete] to delete the personal verification.

Result: The system deletes the personal verification and updates the list.

16 To update the screen and store the changes to the recording, use the [Save] softkey.

Recording a personal verification for a system distribution list

Introduction

It is a good idea to make a voice recording of the title of each system distribution list. This procedure is optional, but a voice title helps you to confirm you have selected the correct list when you enter its number as you compose a message. The list title can describe who is included in the list or the purpose of the list.

Procedure

To record a personal verification for a system distribution list, follow this procedure.

Note: This procedure is optional.

Starting Point: The Main Menu

Step	Action
1	Select User Administration.
2	Select Distribution Lists. **Result:** The system displays the Distribution Lists softkeys screen.
3	Select the [View/Modify] softkey. **Result:** The system prompts for a distribution list number.
4	Type the number of the distribution list for which you are recording a title.
5	Select the [Voice] softkey. **Result:** The system prompts for an extension number.
6	Type the extension number of the telephone set you are going to use to record the title, and press <Return>. **Result:** The phone rings.
7	Pick up the telephone handset. **Result:** The system displays the recording softkeys.
8	Select the [Record] softkey. **Result:** The system displays the [Stop] softkey in place of the [Record] softkey. You hear a tone through the telephone receiver.

Step	Action
9	At the tone, begin speaking into the receiver. **Note:** Recording stops automatically if the recording exceeds the Maximum Prompt Size or the Record Timeout set in the Voice Services Profile. At the tone, record the personal verification.
10	To stop recording, select the [Stop] softkey. **Result:** The recording stops automatically, and the system again displays the recording softkeys.
11	Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 11.
delete the recording	go to step 14.
record the verification again	go to step 8.

12	To review your recording, select the [Play] softkey. **Result:** The system plays the recording. The system displays the [Stop] softkey.
13	To stop the playback at any time, select the [Stop] softkey. **Result:** The system again displays the recording softkeys.
14	To delete the recording, select the [Delete] softkey. **Result:** The system displays the [OK to Delete] and [Cancel] softkeys. You are requested to confirm the deletion.
15	Use the following table to determine the next step.

IF you want to	THEN
cancel the deletion	go to step 16.
confirm the deletion	go to step 17.

16	To cancel the deletion, select the [Cancel] softkey. **Result:** The recording is not deleted. The system again displays the recording softkeys.

Step	Action
17	To delete the recording, select the [OK to Delete] softkey. **Result:** The system deletes the recording. The system again displays the recording softkeys.
18	To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone. **Result:** The system displays the original softkeys. **Note:** When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey. When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.
19	To update the screen and store the changes to the recording, use the [Save] softkey.

Identifying remote site names

Introduction

The site name verification works like a personal verification for network sites. You record the site name verification from the administration terminal. It is used to confirm the site name when a message is addressed or when users receive a message from a network site. A site name can be recorded for Meridian Mail network sites and Network Message Service (NMS) locations.

If no site name is recorded, the system instead plays a recording of the site or location number that identifies the site.

For more information, refer to the *Meridian Networking Installation and Administration Guide* (NTP 555-7001-244).

Remote site name verification

The site name verification is available if MMUI is installed on your system. It works like a personal verification for network sites. You record the site name verification from the administration terminal. It is used to confirm the site name when a message is addressed or when users receive a message from a network site.

For more information, refer to the *Meridian Networking Installation and Administration Guide* (NTP 555-7001-244).

Procedure

To record a site name verification, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Network Administration.
2	Select the type of networking administration.
3	Select the type of site maintenance.
4	Select the [Add] softkey for a new site or the [View/Modify] softkey for an existing site.
5	Select the [Voice] softkey. **Result:** The current screen remains displayed; the softkey display changes to [Cancel]. The system prompts for an extension number.
6	Type the extension number of the telephone set you will use to make the recording, and press <Return>. **Result:** The phone rings.
7	Pick up the telephone handset. **Result:** The system displays the recording softkeys.
8	Select the [Record] softkey. **Result:** The system displays the [Stop] softkey in place of the [Record] softkey. You hear a tone through the telephone receiver.
9	At the tone, begin speaking into the receiver. **Note:** Recording stops automatically if the recording exceeds the Maximum Prompt Size or the Record Timeout set in the Voice Services Profile.
10	To stop recording, select the [Stop] softkey. **Result:** The recording stops automatically, and the system again displays the recording softkeys.
11	Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 11.
delete the recording	go to step 14.
record the verification again	go to step 7.
save the recording	go to step 18.

Step	Action
12	To review your recording, select the [Play] softkey. **Result:** The system plays the recording. The system displays the [Stop] softkey.
13	To stop the playback at any time, select the [Stop] softkey. **Result:** The system again displays the recording softkeys.
14	To delete the recording, select the [Delete] softkey. **Result:** The system displays the [OK to Delete] and [Cancel] softkeys. You are requested to confirm the deletion.
15	Use the following table to determine the next step.

IF you want to	THEN
cancel the deletion	go to step 15.
confirm the deletion	go to step 16.

16	To cancel the deletion, select the [Cancel] softkey. **Result:** The recording is not deleted. The system again displays the recording softkeys.
17	To delete the recording, select the [OK to Delete] softkey. **Result:** The system deletes the recording. The system again displays the recording softkeys.
18	To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone. **Result:** The system displays the original softkeys. **Note:** When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey. When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.
19	To update the screen and store the changes to the recording, use the [Save] softkey.

Recording a personal verification for the broadcast mailbox

Introduction

This topic provides information and procedures for recording a personal verification for the broadcast mailbox.

You can record a personal verification for the broadcast mailbox so that when you enter the mailbox number during message composition, you get a verification that you have entered the correct number.

The personal verification for a broadcast mailbox can say something like: *"Broadcast mailbox 5555."*

To set up a broadcast message, a special mailbox number (the broadcast mailbox number) is defined in the Voice Messaging Options screen. When you compose a broadcast message, you specify this broadcast mailbox number, and all users receive your message.

Recording from the administration terminal

To record a personal verification for the broadcast mailbox from the administration terminal, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Messaging Options.
3	Move the cursor to the Broadcast Mailbox Personal Verification Recorded (Voice) field.
4	Select the [Voice] softkey. **Result:** The system prompts you for a phone number in dialable format.
5	Type the extension of the phone you will use to record the verification, and press <Return>. **Result:** The phone rings.
6	Pick up the receiver. **Result:** The recording softkeys are displayed.

Step	Action
7	Select the [Record] softkey. **Result:** The system displays the [Stop] softkey in place of the [Record] softkey. You hear a tone through the telephone receiver.
8	At the tone, say the verification. **Example:** *"Broadcast mailbox 5555."*
9	To stop recording, select the [Stop] softkey. **Result:** The recording stops automatically, and the system again displays the recording softkeys.
10	Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 11.
save the recording	go to step 13.
rerecord the recording	press the [Delete] key, and go to step 7.

11	To play back the recording, select the [Play] softkey. **Result:** The system plays the recording. The system displays the [Stop] softkey.
12	To stop the playback at any time, select the [Stop] softkey. **Result:** The system again displays the recording softkeys.
13	To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone. **Result:** The system displays the original softkeys. **Note:** When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey. When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.
14	To update the screen and store the changes to the recording, use the [Save] softkey.

Recording and sending broadcast messages

Introduction

This topic explains how you and the users on your system can record and send broadcast messages using the telephone handset.

Definition: broadcast message

A broadcast message is a message that is sent to all Meridian Mail users. When you or the users on your system compose a message to the broadcast mailbox, the message is sent to all users on your Meridian Mail system.

Network broadcast message option for Meridian Mail Networking users

Users who have Meridian Mail Networking (either Meridian Networking or Enterprise Networking) can choose to send broadcast messages to all users at

- a single site, either the local one or a remote one
- a combination of sites (this involves putting in the network prefix numbers and broadcast mailbox number for each site, or incorporating them into a Personal Distribution List)
- all sites

Network broadcast messages sent to multi-customer remote systems will only be delivered to users in the networking customer group.

Enabling network broadcast messaging

To enable network broadcast messaging, you must fill in the Network Broadcast Administration fields when configuring Networking in the Network Configuration screen. See your Network Administration books for details.

You must also record a personal verification for the local broadcast mailbox (see "Recording a personal verification for the broadcast mailbox" on page 5-37.) Otherwise, network broadcast messaging will not work.

Restrictions on network broadcast messages

A user must have “Broadcast Capability” and “Network Broadcast Capability” set to “Yes” in their Class of Service to send network broadcast messages.

The acknowledgment message tag cannot be applied to network broadcast messages, or to any Personal Distribution List containing a network broadcast address, because this could result in the system attempting to return thousands of messages to the sender.

Network broadcast messages can only be sent to sites running MM11 and later releases. Network broadcast messages sent to MM10 and earlier releases will fail, with no NDN delivered to the sender.

Location-specific broadcast message option for NMS-MM users

Users who have NMS-MM can choose to send broadcast messages to all users at

- a single NMS location, either the prime location or a satellite location
- a combination of locations (this involves incorporating the network prefix numbers and broadcast mailbox number for each location into a Personal Distribution List)
- all locations

Note: If Meridian Mail Networking is also installed, all the above applies to locations at remote sites as well as local ones.

Setting up a broadcast mailbox

To set up a broadcast mailbox, you assign a mailbox number to the broadcast mailbox in the Voice Messaging Options screen. You do not need to set up an actual mailbox through User Administration. For more information about setting up broadcast mailboxes, see Chapter 20, “Voice messaging options”.

Who can compose and send broadcast messages

Any user who knows the broadcast mailbox number and has access to a mailbox with broadcast capability can compose and send broadcast messages. It is recommended that users try to avoid sending broadcast messages during busy hours.

Procedure

To record and send a broadcast message, follow these steps.

Step	Action
1	Log on to a Meridian Mail mailbox with broadcast capability.
2	Press **75**, and enter a number to specify the type of broadcast message you want.

IF you want to send a broadcast message to all users at	THEN enter
this site	nothing.
this site, including NMS users	nothing.
a particular NMS location, local or remote	the location's Network Prefix. (If your system uses overlap in its Network Prefixes, ignore the overlap and use the entire prefix.)
a particular remote Meridian Mail Networking site (this includes any NMS locations served by this site)	the site's Network Prefix. (If your system uses overlap in its Network Prefixes, ignore the overlap and use the entire prefix.)
all sites, local and remote (this includes all NMS locations as well)	the Network-Wide Broadcast Prefix. (This is set through the Network Configuration screen. See your Network Administration guide.)

3	Enter the broadcast mailbox number for your local Meridian Mail system (the default is 5555), and press #.
4	Repeat step 2 and step 3 to add other broadcast destinations to the list, if desired.
5	Press # again, to end the list.
6	To start recording, press **5.**
7	At the tone, record your broadcast message.
8	To stop recording, press **#**.

Step	Action
9	To listen to your broadcast message, press **2**.
10	To send the broadcast message, press **79**.
11	To end your voice messaging session, press **83**, and then hang up.

Making Voice Services recordings

Introduction

The Voice Services feature enables you to create custom call answering applications. Voice services recordings include announcement recording, Thru-Dial greetings, fax item confirmation prompts, voice menu greetings, voice menu choices, and voice menu prompts.

This topic provides an overview of making Voice Services recordings. For more information and more detailed procedures, refer to the *Voice Services Application Guide* (NTP 555-7001-325).

Announcements

This service enables you to record messages that can be played back within a voice menu or as a stand-alone service that can be dialed directly by a caller.

Thru-Dial services

These services access predefined DNs or user-prompted DNs that can be used within a voice menu service or as a separate service with a directory number. Thru-Dial services can be created to provide a variety of dialing options to users of Meridian Mail.

Fax on Demand

Fax on Demand is a Meridian Mail feature that allows a caller to obtain information in the form of a fax. Depending on the configuration of this feature on a system, fax documents may be stored either as stand-alone, directly dialed fax items, or as items selected from voice menus.

Voice Menus

The Voice Menus service enables you to create single-layered or multilayered menus that present choices to callers. Callers make their selections by pressing the key on the telephone keypad that corresponds to the action they wish to perform.

Voice Prompt Maintenance

This service enables you to modify the prompts and greetings available in your voice menus and announcements using a telephone.

Procedure To make a Voice Services recording, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Services Administration.
3	Select the type of voice service.
4	Use the following table to determine the next step.

IF you want to	THEN
create a new Voice Service recording	select the [Add] softkey.
add a new voice recording to an existing voice service	select the [View/Modify] softkey.
modify an existing voice recording	select the [View/Modify] softkey.

5 Use the following table to determine the next step.

IF you want to make	THEN move the cursor to the
an Announcement recording	Announcement Recorded field.
a Thru-Dial recording	Greeting Recorded field.
a Fax Item recording	Continuation Prompt Recorded field.
a Voice Menu recording	Greeting Recorded field or Menu Choices Recorded field.
a Voice Form recording	Form Name Recorded field.

6 Select the [Voice] softkey.

7 Type the extension of the phone you will use to make the recording, and press <Return>.

Result: The phone rings.

8 Pick up the receiver.

Result: The recording softkeys are displayed.

Step	Action
9	Select the [Record] softkey. **Result:** The system displays the [Stop] softkey in place of the [Record] softkey. You hear a tone through the telephone receiver.
10	At the tone, make your recording.
11	To stop recording, select the [Stop] softkey. **Result:** The recording stops automatically, and the system again displays the recording softkeys.
12	Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 13.
save the recording	go to step 15.
rerecord the recording	press the [Delete] key, and go to step 9.

13	To play back the recording, select the [Play] softkey. **Result:** The system plays the recording. The system displays the [Stop] softkey.
14	To stop the playback at any time, select the [Stop] softkey. **Result:** The system again displays the recording softkeys.
15	To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone. **Result:** The system displays the original softkeys. **Note:** When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey. When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.
16	To update the screen and store the changes to the recording, use the [Save] softkey.

Section B: VMUIF recordings

In this section

Overview 5-48
VMUIF introductory tutorials and the VMUIF login greeting 5-49
Recording the VMUIF login greeting 5-52

Overview

Introduction

Three recordings are prerecorded for the VMUIF interface:

- the introductory tutorial (for touch tone users)
- the introductory tutorial (for dial pulse users)
- the login greeting

These default recordings are enabled by default.

You can use these default recordings, customize them, or disable them.

This section provides information and procedures for the tutorials and greeting.

VMUIF introductory tutorials and the VMUIF login greeting

Introduction

An introductory tutorial greeting is played to VMUIF subscribers the first time they log in to their mailboxes. This tutorial familiarizes them with the Meridian Mail system.

The default DTMF tutorial

The Meridian Mail system plays the following introductory tutorial the first time a user logs in to a new mailbox from a touch tone telephone (a dual tone multifrequency or DTMF phone).

"You are about to hear an introduction to Call Answering. This service will allow your callers to leave you recorded messages. You can play back your messages from your home phone, or, if you create a password, from any touch tone phone outside your home. You can also record a personalized greeting that will be played to your callers, and you can erase your messages right away, or store them temporarily in your mailbox. Step-by-step instructions will guide you through your sessions. And remember, for help at any time, just press zero."

The default dial pulse tutorial

The Meridian Mail system plays the following introductory tutorial the first time a user logs in to a new mailbox that is set up as a dial pulse user.

"You are about to hear an introduction to Call Answering. This service will allow your callers to leave you recorded messages. You can listen to your messages from your home phone at any time. You can also play your messages from any touch tone phone. And by calling the Greeting Change Service, you can record a personalized greeting that will be played to your callers. Step-by-step instructions will guide you through your sessions. Consult the brochure for more information."

The login greeting

The login greeting is played when subscribers log on to Meridian Mail.

"Welcome to Call Answering."

The custom tutorial

You may prefer to record a custom tutorial to address particular needs of users on your system.

In preparing your tutorial, you may wish to refer to the text of the default tutorials in this section.

Procedure

To record or disable the VMUIF tutorial, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Messaging Options. **Result:** The system displays the Voice Messaging Options screen.
3	Select the VMUIF introductory tutorial for dial pulse or touch tone service.
4	Use the following table to determine the next step.

IF you want to	THEN
disable the tutorial	go to step 5.
record a custom tutorial	go to step 6.

5	Select None.
6	Move the cursor to the Voice/Tutorial Recorded field.
7	Select the [Voice] softkey. **Result:** The system prompts you for a phone number in dialable format.
8	Type the number of the telephone you will use to make the recording, and press <Return>. **Result:** The telephone rings.
9	Pick up the telephone handset. **Result:** The system displays the recording softkeys.
10	Select the [Record] softkey. **Result:** The [Record] softkey changes to the [Stop] softkey.
11	At the tone, record your tutorial.
12	To stop recording, select the [Stop] softkey. **Result:** The recording stops.

Step	Action
13	Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 14.
record the tutorial again	select the [Delete] softkey, and go to step 10.
save the recording	go to step 15.

Step	Action
14	To play back the recording, select the [Play] softkey.
15	To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone. **Result:** The system displays the original softkeys. **Note:** When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey. When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.
16	To update the screen and store the changes to the recording, use the [Save] softkey.
17	To enable the recording, in the Voice Messaging Options screen, move the cursor to the VMUIF Introductory Tutorial (Voice) field, and select Custom.

Recording the VMUIF login greeting

Introduction

You may prefer to customize or disable the default login greeting.

Procedure

To record or disable the VMUIF login greeting, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Messaging Options. **Result:** The system displays the Voice Messaging Options screen.
3	Select Login Greeting (Voice).
4	Use the following table to determine the next step.

IF you want to	THEN
disable the greeting	go to step 5.
record a custom greeting	go to step 7.

5	Select None.
6	Move the cursor to the Login Greeting Recorded field.
7	Select the [Voice] softkey. **Result:** The system prompts you for a phone number in dialable format.
8	Type the number of the telephone from which you will make the recording, and press <Return>. **Result:** The telephone rings.
9	Pick up the telephone handset. **Result:** The system displays the recording softkeys.
10	Select the [Record] softkey. **Result:** The [Record] softkey changes to the [Stop] softkey.
11	At the tone, say your greeting.

Step	Action
12	To stop recording, select the [Stop] softkey. **Result:** The recording stops.
13	Use the following table to determine the next step.

IF you want to	THEN
play back the recording	go to step 14.
record the greeting again	select the [Delete] softkey, and go to step 10.
save the recording	go to step 15.

Step	Action
14	To play back the recording, select the [Play] softkey.
15	To save the recording and disconnect the call, use either the [Return] softkey or the [Disconnect] softkey, and hang up the phone. **Result:** The system displays the original softkeys. **Note:** When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to enter the telephone extension again after selecting the [Voice] softkey. When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must enter the telephone extension again.
16	To update the screen and store the changes to the recording, use the [Save] softkey.
17	To enable the recording, in the Voice Messaging Options screen, move the cursor to the Login Greeting (Voice) field, and select Custom.

Chapter 6

Setting up Meridian Mail security

In this chapter

Overview	6-2
Section A: Telecommunication criminals and the problems they pose	6-3
Section B: Using Basic Access Restrictions features	6-9
Section C: Features that modify access restrictions	6-21
Section D: Controlling remote access to calling privilege	6-39
Section E: Controlling access through Least Cost Routing (BARS/NARS)	6-47
Section F: Controlling access to PBX administration programs	6-73
Section G: Controlling Direct Inward System Access	6-83
Section H: Restriction/Permission lists	6-89
Section I: Controlling access to Meridian Mail services and features	6-103
Section J: Controlling access to Meridian Mail mailboxes	6-123
Section K: Monitoring access to Meridian Mail mailboxes and features	6-149
Section L: Equipment security	6-161

Overview

Introduction

In today's telecommunications environment, every computerized system is potentially open to unauthorized access. As system administrator, it is your responsibility to take all necessary precautions to prevent security breaches. For example, unless your system has been properly secured, someone who is connected to Meridian Mail (such as a user who is logged on to a mailbox, or an external caller who has connected to Meridian Mail through a call answering session or a voice menu) can place unauthorized calls that will be billed to your system.

In this chapter

This chapter is divided into

- an overview which describes the purpose and contents of this chapter
- Section A: Telecommunication criminals and the problems they pose, which describes the types of telecommunication criminals and the problems they pose to your system
- a third part which provides information and instructions on how you can use Meridian 1 software features to control access to your switch

  This part starts at Section B: and ends at Section G:.
- a fourth part which provides information and instructions on how to use Meridian Mail security features

  This part starts at Section H: and ends at Section K:.
- Section L: Equipment security which describes how to control access to your system hardware

Section A: Telecommunication criminals and the problems they pose

In this section

Overview	6-4
Designing a security system	6-7
Ongoing security measures	6-8

Overview

Introduction

Telecom fraud has existed since the 1970s when "telephone criminals," or hackers, called their families and friends using stolen credit calling codes. By the late 1970s, hackers were using modems to access computerized systems from remote locations. By the mid-1980s, they were able to crack codes at computer speed using a personal computer with random number generating programs and autodialers.

Today, telephone operating companies are no longer the primary target for toll fraud as these companies have decreased their vulnerability by aggressively using software controls and prosecuting toll fraud criminals. For this reason, hackers trying to steal codes have migrated to new and potentially more devastating targets—customer premise equipment (for example, the PBX, Meridian Mail, and so on). Hackers are now using PBXs to place thousands of unauthorized calls primarily through inbound 800 numbers and voice mail.

What they gain

Hackers usually want one of the following:

- authorization codes which allow them to use your private branch exchange (PBX) for local and long-distance calls

  Authorization codes can then be sold or stored for future use.
- the use of your voice messaging system for their own purposes

  For example, they can use your system as a bulletin board to exchange lists of calling card numbers, coordinate illegal activities, and so on.
- to degrade your system performance

How they do it

There are several ways in which a hacker can try to access your system. The first is unauthorized access to the PBX; the second is unauthorized access to the voice messaging system, in this case, Meridian Mail; unauthorized access to personal mailboxes; and unauthorized access to the equipment.

Therefore, a good security system has to incorporate elements from PBX and system security, and awareness on the part of your users in order to provide effective security.

Unauthorized access to the PBX

Hackers are using the PBX to place unauthorized calls primarily through inbound 800 numbers and voice mail.

Nortel's Meridian 1 products meet a wide variety of customer requirements. In particular, the Meridian 1 (M1) has security features to help minimize its vulnerability while maintaining its flexibility.

For more information, see Sections B to G.

Unauthorized Meridian Mail access

Hackers may attempt to hack into your voice messaging system so they can use the outdialing feature to make free local- and long-distance calls.

With Meridian Mail, you can reduce, if not eliminate, this abuse by implementing some or all of the recommendations for system access. For more information, see Sections H to K.

Unauthorized mailbox access

Most hackers want access to the outdialing features—they are not concerned with personal mailboxes. If they do hack into a personal mailbox, they usually have some "fun" with it like changing the greeting, listening to messages, and so on.

With Meridian Mail, you can reduce the risk of unauthorized mailbox access by implementing some or all of the recommendations for mailbox access. For more information, see "Controlling access to Meridian Mail mailboxes" on page 6-123.

Unauthorized access to the equipment

Your system hardware could be a potential point of unauthorized access.

What can be done about it?

Inadequate control of calling privileges and of physical access to switching systems can cost your business millions of dollars. To secure your PBX and limit its exposure to corporate espionage and toll fraud, you need to implement security measures for

- PBX access
- Meridian Mail system access
- personal mailbox access
- equipment access

Designing a security system

Introduction

When designing a security system, consider the following two questions:

- How can you train your staff to responsibly use Meridian Mail?
- How can you prevent unauthorized use of your PBX and Meridian Mail system?

Both of these factors will help in keeping your Meridian Mail system safe from individuals who want to abuse your system.

Training your staff

Controlling access privileges to prevent PBX toll fraud and abuse of your telephone system will affect *all* employees in your organization, regardless of their positions or responsibilities. Implementing a communication program about the potential for fraud and abuse of your Meridian Mail communication system will help motivate your employees to prevent such abuse.

Ongoing security measures

Introduction

Once you have established your security practices, you should review them

- several months after the practices have been implemented so you can evaluate the results

  This will help determine if certain practices require modification.
- whenever you notice strange calling patterns

  These patterns will appear on reports listing numbers that are being called from your location or charges that are being billed to your company.

Remember to include your security practices in the orientation session for new employees.

Section B: Using Basic Access Restrictions features

In this section

Overview	6-10
Trunk Group Access Restrictions	6-11
Class of Service	6-13
TGAR/TARG and CLS interaction	6-17
Transfer feature on modems	6-19

Overview

Introduction

By providing internal and external users access only to the facilities and calling privileges that their jobs require, you can greatly decrease the potential for system abuse and toll fraud. With Basic Access Restrictions features, you can deter internal abuse and restrict external access to toll facilities.

The features

The Basic Access Restrictions features you can apply to stations, TIE trunks, and authorization codes are as follows:

- Trunk Group Access Restrictions (TGAR/TARG) controls the specific trunk groups to which a station, TIE trunk, Direct Inward System Access (DISA) directory number, or authorization code has direct access.

  For more information, see "Trunk Group Access Restrictions" on page 6-11.
- Class of Service (CLS) controls the degree of access; that is, once access is provided, CLS determines whether users can make local, TIE trunk, or long-distance calls.

  For more information, see "Class of Service" on page 6-13.

Trunk Group Access Restrictions

Introduction

Trunk Group Access Restrictions (TGAR) controls access to various trunk groups including trunks that interface with the exchange network, with TIE and CCSA networks, and with services such as paging, dictation, and recorded announcements.

How it works

Stations, TIE trunks, DISA directory numbers (DNs), and authorization codes are assigned to a group (TGAR). When users attempt to access a trunk route from a station, TIE trunk, DISA DN, or authorization code, the Meridian 1 software compares their group assignment (TGAR) against the list of denied Trunk Access Restrictions Group (TARG) associated with the trunk route they are trying to access.

If access is permitted, the Meridian 1 software then uses the Class of Service (CLS) assignment to determine call eligibility. The system always uses the most restrictive assignment (CLS or TGAR) to determine call eligibility when a user is trying to access trunk facilities directly.

By partitioning stations, TIE trunks, DISA DNs, and authorization codes into appropriate groups based on your corporate culture, you can stem internal abuse and external fraudulent activity, such as “looping” from PBX to PBX or to other carriers to mask the call’s origin.

Implementing and auditing the feature

Use the following table to implement or audit the TGAR/TARG feature on the Meridian 1.

For	Implement using	Print using
Stations	LD 10/11—TGAR	LD 20 by TN LD 10/11 by TN from Release 19 and up
Authorization codes	LD 88—TGAR	LD 88 by authorization code
TIE trunks	LD 14—TGAR	LD 20 by TN
Trunk groups (Route)	LD 16—TARG	LD 21 by route or access code
DISA DNs	LD 24—DISA	LD 24 by DISA DN

Class of Service

Introduction

Class of Service provides the flexibility to partition stations, TIE trunks, DISA DNs, and authorization codes into calling privilege "levels" that suit your business needs. Again, these features can inhibit internal abuse and help protect your system by preventing users from placing calls through external sources.

Class of Service restriction levels

You can assign any one of the following Class of Service restriction levels to each station, TIE trunk, and authorization code to control the degree of access to the exchange network.

- ***Unrestricted Service (UNR)*** Allowed to originate and receive calls from the exchange network.
- ***Conditionally Unrestricted (CUN)*** Allowed to receive calls from the exchange network. Considered toll-denied for calls placed through direct access to trunk but unrestricted for toll calls placed through Automatic Number Identification (ANI).
- ***Conditionally Toll-Denied (CTD)*** Allowed to receive calls from the exchange network. Considered toll-denied for calls placed through direct access to trunks, but unrestricted for toll calls placed through Basic/Network Alternate Route Selection (BARS/NARS).
- ***Toll-Denied Service (TLD)*** Allowed to receive calls from the exchange network and to dial local exchanges. Calling privileges of toll-denied stations may be modifiable through Code Restriction or New Flexible Code Restriction to allow or deny certain dialing sequences.
- ***Semi-Restricted Service (SRE)*** Allowed to receive calls from the exchange network. Restricted from all dial access to the exchange network but allowed access to TIE trunks. Allowed to access the exchange network through an attendant or an unrestricted station.

Class of Service restriction levels (cont'd)

- ***Fully Restricted Service*** Three classes of Fully Restricted Service are available:
  - ***FRE*** Allowed to originate and receive internal calls. Allowed access to TIE and CCSA networks, and to and from the exchange network using call modification from an unrestricted station. Denied access, either through dialing or through the attendant, to and from the exchange network.
  - ***FR1*** Allowed to originate and receive internal calls. Allowed access to TIE and CCSA networks. Denied access to and from the exchange network.
  - ***FR2*** Allowed to originate and receive internal calls. Denied access to TIE and CCSA networks, and to the exchange network.

Assigning a Class of Service

The following table outlines various call types and indicates whether they are possible within each Class of Service assignment.

	Class of Service assignment						
Call type	**UNR**	**CTD/CUN**	**TLD**	**SRE**	**FRE**	**FR1**	**FR2**
Incoming trunk calls	Yes	Yes	Yes	Yes	Through call modification only (see Note 1)	No	No
Outgoing non-toll trunk call	Yes	Yes	Yes	Attendant or station-extended only	Station-extended only	No	No
Outgoing toll trunk call (see Note 2)	Yes	No direct access. Yes, through BARS, NARS, or CDP if allowed through NCOS	Attendant or station-extended only		NA	No	No
Incoming/ outgoing TIE call	Yes	Yes	Yes	Yes	Yes	Yes	No
Station-to-station call	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Note 1: Call modification (transfer from station, call pickup, or transfer answer from any station) may be allowed or denied for each system.							
Note 2: A toll call to the Meridian 1 is 0+ or 1+ dialing on a central office or foreign exchange trunk.							

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Class of Service feature.

For	Implement using	Print using
Stations	LD 10/11—CLS	LD 20 by TN; LD 10/11 by TN from Release 19 and up LD81 by COS
Authorization codes	LD 88—CLS	LD 88 (by authorization code)
TIE trunks	LD 14—CLS	LD 20 by TN
Trunk groups (Route)	LD 24—CLS	LD 24 (by DISA DN)

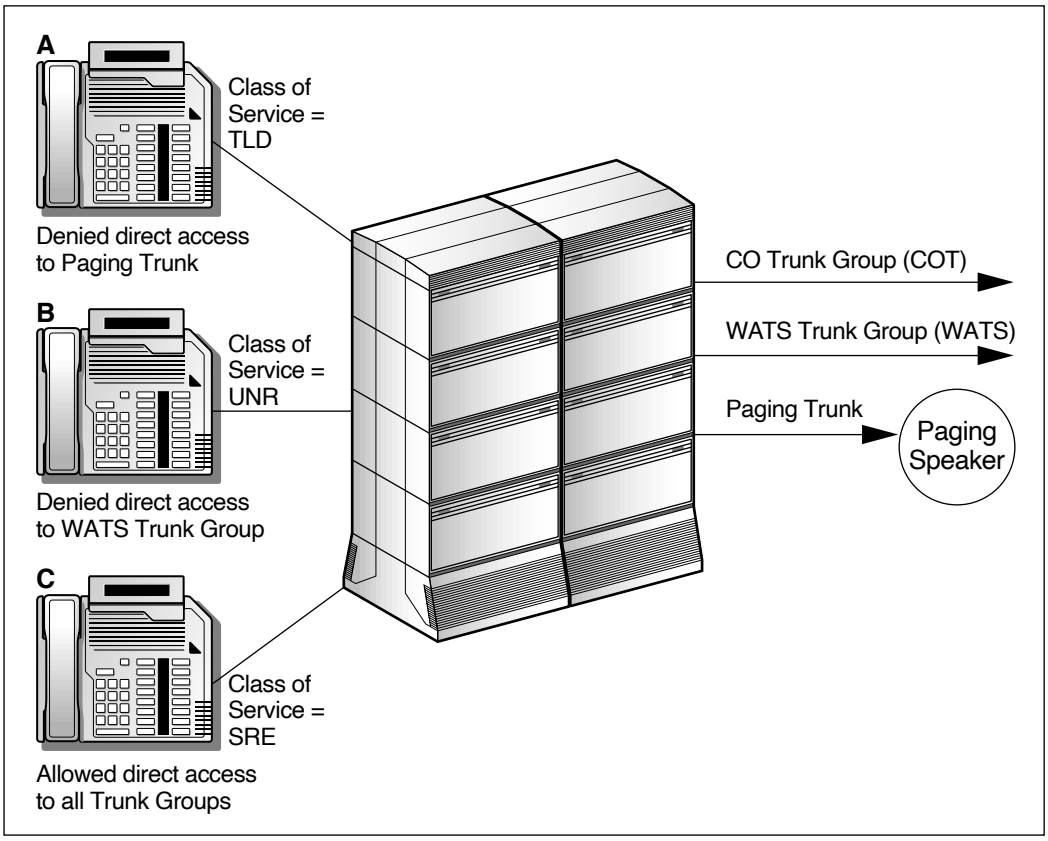
TGAR/TARG and CLS interaction

Introduction

You can use CLS and TGAR/TARG to control access to and from your trunk facilities. By assigning the most appropriate Class of Service (COS) and TGAR, you can limit your system's vulnerability to toll fraud and internal abuse.

Interaction

The following illustration shows the interaction between the Class of Service (CLS) assignment and Trunk Group Access Restrictions (TGAR).



G100446

In this illustration, the following occurs:

- User C dials access code to CO trunk group, followed by 555-6100.
- Meridian 1 checks Trunk Access Restriction Group to see if user has access to CO trunks.

  User C does.
- Meridian 1 checks CLS (SRE) to see if user can make a local call.

  User C cannot make a local call.
- Call is not allowed through CLS.

In summary, when a user attempts to access a trunk route, the Meridian 1 compares the TGAR assignment against the list of denied TARGs associated with the route that the user is trying to access. If the TARG is not listed, the Meridian 1 then uses the CLS assignment to determine call eligibility.

The system uses the most restrictive assignment, CLS or TGAR, to determine call eligibility when a user is attempting to place a call by way of direct access to trunk facilities.

Transfer feature on modems

Introduction

Hackers also use “smart” modems to infiltrate a PBX taking advantage of systems whose 2500 dataports were programmed with unnecessary features. The most common data hack is perpetrated by one “smart” modem calling another and leaving a series of instructions at the receiving modem.

How it works

The instructions require the receiving modem to emulate a switchhook flash (transfer), out pulse a series of numbers from the calling modem, and switchhook again. This effectively transfers the call back to the PBX and out again.

What you can do about it

The modem port usually has calling privileges assigned that are not required for the modem to function. Many times, a 2500-set template is used that is also used for single-line phones. Frequently, the administrator is unaware that the 2500 port will be used for data,

Modem phones should be identified and the transfer feature removed if possible. The default on 2500 sets is “deny.” Be sure the class of service, TGAR, and NCOS do not allow long-distance calling whenever possible.

Section C: Features that modify access restrictions

In this section

Overview	6-22
System Speed Call	6-23
Authorization Codes	6-24
Station Specific Authorization Codes	6-25
Forced Charge Account	6-27
Controlled Class of Service	6-29
Enhanced Controlled Class of Service	6-32
Flexible Feature Codes—Electronic Lock	6-33
Code Restriction	6-34
New Flexible Code Restriction	6-36

Overview

Introduction

The following features can be used to selectively override Class of Service (CLS) and Trunk Group Access Restrictions (TGAR) when you need to extend a station's or TIE trunk's normal calling capabilities:

- System Speed Call

  For more information, see "System Speed Call" on page 6-23.
- Authorization Code

  For more information, see "Authorization Codes" on page 6-24.
- Station Specific Authorization Code

  For more information, see "Station Specific Authorization Codes" on page 6-25.
- Forced Charge Account

  For more information on, see "Forced Charge Account" on page 6-27.
- Controlled Class of Service

  For more information, see "Controlled Class of Service" on page 6-29.
- Enhanced Controlled Class of Service

  For more information, see "Enhanced Controlled Class of Service" on page 6-32.
- Flexible Feature Codes—Electronic Lock

  For more information, see "Flexible Feature Codes—Electronic Lock" on page 6-33.
- Code Restrictions

  For more information, see "Code Restriction" on page 6-34.
- New Flexible Code Restriction

  For more information, see "New Flexible Code Restriction" on page 6-36.

System Speed Call

Introduction

System Speed Call extends the capabilities of the Speed Call feature. In addition to providing abbreviated dialing, using an entry in a System Speed Call list lets the internal user temporarily override the Class of Service and TGAR assigned to a station, and place a call to a telephone number in the System Speed Call list.

How it works

With this feature, you can assign the most appropriate CLS and TGAR restrictions to a station to limit the potential for unauthorized calling, and, at the same time, allow calls to approved destinations. The "approved telephone numbers" that you define in a system Speed Call list extend the station's calling privileges beyond the station restriction levels.

You can assign stations to different System Speed Call lists. You can also designate these stations as either System Speed Call Users (SSUs) or System Speed Call User/Controllers (SSCs) of the list. You can also assign list controlling capabilities to a key on the attendant console. However, this key cannot override CLS and TGAR because the attendant is not subject to these restrictions.

Note: A System Speed Call list can also override the station restrictions imposed through the Least Cost Routing software.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the System Speed Call feature.

For	Implement using	Print using
Stations	LD 10—FTR LD11—SSU, KEY	LD 20 by TN; LD 10/11 by TN from Release 19 and up LD81 by SSU, SSC, KEY
Speed Call list	LD 18—SSC, all prompts	LD 20 by list number
Attendant	LD 12—KEY	LD 20 by TN

Authorization Codes

Introduction

Authorization codes allow users to place business calls from stations normally restricted from doing so. These restricted stations may be located in areas of public access or used by employees who do not require broader calling privileges.

How it works

Authorization codes enable selected users to temporarily override the access restrictions assigned to a station or a TIE trunk. A user enters an authorization code which has an associated Class of Service (CLS), TGAR, and Least Cost Routing or Network Class of Service (NCOS). The user has the calling privileges of the authorization codes rather than those of the station or TIE trunk for the duration of the call.

Considerations

When you implement the Authorization Code feature, you should consider making the authorization codes as long as your corporate culture will allow, assigning unique authorization codes to each user, and allowing calling privileges based on user requirements.

You can also output the codes as part of the Call Detail Records (CDR) to look for call patterns that indicate possible unauthorized access or abuse. You should design and implement procedures for assigning authorization codes to new employees and for deleting codes that are no longer valid because of attrition or abuse.

Note: You may use authorization codes to override the station restrictions imposed through the Least Cost Routing software.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Authorization Codes feature.

For	Implement using Overlay programs/features prompts	Print using Overlay programs
Authorization codes	LD88—all prompts	LD 88 by authorization code

Station Specific Authorization Codes

Introduction

The Station Specific Authorization (Authcode) Code is offered in X11 Release 19 as a separate package. It allows you to define the authorization code access level of a set.

How it works

The Station Specific Authorization Code feature is implemented on a per set basis. The system will cross-check between overlays 10, 11, and 88 to ensure that the authorization code being used is valid. The only time cross-checking is not performed is when authorization codes are deleted from overlays 10 or 11. You must remove the authorization codes from overlay 88 as well as overlays 10 or 11.

Levels of access

There are three levels of authorization code access:

- ***Authcode Unrestricted (AUTU)*** A set programmed AUTU will be allowed to enter any authorization code without additional restrictions.
- ***Authcode Restricted (AUTR)*** When a set is configured AUTR, the authorization code entered by the user must match one of the preassigned authorization codes. Any other authcode will be treated as invalid, and an error message will be generated at the TTY.
- ***Authcode Denied (AUTD)*** No authorization code entry will be accepted for a set configured as AUTD.

Implementing and auditing

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Station Specific Authorization Codes feature.

For	Implement using	Print using
LD 10/11 stations	LD 10/11 (AUTU), AUTR, AUTD MAUT YES/NO SPWD (prompted if MAUT=YES) AUTH	LD 20 by TNB LD 10, 11 by TNB from Release 19 and up
LD 81 ODAS	LD 81 FEAT AUTU, AUDT, AUTD	LD 81 by FEAT
LD 88 Authorization Code	LD 88 AUTH	LD 88 by AUTH

Forced Charge Account

Introduction

With Forced Charge Account (FCA), the system forces the user to act before greater calling privileges are granted.

How it works

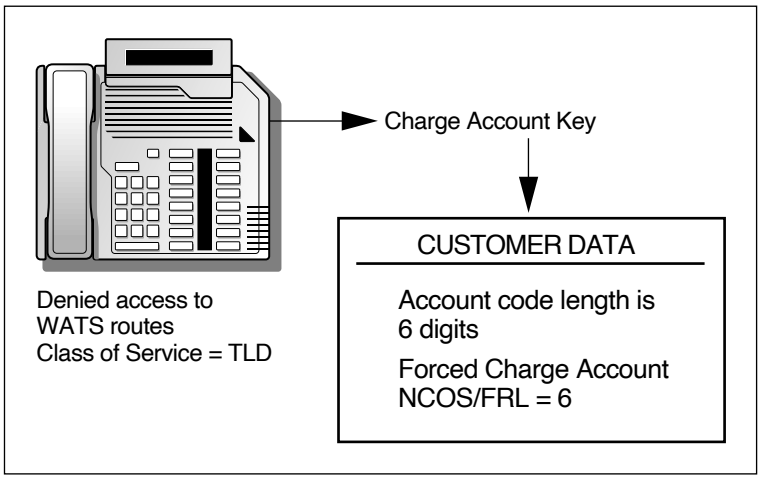
The Forced Charge Account feature temporarily overrides the toll-denied Class of Service Restriction (TLD) provided the user enters an account code before placing a toll call. After the user enters an account code, the Meridian 1 software checks only for a valid account code length—not for valid digits within an account code. Once the Meridian 1 verifies the account code length, the user has an unrestricted Class of Service or the customer-defined Forced Charge Account Network Class of Service (NCOS), or both, for the duration of the call.

The Call Detail Recording (CDR) software outputs a charge record which identifies the charge account used for the call.

Note: You can use the Forced Charge Account feature to override the restrictions imposed through the Least Cost Routing software.

Example

The following illustration is an example of how Forced Charge Account works.



G100450

Example, cont'd

In this example, the following takes place:

- User goes off-hook to obtain a dial tone.
- User presses Charge Account key.
- User dials six-digit account code.
- Account code record is generated in CDR.
- User receives a dial tone and dials a number in the normal manner.
- Set becomes UNR (unrestricted) for this one call.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Forced Charge Account feature.

For	Implement using	Print using
Customer	LD 15—CHLN, FCAF, CHMN, FCNC	LD 21 by CUST, by CDR from Release 19 and up
Stations	LD 10/11—TLD, FCAR	LD 10, 11 by TN from Release 19 and up LD 20 by TN
TIE trunks	LD 14—TLD, FCAR	LD 20 by TN

Controlled Class of Service

Introduction

You can use Controlled Class of Service to lower calling privileges of sets in unsecured areas and still raise their calling privileges when required. This feature is particularly effective in preventing internal abuse.

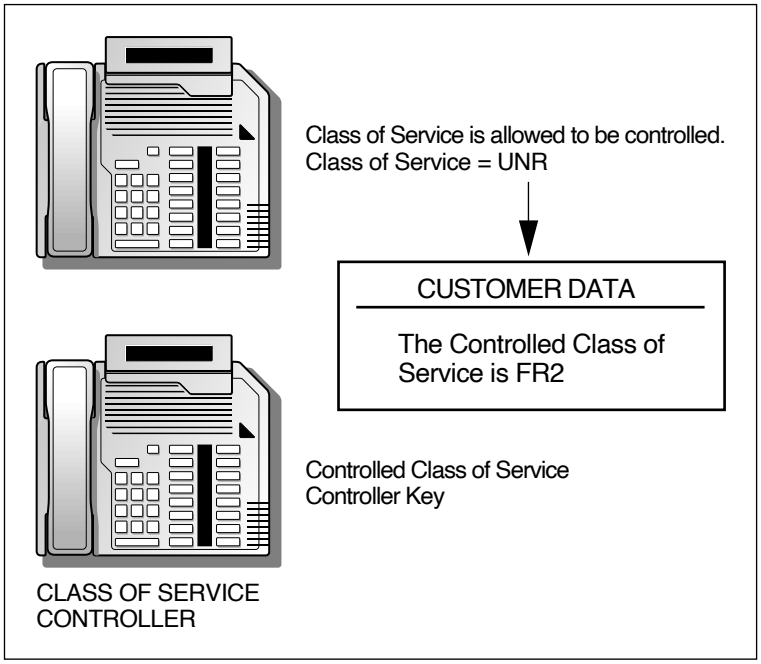
How it works

The Controlled Class of Service (CCOS) feature allows users of SL-1 and Meridian digital sets designated as controllers, and users of TTYs designated as background terminals, to temporarily alter a designated station's Class of Service assignments (CLS). When a station is in the controlled mode, its CLS is derived from the Controlled Class of Service restriction level defined for each customer.

Users of SL-1 and Meridian digital sets designated as controllers can place stations in a controlled mode one at a time whereas background terminals can alter individual, group, or all designated stations at one time.

Example

The following illustration is an example of how the Controlled Class of Service feature works.



G100451

In this example, the controller does the following:

- presses the Controller key
- dials the directory number of the set to be controlled
- presses the Controller key.

  The set is now an FR2 Class of Service

To return that set to the UNR Class of Service, the controller presses the Controller key, dials the DN for the set, and presses the Controller key again. The set will be reset to a UNR Class of Service.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Controlled Class of Service feature.

For	Implement using	Print using
Customers	LD 15—CCRS	LD 21 by CUST or by CCOS
Stations to be controlled	LD 10/11—CLS	LD 10, 11 by TN from Release 19 and up LD 20 by TN
Stations to be controllers	LD 11—KEY	LD 20 by TN LD 81 CCOS Key
Background terminals	LD 17—ADAN, USER	LD 22 by CFN, ADAN from Release 19 and up

Enhanced Controlled Class of Service

Introduction

This enhancement expands the Controlled Class of Service feature to further control calling privileges of stations in unsecured areas. Enhanced Controlled Class of Service (ECCS) extends the controller function of Controlled Class of Service (CCOS) to attendant consoles and the M3000 sets equipped with a Controller key. In addition, this enhancement allows for two more customer-defined levels of CCOS restriction.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Enhanced Controlled Class of Service feature.

For	Implement using	Print using
Customers	LD 15—CCRS, ECC1, ECC2	LD 21 by CUST or by CCOS from Release 19 and up
Stations to be controlled	LD 10/11—CLS	LD 10, 11 by TN from Release 19 and up LD 20 by TN
Stations to be controllers	LD 11—KEY	LD 11 by TN from Release 19 and up LD 20 by TN LD 81 CCOS Key
Attendants to be controllers	LD 12—KEY	LD 20 by TN LD 81 CCOS key
Background terminals	LD 17—USER	LD 22 by CFN, by ADAN from Release 19 and up

Flexible Feature Codes—Electronic Lock

Introduction

Electronic Lock (ELK) allows selected users to activate and deactivate the Controlled Class of Service (CCOS) mode from their stations by entering the Station Control Password (SCPW) and the appropriate Electronic Lock code.

Station users can activate the Electronic Lock feature to prevent unauthorized calls from their sets when they are not able to control physical access. The feature is used typically in the evenings or on weekends.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Electronic Lock feature.

For	Implement using	Print using
Customers	LD 15-CCRS, SCPL	LD 21 by CUST or by CCOS from Release 19 and up
Flexible Feature code	LD 57—FFCT, CODE, ELKA, ELKD	LD 57
Stations	LD 10/11—SCPW, CLS	LD 10/11 by TN from Release 19 and up LD 20 by TN

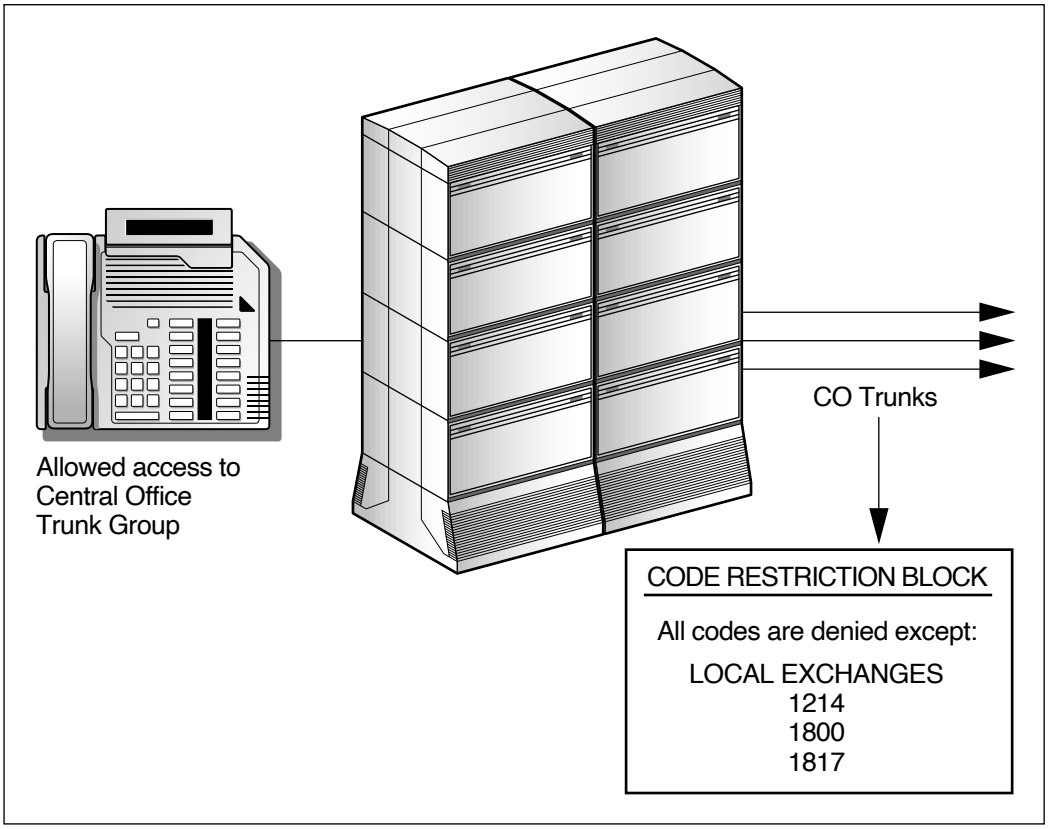
Code Restriction

Introduction

The Code Restriction feature allows toll-denied stations, TIE trunks, DISA DNs, and authorization codes limited access to the toll-exchange network—that is, to CO and FX trunks. For each CO and FX trunk group, you can build a code restriction block that specifies the allowed area codes and exchange codes for toll-denied users accessing those facilities.

Example

The following illustration is an example of how the Code Restriction feature works.



G100452

Example (cont'd)

In this example, the following takes place:

- The user goes off-hook and dials the access code for CO trunks followed by 1-800-555-0110.
- The station is TLD and not normally allowed to dial 1+, but a code restriction is in effect.
- Meridian 1 checks the Code Restriction Table for CO trunks and finds that 1-800 is allowed.
- The call is completed.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the Code Restriction feature.

For	Implement using	Print using
Code Restriction	LD 19 all prompts	LD 21 by CRB
Stations	LD 10/11—CLS=TLD	LD 10/11 by TN from Release 19 and up LD 20 by TN LD 81 by TLD

New Flexible Code Restriction

Introduction

To extend the calling privileges normally associated with toll-denied Class of Service, New Flexible Code Restriction allows you to partition toll-denied users into groups. Each toll-denied group can have unique calling privileges. New Flexible Code Restriction (NFCR) enhances Code Restriction by letting you selectively allow or deny toll-denied stations, TIE trunks, DISA DNs, and authorization codes to make certain calls on outgoing trunk routes. With New Flexible Code Restriction, the Meridian 1 determines whether the toll-denied user can make a call on a specific trunk route by checking the specific digit sequence dialed, the number of digits dialed, or both.

How it works

You can assign toll-denied users to a Network Class of Service (NCOS) and allow or deny calling privileges according to the Facility Restriction Level (FRL) of the NCOS. Toll-denied stations, TIE trunks, and authorization codes can be assigned from 1 to 100 possible NCOS groups. Each NCOS group can be assigned to one of eight possible FRLs.

When the toll-denied user accesses an outgoing route, the Meridian 1 compares the FRL of the user's NCOS to a table that defines the calling privileges associated with that trunk group.

Implementing and auditing the feature

Use the following table to determine which overlay programs and prompts should be used for implementing or auditing the New Flexible Code Restriction feature.

For	Implement using	Print using
Customer	LD 15—NFCR, MAXT	LD 21 by CUST or by ESN from Release 19 and up
Network control	LD 87—NCOS, FRL	LD 87 by NCOS
New Flexible Code Restriction block	LD 49-FCR for all prompts	LD 49 FCR
Route	LD 16—FRL	LD 21 RDB
Station	LD 10/11—NCOS, CLS=TLD	LD 10, 11 by TN from Release 19 and up LD 20 by TN LD 81 by COS, NCOS
DISA	LD 24—NCOS	LD 24 by DISA DN

Section D: Controlling remote access to calling privilege

In this section

Overview	6-40
Call Forward All Calls	6-41
Call Forward External Deny	6-42
Call Forward to Trunk Access Code—DID Calls	6-43
Internal Call Forward	6-44
Flexible Feature Codes—Remote Call Forward	6-45
User Selectable Call Redirection	6-46

Overview

Introduction

Two of the most commonly abused features are Call Forward All Calls and Direct Inward System Access (DISA).

Call Forward

Call Forward is a convenient feature that allows users who are going to be away from their desks to forward their calls to another set or location.

Call Forward All Calls

The Call Forward All Calls feature is assigned on a per station basis and designates the maximum number of digits to which a user may call forward. DISA allows users in remote locations to place calls through your corporate PBX.

Types of abuse

Station users have abused Call Forwarding by forwarding their sets to either a long-distance telephone number or to a trunk access code, then going offsite, and making a call to their sets. With the introduction of Remote Call Forward, non-users can abuse Call Forward if proper controls are not in place.

In this section

This section describes additional controls you can use with the Call Forward features to stem abuse and unauthorized calls.

Call Forward All Calls

Description

Call Forward (CFW) allows users to forward all calls manually to another number either internal or external to the system. The ability to forward a phone outside the system depends not only on the number of digits assigned to the call forward feature, but on the assignment of the feature Call Forward External Allow, also assigned on a phone-by-phone basis.

What you should look for

The default for CFW is 16, adequate for many international calls. Ensure this feature is restricted to the minimum in all cases (usually four—the standard number of digits in an extension). Be aware of the combinations of external forwarding and long digit strings allowed. Permit only where absolutely necessary.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Call Forward All Calls feature.

For	Implement using	Print using
Stations	LD10, 11—CFW	LD 10, 11 by TN from Release 19 and up LD 20 by TN LD 81 by CFW

Call Forward External Deny

Description

This feature provides the option to restrict, on a set-by-set basis, the ability to call forward all calls to an external directory number (DN).

With Release 19, the default value for Call Forward External becomes “deny.”

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Call Forward External Deny feature.

For	Implement using	Print using
Stations	LD 10, 11—CLS	LD 10, 11 by TN from Release 19 and up LD 20 by TN LD 81 by CFXA, CFXD

Call Forward to Trunk Access Code—DID Calls

Description

You may not want your users to call forward their stations to an access code. After all, an unrestricted station forwarding to the central office trunk (COT) access code puts a whole world of calling capabilities at the caller's fingertips. Call Forward to Trunk Access Code provides you with the option to restrict, on a customer-by-customer basis, the ability to call forward direct in dial (DID) calls to a trunk access code.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Call Forward to Trunk Access—DID calls feature.

For	Implement using	Print using
Customer	LD 15—CFTA	LD 21 by customer

Internal Call Forward

Description

Internal Call Forward (ICF) is available for systems using X11 software Release 19 and up. ICF directs all internal calls to a specified location different from the call forward destination of external calls. An internal call is considered an extension-to-extension call, Direct Inward System Access (DISA) call, Group Call, a call over a trunk route designated as internal, an incoming trunk call using private numbering, or an attendant-originated call. The default for this feature is 4 digits but can be defined for up to 23 digits.

How to use ICF

Ensure that Call Forward to Trunk Access Codes is set to “no” in the customer Data Block and that Call Forward External is denied. A combination of these features in the “allow” state would permit users to call forward their phones to BARS/NARS access codes or trunk access codes, and receive a second dial tone when looping through private networks or entering the system through DISA.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Internal Call Forward feature.

For	Implement using	Print using
Customer	LD 15—CFTA	LD 21 by customer
Stations	LD 10—FTR, ICF	LD 10, 11 by TN from Release 19 and up LD 20 by TN LD 81 by ICF
Flexible Feature Codes	LD 57—ICFA, ICFD, ICFV	LD 57 by CODE

Flexible Feature Codes—Remote Call Forward

Description

The Remote Call Forward feature (RCFW) allows a user to activate and deactivate the Call Forward All Calls feature from a remote station.

How RCFW works

Users enter codes to activate and deactivate the feature, and must also enter a station-specific password. You can selectively provide this capability to users as job functions require. The user can also activate this feature from an offsite location by using DISA.

Exercise care in assigning this capability to minimize opportunities for abuse.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Remote Call Forward feature.

For	Implement using	Print using
Customer	LD 15—SCPL	LD 21 by CUST or by CFCO from Release 19 and up
Flexible Feature Code	LD 57—CODE, RCFA, RCFD, RCFV	LD 57 by FFC
Station	LD 10/11—SCPW	LD 21 by TN
DISA	LD 24 by DISA	LD 24 DISA by DN

User Selectable Call Redirection

Introduction

Release 19 introduces the ability to user-select the destination for Forward No Answer, Busy Hunt, External Forward No Answer, and External Hunt. The feature is controlled by Flexible Feature Code, Special Prefix Code, or a User key on a multiline phone.

This feature requires a Station Control Password.

Ensure that the SCPW is unique for each phone with the feature allowed.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the User Selectable Call Redirection feature.

For	Implement using	Print using
LD 10/11 SETS	LD 10 SCPW, CLS, USRA	LD 10, 11 by TN, DN from Release 19 and up LD 20 by TN LD 20 by DN
LD 15 CDB	LD 15 SPCL, FFCS	LD 21 by CUST, by CFW from Release 19 and up
LD 57 FFC	LD 57 USCR	LD 57 by CODE LD 81 by CODE

Section E: Controlling access through Least Cost Routing (BARS/NARS)

In this section

Overview	6-48
Supplemental Digit Recognition	6-50
Supplemental Digit Restriction	6-52
Network Class of Service—Facility Restriction Level	6-55
Network Speed Call	6-58
Network Authorization Code	6-60
Authorization Code Conditionally Last	6-61
Time-of-Day Routing	6-64
Routing Control	6-67
Incoming Trunk Group Exclusion	6-70

Overview

Introduction

Basic Alternate Routing System (BARS) and Network Alternate Routing System (NARS) software allows you to route outgoing calls over the least expensive facility available at the time the user places the call. You can use the BARS/NARS feature to prevent calls to a specific area code or exchange, or to international locations.

How BARS and NARS work

When the user dials an access code followed by the desired number, the software processes and routes the call. Based on the number the user dials, the Meridian 1 system reads a digit translation table. The translation determines which list of alternate routes the system will use to process the call. This list is called a route list index and contains alternate outgoing routes (trunk groups) for call completion.

Because the majority of toll-fraud calls terminate in the 809 area code and in international locations such as Egypt, Pakistan, and Columbia, consider not defining these codes in your translation tables if your business does not require that users call these locations. If your corporate culture requires calls to destinations associated with fraud, you should consider assigning unique route list indexes to each of these destinations. Such a scheme provides the capability to assess normal call volumes and detect variations.

Assessment tools

Statistics are available to indicate the number of calls placed through each route list index. It is TFN001.

Available features

The following features are elements of BARS/NARS which allow you flexibility in restricting calling privileges:

- Supplemental Digit Recognition
- Supplemental Digit Restriction
- Network Class of Service—Facility Restriction Level
- Network Speed Call
- Network Authorization Code
- Authorization Code Conditionally Last

Available features (cont'd)

- Time-of-Day Routing
- Routing Control
- Incoming Trunk Group (TIE) Exclusion

BARS/NARS features to control access privileges

The following table lists the features you should consider implementing depending on the requirements of your business.

If your business requirement is to	Then we recommend you
totally deny an area code or a local exchange	do not define them in the translation table. Calls to those numbers attempted through BARS/NARS are blocked.
deny all access to certain country codes, or exchanges within an area code	use the Supplemental Digit Restriction feature or Translation Data Block. For more information, see "Supplemental Digit Restriction" on page 6-52.
inhibit the use of certain trunk groups	use the Network Class of Service (NCOS) Facility Restriction Level (FRL) and also (optionally) Trunk Group Access Restriction (TGAR) feature. For more information, see "Network Class of Service—Facility Restriction Level" on page 6-55 and "Trunk Group Access Restrictions" on page 6-11.
deny access to certain trunk groups or destinations at a specific time	use the Time-of-Day Routing feature. For more information, see "Time-of-Day Routing" on page 6-64.
deny access to certain destinations after business hours, on weekends and holidays, or at other selected times.	use the Routing Control feature. For more information, see "Routing Control" on page 6-67.
deny calls to certain dialing sequences when those calls originate on TIE trunks	use the Incoming Trunk Group Exclusion. For more information, see "Incoming Trunk Group Exclusion" on page 6-70.

Supplemental Digit Recognition

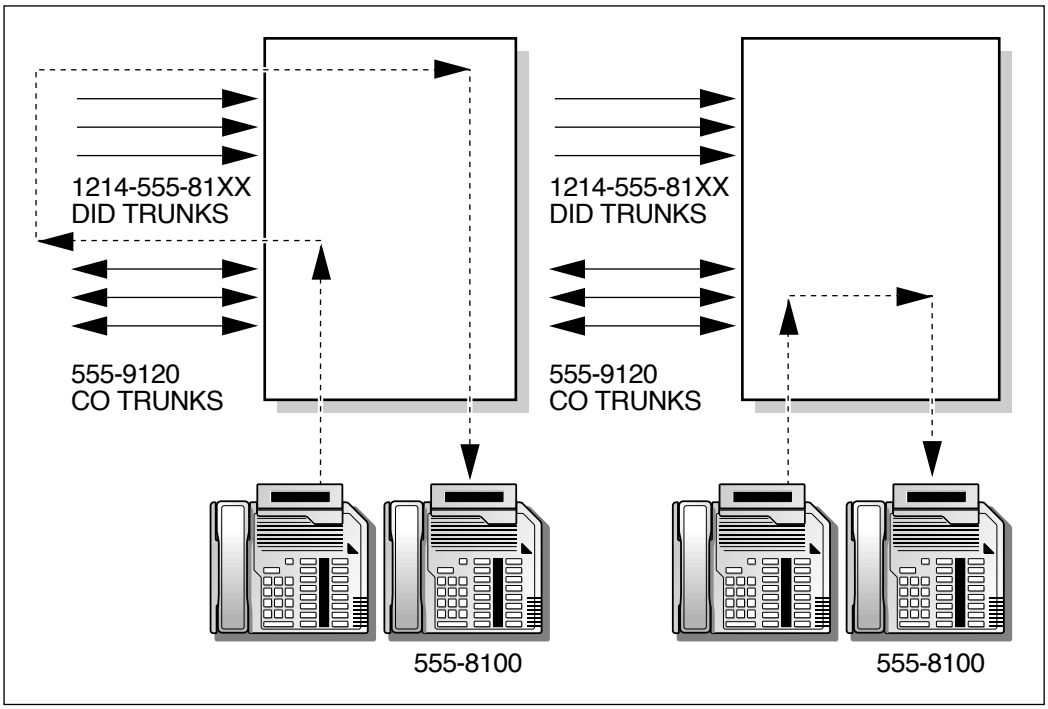
Description

One type of internal abuse or misuse occurs when callers use incoming TIE trunks. Callers on TIE trunks sometimes dial the BARS/NARS access code followed by the whole telephone number of an internal station.

When using Supplemental Digit Recognition, the Meridian 1 “recognizes” dialing sequences associated with internal calls, and thus prevents callers from using two trunks to complete an internal call.

Example

The following figure illustrates how the Supplemental Digit Recognition feature works.



G100453

Example (cont'd)

In this example, the following takes place:

- User A dials 9-555-8100.

  Meridian 1 is not programmed to recognize 555-8100 as an internal number.

  The call is routed out over a CO trunk group and is returned to the Meridian through the DID trunk group. An internal call now requires two trunks to be complete.
- User B dials 9-555-8100.

  Meridian 1 is programmed to recognize 555-8100 as an internal number and deletes 555. Meridian 1 dials 8100. The call is completed internally.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Supplemental Digit Recognition feature.

For	Implement using	Print using
ESN	LD 86—MXSD	LD 86 by FEAT=ESN
Network translation	LD 90—DENY, LDID, LDDD	LD 90 by NPA, NXX, or SPN

Supplemental Digit Restriction

Description

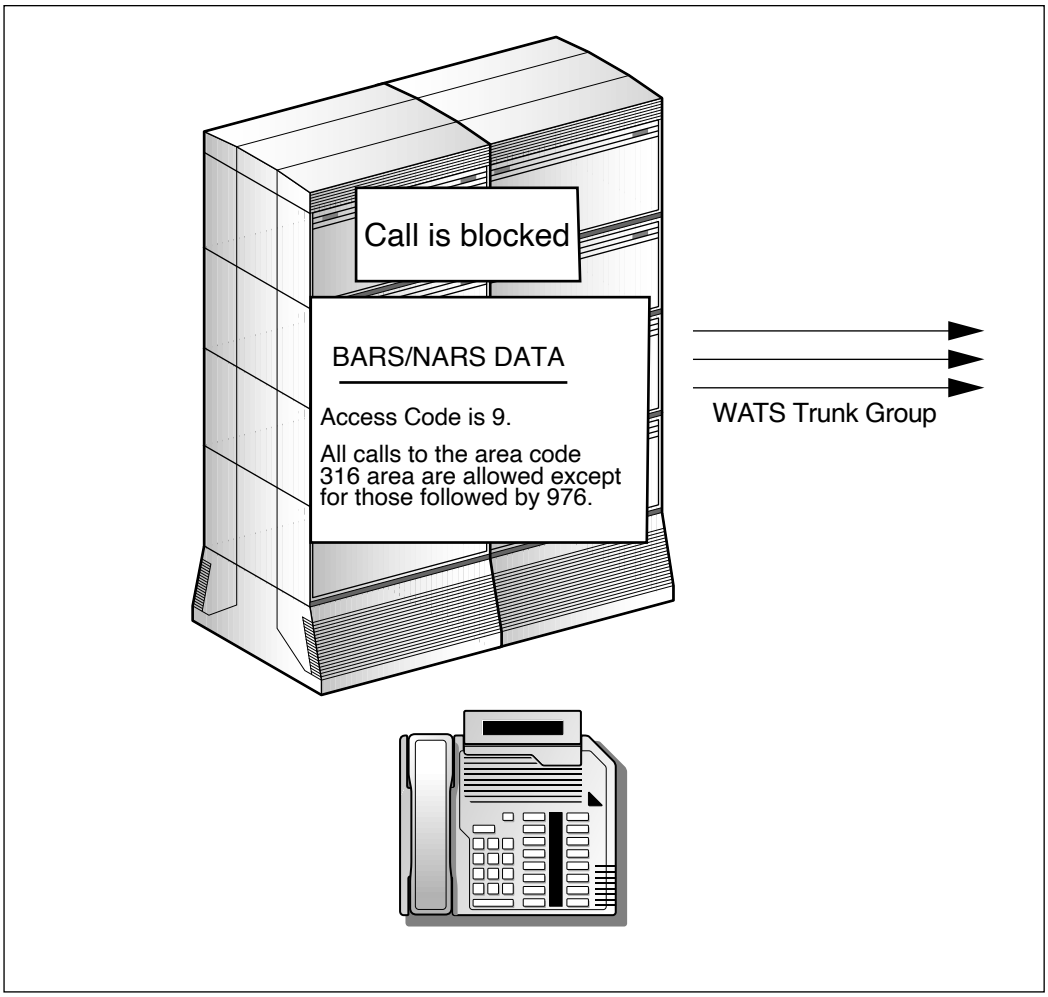
Because most toll-fraud calls are placed to international locations, you can use Supplemental Digit Restriction (SDR) to block calls to international locations that your users do not need to call.

How SDR works

Supplemental Digit Restriction enables you to block calls to certain telephone numbers within exchanges, area codes, or country codes. For example, you may have legitimate international calling requirements to many countries but none to those countries typically associated with fraud. Supplemental Digit Restriction lets you block calls to those countries.

Example

The following figure illustrates how the Supplemental Digit Restriction feature works.



G100454

In this example, the following takes place:

- The user dials 9-1-316-976-9090.
- The 9 triggers the Meridian 1 to use BARS/NARS data.
- Meridian 1 checks the Translation Table for 1316 and finds that 1316, followed by 976, is blocked.
- The call is blocked.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Supplemental Digit Restriction feature.

For	Implement using	Print using
ESN	LD 86—MXSD	LD 86 by FEAT=ESN
Network translation	LD 90—DENY, LDID, LDDD	LD 90 by NPA, NXX, or SPN

Network Class of Service—Facility Restriction Level

Description

A Network Class of Service (NCOS) designation is a group of calling privileges you can assign to a station, TIE trunk, DISA DN, or authorization code.

How NCOS works

The Meridian 1 system uses the NCOS to determine caller treatments and eligibility for outgoing calls that use the Least Cost Routing (BARS/NARS) software. By partitioning stations, TIE trunks, DISA DNs, and authorization codes into unique NCOS groups, you can track the normal calling patterns of each group (TFN002). You can then promptly detect variances which can indicate fraudulent activity, and take action.

Within the NCOS, you can assign the user to one of eight Facility Restriction Levels (FRL). The FRL is compared to the minimum FRL requirement assigned to each entry in a route list. The entries in the route list are trunk routes that are able to place calls to the NPA, NXX, or special number. The routes are listed in the order the system searches them when trying to complete an external call. Callers are eligible to complete a call on an entry in the route list when their FRL is equal to, or higher than, the entry's FRL level.

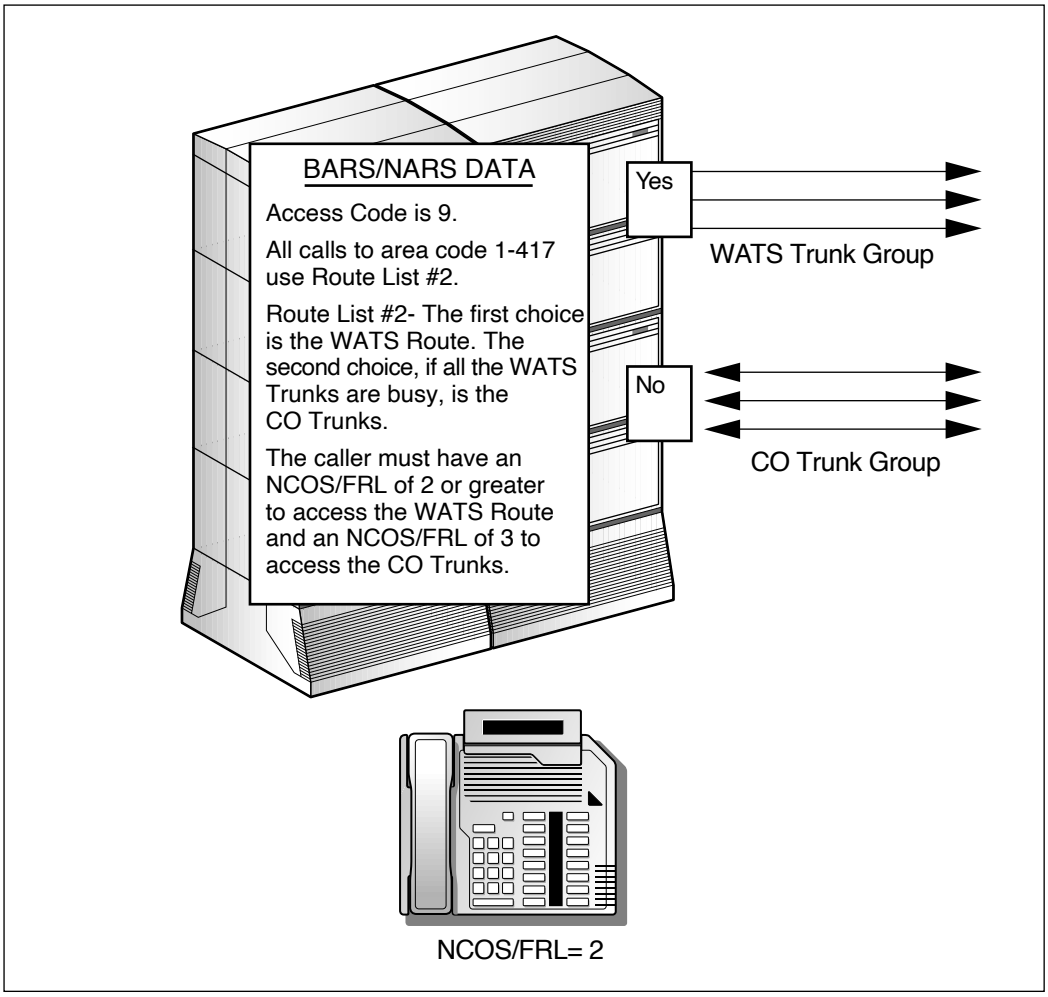
In conjunction with TGAR

The BARS/NARS database can be configured to ignore Trunk Group Access Restrictions (TGAR) or to use them. When TGARs are ignored, the BARS/NARS software assesses the Class of Service and the FRL to determine which call facilities are eligible for a particular call. This configuration allows flexibility in using a given trunk group while forcing users to place calls through BARS/NARS. You can base trunk access for each call on the FRL requirements for the number dialed rather than basing it on the TGAR.

You can also configure the BARS/NARS database to assess TGAR assignments in determining how the system can route a call. In this case, the BARS/NARS software will use the COS, TGAR, and FRL to determine which call facilities are eligible to process a particular call.

Example

The following illustration shows how the NCOS Facility Restriction Level feature works.



G100454

In this example, the following occurs:

- The user dials 9-1-417-555-9090.
- The 9 triggers Meridian 1 to use BARS/NARS data.
- The Meridian 1 searches the Translation Table for 1417.
- Calls to 1417 use Route List Index 2.
- Route List Index 2 is searched for an idle available trunk.

- The first choice is the WATS route.
- The NCOS/FRL assigned to the first choice (2) is compared to the NCOS/FRL (2) of the station.
- The station's NCOS/FRL (2) is equal to, or greater than, the WATS NCOS/FRL (2), so the call is allowed for this choice.
- If all WATS trunks are busy, then the second choice (CO trunks) is checked.
- The NCOS/FRL of the CO trunks (3) is compared to the NCOS/FRL of the station (2).
- The station's NCOS/FRL (2) is lower than the CO trunks' NCOS/FRL (3), so the call cannot be completed over CO trunks.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the NCOS Facility Restriction Level feature.

For	Implement using	Print using
Network control	LD 87—NCTL all prompts	LD 87 FEAT=NCTL by NCOS
Route list index	LD 86—RLB, FRL	LD 86 FEAT=RLB
Authorization code	LD 88—AUT, NCOS	LD 88 TYPE=AUT
Stations	LD 10 and LD 11—NCOS	LD 10, 11 by TN from Release 19 and up LD 20 by TN LD 81 by NCOS
Trunk	LD 14—NCOS	LD 20 by TN
Customer	LD 15—NCOS, FCNC	LD 21 by CUST or ESN/CDR from Release 19 and up
System Speed Call list	LD 18—NCOS	LD 20 by SCL
DISA	LD 24—NCOS	LD 24 by DISA DN

Network Speed Call

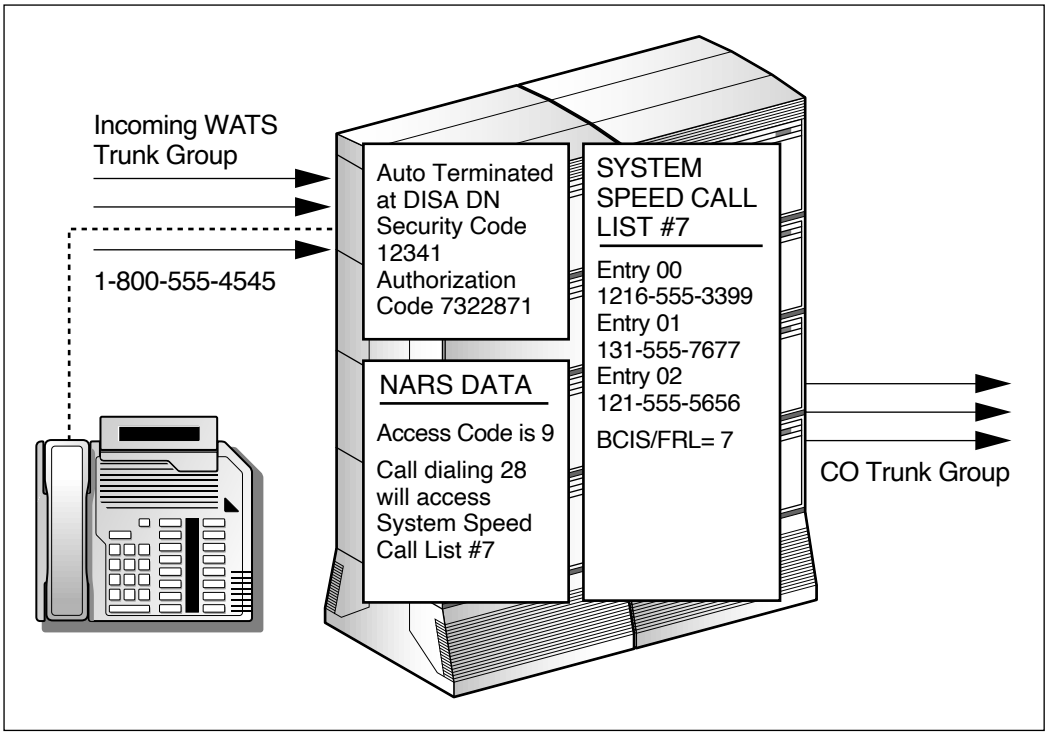
Description

You can enable a user who is normally restricted from making certain types of BARS/NARS calls, to make such a call if the destination is a company-approved number defined in a System Speed Call list. Network Speed Call expands the System Speed Call feature by allowing users to access the System Speed Call feature from the public and private networks.

You can use the Network Speed Call feature in conjunction with a restricted DISA DN. The incoming DISA caller can gain access to approved destinations through the Network Speed Call list.

Example

The following illustration shows how the Network Speed Call feature works.



G100455

Example (cont'd)

In this example, the following occurs:

- The caller dials 1-800-444-4545.
- When dial tone is returned, the user dials 12341.
- When dial tone is returned, the user dials 167322871
- When dial tone is returned, the user dials 9-20-00 to access System Speed Call Number 7.
- 9 triggers the Meridian 1 to use NARS data.
- Meridian 1 checks the Translation Table for 20 and finds 20 to be the Access Code for System Speed Call List 7.
- System Speed Call List is checked for entry 00.
- The call completes to 1-216-555-3399 based on the calling capabilities of NCOS/FRL 7.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Network Speed Call feature.

For	Implement using	Print using
Network translation	LD 90—NSCL all prompts	LD 90 AC1 or AC2, SSCL
System Speed Call	LD 18—SSC all prompts	LD 20 by SCL
Network control	LD 87—NCTL, NSC, LIST	LD 87 by NCOS
Authorization code	LD 88—AUT, NCOS	LD 88 by AUT
Stations	LD 10 and LD 11—NCOS	LD 10, 11 by TN from Release 19 and up LD 20 by TN LD 81 by NCOS
Trunk	LD 14—NCOS	LD 20 by TN
Customer	DL 15—NCOS, FCNC	LD 21 by CUST or ESN/CDR from Release 19 and up
System Speed Call List	LD 18—NCOS	LD 20 by SCL
DISA	LD 24—NCOS	LD 24 by DISA DN

Network Authorization Code

Description

With the Network Authorization Code feature, you can assign up to 20 000 authorization codes of up to 14 digits each, and you have the option of requiring users to enter an authorization code before certain calls can be processed. You may want to use this requirement for certain locations typically associated with unauthorized access like the 809 area code.

Authorization Code Conditionally Last

Introduction

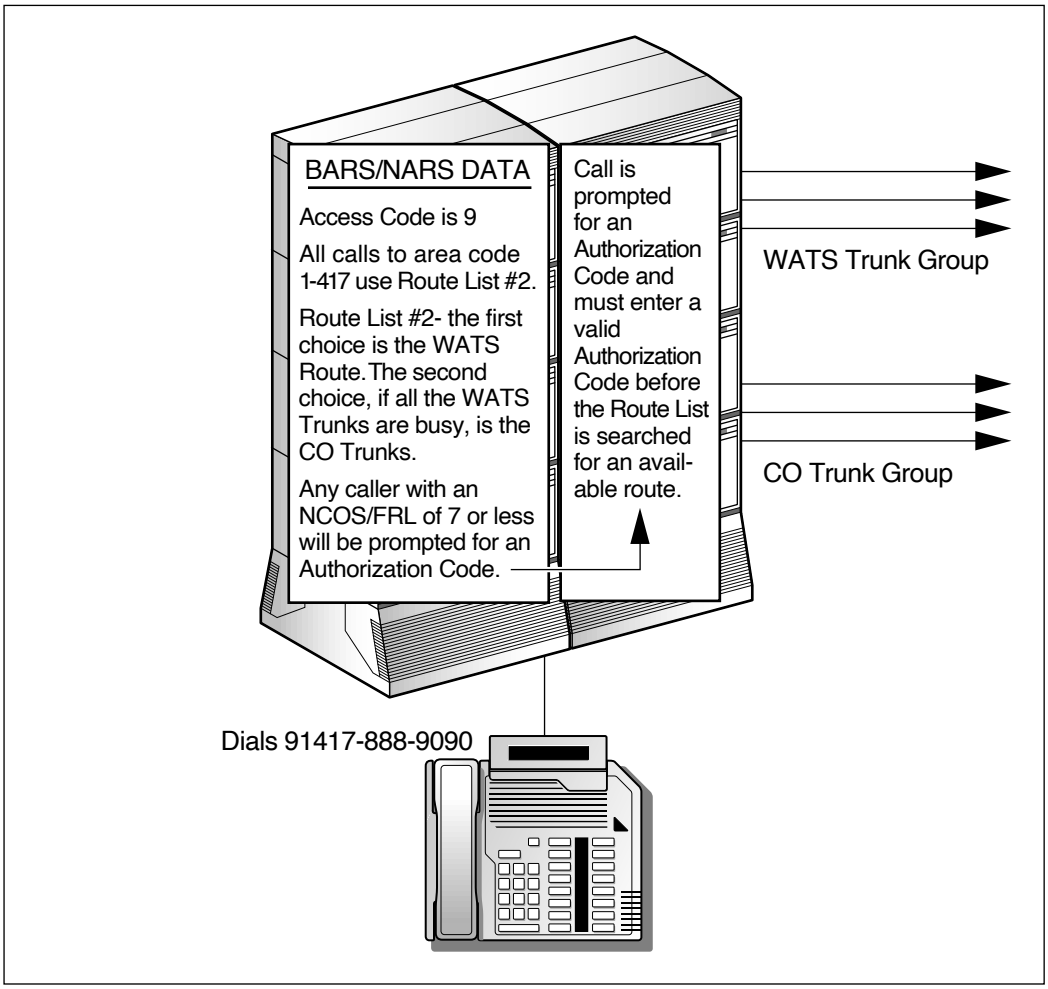
The system can prompt users “conditionally” for an authorization code after they attempt to place a call using the BARS/NARS call processing software. Users who fail to meet the minimum Facility Restriction Level requirement assigned to a route list will hear tones or a recorded announcement indicating that they need to enter an authorization code.

How this feature works

Users must enter a valid authorization code at that point to complete the call. This control provides another level of security by requiring all callers placing calls to international locations or selected area codes, for example, to enter an authorization code.

Example

The following illustration shows how the Authorization Code Conditionally Last feature works.



G100456

In this example, the following takes place:

- The user dials 9-1417-555-3376.
- 9 triggers the Meridian 1 to use the BARS/NARS data.
- The Meridian 1 checks the Translation Table for 1417 and sends calls to Route List Index 2.
- The system checks Route List Index 2 for the minimum NCOS/FRL required; it is found to be 7.

Example (cont'd)

- The NCOS/FRL of 7 is compared to the user's NCOS/FRL, in this case 2.
- Because the user's NCOS/FRL is equal to or lower than the minimum NCOS/FRL for the route list, the user is prompted for an authorization code.
- The user must enter a valid authorization code before the call can be completed. The calling capabilities of the authorization code's NCOS/FRL will determine call eligibility.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Authorization Code Conditionally Last feature.

For	Implement using	Print using
Authorization code	LD 88—all prompts	LD 88 by AUT
Route List Index	LD 86—RLB MFRL	LD 86 by RLB
Network Control	LD 87 —NCTL, NCOS FRL	LD 87 by NCOS
Authorization Code	LD 88—AUT CODE, NCOS	LD 88=AUT
Stations	LD 10 and LD 11—NCOS	LD 10, 11 by TN from Release 19 and up LD 20 by TN LD 81 by NCOS
Trunk	LD 14—NCOS	LD 20 by TN
Customer	LD 15—NCOS, FCNC	LD 21 by CUST or ESN/CDR from Release 19 and up
System Speed Call List	LD 18—NCOS	LD 20 by SCL
DISA	LD 24—NCOS	LD 24 by DISA DN

Time-of-Day Routing

Description

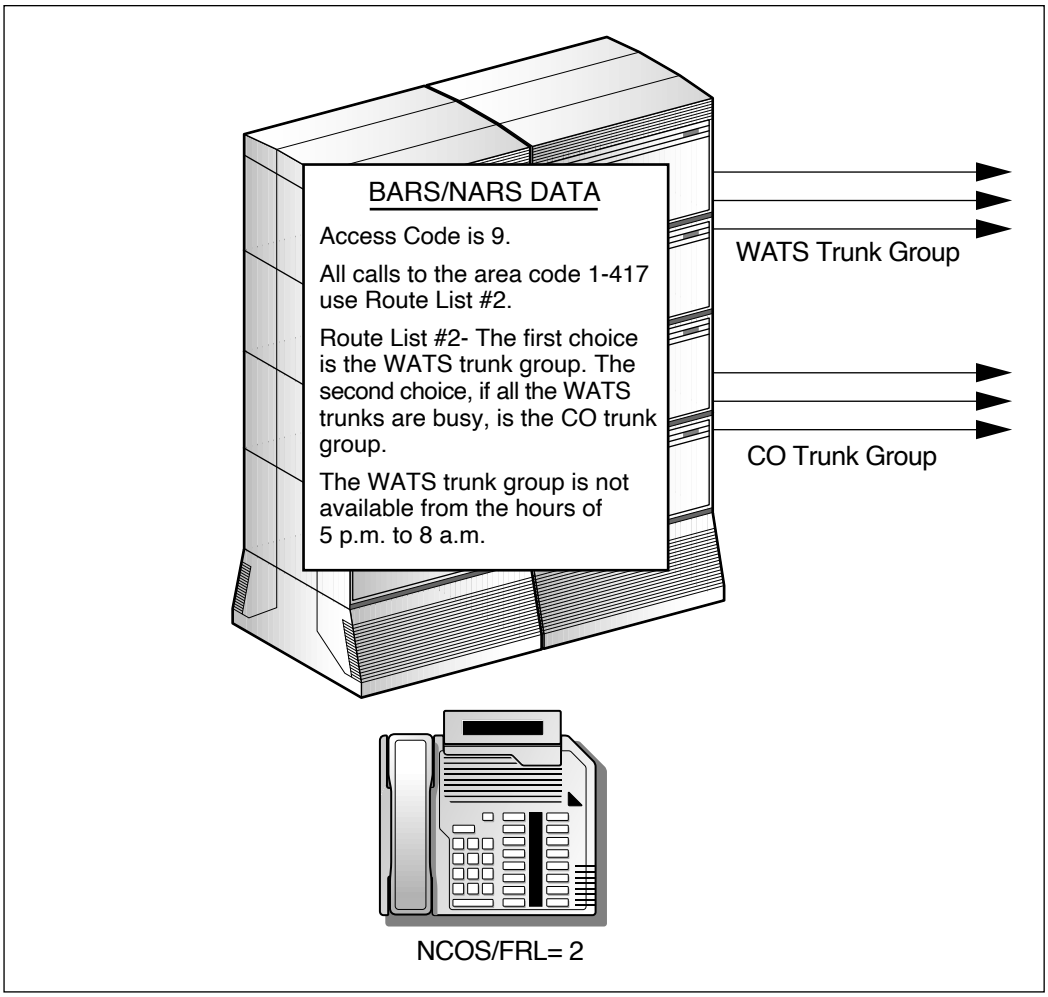
Time-of-day routing allows you to restrict access to certain destinations during specified time frames. For example, because the majority of fraudulent toll calls occur on holidays or after normal business hours, you can use this feature to turn off the route lists supporting calls to international locations or to the 809 area code after hours. Whether you can take this action depends on the needs of your user community.

How this feature works

The Time-of-Day Routing feature specifies the hours that users can access each entry in a route list. BARS/NARS provides for up to eight time-of-day schedules. With this feature you can specify the most cost-effective route alternatives based on the time of day, and restrict employees from calling locations they have no need to call for business purposes at certain hours.

Example

The following illustration shows how the Time-of-Day Routing feature works.



G100457

In the example, the following occurs:

- The user dials 9-1-417-555-9090 at 6:00 p.m.
- 9 triggers the Meridian 1 software to use BARS/NARS data.
- The system checks the Translation Table.
- Calls to 417 use Route List Index 2.

Example (cont'd)

- The system searches Route List Index 2.
- The first choice, a WATS Route, is not available at 6:00 p.m.
- The second choice, CO Trunks, is available, and the call is sent out over the CO trunks.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Time-of-Day Routing feature.

For	Implement using	Print using
ESN	LD 87—ESN TODS	LD 87 by ESN
Route List Index	LD 86—RLB TOD	LD 86 by RLB

Routing Control

Introduction

Again, because the majority of toll fraud and internal abuse occurs after normal business hours, or on weekends or holidays, you may want to program the system to automatically modify users' calling privileges during these times.

Description

The Routing Control feature lets you reduce or raise a user's network access capabilities if necessary.

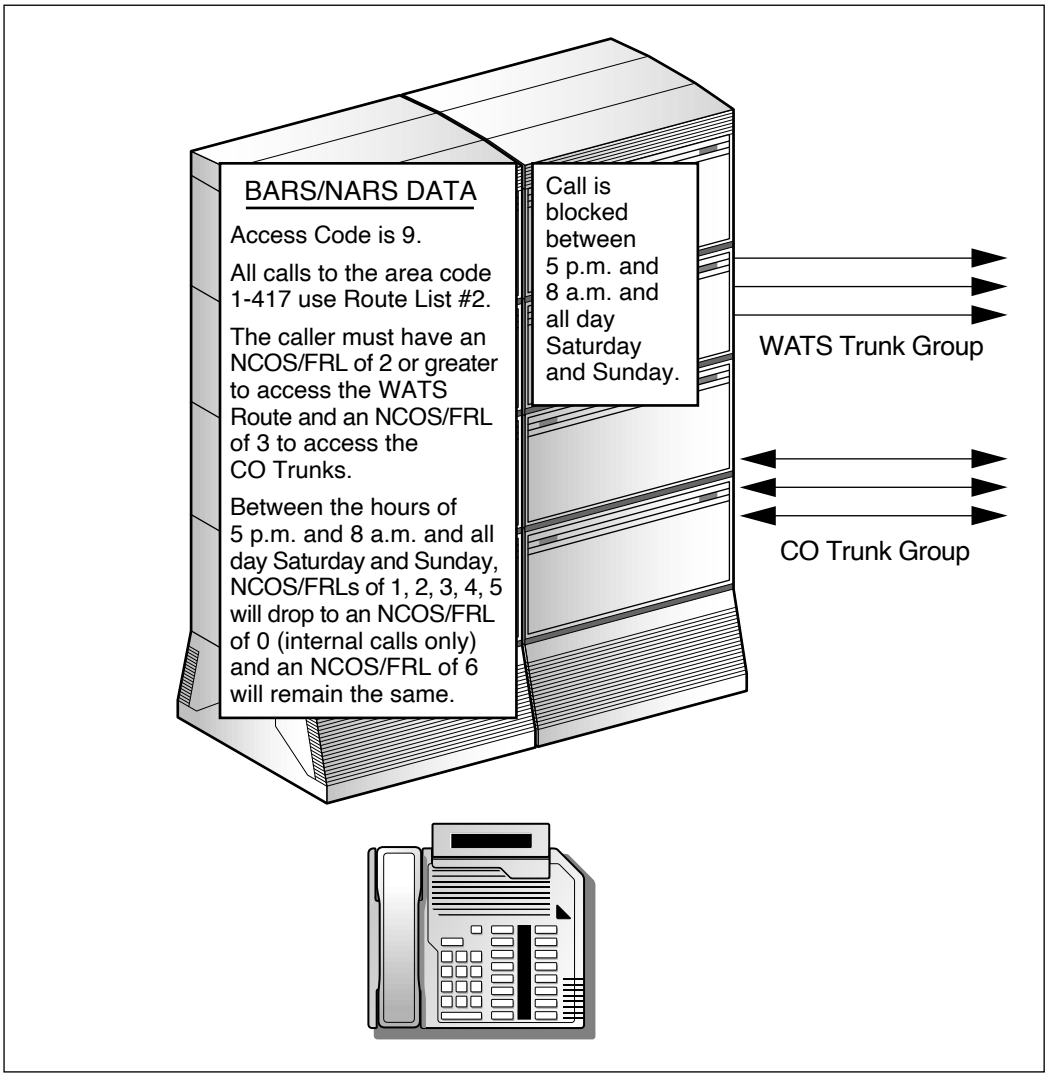
How Routing Control works

Each Network Class of Service (NCOS) is assigned an alternate NCOS when a special time-of-day schedule is in effect or during a specified day of the week. This feature enables you to change calling privileges automatically for a defined time frame each day or on weekends. You can also place a key on the attendant console that will manually activate routing control. With these features, you can implement controls on holidays and in response to critical situations.

Activating this feature prevents people from accessing unattended stations after hours to place unauthorized calls. However, authorization codes are not subject to the alternate NCOS assignments imposed through Routing Control. When users enter a valid authorization code, they are provided with the NCOS assigned to the authorization code for the duration of the call.

Example

The following illustration shows how the Routing Control feature works.



G100458

In this example, the following takes place:

- The user dials 9-1-417-555-4436 at 9:00 p.m.
- 9 triggers the Meridian 1 to use BARS/NARS data.

Example (cont'd)

- Between 5:00 p.m. and 8:00 a.m., all users with an NCOS/FRL of 2 drop to an NCOS/FRL of 0.
- Meridian 1 checks the Translation Table for 1417 and sends the call to Route List Index 2.
- A user must have an NCOS/FRL of 2 to access the WATS routes (first choice) and an NCOS/FRL of 3 to access the CO trunk group (second choice).
- Because it is between 5:00 p.m. and 8:00 a.m., the user's NCOS/FRL is 0.
- This call is not eligible for any route in the Route List Index.
- The call is blocked.

Implementing and auditing the feature

Use the following table to determine which overlay and prompts should be used to implement or audit the Time-of-Day Routing feature.

For	Implement using	Print using
ESN	LD 87—ESN, TODS 7, RTCL, NMAP ETOD	LD 87 ESN
Attendant	LD 12—KEY	LD 20 by TN
Network Control	LD 87—NCTL NCOS	LD 87 by NCOS
Stations	LD 10 and LD 11—NCOS	LD 10, 11 by TN from Release 19 and up LD 20 by TN LD 81 by NCOS
Trunk	LD 14—NCOS	LD 20 by TN
Customer	LD 15—NCOS, FCNC	LD 21 by CUST or ESN/CDR from Release 19 and up
System Speed Call List	LD 18—NCOS	LD 20 by Speed Call List
DISA	LD 24—NCOS	LD 24 by DISA DN

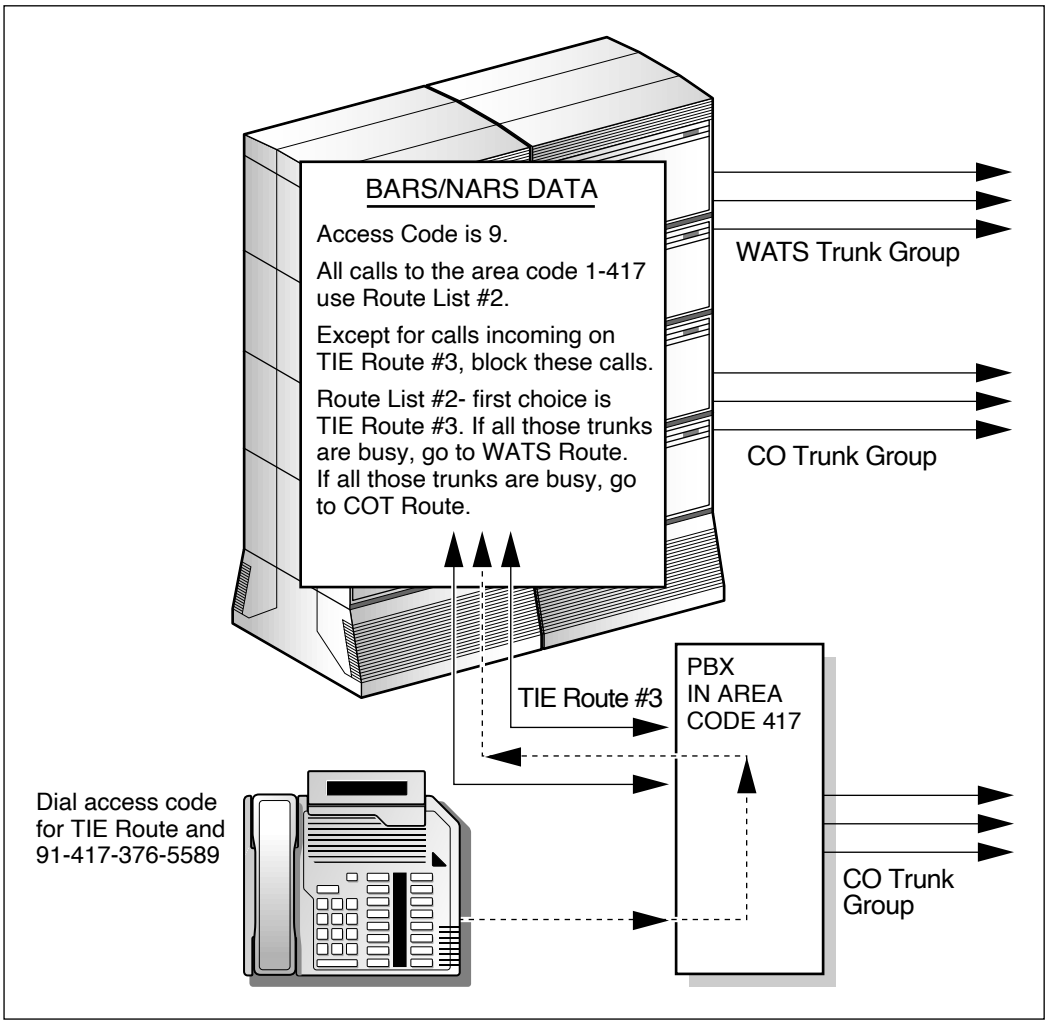
Incoming Trunk Group Exclusion

Description

You may want to control calls originating on various TIE routes. The Incoming Trunk Group Exclusion feature blocks BARS/NARS calls originating on TIE trunks from reaching destinations that employees do not need to reach for business purposes, and keeps users from attempting to circumvent the restrictions that are imposed at their home PBX. Each TIE route is associated with a table that defines the dialing sequences allowed for calls originated on that TIE route.

Example

The following figure illustrates how the Incoming Trunk Group (TIE) Exclusion feature works.



G100459

In this figure, the following occurs:

- The user dials the access code for the TIE route and 9-1-417-555-5589.
- 9 triggers Meridian 1 to use BARS/NARS data.
- BARS/NARS checks the Translation Table for the 417 area code and finds it restricted for calls from TIE Route 3.

Example (cont'd)

- Meridian 1 validates that the call is incoming on TIE Route 3.
- The call is blocked.

Implementing and auditing the feature

Use the following table to determine which overlay and prompts should be used to implement or audit the Incoming Trunk Group Exclusion feature.

For	Implement using	Print using
ESN	LD 87—FEAT=ESN MXSD, MXIX	LD 87 FEAT=ESN
Incoming Trunk Group Exclusion	LD 86—FEAT=ITGE all prompts	LD 86 FEAT=ITGE by Incoming Trunk Group Exclusion Index
Network Translation	LD 90—FEAT=NET ITED, ITEI	LD 90 FEAT=NET by NPA or NXX or SPN

Section F: Controlling access to PBX administration programs

In this section

Overview	6-74
Password control	6-75
Limited access to overlays	6-77
Limited access password—user name	6-78
Single Terminal Access	6-79
Multi-user login	6-80
Input/Output port recovery	6-81
History file	6-82

Overview

Introduction

You can use the following to control access to PBX administration programs:

- Password control
  - Level 1 password
  - Level 2 password

  For more information, see “Password control” on page 6-75.
- Limited access to overlays

  For more information, see “Limited access to overlays” on page 6-77.
- Limited access password—user name

  For more information, see “Limited access password—user name” on page 6-78.
- Single Terminal Access (STA)

  For more information, see “Single Terminal Access” on page 6-79.
- Multi-user login

  For more information, see “Multi-user login” on page 6-80.
- Input/Output port recovery

  For more information, see “Input/Output port recovery” on page 6-81.
- History file

  For more information, see “History file” on page 6-82.

Password control

Introduction

Hackers have been known to access a system to obtain printouts of valid authorization codes, reassign control characteristics, defeat security measures in place, or degrade system performance. By controlling system passwords, you can minimize unauthorized access to the system. You can define a number of passwords that administrators can use to access the system for the purpose of the database.

Two types of passwords

As of X11 Release 16, two types of passwords allow access to all aspects of the database and maintenance programs:

- Level 1 password
- Level 2 password

Level 1 password

You can use the Level 1 password to log on to the switch. Upon entering the valid password, you can change virtually all aspects of the database with the exception of changing the Level 1 and 2 passwords and, if defined, the secure data password associated with assigning authorization codes and DISA parameters.

Implementing and auditing the Level 1 password

Use the following table to determine which overlays and prompts should be used to implement or audit the Level 1 password.

For	Implement using	Print using
Configuration	LD 17—PWD2, NPW1	LD 22 by PWD

Level 2 password

The Level 2 password provides all the capabilities of the Level 1 password, and also allows you to change the Level 1 and Level 2 passwords as well as the secure data password.

Implementing and auditing the Level 2 password

Use the following table to determine which overlays and prompts should be used to implement or audit the Level 2 password.

For	Implement using	Print using
Configuration	LD 17—PWD2, NPW1	LD 22 by PWD

Limited access to overlays

Description

The Limited Access to Overlays (LAPW) feature introduced in X11 Release 16 provides a greater degree of control of password assignment and overlay access. In addition, it expands tracking of switch access.

This feature provides additional security by allowing you to define up to 100 LAPW passwords per system. The LAPW password may be 4 to 16 alphanumeric characters in both uppercase and lowercase. A maximum of four characters are allowed in either Password 1 or Password 2.

How LAPW works

You can define access to specific overlays for each password and specify a “Print-only” capability. You can also configure an audit trail to record the date, time, and password used, and the overlay programs accessed.

The system monitors failed logon attempts, compares the number with a predefined threshold, and locks the entry port if the threshold is exceeded. The Meridian 1 reports lock-out conditions on all TTYs and provides a special report to the next administrator who logs on.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Limited Access to Overlays feature.

For	Implement using	Print using
Configuration	LD 17—LAPW, PWNN, OVLY, CUST, TEN, OPT, LPWED, NLPW, FLTH, LOCK, AUDT, SIZE, INIT	LD 22 by CFN or LAPW from Release 19 and up

Limited access password—user name

Introduction

In addition to Level 1 and Level 2 passwords and the 100 limited access passwords, Release 19 can also require users to enter a user name with up to eight alphanumeric characters. Only the Level 2 password can configure user names, and change and print all passwords.

LAPW users may change their own passwords but not their user names.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Limited Access Password feature.

For	Implement using	Print using
CFN	LD 17—LNAME_OPTION, LOGIN_NAME	LD 22 TYPE CFN, AUDT from Release 19 and up

Single Terminal Access

Description

The Single Terminal Access feature (STA) introduced in Release 19 provides an integrated solution to reduce the number of physical devices needed to administer and maintain a Meridian 1 system and its associated subsystems.

How STA works

A mechanism for ensuring the terminal of the original session when the user intends to switch to another system is provided in the STA application through a user-determined logout sequence. Specified in the database with each STA port, this sequence will automatically be sent to the destination system by the application to prevent users from leaving a session open in the background without logging out. If the logout sequence is not programmed or programmed incorrectly, the user could leave a program open in the background and subject to unauthorized access.

The STA master terminal will use the configured logout sequence to automatically exit from the active and existing background sessions when the modem connection for the terminal experiences carrier dropout.

A password is required before the user can new or change the configuration of STA ports. This process is designed to protect the STA port from unauthorized alteration.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Single Terminal Access feature.

For	Implement using	Print using
Configuration record	LD 17—ADAN, TTY, CTYP, GRP, DNUM, PORT, DES, BPS, PRTY, STOP, BITL, PARM, FUNC, USER, MPRT, APRT	LD 22 by CFN, or ADAN from Release 19 and up

Multi-user login

Description

Multi-user login allows up to three users to simultaneously log in to a Meridian 1 PBX to load and execute overlays. A fourth overlay running in the background or at midnight is also allowed.

The feature is activated and deactivated in Overlay 17.

Release 19 support

Release 19 supports only Set Administration (Overlays 10 and 11), associated print loads (Overlays 20, 21, and 22), Maintenance, Midnight Routines, Background Routines, or Attendant Administration.

Forced logoff

Additionally, a user can force the logoff from a specific terminal when logged in to the Level Password or an appropriate Limited Access Password.

Monitoring input/ output

The monitor command allows a logged in user to monitor the input/output of a different specified terminal either locally or remotely; this feature is assigned on a per password level or to the Level 2 password.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the Multi-user Login feature.

For	Implement using	Print using
CFN	LD 17—PWD2, LAPW, TLOG, SIZE, MULTI-USER, OPT	LD 22 PRT by CFN or LAPW from Release 19 and up

Input/Output port recovery

Introduction

Ports defined as TTY and PRT are controlled by two counters monitoring invalid characters. Ports disabled due to garbage characters or interference can be automatically enabled after a four-minute timer has expired.

Disabled ports can be enabled a maximum of three times in 30 minutes. The fourth time a port is disabled in a 30-minute period requires manual enabling. Messages print at the TTY each time the port disables and reenables.

Implementing and auditing the feature

The documentation is built into the base software.

No alteration is possible.

History file

Description

You may want to track certain system messages or activity and print that information at will. The History file stores system messages in memory. You can access the stored information through a system TTY or from a remote location, and you can print its contents.

How the History file works

You can specify the types of information that you want to store in the History file including maintenance messages (MTC), service change activity (SCH), customer service change activity (CSC), traffic outputs (TRF), and software error messages (ERR and BUG). By storing SCH activity and TRF output messages, you can store records of unauthorized access to the switch and retrieve information associated with calling patterns.

Implementing and auditing the feature

Use the following table to determine which overlays and prompts should be used to implement or audit the History file feature.

For	Implement using	Print using
LD1F Configuration	LD 17—IOTB, HIST, ADAN, USER	LD 22 CFN or ADAN from Release 19 and up

Release 19 enhancements

With Release 19, you may selectively view the History file using the command VHST. Commands allow you to search forward, repeat the last forward or backward search, and perform other various navigational movements within the file.

The History file may also have three categories of files: Log files (see “Multi-user login” on page 6-80), System History file, and Traffic files. Traffic files have two categories: system (scheduled) or user-generated reports. There is one traffic file per system.

These enhancements are included in the base software package.

Section G: Controlling Direct Inward System Access

In this section

Overview	6-84
DISA and security codes	6-85
DISA and Class of Service	6-86
DISA and authorization codes	6-87

Overview

Description: DISA

Direct Inward System Access (DISA) provides a convenient means by which employees, when they are offsite, can place calls to internal extensions, and to private and public network locations by accessing your company's switching system.

How DISA is abused

The type of unauthorized access associated with this feature begins when perpetrators find the telephone number associated with DISA. In most DISA intrusion cases, hackers use PC-based programs to obtain valid DISA DNs, and security and authorization codes. Once a PC program finds a valid DISA telephone number, the PC inputs codes, redials the telephone number repeatedly, and stores the valid codes. Hackers then sell the numbers and codes they obtain illegally to third parties who then use this information for their own "business purposes."

In this section

In this section, you will learn how to effectively manage and monitor the Meridian 1 DISA feature.

DISA and security codes

Introduction

The first level of restricting DISA access is the security code.

How security codes work

If you program your system to require a security code, when the Meridian 1 answers a DISA call, callers must enter the security code assigned to the DISA DN before they can gain access to the system. This security code can be from one to eight digits long.

Remember, the longer the code, the harder it is for a hacker to crack.

DISA and Class of Service

Introduction

The second level of restriction is the class of service assigned to the DISA DN. Each DISA DN has its own Class of Service (COS), Trunk Group Access Restriction (TGAR), and Network Class of Service (NCOS).

How Class of Service works

When the Meridian 1 answers, if you do not require callers to enter authorization codes, then they automatically receive the DISA DN's calling privileges and class of service. You should consider making these controls as restrictive as possible (internal calls only, for example) and force users to enter an authorization code to access trunking facilities.

In addition, if the Meridian 1 records authorization codes in Call Detail Recording (CDR), you can track calls made through DISA and bill them back to users.

Implementing this feature

To implement this feature, see "Class of Service" on page 6-13.

DISA and authorization codes

Introduction

For a third level of security, you can require callers to enter an authorization code before they gain access to system facilities. You can assign authorization codes that are from 1 to 14 digits long. By assigning 14-digit authorization codes, you ensure that the hacker's PC-based code-cracking program has to try more combinations to obtain valid codes.

You can also configure Call Detail Recording to output the authorization codes used for call placement. In reviewing these reports, you should investigate any surge in activity for a given authorization code.

Assigning and changing codes

For further security, you should change authorization codes often and assign one code per person. If you cannot change authorization codes often because you have assigned a large number of codes and communicating the change would be difficult, then consider changing the DISA security code often.

Removal of codes

You should remove the authorization codes of terminated employees immediately. Establish a procedure with Human Resources or your Personnel department to advise you when employees leave the company.

Section H: Restriction/Permission lists

In this section

Overview	6-90
What are restriction/permission lists and codes?	6-91
Defaults	6-93
Understanding how restriction/permission codes work	6-94
Recommendations for using the first four restriction/permission lists	6-97
Defining and applying restriction/permission lists	6-99

Overview

Introduction

In today's telecommunications environment, the same features that provide you with flexibility can also be the source of unauthorized use and abuse.

Meridian Mail features

Features such as remote notification, external call sender, call answering/express messaging thru-dial, and AMIS networking can dial numbers external to your telephone switch. This means that they can be used by users or external callers to place unauthorized long-distance calls at your organization's expense.

Restriction/ permission lists

The primary weapon in your outcalling security arsenal are the restriction/permission lists. These lists are your first line of defense.

What are restriction/permission lists and codes?

Introduction

Restriction/permission lists are an important part of preventing users and callers from abusing your Meridian Mail system.

Definition: restriction/permission list

A restriction/permission list is a group (or set) of restriction codes and permission dialing codes that can be applied to Meridian Mail features or services that are capable of placing outcalls.

Up to 80 lists can be created, but each list must have a unique name. Each list can have up to 30 restriction codes and up to 30 permission codes. Once a list is defined, it can be applied to a number of Meridian Mail features.

Definition: restriction code

A restriction code is a dialing code that Meridian Mail is not permitted to dial. When Meridian Mail is passed a number that begins with a restricted code, the call is blocked.

Restriction codes can be up to 20 digits in length.

Example 1
Your local dialing prefix is 9, your long distance dialing prefix is 91, and your international dialing prefix is 9011. You want to restrict all off-switch dialing. The restriction code is 9.

Example 2
Your long distance dialing prefix is 91 and you want to restrict calls to the 801 area code. The resulting restriction code is 91801.

Definition: permission code

A permission code is a dialing code that Meridian Mail is permitted to dial. These are usually exceptions to the restriction "rules."

Permission codes can be up to 20 digits in length.

Example of a restriction/permission list

In this example, 91 is the long distance dialing prefix and 9011 is the international dialing prefix. All internal extensions begin with 7 and 8.

List Name: Local

Restriction codes: 1 2 3 4 5 6 91 9011

Permission codes: 91617 911

This list restricts all international and long-distance calls, except those to 911 and to the 617 area code. In addition to the permitted codes, it allows on-switch calls to internal extensions beginning with 7 or 8, and local calls beginning with 9.

Defaults

Introduction

The defaults for new installations and conversions are described here. The default values when you first view a restriction/ permission list are also described.

Defaults for new installations

For newly installed Meridian Mail Release 12 systems, all restriction/permission lists are fully restricted. The first four lists are named On_Switch, Local, Long_distance_1, and Long_Distance_2, and the remaining 76 lists are named RPList5 to RPList80 respectively.

> **ATTENTION**
>
> You must modify restriction/permission lists after installation. If you do not, many Meridian Mail features that place outcalls will not work.

Defaults for converted systems

If you have converted to Release 12, the four existing restriction/permission lists remain as they were in the previous release. The new lists are named RPList5 to RPList80 and are fully restricted.

Note: Even though the codes remain the same, you must apply restrictions to any new Release 12 features you implement.

Default list entries

If you have not modified a restriction/permission list, it will be defined as follows the first time you view it:

Restriction codes: 0 1 2 3 4 5 6 7 8 9

Permission codes: (none)

Understanding how restriction/permission codes work

Introduction

The restriction codes in a restriction/permission list specify the general dialing rule. Permission codes are used to indicate any exceptions to the more general rules described by the restriction codes.

Levels of security

It is up to your organization to decide how to configure the restriction/permission lists. They are typically configured to provide various levels of security, from permitting only on-switch dialing (most secure) to allowing all long-distance dialing (least secure).

Examples

The following table contains examples of restriction/permission codes and how Meridian Mail interprets them.

In these examples, 9 is the dialing code for local calls, and 91 is the dialing code for long distance calls.

Restriction code(s)	Permission code(s)	Result
91	91416, 9911	Most long distance calls are restricted, except for 911 calls and numbers in the 416 area code.
1, 2, 5, 6, 7, 8, 9	none	All local and long distance calls are restricted. Internal extensions beginning with 3 or 4 are allowed.
91900	9	1-900 numbers are restricted, but local calls and all other long distance calls are permitted.

Rule

Numbers beginning with a permission code that is shorter than a restriction code and that matches a subset of the restriction code are allowed. They are not restricted.

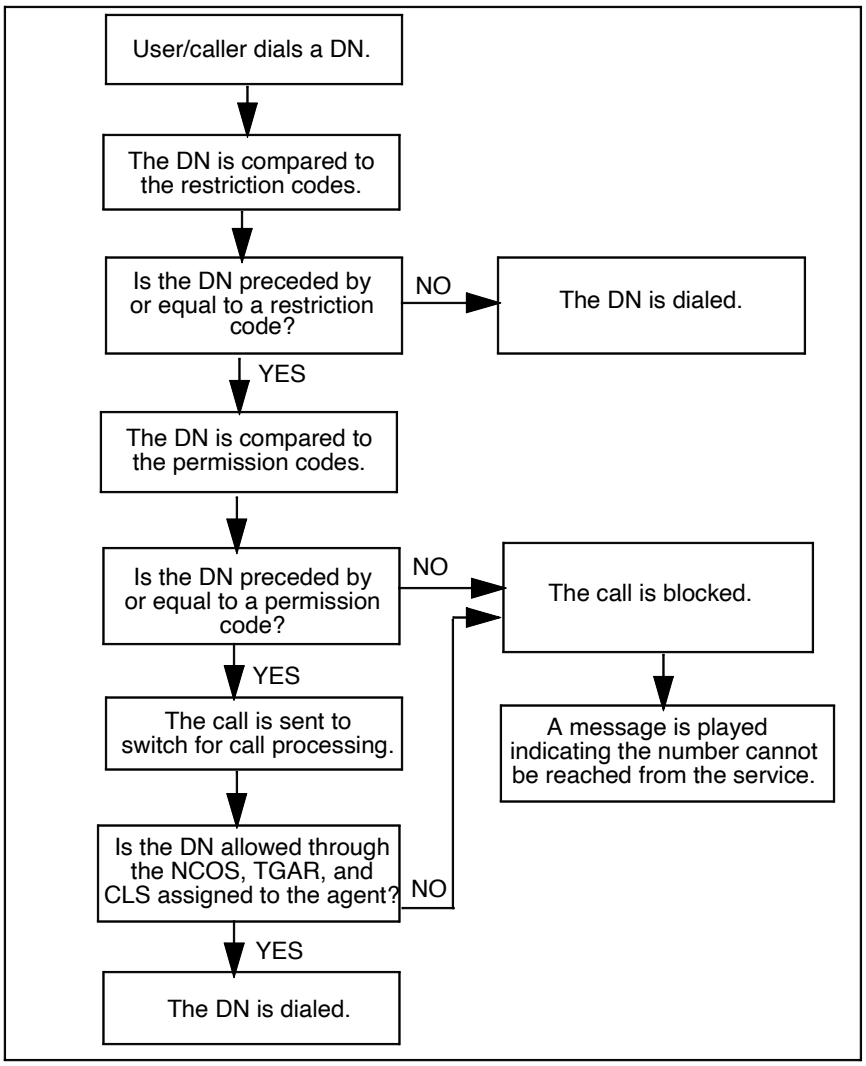
Rule (cont'd)

Example

91900 is a restriction code. 9 is a permission code. Calls beginning with 9 (local calls) or 91 (long distance) are permitted as long as they are not to 91900.

How restriction/ permission codes are processed

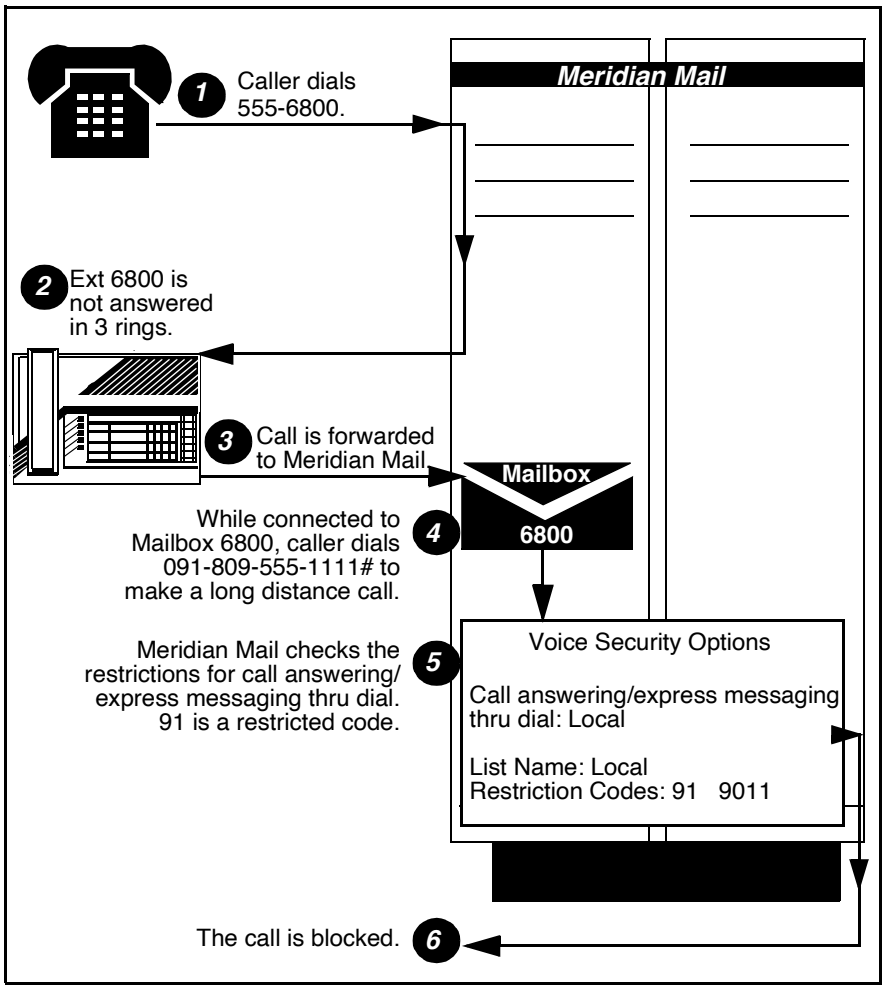
The following flowchart shows how Meridian Mail and the Meridian 1 process restriction and permission codes when a DN is dialed.



Example: Call answering thru-dial

Call answering/express messaging thru-dial allows callers to transfer to another internal extension or valid telephone number once Meridian Mail answers. If the proper restrictions are not placed on this feature, callers will be able to place calls at your organization's expense.

The following illustration shows how restriction/permission codes work in the case of call answering thru-dial.



Recommendations for using the first four restriction/ permission lists

Introduction

The first four restriction/permission lists are named as follows:

- On_Switch
- Local
- Long_Distance_1
- Long_Distance_2

These names can be changed.

Recommendations

Nortel recommends that you use the default restriction/ permission lists as follows.

Note: You are responsible for developing a policy for restricting outcalling that is suitable to your organization's needs.

List name	List function	Restriction codes	Permission codes
On-switch	Permits calls to on-switch extensions only. Restricts all local, long distance, and international calls.	• local dialing prefix • long distance dialing prefix • international dialing prefix	optional (as required)
Local	Permits all on-switch and local calls. Restricts all long distance and international calls.	• long distance dialing prefix • international dialing prefix	optional (as required)

List name	List function	Restriction codes	Permission codes
Long Distance 1	Permits all on-switch calls, local calls, and long distance calls to certain area codes only. Restricts all international calls and long distance calls (in general).	• long distance dialing prefix • international dialing prefix	• specific long distance area codes
Long Distance 2	Permits all on-switch, local, and long distance calls. Restricts all international calls. or Permits all on-switch calls, local calls, and long distance calls to certain area codes only. (Similar in function to Long Distance 1, but permits different area codes.) Restricts all international calls and long distance calls (in general).	• international dialing prefix or • long distance dialing prefix • international dialing prefix • specific area codes	• none or • specific area codes

Defining and applying restriction/permission lists

Introduction

Restriction/permission lists can only be defined through the Restriction/Permission Lists screen. They are, however, applied to specific Meridian Mail features or services through other screens.

Defining restriction/ permission lists

To define restriction/permission lists, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Voice Administration.
2	Select Restriction/Permission Lists. **Result:** The Restriction/Permission Lists screen appears.
3	Position the cursor beside the List number you want to view or modify.
4	Press the [SpaceBar] to highlight the list.
5	Press the [View/Modify] softkey. **Result:** The View/Modify Restriction/Permission List screen appears.
6	Do you want to modify or view the codes in the list?

IF you want to	THEN
modify the list	go to step 7.
view the file	use the cursor keys to scroll through the screen and then go to step 10.

7 Do you want to change the list name?

IF	THEN
yes	press [Backspace] to delete the current name. Enter the new list name.
no	go to step 8.

Step	Action
8	Do you want to change the restriction codes?

IF	THEN
yes	delete the existing code (if not appropriate) and enter a new code. Press <Return> or <Tab> to move to the next field.
no	go to step 9.

9 Do you want to change the permission codes?

IF	THEN
yes	enter the new code. Press <Return> or <Tab> to move to the next field.
no	go to step 10.

10 Do you want to save your changes?

IF	THEN
yes	press [Save].
no	press [Cancel].

Result: The Restriction/Permission Lists screen appears.

Applying restriction/permission lists

The following table identifies which Meridian Mail screens are used to apply restriction/permission lists to Meridian Mail features or services.

To apply restrictions/permissions to the following feature	Use the following screen
Call Answering/Express Messaging Thru-Dial	Voice Security Options
Fax Information service	Session Profile (accessed from the VSDN table; necessary only if Fax on Demand is installed). For more information, refer to the *Fax on Demand Application Guide* (NTP 555-7001-327).
Fax Item Maintenance service	
Voice Menus (that activate fax service)	
Time-of-Day Controllers (that activate fax service)	
Extension dialing (mailbox thru-dial)	Add (or View/Modify) Class of Service
Custom Operator revert	
Remote Notification	
Delivery to Non-User	
External Call Sender	
AMIS Networking	
Thru-Dial service	Add (or View/Modify) Thru-Dial Definition

Section I: Controlling access to Meridian Mail services and features

In this section

Overview	6-104
Custom Revert	6-106
Thru-Dial	6-109
Call Answering or Express Messaging	6-110
Extension dialing (mailbox thru-dial)	6-112
Fax on Demand	6-115
Remote Notification	6-116
Delivery to Non-User	6-118
External Call sender	6-120
AMIS Networking	6-121

Overview

Introduction

Meridian Mail is a voice mail system that is integrated into the Meridian 1 PBX. One of the most feature-rich voice messaging products on the market, the system provides flexible features like Voice Menus which allow callers to choose from lists of services, and Remote Notification which notifies off-site system users that they have messages waiting.

Restriction/ permission lists

You can minimize the risk of toll fraud and system abuse by using the restriction/permission features to control access to your Meridian Mail system and switch. If you fail to put the proper safeguards in place, callers answered by your voice mail system can place toll calls.

Restriction permission lists are applied to features that are capable of dialing outside your switch and are, therefore, a potential source of unauthorized system use and abuse.

Features to which restriction/permission lists can be applied

Restriction/permission lists can be applied to the following features.

Feature	Description
Custom (operator) revert	Users can define their own Custom Revert DN. Assign a list to this feature to restrict the DNs that users can specify.
Thru-dial services	Once connected to a thru-dial service, callers can thru-dial to external numbers if restrictions are not in place. Assign a list to all thru-dialers to restrict the numbers to which callers can thru-dial.
Call answering/ Express messaging Thru-dial	Callers can transfer to other numbers during call answering and express messaging sessions. Assign a list to this feature to restrict the numbers to which callers are allowed to transfer themselves.
Extension dialing (mailbox thru-dial)	Users can thru-dial to other numbers while they are logged on to their mailbox. Assign a list to this feature to restrict the numbers to which they are allowed to thru-dial.

Feature	Description
Fax information service	Callers can request faxes using this service. Assign a list to this feature to restrict the numbers to which faxes are sent.
Fax item maintenance	This service is used to send verification faxes to designated fax phones. Assign a list to this feature to restrict the numbers to which verification faxes can be sent.
Remote notification	Users can set up their own remote notification schedules which specify the remote device (phone, pager) to which notification of new messages should be sent. Assign a list to this feature to restrict the numbers at which users can be remotely notified.
Delivery to non-users	Users can send voice messages to people who do not have mailboxes. Assign a list to this feature to restrict the non-user numbers to which users can send voice messages.
Call sender	Users can return a call with a single telephone set command (9). Assign a list to restrict the numbers they can call back with external call sender.
AMIS Networking	Users can send voice messages to other voice mail systems. Assign a list to this feature to restrict the voice mail systems to which users can send messages.

Custom Revert

Introduction

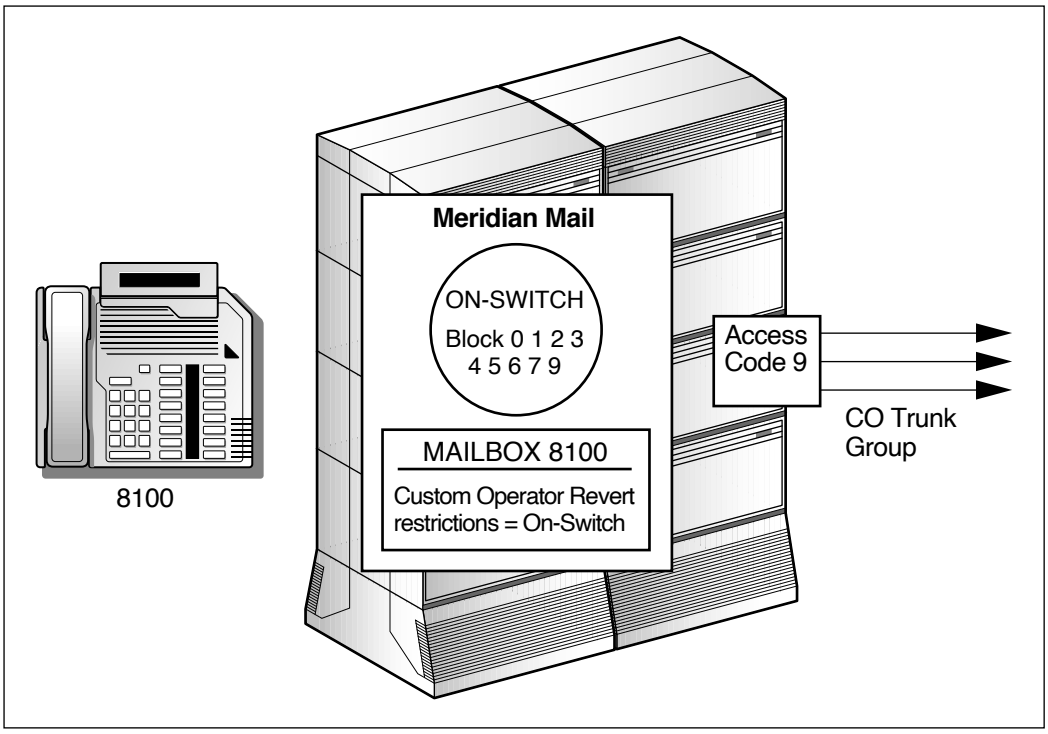
Once Meridian Mail answers, callers may dial zero (0) anytime during the personal greeting or during the record cycle, and transfer to a predefined extension, usually a receptionist or secretary. This extension is the Revert DN.

Description

Each mailbox user can define his or her own Custom Revert DN through the telephone set. To prevent users from (unknowingly) abusing the system, you should assign restriction/permission lists to the revert feature.

Example

The following illustration shows how the Custom Operator Revert feature works.



G100461

Example (cont'd)

In this example, the following takes place:

- The user logs in to Meridian Mail.
- The user activates the Custom Operator Revert feature and attempts to define the operator revert as 9-555-0000.
- Meridian Mail checks the Custom Operator Revert restrictions.
- The On-Switch Table blocks the code 9, and the function is disallowed.

Defining a restriction/ permission list

To define a restriction/permission list, see "Defining and applying restriction/permission lists" on page 6-99.

Assigning a restriction/permission list

To assign a restriction/permission list to the Custom Revert feature, follow these steps.

Step	Action
1	Log in to the administration terminal.
2	Select Class of Service Administration from the Main Menu.
3	Press [View/Modify], and then enter the number of the class of service that the mailbox is using. If you do not know the class a. Press [Find]. b. Press [List]. c. Position the cursor beside the class you want to view or modify, and then press [SpaceBar] to highlight. d. Press [View/Modify]. **Result:** The Class of Service Administration screen for the particular class appears.

Step	Action
4	Position the cursor beside the Custom Revert Restriction/ Permission List field.
5	Enter the number of the restriction/permission list you want to assign to the Custom Revert feature. **Note:** The name of the corresponding restriction/permission list does not appear until the cursor is off the field.
6	Do you want to save your changes?

IF	THEN press
yes	[Save].
no	[Cancel].

Thru-Dial

Introduction

All Thru-Dial services you create using the Voice Menus feature must be adequately protected with an appropriate restriction/permission list.

Defining a restriction/ permission list

To define a restriction/permission list, see "Defining and applying restriction/permission lists" on page 6-99.

Assigning a restriction/permission list

To assign a restriction/permission list to the Thru-Dial service, follow these steps.

Step	Action
1	Log in to the administration terminal.
2	Select Voice Administration from the Main Menu.
3	Select Voice Services Administration from the Voice Administration menu.
4	Select Thru-Dial Definitions.
5	Position the cursor beside the definition, and press the [SpaceBar].
6	Press [View/Modify].
7	Position the cursor beside the Restriction/Permission List field.
8	Enter the number of the restriction/permission list you want to assign to the feature. **Note:** The name of the corresponding restriction/permission list does not appear until the cursor is off the field.
9	Do you want to save your changes? **IF** — **THEN press** yes — [Save]. no — [Cancel].

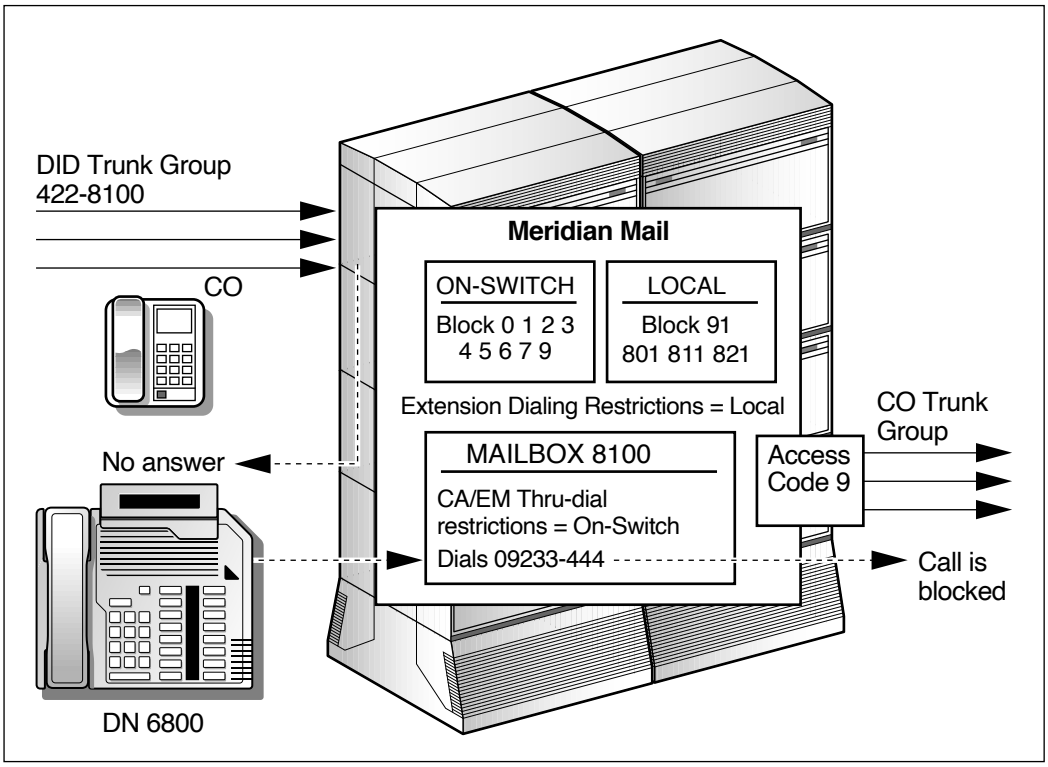
Call Answering or Express Messaging

Description

During a call answering or express messaging session, an external caller could potentially use thru-dial capabilities to place unauthorized calls which would be billed to the system. To use Thru-Dial, a caller must press 0 followed by a dialable DN. (If the caller waits more than two seconds after entering 0, he or she will be connected to an attendant instead.)

Example

The following illustration shows how the extension dialing feature works during a Call Answering/Express Messaging session.



G100462

Example (cont'd)

In this example, the following takes place:

- The caller dials 555-8100. No answer is encountered at extension 8100.
- The caller is forwarded to Meridian Mail.
- Once answered, the caller dials 09233-44.
- Meridian Mail checks the Call Answering/Express Messaging Thru-dial restrictions.
- 9 is not allowed so the call is blocked. If the caller had logged in to Meridian Mail, the call would have been allowed.

Restricting thru-dial capabilities

To prevent callers and users from abusing thru-dial capabilities during call answering or express messaging sessions, make sure an appropriate restriction/permission list is applied to call answering or express messaging thru-dial in the Voice Security Options screen.

To restrict thru-dial capabilities for call answering or express messaging sessions, use the following procedure.

Step	Action
1	Select Voice Administration from the Main Menu.
2	Select Voice Security Options.
3	Move the cursor to the Call Answering/Express Messaging Thru-Dial Restriction/Permission List Number field.
4	Enter the number of the restriction/permission list you want to apply to call answering and express messaging thru-dial. **Note:** The name of the corresponding restriction/permission list does not appear until the cursor is moved off the field.
5	Do you want to save your changes?

IF	THEN press
yes	[Save].
no	[Cancel].

Extension dialing (mailbox thru-dial)

Description

Another standard feature available with Meridian Mail is extension dialing, or Thru-dial for mailboxes. The extension dialing feature allows callers to transfer to another extension number or valid telephone number once they log in to Meridian Mail. Callers can dial zero (0) followed by an extension number, or valid access code, telephone number, and the pound sign (#).

This feature only applies to MMUI systems.

Controls you can exercise

Meridian Mail is shipped with the mailbox Thru-dial feature turned on. You can control access and use of Thru-dial in two ways:

- within the Meridian Mail system
- within the Meridian 1 system through the virtual agent

Controlling access within Meridian Mail

This method allows you to define and apply the restrictions codes that best fit the needs of your user community and the security requirements of your organization.

This method involves

- defining restriction permission lists
  (see "Defining and applying restriction/permission lists" on page 6-99)
- applying restriction/permission lists to features

Note: See "Applying a restriction/permission list" on page 6-113. These codes affect *all* mailbox Thru-dial functions that use the same Class of Service.

Applying a restriction/ permission list

To apply a restriction/permission list, follow these steps.

Step	Action
1	Log in to the administration terminal.
2	Select Class of Service Administration from the Main Menu.
3	Press [View/Modify], and then enter the number of the class of service that the mailbox is using. If you do not know the class a. Press [Find]. b. Press [List]. c. Position the cursor beside the class you want to view or modify, and then press [SpaceBar] to highlight. d. Press [View/Modify]. **Result:** The Class of Service Administration screen for the particular class appears.
4	Position the cursor beside the Extension Dialing Restriction/ Permission List field.
5	Enter the number of the restriction/permission list you want to assign to the Extension dialing feature. **Note:** The name of the corresponding restriction/permission list does not appear until the cursor is off the field.
6	Do you want to save your changes? **IF** — **THEN press** yes — [Save]. no — [Cancel].

Controlling access within the switch

To control access of the Thru-dial feature within the Meridian 1 system, use the following procedure. This method allows you to restrict the Thru-dial feature through the virtual agent.

Note 1: To restrict all access to the outside world through Thru-dial, be sure to restrict both your Least Cost Routing access code and your direct access code to each trunk group in the Meridian 1.

Note 2: Be sure to block access to your Special Prefix (SPRE) code as well.

Step	Action
1	Assign the appropriate Network Class of Service (NCOS). For more information, see “Network Class of Service—Facility Restriction Level” on page 6-55.
2	Assign the appropriate Trunk Group Access Restrictions (TGAR). For more information, see “Trunk Group Access Restrictions” on page 6-11.
3	Assign the appropriate Class of Service (COS). For more information, see “Class of Service” on page 6-13.

The restrictions you impose through the virtual agent apply to Thru-dial functions accessed both through the voice menus feature and at the mailbox level.

Fax on Demand

Description

If Fax on Demand is installed, you will need to determine the restrictions that need to be applied to external callers who request that faxes be delivered using callback delivery. In other words, with callback delivery, callers are asked to specify the number to which a fax should be delivered. You will have to decide if you want faxes to be delivered to all numbers, only local numbers, all long distance numbers, only certain area codes, and so on.

Note: This topic is only applicable to systems that have Fax on Demand installed.

Restricting thru-dial for Fax on Demand

When adding the VSDN of the service through which the fax item will be made accessible, you must specify a session profile. In this session profile, you choose the fax delivery method. If it is set to either Call Back or Caller Choice, you will have to specify a restriction/permission list (also in the session profile).

Refer to the *Fax on Demand Application Guide* (NTP 555-7001-327) for information on securing the callback options.

Remote Notification

Description

Remote Notification allows a user to be notified at a remote telephone or pages when a new message arrives in his or her mailbox. Users can define their own remote notification schedules and target DNs from their telephone sets.

Note: This topic is only applicable to systems that have the Outcalling feature installed.

Restricting target DNs

To restrict the target DNs to which users try to send remote notifications, you must assign a restriction/permission list to the Remote Notification feature in the classes of service you set up.

Defining a restriction/ permission list

To define a restriction/permission list, see "Defining and applying restriction/permission lists" on page 6-99.

Applying a restriction/ permission list

To apply a restriction/permission list to the Remote Notification, follow these steps.

Step	Action
1	Log in to the administration terminal.
2	Select Class of Service Administration from the Main Menu.
3	Press [View/Modify], and then enter the number of the class of service that the mailbox is using. If you do not know the class a. Press [Find]. b. Press [List]. c. Position the cursor beside the class you want to view or modify, and then press [SpaceBar] to highlight. d. Press [View/Modify]. **Result:** The Class of Service Administration screen for the particular class appears.

Step	Action
4	Do you want to enable Remote Notification capabilities for this class of service?

IF	THEN go to
yes	step 5.
no	step 9.

5 Set the Remote Notification Capability field to Yes.

Result: The following four fields will appear:

- Remote Notification Restriction/Permission List
- Remote Notification Keypad Interface
- Remote Notification Retry Limits and Frequency
- RN Business Days

6 Enter the number of the restriction/permission list you want to assign to the feature.

Note: The name of the corresponding restriction/permission list does not appear until the cursor is off the field.

7 Do you want your users in this class of service to be able to use their keypad interface to change the remote notification DN?

Note: The Keypad Interface field applies only to MMUI systems.

IF	THEN set the Keypad Interface field to
yes	yes.
no	no.

8 Enter the retry limits and frequencies for the following:

- Busy
- No Answer
- Answered

9 Select the business days on which remote notification will (not) be available.

10 Do you want to save your changes?

IF	THEN press
yes	[Save].
no	[Cancel].

Delivery to Non-User

Description

Delivery to Non-User (DNU) allows a Meridian Mail user to compose and send a voice message to someone who is not a Meridian Mail user. To restrict the numbers to which users are allowed to send voice messages, assign an appropriate restriction/permission list to the Delivery to Non-User feature in the classes of service you set up.

Note: This topic is only applicable to systems that have the Outcalling feature installed.

Defining a restriction/ permission list

To define a restriction/permission list, see "Defining and applying restriction/permission lists" on page 6-99.

Applying a restriction/ permission list

To apply a restriction/permission list to the Delivery to Non-user feature, follow these steps.

Step	Action
1	Log in to the administration terminal.
2	Select Class of Service Administration from the Main Menu.
3	Press [View/Modify], and then enter the number of the class of service that the mailbox is using. If you do not know the class a. Press [Find]. b. Press [List]. c. Position the cursor beside the class you want to view or modify, and then press [SpaceBar] to highlight. d. Press [View/Modify]. **Result:** The Class of Service Administration screen for the particular class appears.
4	Do you want to enable Delivery to Non-User capabilities for this class of service?

IF	THEN go to
yes	step 5.
no	step 9.

Step	Action
5	Set the Delivery to Non-User Capability field to Yes. **Result:** The following three fields appear: • Delivery to Non-User Restriction/Permission List • Send Messages via DNU if Mailbox Not Found • DNU DTMF Confirmation Required
6	Enter the number of the restriction/permission list you want to assign to the feature. **Note:** The name of the corresponding restriction/permission list does not appear until the cursor is off the field.
7	Do you want to send messages if the mailbox is not found?

IF	THEN set the Send Messages via DNU if Mailbox Not Found field to
yes	Yes.
no	No.

Step	Action
8	Do you require a DTMF confirmation?

IF	THEN set the DNU DTMF Confirmation Required field to
yes	Yes.
no	No.

Step	Action
9	Do you want to save your changes?

IF	THEN press
yes	[Save].
no	[Cancel].

External Call sender

Description

This feature allows a Meridian Mail user to immediately call back someone who has left a message and who is external to the switch, by pressing 9 after listening to the message. (This only applies to messages that have been left during call answering sessions, and composed voice messages.)

Defining a restriction/ permission list

To define a restriction/permission list, see "Defining and applying restriction/permission lists" on page 6-99.

Applying a restriction/ permission list

To apply a restriction/permission list to External Call Sender, follow these steps.

Step	Action
1	Log in to the administration terminal.
2	Select Class of Service Administration from the Main Menu.
3	Press [View/Modify], and then enter the number of the class of service that the mailbox is using. If you do not know the class a. Press [Find]. b. Press [List]. c. Position the cursor beside the class you want to view or modify, and then press [SpaceBar] to highlight. d. Press [View/Modify]. **Result:** The Class of Service Administration screen for the particular class appears.
4	Position the cursor beside the External Call Sender Restriction/ Permission List field.
5	Enter the number of the restriction/permission list you want to assign to the Call Sender feature. **Note:** The name of the corresponding restriction/permission list does not appear until the cursor is off the field.
6	Do you want to save your changes? **IF** — **THEN press** yes — [Save]. no — [Cancel].

AMIS Networking

Description

When a user composes a voice message and tries to send it to an AMIS site (that is not defined as a virtual node), Meridian Mail checks the restriction/permission list that is assigned to AMIS networking to see if it is restricted. The restriction/permission list is assigned to AMIS networking in classes of service.

Note: This topic is only applicable to systems that have the AMIS Networking feature installed.

Virtual Node AMIS

In the case of Virtual Node AMIS, where the local site also has Meridian Networking, these restrictions do not apply to remote AMIS sites that are defined as virtual nodes in the local network database.

For more information on Virtual Node AMIS, refer to the *Virtual Node AMIS Installation and Administration Guide* (NTP 555-7001-245).

Defining a restriction/ permission list

To define a restriction/permission list, see "Defining and applying restriction/permission lists" on page 6-99.

Applying a restriction/ permission list

To apply a restriction/permission list to AMIS Networking, follow these steps.

Step	Action
1	Log in to the administration terminal.
2	Select Class of Service Administration from the Main Menu.
3	Press [View/Modify], and then enter the number of the class of service that the mailbox is using. If you do not know the class a. Press [Find]. b. Press [List]. c. Position the cursor beside the class you want to view or modify, and then press [SpaceBar] to highlight. d. Press [View/Modify]. **Result:** The Class of Service Administration screen for the particular class appears.

Step	Action

4 Do you want mailbox users assigned to this class of service to be able to receive AMIS Open Network Messages?

IF	THEN set the Receive AMIS Open Network Messages field to
yes	Yes.
no	No.

5 Do you want mailbox users assigned to this class of service to be able to compose and send AMIS Open Network Messages?

IF	THEN set the Compose/Send AMIS Open Network Messages field to
yes	Yes.
no	No.

Result: The following field appears when the field is set to Yes:

- AMIS Open Network Restriction/Permission List

6 Enter the number of the restriction/permission list you want to apply to this class of service in the AMIS Open Networking Restriction/Permission List field.

Note: The name of the restriction/permission list will not appear until the cursor is off the field or the changes have been saved.

7 Do you want to save your changes?

IF	THEN press
yes	[Save].
no	[Cancel].

Section J: Controlling access to Meridian Mail mailboxes

In this section

Overview	6-124
Using the Voice Security Options screen	6-125
Default security settings	6-131
Initial password change	6-133
Password display suppression	6-135
Password prefix	6-136
Password length	6-138
Forced regular password changes	6-139
Invalid logon attempts	6-142
Modifying mailbox security settings	6-146
Restricting off-site access to mailboxes	6-147
Disabling unused mailboxes	6-148

Overview

Introduction

Mailboxes are a potential source of unauthorized system use if proper safeguards are not put in place.

The kind of damage a hacker can do

The damage a hacker can do depends on what has been accessed:

- A personal mailbox *without* thru-dial capabilities

  This causes minimal damage as the hacker has only gained access to the personal mailbox. In this case, the hacker would have access to all of the mailbox and message commands and could record obscene greetings, listen to messages, and so on.
- A personal mailbox *with* thru-dial capabilities

  This can cause significant damage to your PBX and Meridian Mail system, especially if the hacker is able to break in to the system.
- The business or Meridian Mail system

  This can cause significant damage to your PBX and Meridian Mail system since this mailbox usually allows users calling in access to the thru-dial feature.

Proactive mailbox security measures

Meridian Mail provides four ways that you can control the level of security for users' mailboxes:

1. Use the password prefix and increase the minimum password length to make passwords harder to guess.
2. Force users to change their passwords regularly.
3. Control the number of maximum invalid logon attempts.
4. Disable external logon to mailboxes (when the highest level of security possible is required).

Using the Voice Security Options screen

Introduction

The Voice Security Options screen allows you to control various security features and set restriction and permission codes that can be applied to features such as call answering, call sender, Express Messaging, mailbox Thru-Dial, and AMIS networking

Voice Security Options screen

Part 1

This is the first part of the Voice Security Options screen.

```
                          Voice Administration
Voice Security Options

Password Prefix:                                          _

Maximum Invalid Logon Attempts Permitted per session:  3_

Maximum Invalid Logon Attempts Permitted per mailbox:  9_

Maximum Days Permitted Between Password Changes:       30

Password Expiry Warning (days):                        5_

Minimum Number of Password Changes Before Repeats:     5

Minimum Password Length:                               4_

External Logon:                                        Enabled
                                                                MORE BELOW
Select a softkey >

   Save        Cancel
```

Part 2

To view the additional fields in part 2 of the screen, press the <Page down> key or the down arrow.

```
                          Voice Administration                    MORE ABOVE
Voice Security Options

Call Answering/Express Messaging Thru_dial
Restriction/Permission List Number:                    2_ Name: Local

Force Password Change on Initial Logon:                No Yes

Suppress Display of Telset Password:                   No Yes

System Access Monitoring Period from (hh:mm):          23:00 to (hh:mm): 05:00

Monitor All Thru-Dials during Monitoring Period:       No Yes Always_Monitor

Monitor CLIDs during Monitoring Period:                No Yes Always_Monitor

CLID Format    CLIDs to Monitor
Internal:      _______________ _______________ _______________ _______________
               _______________ _______________ _______________ _______________
                                                                    MORE BELOW
Select a softkey >

   Save        Cancel
```

Field descriptions

The following fields are used to protect mailboxes against unauthorized use. The fields used to monitor mailbox access can be found in Section K: Monitoring access to Meridian Mail mailboxes and features.

Password Prefix	
Description	The Password Prefix is a set of (up to four) digits that is inserted at the start of the default mailbox password whenever you create a new mailbox.
Default	System-generated four-digit code
Maximum Length	4 digits The prefix plus the user's DN cannot exceed 16 digits.

Maximum Invalid Logon Attempts Permitted per Session	
Description	This is the maximum number of times a user or caller can enter an invalid password within one logon session.
Default	3
Valid Range	1 to 99

Maximum Invalid Logon Attempts Permitted per Mailbox	
Description	This is the number of maximum invalid passwords that can be entered for a mailbox. This does not apply to the current logon session only. The number of invalid logons are counted over time.
Default	9
Valid Range	1 to 99

Maximum Days Permitted Between Password Changes	
Description	This field determines how often users are forced to change their mailbox passwords.
Default	30
Valid Range	0 to 90 0 indicates users do not have to change passwords.
Dependencies	MMUI only

Password Expiry Warning (days)	
Description	When a user's password is about to expire, a warning is played to notify the user and give him or her the chance to change it before it expires. This field determines how many days before password expiry the warning is played.
Default	5
Valid Range	0 to 60 0 indicates that a warning will not be played.
Dependencies	MMUI only Displayed when the maximum days between password changes is one or greater.

Minimum Number of Password Changes Before Repeats	
Description	This field determines the number of different passwords that must be used before the same password can be reused.
Default	5
Valid Range	0 to 5 0 indicates that users can reuse the same password.
Dependencies	MMUI only Displayed when the maximum days between password changes is one or greater.

Minimum Password Length	
Description	This is the minimum number of digits required in passwords that are entered from the telephone keypad. This includes mailbox passwords and access and update passwords for voice services.
Default	4
Valid Range	4 to 16
Dependencies	MMUI only.

External Logon	
Description	This feature is usually enabled to allow users to log on to their mailboxes from remote off-switch phones.This feature can be disabled to provide maximum security. When disabled, users cannot log on to their mailboxes from off-switch phones.
Default	Enabled
To disable	Call your Nortel distributor to disable this feature. **ATTENTION** Once disabled, this feature can never be reenabled.
Valid Options	Enabled, Disabled
Dependencies	MMUI only

Call Answering/Express Messaging Thru-Dial Restriction/Permission List Number	
Description	This field indicates which Restriction/Permission List should be applied to Call Answering/Express Messaging Thru-Dials.
Default	None

Force Password Change on Initial Logon	
Description	This field compels users who are logging in to their mailbox for the first time to immediately change the default password.
Default	Yes
Dependencies	This field is displayed only if the interface is MMUI.

Suppress Display of Telset Password	
Description	This field suppresses the display of password digits by replacing them with dashes on telephones with displays.
Default	Yes
Dependencies	None

System Access Monitoring Period from (hh:mm)	
Description	This field indicates the monitoring period during which any or all of the following is monitored: • mailbox logons for requested users • the use of Thru-Dial services • the use of a mailbox or Thru-Dial service from a specified CLID
Default	Start time: 23:00 End time: 05:00

Monitor All Thru-Dials during Monitoring Period	
Description	This field indicates whether all Thru-Dial services (from a mailbox, voice menu, or directly from a VSDN) are to be monitored, and if yes, when.
Default	No
Valid Options	No, Yes, Always_Monitor If Yes, you are prompted for the monitoring period.

Monitor CLIDs during Monitoring Period	
Description	This field indicates whether calling line IDs (CLIDs) are to be monitored during logon or by the Thru-Dial service, and if yes, when.
Default	No
Valid Options	No, Yes, Always_Monitor If Yes, you are prompted for the monitoring period.

CLID Format—Internal—CLIDs to Monitor	
Description	These are the internal CLIDs to be monitored during login or by the Thru-Dial service.
Default	None
Dependencies	The Monitor CLIDs during Monitoring Period field is set to Yes or Always_Monitor.

CLID Format—External—CLIDs to Monitor	
Description	These are the external CLIDs to be monitored during login or by the Thru-Dial service.
Default	None
Dependencies	The Monitor CLIDs during Monitoring Period field is set to Yes or Always_Monitor.

Default security settings

Purpose

On a newly installed system, the security parameters are configured with default settings. These defaults may be appropriate for your system. If this is the case, you will not have to modify the settings.

However, the default settings may not adequately secure your Meridian Mail system to meet your business requirements.

Security checklist

Review the checklist below to determine if you need to change any of the default values that are assigned to passwords. You can also fill in this checklist with your new settings.

Information about these parameters is provided on the following pages.

Parameter	Default value
Password Prefix	4-digit code
Maximum Invalid Logon Attempts Permitted per Mailbox	9
Maximum Invalid Logon Attempts Permitted per Session	3
Maximum Days Permitted Between Password Changes	30
Password Expiry Warning (days)	5
Minimum Number of Password Changes before Repeats	5
Minimum Password Length	4
External Logon	Enabled
Call Answering/Express Messaging Thru-Dial Restriction/Permission List Number	None
Force Password Change on Initial Logon	Yes
Suppress Display of Telset Password	Yes

Parameter	Default value
System Access Monitoring Period from (hh:mm)	23:00 to 05:00
Monitor All Thru-Dials during Monitoring Period	No
Monitor CLIDs during Monitoring Period	No
CLID Format—Internal—CLIDs to Monitor	None
CLID Format—External—CLIDs to Monitor	None

Initial password change

Introduction

Another measure to enhance security is to ensure that users change their initial password. This way, unauthorized access is prevented by those who may know the password prefix and mailbox number.

The initial password change feature provides the ability to force users to change their password the first time they log in.

How it works

When users log in to their mailbox for the first time, their default password is treated as "expired," and they are forced to change their password at this time.

Note: When a user enters his or her password for the first time, and any time thereafter, it is not displayed on the telephone set display. For more information on this feature, see "Password display suppression" on page 6-135.

This feature is enabled for all systems.

This feature only applies to MMUI mailboxes including Hospitality staff users. For VMUIF systems, this feature will be disabled, and it will not apply to hospitality guest users.

Enforcing an initial password change

To ensure that new users are forced to change their passwords when they log in for the first time, use the following procedure.

Step	Action
1	Select Voice Administration from the Main Menu. **Result:** The Voice Administration menu appears.
2	Select Voice Security Options. **Result:** The Voice Security Options screen appears.
3	Select Yes in the Force Password Change on Initial Logon field.
4	Do you want to save the configuration?

IF	THEN press
yes	[Save].
no	[Cancel].

Password display suppression

Introduction

The password display suppression feature prevents display of entered password digits on telephone sets that have display screens. This prevents “shoulder surfers” from seeing your password.

How password display suppression works

When users enter their passwords, each digit in the password is replaced by a dash (-). The pound (#) key continues to be displayed as #, but the star (*) key is displayed as a dash if the feature is enabled.

This feature is not supported for external calls because the local switch has no control on the suppression capability.

Suppressing the display

To suppress the display of password each time a user logs in to Meridian Mail, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Select Voice Administration. **Result:** The Voice Administration menu appears.
2	Select Voice Security Options. **Result:** The Voice Security Options screen appears.
3	Select Yes in the Suppress Display of Telset Password field.
4	Do you want to save the configuration?

IF	THEN press
yes	[Save].
no	[Cancel].

Password prefix

Introduction

When a new mailbox is created, the default password is the user's extension number. Until the user changes the default password, this may be a potentially serious security risk.

Password prefix

A password prefix provides another level of security by appending a short code before the default password. This code can be between two to four digits in length.

When a password prefix is defined, it is inserted at the beginning of the default mailbox password—the prefix is only inserted for new mailboxes.

Example

If mailbox 2339 is created and a password prefix of 34 has been defined, then the mailbox user will enter 342339 as the password the first time he or she logs in to Meridian Mail.

How prefixes work

The password prefix only applies to new MMUI users regardless of whether it is being defined for the first time or has been changed. VMUIF users continue to have their default password set to null and must log in from their "home phone" to change their password.

The password prefix applies only until the user changes the password. For example, when the user of mailbox 2339 changes the password for the first time, the prefix is no longer required.

Guidelines

Change the password prefix on a regular basis for maximum security. When you change the password prefix, it does not affect existing mailboxes, only newly created mailboxes.

Setting up the password prefix

To apply a password prefix, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Select Voice Administration. **Result:** The Voice Administration menu appears.
2	Select Voice Security Options. **Result:** The Voice Security Options screen appears.
3	Enter the prefix in the Password Prefix field. **Note:** The combined password prefix and the actual password cannot exceed 16 digits in length.
4	Do you want to save the configuration?

IF	THEN press
yes	[Save].
no	[Cancel].

Password length

Introduction

The length of the password, in conjunction with other mailbox features, can make it very difficult for hackers to break into your Meridian Mail system. You should never depend on one feature alone to safeguard your system.

Note: The password length feature only applies to MMUI systems.

How having a long password increases security

A long password increases your security provided that the password and the mailbox number are *not* the same. Having a long password means that there are more combinations to enter which could discourage the hacker.

Defining the password length

To define the minimum password length, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Select Voice Administration. **Result:** The Voice Administration screen appears.
2	Select Voice Security Options. **Result:** The Voice Security Options screen appears.
3	Set the password length in the Minimum Password Length field. **Note:** The password length including the password prefix cannot exceed 16 digits in length.
4	Do you want to save the configuration? **IF** — **THEN press** Yes — [Save]. No — [Cancel].

Forced regular password changes

Introduction

Forced password changes help increase security especially if they are done regularly. By compelling mailbox users to change their passwords and encouraging them to vary the length, it makes it very difficult for hackers to guess your password patterns.

Who can change the password

The mailbox password is changeable by both the administrator and the mailbox user. It can be altered as often as desired.

Relevant fields

The following fields in the Voice Security Options screen are related to forced password changes. The second and third fields are displayed only if the first field is set to a value of 1 or more:

- Maximum Days Permitted Between Password Changes
- Password Expiry Warning (days)
- Minimum Number of Password Changes before Repeats

Note: These fields apply to the MMUI interface only.

For more information on the Voice Security Options screen and its fields, see "Modifying mailbox security settings" on page 6-146.

Maximum days between password changes

You can either force users to change their passwords on a regular basis, or you can allow them to change them when or if they want.

Default

On a newly installed system, the default setting forces users to change their passwords every 30 days. You can choose a value between 0 and 90 days.

Guideline

Forcing users to change their passwords on a regular basis is recommended since this results in a much greater level of security.

Expired passwords

If a user's password expires, the user is not allowed to retrieve messages until he or she changes the password.

> **ATTENTION**
>
> If you change this value from 0 to another value on an operational system, user passwords expire immediately. Make this change during a slow traffic time and inform users of the change. After the change, you may notice a number of 3134 DR SEERs that indicate users did not change their passwords when prompted.

Password expiry warning

If the maximum days between password changes is set to 1 or more, you can play an expiry warning message to users before their password is about to expire. This warning reminds the user that the password is going to expire in X days and gives the user the chance to change the password before it expires.

This field gives you control over when this password is played.

WHEN this field is set to	THEN the warning will
a value between 1 and 60	be played this many days before the password is set to expire.
0	not be played. When the user's password expires, he or she will be prompted for a new password at logon.

Minimum password changes before repeats

To further increase mailbox security, you can force users to use a different password whenever their password expires. Otherwise, users may simply enter the same password over and over every time their password expires.

This setting is not applicable if the maximum days permitted between password changes is zero (0).

Enforcing regular password changes

To set up your system so that mailbox users will have to change their passwords, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Select Voice Administration. **Result:** The Voice Administration menu screen appears.
2	Select Voice Security Options. **Result:** The Voice Security Options screen appears.
3	Set the expiration period in the Maximum Days Permitted Between Password Changes field. **Note:** The valid range is from 0 to 90 days and the default is 30. If you set this field to 0, the users are not forced to change their password and you do not have to configure any other fields. In this case, go to step 6 to save or cancel the changes.
4	Set the number of days of advance notice that users will hear before their password expires in the Password Expiry Warning (days) field.
5	Set the number of passwords that have to expire before a user can reuse an old password in the Minimum Number of Password Changes Before Repeat field.
6	Do you want to save the configuration?

IF	THEN press
yes	[Save].
no	[Cancel].

Invalid logon attempts

Introduction

The Invalid Logon Attempts feature allows you to define the number of times, within a range of one to nine, that a caller can enter an invalid logon password for a mailbox before the system disables the mailbox. Once the mailbox is disabled, only the system administrator can reenable it at the administration terminal. When a mailbox is disabled, Meridian Mail still takes and stores incoming messages but does not permit logons.

The feature is useful in preventing hackers from entering one password after another until they gain access to a mailbox.

The feature also allows you to specify the number of invalid logon attempts per session as well as per mailbox. This discourages hackers from hopping around from one mailbox to another, disabling them with invalid logon attempts.

Relevant fields

There are two fields in the Voice Security Options screen that control the number of allowable invalid logon attempts:

- Maximum Invalid Logon Attempts Permitted per Session
- Maximum Invalid Logon Attempts Permitted per Mailbox

For more information on the Voice Security Options screen and its fields, see “Modifying mailbox security settings” on page 6-146.

Invalid logons per session

This field determines how many invalid passwords can be entered in a row during one logon session. If this limit is reached, the logon session is terminated.

Example

If a hacker knows your Meridian Mail access code and some DNs, this is what would happen if your maximum invalid logon attempts per session were set to 3.

Attempt	Description
1	The hacker tries logging in to mailbox 2498 but enters an incorrect password.
2	The hacker tries logging in to mailbox 2498 again but enters an incorrect password.
3	The hacker tries logging in to mailbox 2475 but enters an incorrect password.
	The logon session is terminated.

Invalid logons per mailbox

Meridian Mail also keeps track of how many invalid logon attempts have been made on each mailbox. This does not apply to the current logon session only. The number of invalid passwords entered is counted over time.

The counter is reset to 0 when the user changes the password.

If the limit is reached, the mailbox is disabled. Meridian Mail still takes and records incoming messages, but does not allow the user to log on.

Disabling a mailbox

To specify how many invalid logon attempts will be allowed before a mailbox is disabled, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Select Voice Administration. **Result:** The Voice Administration menu screen appears.
2	Select Voice Security Options. **Result:** The Voice Security Options screen appears.
3	Set the number of invalid logon attempts per session in the Maximum Invalid Logon Attempts Permitted per Session field. The valid range is from 1 to 99, and the default is 3.
4	Set the number of invalid logon attempts per mailbox in the Maximum Invalid Logon Attempts Permitted per Mailbox field. The valid range is from 1 to 99, and the default is 9.
5	Do you want to save the configuration?

IF	THEN press
yes	[Save].
no	[Cancel].

Reenabling an MMUI mailbox

To reenable a disabled MMUI mailbox, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Choose User Administration.
2	Choose Local Voice User.
3	Do you know the user's DN?

IF	THEN
yes	press [View/Modify]. Enter the user's DN and press <Return>. Go to step 9.
no	follow step 4 to step 8.

Step	Action
4	Press [Find] to do a search.
5	Specify the criteria for the search.
6	Press [List].
7	Position the cursor beside the user you want to modify and press the spacebar to highlight the entry.
8	Press [View/Modify].
9	Move the cursor to the Logon Status field.
10	Select Enabled.
11	Do you want to save the configuration?

IF	THEN press
yes	[Save].
no	[Cancel].

Reenabling a VMUIF mailbox

The setting in the Mailbox Lockout Duration field determines how a VMUIF mailbox has to be reenabled. This field is located in the View/Modify Class of Service screen. The duration is specified in hours and minutes (hh:mm).

WHEN the lockout duration is	THEN
00:01 or greater	the mailbox will be automatically reenabled after the specified time.
00:00 (zero)	you must manually reenable the mailbox in the Logon Status field in the View/Modify Local Voice User screen. The procedure is the same as “Reenabling an MMUI mailbox” on page 6-144.

Modifying mailbox security settings

When to use

Follow this procedure

- after installation, if some or all of the default settings do not meet your organization's requirements
- to change the current settings to reflect a new security policy or tougher security measures

Procedure

To modify current mailbox security settings, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Security Options. **Result:** The Voice Security Options screen appears.
3	Modify some or all of the following fields to meet your security requirements: • Password Prefix • Maximum Invalid Logon Attempts Permitted per Session • Maximum Invalid Logon Attempts Permitted per Mailbox • Maximum Days Permitted Between Password Changes • Password Expiry Warning • Minimum Number of Password Changes before Repeats • Minimum Password Length • Force Password Change on Initial Logon • Suppress Display of Telset Password For more information, see the appropriate topics.
4	Do you want to save the configuration?

IF	THEN press
yes	[Save].
no	[Cancel].

Restricting off-site access to mailboxes

Introduction

External logon is enabled by default, allowing users to log on to their mailboxes from phones that are external to the switch. If security is of the highest priority, Meridian Mail provides a facility allowing the system to restrict access to a mailbox from an offsite location.

Implementing this feature

This feature (SW7007) can be ordered from a Nortel sales representative and is implemented by authorized field technicians.

> **ATTENTION**
>
> Once the external logon feature is disabled on the system, it can *never* be reenabled.

Disabling unused mailboxes

Introduction

Whenever employees are terminated, you should immediately disable their mailbox. This prevents them from abusing your system by billing toll calls to your company.

You should make arrangements with your Personnel department to inform you of terminations so you can disable system access.

Procedure

To disable an unused mailbox, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Select User Administration.
2	Select Local Voice User.
3	Press [View/Modify], and then enter the local voice user. If you do not know the local voice user, do the following: a. Press the [Find] softkey followed by the [List] softkey. b. Position the cursor beside the user you want to view or modify, and press the [SpaceBar]. c. Press [View/Modify].
4	Position the cursor on the Logon Status field.
5	Set the field to Disabled to disable the mailbox.
6	Press [Save] to save the configuration.

Section K: Monitoring access to Meridian Mail mailboxes and features

In this section

Overview	6-150
Hacker Monitor	6-151
Mailbox Login Monitoring	6-152
Thru-Dial Monitoring	6-154
CLID Monitoring	6-157
The Services Summary Traffic report	6-160

Overview

Introduction

This section of the chapter describes the reports and features in Meridian Mail intended to assist you in identifying attempts to violate the security of your system.

These include the following:

- the Services Summary Traffic report
- the Hacker Monitor feature
- mailbox login monitoring
- Thru-Dial monitoring
- CLID monitoring

Hacker Monitor

Introduction

This feature enables you to monitor selected or all mailbox logins and Thru-Dials, which helps you to check for activity on your system that may indicate the presence of hackers.

When this feature is combined with the SEER Mailbox feature, you can be notified through Remote Notification when a suspected unauthorized user attempts a Thru-Dial or enters a particular mailbox.

Description

The Hacker Monitor capability is provided by three different methods:

- by monitoring mailbox logins (see “Mailbox Login Monitoring” on page 6-152)
- by monitoring the use of Thru-Dial services (see “Thru-Dial Monitoring” on page 6-154)
- by monitoring mailbox logins or attempted Thru-Dials from specified calling line identification numbers (CLIDs) (see “CLID Monitoring” on page 6-157)

Mailbox Login Monitoring

Introduction

Possible hacker activity may be detected by monitoring mailbox logins of requested local voice users.

How to do it

You use the System Access Monitoring Period field on the Voice Security Options screen and the Monitor Mailbox during Monitoring Period field on the Local Voice User screen to set up mailbox login monitoring.

Field descriptions

This table describes the fields that are used to set up mailbox monitoring.

System Access Monitoring Period	
Description	This field indicates the monitoring period during which any or all of the following is monitored: • mailbox logins for requested users • the use of Thru-Dial services • the use of a mailbox or Thru-Dial service from a specified CLID
Default	Start time: 23:00 End time: 5:00 Both the start and the end time for this period are specified in the hh:mm format using the 24-hour clock.
Monitor Mailbox during Monitoring Period	
Description	When this field is set to Yes, all logins into the mailbox during the system access monitoring period will result in SEER 2262 being issued for MMUI users or SEER 5662 being issued for VMUIF users.
Default	No
References	For more information on local voice users, see Chapter 8, “Local voice users”.

Procedure

To monitor mailbox logins, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Security Options.
3	Specify a time interval in the System Access Monitoring Period field.
4	Press [Save].
5	Return to the Main Menu .
6	Select User Administration.
7	Select Local Voice Users.
8	Select the local voice user you want to modify or add. For more information on modifying or adding local voice users, see Chapter 8, “Local voice users”.
9	Set the Monitor Mailbox during Monitoring Period field to Yes.
10	Press [Save].

Thru-Dial Monitoring

Introduction

Possible hacker activity may be detected by monitoring selected or all Thru-Dial services used either during the system access monitoring period or at all times.

How to do it

Use the Voice Security Options screen and the Thru-Dial Definition screen to set up Thru-Dial Monitoring.

Note: The monitoring period is determined by the values entered in the System Access Monitoring Period from (hh:mm) field on the Voice Security Options screen.

IF you want to monitor	THEN in the Voice Security Options screen	AND in the Thru-Dial Definition screen
all Thru-Dials	set the Monitor all Thru-Dials during Monitoring Period field to Yes or Always_Monitor	no action is required.
specified Thru-Dials	set the Monitor all Thru-Dials during Monitoring Period field to No	for the desired service, set the Monitor this Service during Monitoring Period field to Yes.

Field descriptions

You will find descriptions of the Voice Security Options fields on page 6-125. For descriptions of the fields in the Thru-Dial Definition screen, see Chapter 26, “Class of Service administration”.

Field descriptions (cont'd)

The following table only describes those fields which are used to set up Thru-Dial monitoring.

System Access Monitoring Period from (hh:mm)	
Description	This field indicates the monitoring period during which one or all of the following will be monitored: • mailbox logons for requested users • the use of Thru-Dial services • the use of a mailbox or Thru-Dial service from a specified CLID
Default	Start time: 23:00 End time: 05:00
Available on	Voice Security Options screen

Monitor All Thru-Dials during Monitoring Period	
Description	When this field is set to Yes, all accesses to the Thru-Dial service (from a mailbox, voice menu, or directly from a VSDN) during the system access monitoring period will result in a 10613 informational SEER. Included in this SEER is the CLID of the user. When this field is set to Always_Monitor, any access to the Thru-Dial service at any time will result in a class 106 informational SEER.
Default	No
Available on	Voice Security Options screen

Monitor this Service during Monitoring Period	
Description	When this field is set to Yes, all accesses to this Thru-Dial service during the system access monitoring period will result in a 10613 informational SEER. Included in this SEER is the CLID of the user.
Default	No
Available on	Thru-Dial Definition screen

Monitoring all Thru-Dials

To monitor all Thru-Dials, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Security Options.
3	Set the Monitor all Thru-Dials during Monitoring Period field to Yes or Always_Monitor.

IF you have set this field to	THEN go to
Yes	step 4.
Always_Monitor	step 5.

Step	Action
4	Set the monitoring period in System Access Monitoring Period from (hh:mm) field.
5	Press [Save].

Monitoring specific Thru-Dials

To monitor a specific Thru-Dial, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Security Options.
3	Set the Monitor all Thru-Dials during Monitoring Period field to No.
4	Set the monitoring period in System Access Monitoring Period from (hh:mm) field.
5	Press [Save].
6	Go to the Thru-Dial Definitions screen.
7	Select the thru-dial definition you want to modify or add. Fore more information on thru-dials, refer to the *Voice Services Application Guide* (NTP 555-7001-325).
8	Set the Monitor this Service during Monitoring Period field to Yes.
9	Press [Save].

CLID Monitoring

Introduction

Possible hacker activity may be detected by monitoring mailbox logins or thru-dials that have been attempted from a specified calling line ID (CLID).

You can specify the type of CLID (Internal or External) and a string of digits (up to 15) of a CLID. That is, you can specify the complete CLID, the area code only, or the area code and office code. Up to 12 CLIDs can be entered for each type of CLID format. For more information on CLID, see Chapter 17, “Dialing translations”.

How to do it

Use the Voice Security Options screen to set up CLID Monitoring.

IF you want to monitor	THEN in the Voice Security Options screen	AND in the Voice Security Options screen
CLIDs	set the Monitor CLIDs during Monitoring Period field to Yes or Always_Monitor	enter the numbers in the CLIDs to Monitor field.

Monitoring a subset of a CLID

If a subset of a CLID is to be monitored (an office code, for instance), this string of digits will be compared only to the beginning of the CLID and not with the number. Thus, if you want to monitor the office code, you must also specify the area code.

Remote notification of mailbox logons

When this feature is combined with the SEER Trigger Message feature, you can be notified through Remote Notification when a suspected unauthorized user attempts to access Thru-Dial or enters a particular mailbox.

Field descriptions

The following table only describes those fields which are used to set up CLID monitoring. For descriptions of all the Voice Security Options fields, see "Using the Voice Security Options screen" on page 6-125.

Monitor CLIDs during Monitoring Period	
Description	This field indicates whether CLIDs are to be monitored by the Voice Messaging Service during login or by the Thru-Dial service. This field also indicates when this monitoring should take place. When this field is set to No, CLIDs are not monitored, even if there are entries in the CLIDs to Monitor field. When this field is set to Yes, CLIDs are monitored during the system access monitoring period only. When this field is set to Always_Monitor, CLIDs are monitored at all times.
Default	No

CLIDs to Monitor	
Description	You can enter up to 12 CLIDs. These CLIDs are monitored by Voice Messaging on mailbox login or by the Thru-Dial service if the Monitor CLIDs during Monitoring Period is set to Yes or Always_Monitor.
Maximum length	CLIDs can be up to 15 digits in length.
Format	You can enter complete CLIDs, area codes only, or area codes and office codes. Do not include any dialing prefixes, such as ESN prefixes, in the numbers you enter.
Examples	4165551234 is a complete CLID. 416 is an area code. All CLIDs from this area code are monitored. 416555 is an area code and exchange code. All CLIDs in the 555 exchange in the 416 area code are monitored.
Default	None

SEERs issued

An informational SEER is issued if the CLID of a caller matches one of the numbers specified in the Voice Security Options screen during a mailbox login or Thru-Dial access. The informational SEERs can be 5562, 2262, or 10612. For more information on SEERs, refer to the *Maintenance Messages (SEERs)* (NTP 555-7001-510).

Procedure

To monitor calling line IDs, follow these steps.

Starting Point: The Meridian Mail Main Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Security Options.
3	Set the Monitor CLIDs during Monitoring Period field to Yes or Always_ Monitor.

IF you have set this field to	THEN go to
Yes	step 4.
Always_Monitor	step 5.

4	Set the monitoring period in the format hh:mm.
5	Enter the internal CLIDs to be monitored in the CLID Format—Internal block.
6	Enter the external CLIDs to be monitored in the CLID Format—External block.
7	Press [Save].

The Services Summary Traffic report

Introduction

This report provides statistics for each of the voice services installed on your system. It records the number of times a user dials a service (the number of accesses) during the reporting period and the average length of each access. The report records both direct and indirect accesses.

Direct accesses occur when a user dials the DN of the menu, announcement, or fax item.

Indirect accesses occur when a service is accessed from another service through a menu selection or a time-of-day controller.

For more information, see "Services Summary report" on page 31-12.

Report availability

This report is available on all systems.

Report frequency

Run this report regularly to check for unusually long Thru-Dial sessions or for unusual numbers of after-hours Thru-Dial sessions. These may be a sign that hackers are present on your system.

What to do

If you suspect hackers are accessing the Thru-Dial feature, first check how the Thru-Dial service is set up to see whether the Operational Measurements (OM) data are unusual. For example, if executives call in and access a Thru-Dial service, then you can expect an average number of calls. If this average is exceeded, it may be an indication of hacker activity.

If your research still suggests the presence of hackers, review the dialing restrictions for Thru-Dial. For details, refer to the *Voice Services Application Guide* (NTP 555-7001-325).

If you are using an access password for Thru-Dial, change the access password, and continue to monitor the Thru-Dial usage.

Section L: Equipment security

In this section

Overview	6-162
Switchroom access	6-163
Administration terminals	6-164
Meridian Mail and switch printouts	6-165

Overview

Introduction

This section of the chapter discusses security measures that you should exercise to safeguard the Meridian Mail and switch hardware.

General security measures

The following is a list of general security measures you can take to secure your Meridian Mail and PBX:

- Limit access to your switchroom and escort all visitors.
- Keep a list of authorized technicians on hand. Whenever a regular technician appears, ask for ID to ensure that he or she is still employed by the company.
- Establish procedures for temporary technicians. Ask the technician for ID and to sign in, and issue a visitor's badge. If the technician does not have a company ID, check with the company to ensure that the person is a valid employee.

Switchroom access

Introduction

When a switchroom is not secure, criminals can gain access to all your system resources. Their activity can be as benign as turning off printers or as malicious as removing cards from your switch and rendering your system inoperable.

Security measures

The following is a list of safety measures you should exercise:

- Physically lock the room in which your equipment is located.
- Use combination locks—hardkey locks can easily be broken. Nortel recommends using an electronic key and program to safeguard your equipment room.
- Change the combination regularly and only inform those who need to know the new combination.

Administration terminals

Introduction

There are two facilities provided for protecting against unauthorized access to the Meridian Mail administration terminal:

- the administration password
- hardware-based remote access restriction

Administration password

The administration terminal is password protected. When Meridian Mail is first installed, there is a default password. The first time you log on to the Meridian Mail administration terminal, you are forced to change this default password. You are recommended to change this password on a regular basis to maximize system security.

Passwords can be between 1 and 16 characters in length. However, it is recommended that the password be no less than seven characters in length. The longer the password, the less likely it is that someone will guess it.

Always log off before you leave the administration terminal, even if only for a short period.

Remote access restriction

If remote access is enabled on your system, anyone can dial in and commandeer your system. Remote access should not be enabled unless required (for example, for remote support personnel to work on your system).

Modular Option EC (ModOpEC) systems have an internal modem which is enabled using the <Ctrl> <w> key sequence. When a remote access session is in progress, local access is prohibited.

Non-EC systems are configured with an A/B switchbox between the terminal and the modem. When the switch is set to the modem setting, the system can be remotely accessed (but not from the local terminal). When the switch is set to the terminal setting, access is only possible from the local terminal. The switch is controllable at the site and must be switched manually.

Meridian Mail and switch printouts

Introduction

"*One man's garbage is another man's treasure*."

Anonymous

This is very true for the telecommunication criminal known as the "dumpster diver." These divers search through your garbage looking for printouts or records of your system's codes.

Security measures

Do not throw out call detail records and credit card receipts. Dispose of these materials, including switch printouts and old documentation, as you do any proprietary materials.

Chapter 7

User administration—an overview

In this chapter

Section A: Introduction to User Administration	7-3
Section B: New user planning	7-15

Section A: Introduction to User Administration

In this section

The User Administration menu	7-4
Types of users	7-7
Distribution lists	7-10
Limitations and guidelines	7-11
Support for multiple appearance DNs	7-12

The User Administration menu

The User Administration menu

This is the User Administration menu, the starting point for all user administration tasks. In this example of the screen, the Network Message Service (NMS) and Meridian Networking features are installed.

```
                    User Administration

          1  Local Voice User
          2  Remote Voice User
          3  Directory Entry User
          4  Distribution Lists
          5  Set Default User Administration Context

Select an item > 
Current context is: Unknown
     Exit
```

Local Voice User

This menu item allows you to add, view, modify, and delete local voice users. Local voice users have mailboxes on your local Meridian Mail site.

Remote Voice User

This menu item is displayed if the Meridian Networking feature is installed. It allows you to add, view, modify, and delete remote voice users. Remote voice users are users at remote sites that are added to your local site's database.

Directory Entry User

This menu item allows you to add, view, modify, and delete directory entry users. Directory entry users do not have mailboxes.

Distribution Lists

This menu item allows you to add, view, modify, and delete distribution lists. Distribution lists are used to send messages to a number of people.

Set Default User Administration Context

This menu item is displayed if the Network Message Service (NMS) feature is installed on your system. It allows you to select one of the NMS locations and make it the default (or current) location so that you can add users to it, or delete users from it.

Related chapters

This table directs you to the chapters that contain information about each of the items in the User Administration menu.

For the following option	Refer to
Local Voice User	Chapter 8, “Local voice users”
Remote Voice User	Chapter 9, “Remote voice users”
Directory Entry User	Chapter 10, “Directory entry users”
Distribution Lists	Chapter 11, “Distribution lists”
Set Default User Administration Context	Page 8-8 in “Local voice users”

Types of users

Three types of users

There are three types of users that you can add to Meridian Mail:

- local voice users
- remote voice users
- directory entry users

Local voice users

Local voice users have extensions on the local switch.

Local voice users have mailboxes with call answering and voice messaging capability. This means the following:

- If the user is away from his or her phone, callers are forwarded to the user's mailbox to leave a message.
- The user can compose and send voice messages to other users.

Voice Messaging interfaces

There are three Voice Messaging interfaces. Each customer can only use one of the installed interfaces. This is set up when the customer is added.

Interface	Description
MMUI	This is full-featured Voice Messaging that provides users with call answering and voice messaging capabilities.
VMUIF	This is a call answering interface intended for users who primarily need call answering capability only (although compose capability can be enabled in users' classes of service).
Hospitality	This interface is intended for the hospitality industry and is available only if Hospitality Voice Messaging is installed. It provides two specialized interfaces: one for guests and one for staff.

Remote voice users

Users can be added as remote voice users only if the Meridian Networking feature is installed.

When you add a user who is located at a remote Meridian Mail site as a remote voice user, you are adding that user to your local user database.

Benefits

The benefits of adding users at remote sites to your local site's database as remote voice users are as follows:

- Whenever 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 Name Dialing and Name Addressing to call and compose messages to remote voice users.
- While listening to a message left by a remote voice user, a local user can use Call Sender (press 9 on the keypad) to immediately call back the originator of the message.
- External callers can name-dial remote voice users (if this feature is enabled).
- Remote voice users can be added to distribution lists.

Types of remote voice users

There are two types of remote voice users.

User type	Description
Permanent	Permanent users remain on the system until you delete them using User Administration.
Temporary	If the number of temporary users exceeds the maximum, those who have not been active for a long time are automatically deleted by the system during nightly audits.

Directory entry users

Directory entry users are registered in the Meridian Mail directory. However, they do not have mailboxes. This means that they do not have access to call answering or voice messaging capability.

They can, however, be reached by features such as Name Dialing and Thru-Dialers.

Example

You have added Rupert Haynes as a directory entry user. If he does not answer his phone, callers are not forwarded to Meridian Mail in order to leave a message. He also cannot compose and send voice messages to other users.

However, when a caller accesses a thru-dial service and enters Rupert's extension (or name, if name dialing is used), his phone rings.

Distribution lists

Description

A distribution list is a list of mailbox numbers. When you enter the distribution list number during message composition, the message is sent to all of the mailbox numbers in the list.

Distribution lists, therefore, make it easier and quicker to address messages to groups of people. Once the distribution list has been created, you only need to enter one number during message composition (the distribution list number).

Personal versus system distribution lists

Users can create their own distribution lists from the telephone set. These are known as personal distribution lists.

The distribution lists that you create through User Administration are system distribution lists, and are created and maintained by the system administrator, not users.

You can add up to 120 mailbox numbers to a system distribution list. Users can add up to 99 mailbox numbers to personal distribution lists.

Limitations and guidelines

Multiple Administration Terminals

If the Multiple Administration Terminals (MAT) feature is installed, you can perform User Administration from a secondary terminal.

If more than one administrator accesses a user or distribution list at the same time, the administrator who first gained access to the user or list can modify the information. The other administrator can only view the information (no [Save] softkeys are displayed in the User Administration screens).

Nightly audits

Meridian Mail performs a system audit every day at 2:30 a.m. This audit can take anywhere from ten minutes to two hours. The more changes that have been made to the system since the last audit, the longer the audit will take.

> **CAUTION**
>
> **Risk of Interrupted Service**
>
> Do not perform user administration during the nightly audit. Doing so may cause loss of service.

Support for multiple appearance DNs

Description: MADN

A Multiple Appearance DN (MADN) is a directory number (DN) that is programmed on several phone sets.

Usage

Multiple Appearance DNs are typically used in customer support environments in which you want to ensure that calls are answered. MADNs allow more than one call to be handled at a time.

How MADNs work

A call to a multiple appearance DN rings a number of phone sets, increasing the chances that the call will be answered.

The primary phone

The telephone set on which the MADN is programmed as key 0 is considered the primary phone.

Example

DN 5000 is programmed on four Meridian 1/SL-1 terminal numbers (TNs):

- DN 5000 is programmed as key 3 on TN 0-0-1-0.
- DN 5000 is programmed as key 4 on TN 0-0-5-7.
- DN 5000 is programmed as key 0 on TN 26-0-4-2. This is the primary phone.
- DN 5000 is programmed as key 1 on TN 26-0-4-3.

A call comes in to the customer support center. All four telephone sets ring.

When someone answers the call, the other phones stop ringing. When another call comes in on DN 5000, the three remaining telephone sets ring even though the first call is still in progress.

How Meridian Mail treats MADNs

Multiple appearance DNs are treated as one DN by Meridian Mail. How the primary phone is programmed determines what happens to a call when it is not answered in the predetermined number of rings or when all telephones are busy.

Programming requirement

The primary phone must be programmed to forward to the voice messaging DN on busy and no answer conditions. Otherwise, calls will not get forwarded to Meridian Mail when all telephone sets are busy or when a call goes unanswered.

Section B: New user planning

In this section

Overview	7-16
Class of service planning	7-17
Distributing local voice users evenly over volumes	7-19
Guidelines for adding users to a system that has disk shadowing	7-21
Guidelines for adding a large number of users	7-22
How user models in pre-Release 9 systems are converted to classes of service	7-23

Overview

Introduction

This section describes how to plan the task of adding users to a newly installed system.

Planning tasks

Before you begin adding users to your system, you should do the following.

1. Identify the types of users that you will be adding to the system.

   Will you be adding remote voice users or directory entry users, or both, in addition to local voice users?
2. Classify local voice users into categories that serve as the basis for your classes of service.

   See “Class of service planning” on page 7-17.
3. If you have disk shadowing on some nodes but not on others, identify which local voice users should be put on the shadowed nodes.

   See “Guidelines for adding users to a system that has disk shadowing” on page 7-21.
4. If you are adding a large number of users (600 or more) within a 24-hour period, review the guidelines on page 7-22.

Class of service planning

Introduction

Classes of service (COSs) act as templates to simplify the process of adding and maintaining local voice users.

When you create a class of service, you specify three types of information about the users to which the class of service will be assigned:

- which features are enabled/disabled
- limitations and attributes
- which restriction/permission lists are applied to certain features

When you assign a class of service to a user, all of the attributes defined in the class of service are applied to the user.

When you modify a class of service, all users who are assigned to that class of service are immediately updated.

Example

These are some of the features you can enable/disable in classes of service:

- Delivery to Non-User
- Remote Notification
- AMIS Networking

These are some of the limitations and attributes you can specify:

- maximum lengths for composed and call answering messages
- maximum voice storage limit
- how long read messages are stored before being deleted
- whether invalid personal distribution list addresses are automatically deleted

You can assign restriction/permission lists to features such as

- Extension Dialing
- External Call Sender
- Custom Revert

When to create classes of service

Because each local voice user must be assigned to a class of service, classes of service must be defined before you begin adding local voice users to your system.

Classifying users

Classify your users into types, and then create classes of service that meet the needs and requirements of each type.

Example

You might create classes of service for different departments or jobs, or both, that have different usage profiles and requirements:

- Sales
- Engineering
- Marketing
- Manager
- Secretary

See also

For more information about classes of service, see Chapter 26, “Class of Service administration”.

Distributing local voice users evenly over volumes

Introduction

Meridian Mail systems can have from one to five nodes, each of which contains a hard disk drive for data storage. These disk drives are partitioned into volumes.

When you add a local voice user, the user must be assigned to a particular volume. This is where all user-related data and voice are stored, such as mailbox information, personal greetings, voice messages, and voice prompts.

User volumes

This table indicates user volume names and where they are distributed across the various nodes.

Number of Nodes →

Node # ↕

	1 Node	2 Nodes	3 Nodes	4 Nodes	5 Nodes
Node 1	VS2	VS2	VS2*	VS2*	VS2*
Node 2		VS202	VS202	VS202	VS202
Node 3			VS203	VS203	VS203
Node 4				VS204	VS204
Node 5					VS205

Note: The asterisk (*) indicates that the volume contains only voice prompts and is considered to be a system volume, not a user volume.

The default volume

When you press the [Add] softkey to enter the Add a Local Voice User screen, the volume that is selected as the default is the volume with the greatest amount of free space at that time. All users that you add during a single session are added to that volume by default, unless you specify otherwise.

When you exit the Add a Local Voice User screen and then reenter it, the system reassesses which volume has the most available space and that volume becomes the new default.

Recommendations

To guarantee an effective distribution of users, the following actions are recommended:

- Distribute local voice users across volumes randomly in such a manner that does not result in heavy users all being assigned to the same volume(s).
- Spread employees in the same department across a number of nodes (do not place them all on the same node). This way, if a node is taken out of service for troubleshooting, the entire department will not be affected.

Disk usage information

Monitor disk usage on a regular basis to ensure that user volumes do not fill up. This is done by generating the Disk Usage report.

For more information about the Disk Usage report, see "Disk Usage Detail report" on page 31-52 in Chapter 31, "Operational Measurements traffic reports."

Moving users from a full volume

If a volume becomes (nearly) full, you can use the Move User utility to move local voice users from one volume to another. This utility is accessible from the Tools menu.

Refer to *System Administration Tools* (NTP 555-7001-305) for details.

Guidelines for adding users to a system that has disk shadowing

Introduction

Disk shadowing is an optional feature that is available on the Modular Option EC platform. It provides protection against data loss in the event of disk failure.

How it works

This feature works by writing new information to two disks at the same time. If one disk fails, it is taken out of service without service interruption. Disks are shadowed on a node-by-node basis.

If a shadowed disk fails, voice messages of users on that node are not lost since they will be on the second disk of the shadowed pair.

Before you add users

Before adding users, you need to do the following.

1. Determine which nodes are shadowed and which are not.
2. Identify which users you want to put on shadowed nodes.

   Local voice users whose messages may not be critical can be placed on nonshadowed nodes.

Guidelines for adding a large number of users

Recommendation

Avoid adding a large number of users (1000 or more) within a 24-hour period. Every 24 hours, a nightly audit takes place between 2:30 a.m. and 5:00 a.m. When a large number of users is added between audits, the directory that stores user information can become unbalanced and perform less efficiently.

Guidelines

If you must add a large number of users between audits, follow these guidelines:

- Ensure that the number of local voice users to be added is within the engineering guidelines for the system.
- Add users in reverse alphabetical order.

  When you add users in alphabetical order, performance gradually degrades as you add more users. This degradation in performance is corrected when the next nightly audit occurs.
- Distribute local voice users across volumes as evenly as possible.
- If you add a lot of users who either belong to the same department or who have mailbox numbers beginning with the same numbers, the system will begin to slow down as you add more users. Therefore, try to add users in a more random fashion to avoid performance degradation.

System slowdown while adding users

If you notice that the system is slowing down as you add users, stop. You can force an audit from the Tools menu using the Rebalance Directory tool. However, do not force an audit during a busy traffic time. During a forced audit, you will not be able to add more users.

For more information about this utility, refer to *System Administration Tools* (NTP 555-7001-305).

How user models in pre-Release 9 systems are converted to classes of service

Introduction

Classes of service (COSs) replaced user models in Meridian Mail Release 9. Prior to Release 9, a user model was assigned to each user. However, if you modified the user model, it was changed for that user only. You could not propagate changes to a user model to all local voice users that were added using that model.

How user models are converted to COSs

When you convert to Meridian Mail 12 from a release prior to Meridian Mail 9, all existing local voice users are assigned to a personal class of service. This means that each user has a unique class of service that is not connected to any of the system classes of service. Therefore, local voice users must be reassigned to system classes of service after a conversion.

COS conversion utility

The COS Conversion utility is available from the Tools menu and should be used when converting from a system that used user models to one that uses classes of service.

For more information about this utility, refer to *System Administration Tools* (NTP 555-7001-305).

How it works

This utility checks each local voice user's personal class of service.

WHEN the personal COS	THEN
matches an existing system COS	the local voice user is assigned to the matching system COS.
does not match an existing system COS	the personal COS is used for that user.

How to use this utility

You can use the COS Conversion utility to do one or both of the following:

- View unassigned local voice users, and then create a system class of service based on the personal class of service.
- Assign unassigned users to defined system classes of service.

Chapter 8

Local voice users

In this chapter

Section A: Adding local voice users 8-3

Section B: Finding local voice users 8-45

Section C: Modifying and deleting local voice users 8-79

Section A: Adding local voice users

In this section

Integrated mailbox administration	8-4
Before you begin adding local voice users	8-5
Adding a local voice user	8-6
Setting the default administration context for NMS	8-8
Accessing the Add Local Voice User screen	8-10
The Add Local Voice User screen	8-13
Entering user information	8-15
Assigning a user to a class of service	8-20
Primary DN and extension DNs	8-24
The revert DN	8-26
See “Specifying the primary DN, extension DNs, the revert DN, and message waiting indication DN” on page 8-31.	8-28
Specifying the primary DN, extension DNs, the revert DN, and message waiting indication DN	8-31
Recording a personal verification for a user	8-34
Creating a remote notification schedule for a user	8-36
Setting other local voice user characteristics	8-39

Integrated mailbox administration

Description

Integrated Mailbox Administration (IMA) is a feature that allows you to add mailboxes for users at the Meridian 1 terminal. This feature was introduced in Release 9.0 of Meridian Mail and Release 19 of X11. In X11, this feature is known as Voice Mailbox Administration (VMBA).

Other types of users

The following types of mailboxes and users cannot be added using VMBA and, therefore, must be added through User Administration in Meridian Mail:

- guest mailboxes (Hospitality voice messaging)
- local voice users at satellite NMS locations
- remote voice users
- directory entry users

Fields you cannot change in User Administration

If you add mailboxes using VMBA, you cannot modify any of the following fields in Meridian Mail User Administration. These fields are controlled by VMBA on the Meridian 1.

X11 Field	Meridian Mail Field
DN	Mailbox Number, Primary DN
VMBA Class of Service	Class of Service
CPND Name	Last Name, First Name, Initials
Second DN	Second of the Extension DN fields
Third DN	Third of the Extension DN fields

If you change any of these fields in Meridian Mail, discrepancies may arise. Periodic audits are performed on the Meridian 1. During these audits, VMBA settings override any settings configured in Meridian Mail.

See also

For more information about the Integrated Mailbox Administration feature, see Appendix A, "Integrated Mailbox Administration".

Before you begin adding local voice users

Introduction

Before you begin adding local voice users, consider the following points.

Classes of service

All local voice users must be assigned to a class of service. Classes of service should be defined before you begin adding local voice users.

Have you created all of the necessary classes of services? If you have not, do the following:

- Create all the classes of service that you need.
  See Chapter 26, "Class of Service administration. "
- Add the classes of service to the system.
  See "Assigning Classes of Service to the system" on page 26-49.

Password for MMUI users

All MMUI users must have a password. When you add a new local voice user, the system assigns a default password (the user's mailbox number).

To make this initial default password more secure, you can enter a password prefix in the Voice Security Options screen. This prefix is added in front of the user's mailbox number to make initial passwords more difficult to guess.

Passwords for VMUIF users

A default password is not assigned to new VMUIF users. A VMUIF user that does not have a password can access Meridian Mail from his or her "home phone" only.

Users who want to be able to log in from any phone need a password. This includes users who want remote notification capability, since users need to be able to call in from any phone in order to log in and listen to messages.

You can either leave it up to users to create their own passwords from the telephone set or create a password for VMUIF users. See "Changing a user's password" on page 8-93.

Adding a local voice user

Introduction

Local voice users are added in the Add a Local Voice User screen. There are a number of things you must do in this screen in order to define a local voice user.

Procedure

This is a high-level procedure that lists the steps involved in adding a local voice user. Detailed step-by-step procedures are provided on the following pages.

Step	Action	Page
1	Do you want to add a number of users to an NMS location? • If yes, set the default administration context. • If no, go to step 2.	8-8
2	Access the Add Local Voice User screen.	8-10
3	Enter user information such as the user's first and last names.	8-15
4	Assign the user to a class of service.	8-20
5	Specify the following DNs for the user if necessary: • up to seven additional extension DNs • a revert DN • the MWI DN (if different from the mailbox number)	8-24
6	Record a personal verification for the user if necessary. **Note:** Most users record their own verifications.	8-34

Step	Action	Page
7	If remote notification is enabled for the user, create a remote notification schedule if necessary. **Note:** Users can create their own schedules from the telephone set.	8-36
8	Change the following if necessary: • If the interface is MMUI, disable/enable name dialing by external callers (default is enabled). • If Hospitality is installed, set the hospitality user class (default is guest). • If the interface is VMUIF, select the volume level. • If more than one language is installed, select the user's preferred language.	8-39
9	Save the local voice user.	8-43

Setting the default administration context for NMS

Introduction

When the Network Message Service (NMS) is installed, all local voice users are associated with a particular NMS location. You must specify this location whenever you

- add a new local voice user
- modify or delete an existing local voice user
- add a local voice user to a distribution list

The system default

The system default is the prime NMS location.

How to use the default administration context

If you want to add or delete a number of users to or from the same location, rather than entering the location for each user, you can make their location the default location (administration context). This means that you will not have to specify the location in the Add or Delete Local Voice Users screens for each user. The user will be automatically added to or deleted from the location that is specified as the default administration context.

How long the default context stays in effect

The new context stays in effect only as long as you remain in User Administration. Once you exit User Administration, the system resets the default administration context to the prime location.

You, therefore, need to set the default administration context whenever you enter User Administration if you plan on adding, modifying, or deleting a number of users to the same location.

Procedure

To set the default administration context, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select User Administration.
2	Select Set Default User Administration Context. **Result:** The Set Default User Administration Context Screen is displayed.
3	Move the cursor to the location you want to make the new default and press <spacebar> to select it.
4	Do you want to save the selected location as the new default administration context? • If yes, press [Save]. • If no, press [Cancel].

Accessing the Add Local Voice User screen

Mailbox numbers

To access the Add Local Voice User screen, you must enter the user's mailbox number.

Valid range

The mailbox number can be up to 18 digits long. It can be a number between 10 and 999999999999999999.

System addressing length

If the system addressing length is set to a non-zero value, the length of all mailbox numbers must equal the system addressing length.

The system addressing length is defined in the General Options screen.

Potential conflicts

Make sure mailbox numbers do not conflict with any of the following numbers:

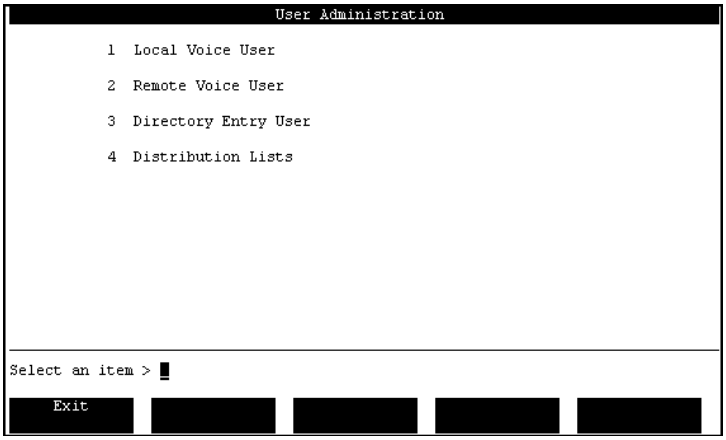
- the broadcast mailbox number (default is 5555)
- the network broadcast prefix
- other DNs
- the name dialing prefix (default is 11)
- the delivery to non-user prefix
- system distribution list numbers
- other mailbox numbers
- the AMIS compose prefix (default is 13)
- the personal distribution list prefix (VMUIF only)
- NMS location prefixes (if NMS is installed)
- networking prefixes (if networking is installed)

Procedure

To access the Add Local Voice User screen, follow these steps.

Starting Point: Main Menu

Step	Action
1	Select User Administration. **Result:** The User Administration Menu is displayed.



Step	Action
2	Select Local Voice User. **Result:** This screen is displayed if Integrated Mailbox Administration (IMA) is installed.

```
User Administration

To display the List of Local Voice Users select
the Find softkey followed by the List softkey.

WARNING: If the switch software release is X11R19 or later and
the IMA feature on the switch is enabled then the administration
of mailboxes can also be performed on the switch. Any additions,
modifications, or deletions of mailboxes done via Meridian Mail
Administration could be overridden by the switch administration
of these same mailboxes.

Select a softkey >

Exit   Add   View/Modify   Delete   Find
```

This screen is displayed if IMA is not installed.

```
User Administration

To display the List of Local Voice Users select
the Find softkey followed by the List softkey.

Select a softkey >

Exit   Add   View/Modify   Delete   Find
```

3	Press the [Add] softkey. **Result:** You are prompted for a mailbox number.
4	Enter the user's mailbox number and press <Return>. **Result:** The Add Local Voice User screen is displayed. The number you entered is used to fill in the following fields: Mailbox Number, Primary Extension DN, and Message Waiting Indication DN.

The Add Local Voice User screen

Feature-dependent fields

The fields that appear in this screen will vary depending on the following factors:

- When the interface is MMUI, the following fields are displayed (that are not applicable to VMUIF):
  - Department
  - Name Dialable by External Callers
- When the interface is VMUIF, the following field is displayed (that is not applicable to MMUI):
  - Volume level
- If Remote Notification is enabled in the user's class of service, the Remote Notification Schedules field is displayed.
- If NMS is installed, two additional fields are displayed at the top of the screen. These are Location Prefix and Location Name.
- If Hospitality is installed, the Hospitality User Class field is displayed after the Name Dialable by External Callers field.
- If multiple languages are installed, the Preferred Language field is displayed at the bottom of the screen.

The screen

This is the MMUI version of the Add Local Voice User screen. NMS is not installed in this example.

Part 1

```
                          User Administration
Add Local Voice User

Mailbox Number:      7787934            Volume ID:  202

Storage Used:        0

Last Name:           ____________________________________

First Name:          ____________________   Initials: _____

Department:          ________________________________

Class of Service:    Personal       001_Test_1     002_clerical   003_foreign
(Use More Detail Key)004_executive  005_field_supp 006_temporary

Primary DN:                                 7787934

Extension DNs:                              ____________________________
                                                                   MORE BELOW

 Save      Cancel     More Detail   Change      Voice
                                    Password
```

Part 2

```
                          User Administration                      MORE ABOVE
Add Local Voice User

Revert DN:                                  7000

Message Waiting Indication DN:              7551

Personal Verification Recorded (Voice):     No

Remote Notification Schedules:      ——      No Yes
(Use More Detail Key)

Monitor Mailbox during Monitoring Period:   No Yes

Name Dialable by External Callers:          No Yes

Logon Status:                               Disabled Enabled

Preferred Language:                         American_English
                                                                   MORE BELOW

 Save      Cancel     More Detail   Change      Voice
                                    Password
```

Entering user information

Introduction

The first step in adding a local voice user is to enter information about the user such as the user's first and last names, and the department to which the user belongs.

The Add Local Voice User screen

The dotted box highlights the fields in which you enter user information.

System with the Network Message Service (NMS)

```
                          User Administration
Add Local Voice User

Location prefix:      6            Location Name: prime

Mailbox Number:       7896                 Volume ID:  202

Storage Used:         0

Last Name:

First Name:                        Initials:

Department:

Class of Service:     Personal     001_ptt_load   013_Guest_Clas
(Use More Detail Key)

Primary DN:                                7896
                                                                MORE BELOW

   Save      Cancel     More Detail   Change      Voice
                                      Password
```

System without NMS

```
                          User Administration
Add Local Voice User

Mailbox Number:       7787934              Volume ID:  202

Storage Used:         0

Last Name:

First Name:                        Initials:

Department:

Class of Service:     Personal     001_Test_1     002_clerical   003_foreign
(Use More Detail Key) 004_executive 005_field_supp 006_temporary

Primary DN:                                7787934

Extension DNs:
                                                                MORE BELOW

   Save      Cancel     More Detail   Change      Voice
                                      Password
```

Field descriptions

This table describes the fields in which you enter user information.

Location Prefix	
Description	This prefix identifies the location in the NMS network at which the user is located.
Feature dependencies	This field is displayed only if Network Message Service (NMS) is installed.
See Also	See “Setting the default administration context for NMS” on page 8-8.
Location Name	
Description	This is a read-only field that indicates the name of the NMS location at which the user is located.
Mailbox Number	
Description	The user’s mailbox number
Default	The number you entered to access the Add Local Voice User screen
Maximum length	18 digits
Valid Range	10 to 999999999999999999
Mandatory	The user cannot be saved if this field is blank.
Volume ID	
Description	This is the hard disk volume to which the local voice user is assigned. This is the volume where user messages and user profiles are stored.
Default	The volume with the greatest amount of free space at the time the [Add] softkey is pressed.

Storage used	
Description	This read-only field indicates how many minutes of voice messages are stored for this user. This number is rounded up to the nearest minute.
VMUIF submailboxes	If submailboxes are enabled, this number also indicates the storage space taken up by all submailbox greetings and voice messages.

Last Name and First Name	
Description	The user's first and last names.
Maximum length	You can enter up to 41 characters for the last name and 21 characters for the first name.
Restricted characters	Do not use the following characters in these fields: plus sign (+), underscore (_), or question mark (?).
Attention	Make sure the spelling is correct and use alphanumeric characters only. These fields are used by name dialing and name addressing.

Initials	
Description	Initials can be used to distinguish users with identical first and last names. They are not used by the name dialing and name addressing feature.
Default	Blank If you leave this field blank, Meridian Mail will automatically insert the first initial of the user's first name when you save the user.
Maximum length	5 characters

Department	
Description	The user's department
Interface	MMUI only
Default	This field is blank for the first user you add. For subsequent users, this field defaults to the department entered for the last user you added.
Maximum length	31 characters Make the first 12 characters unique. If you want to later find users based on department, the List of Local Voice Users screen displays only the first 12 characters of the department name.
Restricted characters	Do not use the following characters in these fields: plus sign (+), underscore (_), or question mark (?).

Procedure

To enter user information, follow these steps.

Starting Point: The Add Local Voice User screen

Step	Action
1	Is NMS installed? • If yes, go to step 2. • If no, go to step 3.
2	Does the user belong to the location that is currently the default administration context? • If yes, go to step 3. • If no, enter the prefix of the NMS location at which the user is located in the Location Prefix field.
3	Is the current volume the volume to which you want to assign the user? • If yes, go to step 4. • If no, change the volume ID.
4	Enter the user's last name.
5	Enter the user's first name.

Step	Action
6	Enter the user's initials if needed to distinguish this user from another user with the same first and last name.
7	If the interface is MMUI, enter the user's department. **Note:** Make sure that the first 12 characters are unique.
8	Go to page 8-20 to continue defining the user.

Assigning a user to a class of service

Introduction

All local voice users must be assigned to a class of service. The class of service to which a user belongs determines things like the user's voice storage limit, the maximum message length, and the retention period for read messages.

Personal classes of service versus defined classes of service

You should assign most users to one of the classes of service you have already defined in Class of Service Administration. However, there may be some users with special requirements. Instead of defining a class of service for just one user (through Class of Service Administration), create a unique personal class of service here in the Add Local Voice User screen.

To assign a user to a defined class of service, see "Assigning a user to a defined class of service" on page 8-21.

To create a personal class of service for a user, see "Creating a personal class of service" on page 8-22.

Maintenance issues

Each personal class of service that you create will have to be maintained separately. You should, therefore, minimize the number of personal classes of service that you create.

Assigning a user to a defined class of service

To assign a user to a class of service that has been defined in Class of Service Administration, follow these steps.

Starting Point: The Add Local Voice User screen

Step	Action
1	Move your cursor to the Class of Service field, and select the class of service to which you want to assign the user.

```
                              User Administration
Add Local Voice User

Mailbox Number:      7787934            Volume ID:  202

Storage Used:        0

Last Name:           ____________________________________________

First Name:          ______________________   Initials: _____

Department:          ____________________________________

Class of Service:    Personal        001_Test_1     002_clerical   003_foreign
(Use More Detail Key)004_executive  005_field_supp 006_temporary

Primary DN:                                7787934

Extension DNs:                             ____________________________
                                                                   MORE BELOW

 Save      Cancel      More Detail     Change      Voice
                                      Password
```

2 Do you want to view the class of service definition to verify that this is an appropriate class of service for this user?
- If yes, go to step 3.
- If no, go to step 6.

3 Press the [More Detail] softkey.

Result: The Class of Service definition is displayed. You cannot modify any fields in this screen.

4 Review the class of service configuration to see if it is appropriate for the user.

5 Press the [Return to Basic Fields] softkey to return to the Add Local Voice User screen.

6 Go to page 8-24 to continue defining the local voice user.

Creating a personal class of service

To create a unique personal class of service for a user, follow these steps.

Starting Point: The Add Local Voice User screen

Step	Action
1	Move your cursor to the Class of Service field, and select Personal.

```
                              User Administration
Add Local Voice User

Mailbox Number:      7787934            Volume ID:  202

Storage Used:        0

Last Name:           ____________________________________

First Name:          ____________________   Initials: _____

Department:          ____________________________

Class of Service:    Personal       001_Test_1     002_clerical   003_foreign
(Use More Detail Key)004_executive  005_field_supp 006_temporary

Primary DN:                                 7787934

Extension DNs:                              ____________________
                                                                   MORE BELOW

 Save      Cancel     More Detail   Change      Voice
                                    Password
```

2 Press the [More Detail] softkey.

Result: The View Class of Service screen is displayed.

```
VMUI VM                       User Administration
View Class of Service

Class of Service Number:                    0

Class of Service Name:                      Personal

Voice Messaging Interface Type:             VMUI VMUIF

Personal Verification Changeable by User:   No Yes

Voice Storage Limit (minutes):              3

Maximum Message Length (mm:ss):             03:00

Delayed Prompts:                            No Yes

Dual Language Prompting:                    No Yes
                                                                   MORE BELOW
The Class of Service data will be saved only if the user is saved.

 Return to
 Basic Fields
```

3 Make the necessary modifications.

See Chapter 26, “Class of Service administration. ”

Step	Action
4	Press the [Return to Basic Fields] softkey when you are done modifying the class of service. **Result:** The Add Local Voice User screen is displayed. **Note:** The personal class of service will be saved when you save the local voice user.
5	Go to page 8-24 to continue defining the local voice user.

Primary DN and extension DNs

Introduction

The next step in adding a local voice user is to identify and define the extension DNs, including the primary DN, associated with the user.

Definition: extension DNs

An extension DN is a dialable number that, when dialed, rings a telephone.

When telephone set configuration is done in the Meridian 1, one or more DNs are defined for each telephone set. These are the extension DNs that you need to enter in Meridian Mail for each user.

Definition: primary DN

The primary DN is the "main" extension DN. All phones will have a primary DN.

The primary DN field

When you add a mailbox user, the Primary DN field is prefilled with the mailbox number that you entered to access the Add Local Voice User screen.

Call sender

When a user uses the Call Sender feature to call the sender of a message, Call Sender attempts to place the call to the primary DN only.

Note: The Call Sender feature can be supported on a network with CO trunks if

1. the network is configured in the "None" dialing plan
2. the "Dial Prefix" field is properly defined

Extension DNs

In addition to the primary DN, users can have a number of additional DNs programmed on their telephone sets. Meridian Mail supports seven additional extension DNs in addition to the primary DN, for a total of eight supported extension DNs.

Requirements

All DNs defined on a user's telephone set must be defined in Meridian Mail. If a call comes in on a non-primary extension DN which is not defined for the mailbox user, the mailbox will not be found and, as a result, messages cannot be left.

Mailboxes for users without phones

You can create a mailbox (add a local voice user) for people who do not have phones. To do this, make all DN fields blank.

Callers can use thru-dial services and express messaging to leave messages for these users. Users can then call into their mailbox from any phone in order to pick up voice messages.

Entering the extension DNs (primary and non-primary)

See "Specifying the primary DN, extension DNs, the revert DN, and message waiting indication DN" on page 8-31.

Duplicating extension DNs

Extension DNs should not duplicate any other DN already registered in Meridian Mail, either as a primary or a secondary DN. Meridian Mail prevents duplications, unless you have changed the "Allow Duplicate User DNs" field setting to Yes in the General Options screen (the default is No).

In the case of a duplication, Meridian Mail will only ring one of the DNs, not both, when the number is dialed.

The revert DN

Introduction

Another type of DN that is associated with each user is the revert DN.

Definition: revert DN

The revert DN is a directory number to which callers or users are transferred under certain specific conditions.

When the revert DN is used

The revert DN is used under two conditions:

Call answering

A caller can press “0” during a call answering session in order to transfer to another number (such as that of an attendant or secretary). This gives callers the chance to transfer to a person for assistance.

Mailbox thru-dial (extension dialing)

Mailbox thru-dial allows MMUI users to dial a number while they are logged in to their mailbox. The user enters “0” followed by the number. If the user waits for more than 2 seconds after entering “0,” he or she is transferred to the revert DN.

Revert for MMUI users

For MMUI users, you can specify a system-wide revert DN. This is done in the Attendant DN field in the General Options screen. The attendant DN is used if there is no revert DN defined for a user.

Custom revert

The MMUI telephone set interface has a feature called Custom Revert that allows MMUI users to define their own revert DNs. You can either

- allow users to define their own revert DNs

  or

- prohibit users from defining their own DNs and define one system-wide revert DN for all users

  In this case, you can still define a different revert DN for users in the Add or View/Modify Local Voice User screen.

Allowing MMUI users to define their own revert DNs

To allow MMUI users to define their own revert DNs through the telephone set, you must ensure that appropriate restrictions are applied to the Custom Revert feature so that users do not enter unauthorized DNs, such as long distance numbers.

To allow users to define their own revert DNs, you must do the following.

1. Define an Attendant DN in the General Options screen.

   This will serve as a default or backup for users who do not define a revert DN.

   See “Setting the attendant DN” on page 13-15.

2. Create a restriction/permission list that contains the restriction and permission codes you want to apply to the Custom Revert feature.

   This list cannot have all digits from 0 to 9 as restriction codes (the default). At least some digits have to be permitted to allow users to specify a DN.

   See the section “Restriction/Permission lists” on page 6-89.

3. In the classes of service to which you will be assigning users, select one of the above restriction/permission lists in the Custom Revert Restriction/Permission List field.

   This imposes the proper restrictions on the DNs that users try to define as their custom revert DNs.

   See “The Add Class of Service screen (MMUI)” on page 26-13.

4. Assign users to the appropriate class(es) of service.

5. Leave the Revert DN field blank in the Add Local Voice User screen, or enter the DN if you know where the user wants to revert calls.

Prohibiting MMUI users from defining revert DNs

To prohibit MMUI users from defining their own Revert DNs, you must assign a restriction/permission list that has the digits 0 to 9 as restriction codes to the custom revert feature.

This does not prevent you from defining a Revert DN in User Administration. It only affects telephone set definition of this DN.

To prohibit users from defining their own revert DNs, you must do the following.

1. Define an Attendant DN in General Options.

   This will serve as the revert DN for all users.

   See "Setting the attendant DN" on page 13-15.
2. Create a restriction/permission list in which the digits 0 to 9 are entered as restriction codes.

   See the section "Restriction/Permission lists" on page 6-89.
3. In the classes of service to which you will be assigning users, select the fully restricted restriction/permission list in the Custom Revert Restriction/Permission List field.

   See "The Add Class of Service screen (MMUI)" on page 26-13.
4. Assign users to the class of service.
5. Leave the Revert DN field blank in the Add Local Voice User screen if the Attendant DN is appropriate for the user; or, enter a different revert DN for the user.

Revert for VMUIF users

You cannot configure an Attendant DN if VMUIF is installed on the system. This means that if no Revert DN is defined for a VMUIF user, callers will not be able to press "0" to transfer to another DN.

For most VMUIF users, this is desirable. However, if revert capability is required for a user, you must define a Revert DN in the Add Local Voice User screen.

Entering the revert DN

See "Specifying the primary DN, extension DNs, the revert DN, and message waiting indication DN" on page 8-31.

The message waiting indication DN

Introduction

The next DN that is associated with a local voice user is the message waiting indication (MWI) DN.

Description

This is the DN to which the message waiting indication (flashing light or stutter dial tone) is sent

- when the user has a new voice message waiting to be read
- in a hospitality system, to notify the user of an external message

  An external message can be a written message that has been taken by the front desk, in which case the front desk clerk can turn a guest's MWI on in order to notify the guest of the message. The MWI can also be used to indicate that there is a message waiting that can be accessed through the hotel's TV messaging system.
- from an ACCESS application to indicate that a certain type of message has been received for the user (The message type depends on the ACCESS application.)

The default MWI DN

When you add a local voice user, this DN is automatically set to the number you entered as the mailbox number to access the Add Local Voice User screen. Typically, you leave this DN as it is so that it is the same as the mailbox number and primary DN. This is because you usually want the indication to go to the user's phone where the user will see the indication.

Choosing another MWI DN

However, there are a number of cases where the MWI DN should be configured as something other than the user's primary DN. These conditions are outlined in this table.

IF	THEN
the user wants the indication to go to another phone, such as a secretary's	enter the other person's primary DN as the MWI DN.
the user has a mailbox only, but no physical phone	make the MWI DN field blank.

Example

A senior executive has requested that her secretary be notified of her new voice messages so that the secretary can screen them. In the executive's mailbox setup, you enter the secretary's primary DN as the MWI DN. However, this is also the secretary's MWI DN. This means that the secretary will not be able to tell who new messages are for. The secretary will have to log on to both mailboxes to find out.

Entering the MWI DN

See "Specifying the primary DN, extension DNs, the revert DN, and message waiting indication DN" on page 8-31.

Specifying the primary DN, extension DNs, the revert DN, and message waiting indication DN

DN fields in the Add Local Voice User screen

The dotted box highlights the fields that are used to define user DNs.

```
                          User Administration                    MORE ABOVE
Add Local Voice User
Primary DN:                                  4142
Extension DNs:
Revert DN:
Message Waiting Indication DN:               4142
Personal Verification Recorded (Voice):      No
                                                                 MORE BELOW
Save        Cancel        More Detail        Change Password        Voice
```

Field descriptions

This table describes the fields you use to define DNs that are associated with a user.

Primary DN	
Description	When dialed, this number rings a user's telephone. It is the number used for Call Sender and Name Dialing.
Maximum length	30 digits
Default	This field is filled in with the mailbox number you entered to access the Add Local Voice User screen.
More information	See "Primary DN and extension DNs" on page 8-24.

Extension DNs	
Description	These fields allow seven secondary DNs to be entered. This means that a caller can dial any one of these numbers and reach the user.
Maximum length	30 digits
Default	Blank
More information	See “Primary DN and extension DNs” on page 8-24.

Revert DN	
Description	This is the DN to which calls are transferred when • a caller presses “0” during a call answering session • an MMUI user trying to use mailbox thru-dial waits more than 2 seconds after dialing the “0”
Maximum length	30 digits
Default	Blank
More information	See “The revert DN” on page 8-26.

Message Waiting Indication DN	
Description	This is the DN to which message waiting indications are sent when the user has unread voice messages, external HVS messages, or messages from an ACCESS application. This DN is usually the same as the user’s primary DN.
Conditions of display	This field is displayed if the Message Waiting Indication Options field in the user’s Class of Service is set to something other than None.
Default	The mailbox number you entered to access the Add Local Voice User screen
More information	See “The message waiting indication DN” on page 8-29.

Procedure To specify DNs for the user, follow these steps.

Starting Point: The Local Voice User screen

Step	Action
1	Does the user have a phone? • If yes, go to step 2. • If no, make all DN fields blank, and go to step 4.
2	Does the user have more than one DN? • If yes, go to step 3. • If no, go to step 4.
3	Enter the user's other DN(s) in the Extension DN fields. **Note:** For details, see "Primary DN and extension DNs" on page 8-24.
4	Enter a Revert DN if necessary. **Note:** For details, see "The revert DN" on page 8-26.
5	Change the Message Waiting Indication DN if necessary.

IF	THEN
the user should be notified of new messages at his or her phone	leave the default MWI DN (same as mailbox number).
the user does not have a phone	delete the MWI DN.
the user wants someone else to be notified of his or her messages	enter that person's DN in the MWI DN field.

Note: For more information, see "See "Specifying the primary DN, extension DNs, the revert DN, and message waiting indication DN" on page 8-31." on page 8-28.

6 Continue defining the local voice user.

IF you want to	THEN go to
record a personal verification for the user	page 8-34.
create a remote notification schedule for the user	page 8-36.
define other local voice user characteristics	page 8-39.

Recording a personal verification for a user

Introduction

Ideally, users should record personal verifications in their own voice. However, as administrator, you can record personal verifications from the administration terminal on behalf of users.

When to use

If the user belongs to a class of service in which the Personal Verification Changeable by User field is set to No and the user needs a personal verification, you will have to record it for him or her.

Procedure

To record a personal verification, follow these steps.

Starting Point: The Add Local Voice User screen

Step	Action
1	Put the cursor on the Personal Verification Recorded (Voice) field.
2	Press the [Voice] softkey.
3	Enter the extension of the phone you will use to record the verification, and press <Return>. **Result:** The phone rings.
4	Pick up the receiver. **Result:** The recording softkeys are displayed.
5	Press the [Record] softkey.
6	At the sound of the beep, speak the user's name (and, optionally, the user's extension). **Example:** *"Heather McGee at extension 8523."*
7	Press the [Stop] key to stop recording.
8	Do you want to verify the recording? • If yes, press the [Play] softkey. • If no, go to step 10.

Step	Action
9	Do you want to rerecord the verification? • If yes, repeat steps 5 to 8. • If no, go to step 10.
10	Do you need to record personal verifications for any other users? • If yes, press the [Return] softkey and do not hang up the receiver. The next time you press [Voice] to record another verification, you will not have to reenter the phone extension since the line has not been disconnected. • If no, press the [Disconnect] softkey and hang up the receiver.
11	Continue defining the local voice user.

IF you want to	THEN go to
create a remote notification schedule for the user	page 8-36.
define other local voice user characteristics	page 8-39.

Creating a remote notification schedule for a user

Introduction

The Remote Notification Schedules field is displayed if

- Outcalling is installed
- the Remote Notification Capability field in the user's class of service is set to Yes

User-defined versus administrator-defined

Users can create their own remote notification schedules from their telephone sets. You may, however, have to create remote notification schedules for users under the following conditions:

- The Remote Notification Keypad Interface field in the user's class of service is set to No, and the user cannot create his or her own schedule from the telephone set.
- A user does not want to use the telephone set interface to create a schedule and asks you to create it for him or her.
- New features in Meridian Mail 12 (concerning the type of remote notification a user receives) cannot be accessed through the telephone keypad interface, and your user requires them.

See also

For more information about remote notification schedules, refer to the *Outcalling Guide* (NTP 555-7001-320).

Procedure

To create a remote notification schedule for a user, follow these steps.

Starting Point: The Add Local Voice User screen

Step	Action
1	Put your cursor on the Remote Notification Schedules field and press the [More Detail] softkey. **Result:** The Outcalling fields are displayed.

```
                          User Administration
Add Local Voice User - Outcalling Fields

Current State of Remote Notification:   Off

Message Remote Notification Options:    Any Urgent

Business Days Schedule:

Period 1 from (hh:mm):       to (hh:mm):       Disabled Enabled
   For successful notification, mailbox login: Required NotRequired
   Target 1 DN:                                Phone Tone Voice Numeric Service
   Target 2 DN:                                Phone Tone Voice Numeric Service
   Target 3 DN: ____________________________   Phone Tone Voice Numeric Service

Period 2 from (hh:mm):       to (hh:mm):       Disabled Enabled
   For successful notification, mailbox login: Required NotRequired
   Target 1 DN:                                Phone Tone Voice Numeric Service
   Target 2 DN:                                Phone Tone Voice Numeric Service
                                                                    MORE BELOW
The Outcalling Fields data will be saved only if the user is saved.

 Return to
 Basic Fields
```

2 Create a business day schedule. For each required time period

a. Enter the from and to time.

b. Select Enabled to enable the time period.

c. Specify whether the user must log into their mailbox for Meridian Mail to consider the notification “successful” and stop its notification attempts.

d. Enter up to three target DNs.

e. For each target DN, specify the type of device.

For pagers, specify the Pager Callback Number. For general access pager services, enter the Pager ID Number.

3 Create a nonbusiness days schedule. For each required time period, repeat steps 2a. to 2d.

4 Do you need to create a temporary schedule?

- If yes, repeat steps 2a. to 2d. for each required time period.
- If no, go to step 5.

Step	Action
5	Press the [Return to Basic Fields] softkey to return to the basic fields in the Add Local Voice User screen.
6	Go to page 8-39 to continue defining the local voice user.

Setting other local voice user characteristics

Introduction

To finish defining a local voice user, you may have to modify some or all of the remaining fields:

- Monitor Mailbox during Monitoring Period
- Name Dialable by External Callers (MMUI only)
- Hospitality User Class (if Hospitality is installed and used by the customer)
- Volume Level (VMUIF only)
- Preferred Language (if multiple languages are installed)

Relevant fields: MMUI

The dotted box highlights the fields that are available when the interface is MMUI.

```
                          User Administration                    MORE ABOVE
Add Local Voice User

Revert DN:                                  7000

Message Waiting Indication DN:              7551

Personal Verification Recorded (Voice):     No

Remote Notification Schedules:              No Yes
(Use More Detail Key)

Monitor Mailbox during Monitoring Period:   No Yes

Name Dialable by External Callers:          No Yes

Logon Status:                               Disabled Enabled

Preferred Language:                         American English
                                                                   MORE BELOW

 Save      Cancel     More Detail   Change      Voice
                                    Password
```

Relevant fields: VMUIF

The dotted box highlights the fields that are available when the interface is VMUIF.

```
                    User Administration                    MORE ABOVE
Add Local Voice User

                                          ____________________________
                                          ____________________________

Revert DN:                                ____________________________

Message Waiting Indication DN:            5812_______________________

Personal Verification Recorded (Voice):   No

Monitor Mailbox during Monitoring Period: No Yes

Logon Status:                             Disabled Enabled

Volume Level                              Normal Loud Louder Loudest

Preferred Language:                       American_English Canadian_French

 Save    Cancel    More Detail    Change Password    Voice
```

Field descriptions

This table describes the fields that are used to define the remaining local voice user characteristics.

Monitor Mailbox during Monitoring Period	
Description	This field determines whether the mailbox is monitored for logons. This is a security feature that you can use when you suspect a hacker is trying to get into a particular mailbox. Typically, you would not enable this feature for new users, but only for existing users when hacker activity is suspected.
Interface	MMUI and VMUIF
Default	No
More information	See “Monitoring mailbox logins for suspected hacker activity” on page 8-94.

Name Dialable by External Callers	
Description	This field determines whether external callers can use name dialing to call the user. For users that have their calls screened, you might want to disable this feature. Otherwise, any caller can get through to the user's extension through a thru-dialer by entering their name.
Interface	MMUI
Default	Yes
Valid Options	Yes, No

Hospitality User Class	
Description	This field indicates whether the mailbox belongs to a staff member or guest.
Feature dependencies	This field is displayed only if Hospitality is installed.
Default	Guest
Valid Options	Guest, Staff

Volume Level	
Description	This is the volume level at which recorded prompts and voice messages are played.
Interface	VMUIF
Default	Normal
Valid Options	Normal, Loud, Louder, Loudest

Preferred Language	
Description	This is the language in which prompts are played to the user during a login session and to callers during call answering and express messaging.
Feature dependencies	This field is displayed only if more than one language is installed on the system.
System override	If the Default Language Overrides User's Preferred Language field in the Voice Messaging Options screen is set to Yes, call answering and express messaging prompts will be played to callers in the system default language. Prompts to the user while logged in to Meridian Mail continue to be played in the user's preferred language.
Default	The first language in the list
More information	See "The default language and the user's preferred language" on page 20-13.

Procedure

To set the remaining local voice user characteristics, follow these steps.

Starting Point: The Add Local Voice User screen

Step	Action
1	Do you want to prohibit external callers from using name dialing to call this user? • If yes, set the Name Dialable by External Callers field to No. • If no, leave the Name Dialable by External Callers field set to Yes.
2	If Hospitality is installed, are you adding a mailbox for a guest? • If yes, leave the Hospitality User Class as “Guest.” • If no, set the Hospitality User Class field to “Staff.”
3	If VMUIF is installed, change the volume level if necessary.
4	If more than one language is installed on the system, specify the user’s preferred language.
5	Do you want to save the local voice user as currently defined? • If yes, press the [Save] softkey. **Note:** If the entered DN is already in use by another Local Voice User or Remote Voice User, a warning message will appear. You can either modify the DN or press the [Save] softkey to save the DN for the user who originally had the DN. • If no, make any necessary changes and then press [Save], or press [Cancel] if you do not want to add this user.

Section B: Finding local voice users

In this section

Overview	8-46
Wildcard characters	8-47
Accessing the Find Local Voice Users screen	8-49
The Find Local Voice Users screen	8-50
Restrictions on how you can combine search criteria	8-67
Finding, listing, and printing local voice users	8-69
Reassigning a subset of local voice users to another class of service	8-73

Overview

Introduction

The Find function allows you to find a single local voice user or a subset of local voice users that meet the search criteria that you specify in the Find Local Voice User screen.

Examples of use

Here are some examples of how you can use the Find function. You can

- find Pierre LaMontaigne's user profile when you do not know his mailbox number
- find all users who belong to Class of Service 12 and reassign them to Class of Service 9
- find all users who are in the Marketing department that do not have Remote Notification capability, and reassign them to a class of service in which Remote Notification is enabled
- find all users who have exceeded their voice storage limit
- find all users whose primary DN differs from their MWI DN
- find all users in the Customer Documentation department, which has been renamed the Information Products department, so that you can update their department definitions
- find all users whose mailboxes are disabled (due to too many invalid logon attempts)
- find all users who have a specific voice storage limit so that you can either increase or decrease this limit
- find all users whose passwords have expired
- find all users on a particular volume (which is overloaded) so that you can move some of them to another volume

Wildcard characters

Definition: wildcard

A wildcard is a character that is used in a search string to represent an unknown or variable character or string of characters.

Purpose

Wildcards have two main purposes. They allow you to find

- a particular user when you do not know the user's mailbox number and have only partial information about the user
- a range of users

Types of wildcards

There are two wildcards that you can use.

Wildcard	Description
_	The underscore (_) replaces a single character.
+	The plus sign (+) replaces a string of characters.

Where you can use wildcards

You can enter wildcards in the following fields:

- Mailbox Number
- Last Name
- First Name
- Department
- Extension Number (DN)
- Message Waiting Indication DN

Examples

The following examples show how wildcards can be used to find a range of users.

You enter	Result
“210_” in the Mailbox Number field	All mailboxes in the range 2100 to 2109 are found.
“7_99” in the Extension Number field	Users with the following extension DNs are found: 7099, 7199, 7299, 7399, 7499, 7599, 7699, 7799, 7899, and 7999.
“3+” in the Mailbox Number field	All mailboxes beginning with 3 are found.
“+Engineering” in the Department field	Users belonging to all engineering departments are found (such as Software Engineering, Hardware Engineering, and Information Engineering).

Accessing the Find Local Voice Users screen

Procedure

To access the Find Local Voice Users screen, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select User Administration.
2	Select Local Voice User.
3	Press the [Find] softkey. **Result:** The Find Local Voice Users screen is displayed.

The Find Local Voice Users screen

Introduction

The fields in the Find Local Voice Users screen vary depending on the interface (MMUI or VMUIF).

The screen: MMUI version

This is how the Find Local Voice Users screen looks when the interface is MMUI.

Part 1

```
                              User Administration
Find Local Voice Users

Status:          Any Enabled Disabled Expired Violation
Mailbox Number:                                  Volume ID:    COS:
Last Name:
First Name:
Department:
Extension Number (DN):
Message Waiting Indication DN:
Revert DN:
Voice Storage Limit (minutes):
Read Message Retention (days):
Minimum Number of Invalid Logon Attempts:
Minimum Number of Days since Last Logon:
Minimum Number of Days since Pswd Changed:
Maximum Message Length (mm:ss):
Maximum CA Message Length (mm:ss):
Receive Composed Messages:                Any No Yes
                                                                    MORE BELOW
Select a softkey >

     Exit      Assign to COS      List       Print
```

Part 2

```
                              User Administration                   MORE ABOVE
Find Local Voice Users

Auto Logon:                                Any No Yes
Broadcast Capability:                      Any No Yes
Administrator Capability:                  Any No Yes
Internal Personal Greeting Recorded:       Any No Yes
External Personal Greeting Recorded:       Any No Yes
Temporary Absence Greeting Recorded:       Any No Yes
Auto Deletion of Invalid PDL Addresses:    Any No Yes
Personal Verification Changeable by User:  Any No Yes
Name Dialable by External Callers:         Any No Yes
Voice Storage Limit Exceeded:              Any No Yes
Primary DN differs from MWI DN:            Any No Yes
Delivery to Non-User Capability:           Any No Yes
Send Message via DNU if Mailbox Not Found: Any No Yes
Remote Notification Capability:            Any No Yes
Current State of Remote Notification:      Any On Off Off_by_Retry
                                           Off_by_Called_Party Off_due_to_BadDN
                                                                    MORE BELOW
Select a softkey >

     Exit      Assign to COS      List       Print
```

Part 3

```
                              User Administration                    MORE ABOVE
Find Local Voice Users

Name Dialable by External Callers:        Any No Yes
Voice Storage Limit Exceeded:             Any No Yes
Primary DN differs from MWI DN:           Any No Yes
Delivery to Non-User Capability:          Any No Yes
Send Message via DNU if Mailbox Not Found:Any No Yes
Remote Notification Capability:           Any No Yes
Current State of Remote Notification:     Any On Off Off_by_Retry
                                          Off_by_Called_Party Off_due_to_BadDN
Message Remote Notification Option:       Any All Urgent
Remote Notification Keypad Interface:     Any No Yes
Preferred Language:                       Any American_English
                                          Latin_American_Spanish
Message Waiting Indication Options:       Any None All Urgent
Personal Verification Status:             Any Not_Recorded Recorded

Display the List in MWI Status Format:    No Yes
Select a softkey >

     Exit      Assign to COS      List       Print
```

The screen: VMUIF version

This is how the Find Local Voice Users screen looks when the interface is VMUIF.

Part 1

```
VMUIF VM                      User Administration
Find Local Voice Users

Status:          Any Enabled Disabled Expired Violation
Mailbox Number:  ________________                Volume ID: ____  COS: ____
Last Name:       ____________________________________________________
First Name:      ____________________________
Extension Number (DN):                    ____________________________________
Message Waiting Indication DN:            ____________________________________
Revert DN:                                ____________________________________
Voice Storage Limit (minutes):            _____
Read Message Retention (days):            ____
Minimum Number of Invalid Logon Attempts: ___
Minimum Number of Days since Last Logon:  ___
Maximum Message Length (mm:ss):           _________
Maximum CA Message Length (mm:ss):        _________
Maximum Personal Greeting Length (mm:ss): _________
Maximum Number of SubMailboxes:
Login from Call Answering:                Any No Owner Group
                                                                   MORE BELOW
Select a softkey >

     Exit      Assign to COS      List       Print
```

Part 2

```
VMUIF VM                    User Administration                    MORE ABOVE
Find Local Voice Users

Receive Messages for Call Answering:      Any No Yes
Call Sender:                              Any No Yes
Calls were Rejected after Mailbox Full:   Any No Yes
Personal Greeting Recorded:               Any No Yes
Compose Capability:                       Any No Yes
Receive Composed Messages:                Any No Yes
Auto Logon:                               Any No Yes
Broadcast Capability:                     Any No Yes
Voice Storage Limit Exceeded:             Any No Yes
Primary DN differs from MWI DN:           Any No Yes
Delivery to Non-User Capability:          Any No Yes
Send Message via DNU if Mailbox Not Found:Any No Yes
Remote Notification Capability:           Any No Yes
Current State of Remote Notification:     Any On Off Off_by_Retry
                                          Off_by_Called_Party Off_due_to_BadDN
Message Waiting Indication Options:       Any None All Urgent
                                                                   MORE BELOW
Select a softkey >

   Exit      Assign to COS      List       Print
```

Part 3

```
VMUIF VM                    User Administration                    MORE ABOVE
Find Local Voice Users

Personal Greeting Recorded:               Any No Yes
Compose Capability:                       Any No Yes
Receive Composed Messages:                Any No Yes
Auto Logon:                               Any No Yes
Broadcast Capability:                     Any No Yes
Voice Storage Limit Exceeded:             Any No Yes
Primary DN differs from MWI DN:           Any No Yes
Delivery to Non-User Capability:          Any No Yes
Send Message via DNU if Mailbox Not Found:Any No Yes
Remote Notification Capability:           Any No Yes
Current State of Remote Notification:     Any On Off Off_by_Retry
                                          Off_by_Called_Party Off_due_to_BadDN
Message Waiting Indication Options:       Any None All Urgent
Personal Verification Status:             Any Not_Recorded Recorded

Display the List in MWI Status Format:    No Yes

Select a softkey >

   Exit      Assign to COS      List       Print
```

Field descriptions

These are the fields in the Find Local Voice Users screen that you can fill in to specify your search criteria.

Status	
Description	Use this field to find users with a particular mailbox status.
Default	Any
Valid Options	Any, Enabled, Disabled, Expired, Violation • *Any* finds all users. • *Enabled* finds all users whose mailboxes are enabled. • *Disabled* finds all users whose mailboxes have been disabled from the MMI or due to too many invalid logon attempts per mailbox. This maximum logon attempts value is defined in the Voice Security Options screen. • *Expired* finds all users whose passwords have expired. • *Violation* finds all users whose maximum number of invalid logon attempts per session has been reached or exceeded. This maximum is defined in the Voice Security Options screen.

Mailbox Number	
Description	Use this field to find users within a certain range of consecutive mailbox numbers. This requires the use of wildcards.
Maximum Length	You can enter up to 18 characters. IF NMS, Meridian Networking, or Enterprise Networking is installed, you can enter up to 28 characters. This is because you need to enter the location/network prefix and the mailbox number.

Volume ID	
Description	Use this field to find all users on a particular volume.
Default	Blank
Valid Options	Any valid user volume

COS	
Description	Use this field to find all users who are assigned to a particular class of service.
Default	Blank
Valid Options	Any class of service that has been created and assigned to the system
See Also	If you enter a number in this field, you cannot use any of the fields which concern COS-controlled features. See “Restrictions on how you can combine search criteria” on page 8-67.

Last Name	
Description	Use this field if you want to find a particular user. Use wildcards if you are unsure of the exact spelling.
Default	Blank

First Name	
Description	Use this field if you want to find a particular user. Use wildcards if you are unsure of the spelling.
Default	Blank

Department	
Description	Use this field to find users who belong to a particular department. Use wildcard characters if you are unsure of the exact name or spelling, or if you want to find users in a number of similarly named departments.
Interface	MMUI only
Default	Blank

Extension Number (DN)	
Description	Use this field if you want to find users with a particular primary extension DN. Use wildcards to find users within a range of DNs.
Default	Blank

Message Waiting Indication DN	
Description	Use this field if you want to find users with a particular message waiting indication DN.
Default	Blank

Revert DN	
Description	Use this field to find users who have a specific Revert DN.
Default	Blank
Maximum Length	You can enter a DN up to 30 digits in length.

Voice Storage Limit (minutes)	
Description	Use this field to find users that have a specific voice storage limit.
Default	Blank
Valid Range	1 to 360

Read Message Retention (days)	
Description	Use this field to find users who have their messages automatically deleted after a specified number of days. ***Note:*** The number of days that a message is stored may be set in either the Maximum Read Message Retention field of the customer's Voice Messaging Options or in the Read Message Retention field in the user's Class of Service. When searching with this parameter, the smaller of the two values is used.
Default	Blank
Valid Range	0 to 99

Minimum Number of Invalid Logon Attempts	
Description	Use this field to find users who have at least the specified number of invalid logon attempts. This field is useful for monitoring possible attempts at unauthorized logon.
Default	Blank
Valid Range	0 to 99

Minimum Number of Days since Last Logon	
Description	Use this field to find users who have not logged into their mailbox in at least the specified number of days.
Default	Blank
Valid Range	0 to 99

Minimum Number of Days since Pswd Changed	
Description	Use this field to find users who have not changed their mailbox logon password in at least the specified number of days.
Interface	MMUI only
Default	Blank
Valid Range	0 to 99

Maximum Message Length (mm:ss)	
Description	Use this field to find users who have a specific maximum allowable message length. This is for composed voice messages.
Default	Blank
Valid Range	00:30 to 99:00 in 10-second increments

Maximum CA Message Length (mm:ss)	
Description	Use this field to find users who have a specific maximum allowable call answering message length. These are messages left by callers.
Default	Blank
Valid Range	00:30 to 99:00 in 10-second increments

Maximum Personal Greeting Length (mm:ss)	
Description	Use this field to find users who have a specific maximum personal greeting length.
Interface	VMUIF only
Default	Blank
Valid Range	00:30 to 05:00 in 10-second increments

Maximum Number of SubMailboxes	
Description	Use this field to find users who have a specific maximum number of submailboxes.
Interface	VMUIF only
Default	Blank
Valid Range	0 to 8

Login from Call Answering	
Description	Use this field to find users who are allowed, or not allowed, to log in to their own mailbox while in a call answering session.
Interface	VMUIF only
Default	Any
Valid Options	Any, No, Owner • *Any* finds all users. • *No* finds users who are not allowed to log in to their mailbox during a call answering session. • *Owner* finds users who are allowed to log in only if they are connected to their own mailbox.

Receive Messages for Call Answering	
Description	Use this field to find users who are allowed, or not allowed, to receive call answering messages.
Interface	VMUIF only
Default	Any
Valid Options	Any, No, Yes

Call Sender	
Description	Use this field to find users who have, or do not have, the capability to call the sender of a message.
Interface	VMUIF only
Default	Any
Valid Options	Any, No, Yes

Calls were Rejected after Mailbox Full	
Description	Use this field to find users who have, or have not had, calls rejected because their mailbox is full.
Interface	VMUIF only
Default	Any
Valid Options	Any, No, Yes

Personal Greeting Recorded	
Description	Use this field to find users who have, or do not have, a personal greeting recorded.
Interface	VMUIF only
Default	Any
Valid Options	Any, No, Yes

Compose Capability	
Description	Use this field to find users who are allowed, or not allowed, to compose messages.
Interface	VMUIF only
Default	Any
Valid Options	Any, No, Yes

Receive Composed Messages	
Description	Use this field to find users who are allowed, or not allowed, to receive composed messages.
Default	Any
Valid Options	Any, No, Yes

Auto Logon	
Description	Use this field to find users who are allowed, or not allowed, to log in to their mailbox without entering a mailbox number or password.
Default	Any
Valid Options	Any, No, Yes

Broadcast Capability	
Description	Use this field to find users who have, or do not have, broadcast capability.
Default	Any
Valid Options	Any, No, Yes

Network Broadcast Capability	
Description	Use this field to find users who have, or do not have, network broadcast capability. ***Note:*** This field is displayed only if the Networking feature is installed and enabled for the customer.
Interface	MMUI only
Default	Any
Valid Options	Any, No, Yes

Administrator Capability	
Description	Use this field to find users who have, or do not have, administrator capability.
Interface	MMUI only
Default	Any
Valid Options	Any, No, Yes

Internal Personal Greeting Recorded	
Description	Use this field to find users who have, or do not have, an internal personal greeting recorded.
Interface	MMUI only
Default	Any
Valid Options	Any, No, Yes

External Personal Greeting Recorded	
Description	Use this field to find users who have, or do not have, an external personal greeting recorded.
Interface	MMUI only
Default	Any
Valid Options	Any, No, Yes

Temporary Absence Greeting Recorded	
Description	Use this field to find users who have, or do not have, a temporary absence greeting recorded. ***Note:*** If the Temporary Absence Greeting expiry date has passed, then the corresponding mailbox field will be reset to No when the user logs in to their mailbox.
Interface	MMUI only
Default	Any
Valid Options	Any, No, Yes

Auto Deletion of Invalid PDL Addresses	
Description	Use this field to find users who have, or do not have, mailboxes with the capability to automatically delete invalid addresses from personal distribution lists.
Interface	MMUI only
Default	Any
Valid Options	Any, No, Yes

Personal Verification Changeable by User	
Description	Use this field to find users who have, or do not have, the capability to change their personal verification.
Interface	MMUI only
Default	Any
Valid Options	Any, No , Yes

Name Dialable by External Callers	
Description	Use this field to find users who can, or cannot, be name dialed by external callers.
Interface	MMUI only
Default	Any
Valid Options	Any, No, Yes

Voice Storage Limit Exceeded	
Description	Use this field to find users who have, or have not, exceeded their voice storage limit.
Default	Any
Valid Options	Any, No, Yes

Primary DN differs from MWI DN	
Description	Use this field to find users whose primary DN and MWI DN are different or identical.
Default	Any
Valid Options	Any, No, Yes

Delivery to Non-User Capability	
Description	Use this field to find users who have, or do not have, delivery to nonuser capability.
Feature dependencies	This field is displayed only if Outcalling is installed.
Default	Any
Valid Options	Any, No, Yes

Send Message via DNU if Mailbox Not Found	
Description	Use this field to find users who have, or do not have, implicit DNU capability.
Feature dependencies	This field is displayed if Outcalling is installed.
Default	Any
Valid Options	Any, No, Yes

Remote Notification Capability	
Description	Use this field to find users who have, or do not have, remote notification capability.
Feature dependencies	This field is displayed if Outcalling is installed.
Default	Any
Valid Options	Any, No, Yes

Current State of Remote Notification	
Description	Use this field to find users according to their current state of remote notification.
Default	Any
Feature dependencies	This field is displayed if Outcalling is installed.
Valid Options	Any, On, Off, Off_by_Retry, Off_by_Called_Party, Off_due_to_BadDN • *Any* finds all users. • *On* finds all users whose current remote notification state is on. • *Off* finds all users whose current remote notification state is off. • *Off_by_Retry* finds all users whose remote notification state has been turned off after reaching the maximum number of retries. • *Off_by_Called_Party* finds all users whose remote notification state has been turned off by the called party. • *Off_due_to_BadDN* finds all users whose remote notification state has been turned off because a nonfunctional DN was called.

Message Remote Notification Option	
Description	Use this field to find users who are notified when a message is deposited in their mailbox.
Feature dependencies	This field is displayed if Outcalling is installed.
Interface	MMUI only
Default	Any
Valid Options	Any, All, Urgent • *Any* finds all users. • *All* finds all users who are notified when any message is deposited in their mailbox. • *Urgent* finds all users who are notified only when a message marked as Urgent is deposited in their mailbox.

Remote Notification Keypad Interface	
Description	Use this field to find users who have, or do not have, the capability to set up their own remote notification schedules.
Feature dependencies	This field is displayed if Outcalling is installed.
Interface	MMUI only
Default	Any
Valid Options	Any, No, Yes

Receive AMIS Open Network Messages	
Description	Use this field to find users who are allowed, or not allowed, to receive AMIS open network messages.
Feature dependencies	This field is displayed if AMIS is installed.
Default	Any
Valid Options	Any, No, Yes

Compose/Send AMIS Open Network Messages	
Description	Use this field to find users who are allowed, or not allowed, to compose and send AMIS open network messages.
Feature dependencies	This field is displayed only if AMIS networking is installed.
Default	Any
Valid Options	Any, No, Yes

Preferred Language	
Description	Use this field to find users who have a specific preferred language.
Feature dependencies	This field is displayed only if more than one language is installed.
Default	Any
Valid Options	Any one of the listed installed languages

Message Waiting Indication Options	
Description	Use this field to find users by when they receive their message waiting indication for new messages, depending on priority.
Default	Any
Valid Options	Any, None, All, Urgent • *Any* finds all users. • *None* finds all users who do not receive a message waiting indication. • *All* finds all users who receive a message waiting indication for any message. • *Urgent* finds all users who receive a message waiting indication only for messages marked as Urgent.

Personal Verification Status	
Description	Use this field to find users who do not have, or have, a recorded personal verification.
Default	Any
Valid Options	Any, Not Recorded, Recorded

Display the List in MWI Status Format

Description

Use this field to select the format in which you want the list of found users to be displayed or printed. Your selection determines the kind of information that is displayed for each found user.

Default

No

Valid Options

No, Yes

- ***No*** displays the list in General format.

```
User Administration
List of Local Voice Users
                                                          Storage Personal
                                                     COS  Used    Verific.
 Name          Mailbox                Department     Num. (mins)  Recorded
▌Gabriel,David 7555                   Hardware Eng     2     0     No
 Hardy,William 7557                   Hardware Eng     1     0     No
 Jones,Peter   7554                   Hardware Eng     2     0     No
 LaMontaigne,P 7610                   Hardware Eng     1     0     No
 Roberts,Erica 7556                   Hardware Eng     3     0     No

Select a softkey >
[Exit] [Toggle Cos Assignment] [View/Modify] [Delete] [Voice]
```

- ***Yes*** displays the list in MWI Status format.

```
User Administration
List of Local Voice Users (MWI Status)
                                                  Read  Unread  Text  MWI
 Name          DN                Mailbox          Msgs  Msgs    Msgs  Status
▌Gabriel,Davi  7555              7555               0     0       0   Off
 Hardy,Willia  7557              7557               0     0       0   Off
 Jones,Peter   7554              7554               0     0       0   Off
 LaMontaigne,  7610              7610               0     0       0   Off
 Roberts,Eric  7556              7556               0     0       0   Off

Select a softkey >
[Exit] [Toggle Cos Assignment] [View/Modify] [Delete] [Voice]
```

Restrictions on how you can combine search criteria

Restriction

If you enter a Class of Service number in the COS field, you cannot use any of the class of service feature fields that appear in the Find Local Voice Users screen. If you do so, a message notifies you that this type of search is not allowed.

Rationale

This prevents you from entering self-contradictory combinations that would result in no users being found.

Example

If you enter 12 in the COS field and set DNU Capability to Yes, but DNU is disabled in that class of service, you have a conflict which results in no users being retrieved.

Class of Service fields in the Find screen

The following fields in the Find Local Voice User screen are class of service fields and, therefore, cannot be used in combination with the COS field:

- Voice Storage Limit
- Read Message Retention Time
- Maximum Message Length
- Maximum Call Answering Message Length
- Maximum Personal Greeting Length (VMUIF only)
- Maximum Number of SubMailboxes (VMUIF only)
- Login from Call Answering (VMUIF only)
- Receive Messages for Call Answering (VMUIF only)
- Call Sender (VMUIF only)
- Compose Capability (VMUIF only)
- Receive Composed Messages
- Auto Logon
- Broadcast Capability
- Network Broadcast Capability (MMUI only)
- Administrator Capability (MMUI only)
- Auto Deletion of Invalid PDL Addresses (MMUI only)
- Personal Verification Changeable by User (MMUI only)
- Delivery to Non-User Capability (Outcalling feature)

- Send Message via DNU if Mailbox Not Found (Outcalling feature)
- Remote Notification Capability (Outcalling feature)
- Remote Notification Keypad Interface (MMUI only, Outcalling feature)
- Receive AMIS Open Network Messages (AMIS feature)
- Compose/Send AMIS Open Network Messages (AMIS)
- Message Waiting Indication Options

Finding, listing, and printing local voice users

Introduction

You can enter many different combinations of search criteria in the Find Local Voice Users screen.

The procedure that begins on page 8-70 is generic and applies to all types of searches. Several examples follow this procedure to show you how you would perform certain kinds of searches.

Purpose

You can use the find function in order to

- list the found users on the screen
- print a list of the found users
- reassign the found users to another class of service
- view or modify any of the found local voice users
- delete any of the found local voice users
- record a personal verification for any of the found local voice users

Reassigning users to another COS

If you want to reassign found local voice users to another class of service, see "Reassigning a subset of local voice users to another class of service" on page 8-73, and use that procedure instead of this one.

Specifying search criteria

You only need to change a search field if that field is part of your search criteria. All other fields should be left so that they display their default setting (blank or Any). When you leave a field at its default setting, it is disregarded in the search.

Example

You want to find all users in a particular department that have remote notification capability. You leave all other fields set to their default values.

Since, for example, Delivery to Non-User capability was not changed from its default value of Any, users that have it enabled and users who do not have it enabled will be found. Delivery to Non-User capability is not a relevant search criteria.

Procedure

This is a generic procedure that describes the steps to perform any kind of search.

Starting Point: The Find Local Voice Users screen

Step	Action
1	Determine the search criteria that will find all of the users you are looking for.
2	Fill in the necessary fields in order to define your search criteria. **Note:** Field descriptions begin on page 8-53.
3	Select the format in which you want to display or print the list of found users.

IF you want to	THEN set
see the following information • mailbox number • department • COS number • storage used • if the user has a personal verification	the Display the List in MWI Status Format field to No.
see the following information • DN • mailbox number • number of read messages • number of unread messages • number of text messages • the MWI status	the Display the List in MWI Status Format field to Yes.

Step	Action
4	List, print, or assign found users to another class of service.

IF you want to	THEN
list the found users	go to step 5.
print the found users	go to step 8.
assign found users to another COS	go to page 8-73.
cancel the search	press [Exit].

Step	Action
5	Press the [List] softkey. **Result:** The List of Local Voice Users screen is displayed.

```
                              User Administration
List of Local Voice Users
                                                                  Storage Personal
                                                            COS   Used    Verific.
  Name           Mailbox                      Department    Num.  (mins)  Recorded
  Gabriel,David  7555                         Hardware Eng    2      0      No
  Hardy,William  7557                         Hardware Eng    1      0      No
  Jones,Peter    7554                         Hardware Eng    2      0      No
  LaMontaigne,P  7610                         Hardware Eng    1      0      No
  Roberts,Erica  7556                         Hardware Eng    3      0      No

Select a softkey >

 Exit   Toggle Cos Assignment   View/Modify   Delete   Voice
```

6 Do you want to modify or delete a local voice user or record a personal verification?

- If yes, go to step 7.
- If no, press [Exit] to return to the Find Local Voice Users screen.

7 Select the user by moving your cursor to the user's name and pressing the <spacebar>.

IF you want to	THEN press	AND go to
view or modify a local voice user	[View/Modify]	page 8-80.
delete a local voice user	[Delete]	page 8-97.
record a personal verification for the user	[Voice]	page 8-34.

8 Press the [Print] softkey.

Result: The Printing softkeys are displayed.

9 Do you want to continue printing?

- If yes, press the [Continue Printing] softkey.

  Note: You can stop printing once started by pressing [Cancel Printing].
- If no, press the [Cancel Printing] softkey.

Example 1

You want to find and print all users in the Marketing department who have exceeded their voice storage limit.

Step	Action
1	Enter Marketing in the Department field.
2	Set Voice Storage Limit Exceeded to Yes.
3	Do you want the list in MWI status format? • If yes, set the Display the List in MWI Status Format field to Yes. • If no, set the Display the List in MWI Status Format field to No.
4	Press [Print]. **Result:** A list of the found users is printed.

Example 2

You want to find and list all users assigned to class of service 12 who have not recorded a personal verification.

Step	Action
1	Enter 12 in the COS field.
2	Set Personal Verification Status to Not_Recorded.
3	Do you want the list in MWI status format? • If yes, set the Display the List in MWI Status Format field to Yes. • If no, set the Display the List in MWI Status Format field to No.
4	Press [List]. **Result:** The found users are listed on the screen.

Reassigning a subset of local voice users to another class of service

When to use

Use this procedure when you want to

- find a group of local voice users that meet a certain set of search criteria and reassign them to another class of service
- find all users in a particular class of service and reassign them to a different class of service

Toggle COS assignment

If you want to reassign users who meet a certain set of search criteria to another class of service, you should verify the list of found users before you actually reassign them.

You may find that you have not found all required users, in which case you will have to redefine the search criteria; or, you may find that you have found some users who you do not want to reassign.

If you do not want to reassign some of the found users to another class of service, you can use the [Toggle COS Assignment] softkey to deselect them.

Reassigning users from one COS to another

If you want to reassign users from one class of service to another, you must enter the class of service number in the COS field. You will not be able to use any of the other class of service fields in the Find Local Voice Users screen. For a list of these fields, see “Restrictions on how you can combine search criteria” on page 8-67.

Reassigning users to another COS

To reassign found local voice users to another class of service, follow these steps.

Starting Point: The Find Local Voice Users screen

Step	Action
1	Do you want to reassign users in one class of service to another class of service? • If yes, enter the users' current class of service number in the COS field and go to step 11. • If no, go to step 2.
2	Fill in the necessary fields to define your search criteria. **Attention:** If you enter a number in the COS field, you cannot use any of the other class of service fields in this screen. **Note:** Field descriptions begin on page 8-53.
3	Select the format in which you want to display or print the list of found users.

IF you want to	THEN set
see the following information • mailbox number • department • COS number • storage used • personal verification status	the Display the List in MWI Status Format field to No.
see the following information • DN • mailbox number • number of read messages • number of unread messages • number of text messages • the MWI status	the Display the List in MWI Status Format field to Yes.

Step	Action
4	Press the [List] softkey. **Result:** The List Local Voice Users screen is displayed.

```
                              User Administration
List of Local Voice Users
                                                                 Storage Personal
                                                            COS  Used    Verific.
  Name           Mailbox                      Department    Num. (mins)  Recorded
  Lawrence,Dona  7604                         Marketing       1     0     No
  Miller,June    7605                         Marketing       1     0     No
  Samuels,Jack   7602                         Marketing       1     0     No
  Wharton,Ellen  7603                         Marketing       1     0     No

Select a softkey >

 Exit   Toggle Cos Assignment   View/Modify   Delete   Voice
```

5 Does the list contain all of the users you want to reassign?

- If yes, go to step 6.
- If no, redefine the search criteria.

  Press [Exit] to return to the Find screen, and repeat steps 2 to 4 until all users you want to reassign have been found.

6 Does the list contain any users *who you do not want* to reassign to another class of service?

- If yes, go to step 7.
- If no, go to step 10.

7 Select the user you do not want to reassign by moving your cursor to the user's name and pressing the spacebar.

Result: The user is highlighted.

Step	Action
8	Press the [Toggle COS Assignment] softkey. **Result:** An asterisk appears next to the user's name. This asterisk indicates that the user will not be reassigned to the new class of service.

```
                          User Administration
List of Local Voice Users
                                                          Storage Personal
                                                     COS  Used    Verific.
  Name           Mailbox                Department    Num. (mins)  Recorded
▌ Lawrence,Dona  7604                   Marketing       1     0     No
* Miller,June    7605                   Marketing       1     0     No
  Samuels,Jack   7602                   Marketing       1     0     No
  Wharton,Ellen  7603                   Marketing       1     0     No

Select a softkey >

 Exit   Toggle Cos Assignment   View/Modify   Delete   Voice
```

9	Are there any other users you do not want to reassign? • If yes, repeat steps 7 to 8 until you have deselected all users you do not want to reassign. • If no, go to step 10.
10	Press [Exit] to return to the Find Local Voice Users screen.
11	Press [Assign to COS] to reassign the found users. **Result:** You are prompted for a COS number.
12	Enter the number of the class of service to which you want to reassign the users and press Return. **Result:** As users are reassigned, a message is displayed, counting each user who is added to the new class of service.
13	If you want to abort the operation at any time, press the [Abort] softkey. **Result:** This stops the reassignment. However, it cannot undo any users who have already been reassigned.

When reassignment is complete

Once all users have been reassigned to the specified class of service, a message and a SEER are sent, stating that the COS assignment is complete. This message and SEER also report the number of users who were assigned and the number of users who failed to be reassigned.

Section C: Modifying and deleting local voice users

In this section

Accessing the View/Modify Local Voice User screen	8-80
Viewing and modifying a local voice user	8-84
Checking a user's status	8-86
Enabling a disabled mailbox	8-91
Changing a user's password	8-93
Monitoring mailbox logins for suspected hacker activity	8-94
Reassigning a mailbox to another user	8-96
Deleting a local voice user	8-97

Accessing the View/Modify Local Voice User screen

Introduction

You may or may not know the mailbox number of the user you want to view or modify. Use this table to decide which procedure to follow to access the View/Modify Local Voice User screen.

IF	THEN follow
you know the user's mailbox number	the procedure on this page.
you do not know the user's mailbox number	the procedure on page 8-81.

Accessing the screen when you know the mailbox number

To access the View/Modify Local Voice User screen directly, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select User Administration.
2	Select Local Voice User.
3	Press the [View/Modify] softkey. **Result:** You are prompted for a mailbox number.

Step	Action
4	Enter the user's mailbox number and press <Return>. **Result:** The View/Modify Local Voice User screen is displayed.

```
                          User Administration
View/Modify Local Voice User

Mailbox Number:      7556                    Volume ID:  202

Storage Used:        2

Last Name:           Roberts

First Name:          Erica                   Initials:

Department:          Hardware Eng

Class of Service:    Personal       001 ptt_load    013_Guest_Clas
(Use More Detail Key)

Primary DN:                                 7556

Extension DNs:                              4142
                                                                MORE BELOW

   Save        Cancel      More Detail    Change        Voice
                                          Password
```

Finding a local voice user and accessing the screen

To find the local voice user you want to modify when you do not know the mailbox number, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select User Administration.
2	Select Local Voice User.

Step	Action
3	Press [Find]. **Result:** The Find Local Voice Users screen is displayed.

```
                          User Administration
Find Local Voice Users

Status:          Any Enabled Disabled Expired Violation
Mailbox Number:                                  Volume ID:    COS:
Last Name:
First Name:
Department:
Extension Number (DN):
Message Waiting Indication DN:
Revert DN:
Voice Storage Limit (minutes):
Read Message Retention (days):
Minimum Number of Invalid Logon Attempts:
Minimum Number of Days since Last Logon:
Minimum Number of Days since Pswd Changed:
Maximum Message Length (mm:ss):
Maximum CA Message Length (mm:ss):
Receive Composed Messages:       Any No Yes
                                                                MORE BELOW
Select a softkey >

 Exit   Assign to COS   List   Print
```

4	Enter the information you know about the user.
5	Press [List]. **Result:** The List of Local Voice Users screen is displayed.

```
                          User Administration
List of Local Voice Users
                                                          Storage  Personal
                                                     COS  Used     Verific.
 Name          Mailbox                Department     Num. (mins)   Recorded
 Gabriel,David 7555                   Hardware Eng     2     0      No
 Hardy,William 7557                   Hardware Eng     1     0      No
 Jones,Peter   7554                   Hardware Eng     2     0      No
 LaMontaigne,P 7610                   Hardware Eng     1     0      No
 Roberts,Erica 7556                   Hardware Eng     3     0      No

Select a softkey >

 Exit   Toggle Cos Assignment   View/Modify   Delete   Voice
```

Step	Action
6	Select the user you want to view or modify by moving your cursor to the user's name and pressing the spacebar.
7	Press [View/Modify]. **Result:** The View/Modify Local Voice User screen is displayed.

```
                              User Administration
View/Modify Local Voice User

Mailbox Number:      7556                    Volume ID:  202

Storage Used:        2

Last Name:           Roberts

First Name:          Erica                   Initials:

Department:          Hardware Eng

Class of Service:    Personal        001_ptt_load    013_Guest_Clas
(Use More Detail Key)

Primary DN:                                  7556

Extension DNs:                               4142
                                                                MORE BELOW

   Save        Cancel      More Detail    Change        Voice
                                          Password
```

Viewing and modifying a local voice user

Introduction

Once you access the View/Modify Local Voice User screen, it functions exactly like the Add Local Voice User screen. Most of the procedures are, therefore, in Section A:: Adding local voice users. Several procedures that are unique to modifying an existing local voice user are described in this section. These are

- changing the user's last name
- enabling a disabled mailbox
- changing the user's password

Deciding what you need to modify

Use this table to decide what you need to modify in the user profile, and then find the page.

IF you want to	THEN go to
check the user's status	page 8-86.
change other user information (such as department)	page 8-15.
reassign the user to another class of service	page 8-20.
reassign a subset of users to another class of service	page 8-73.
create a personal class of service	page 8-22.
modify the revert DN, MWI DN, or extension DNs	page 8-31.
record a personal verification for a user	page 8-34.
create a remote notification schedule for a user	page 8-36.
monitor a mailbox for suspected hacker activity	page 8-94.
modify any of these local voice user characteristics: • name dialable by external callers • hospitality user class (if Hospitality is installed) • volume level (VMUIF only) • preferred language (multilingual systems only)	page 8-39.

IF you want to	THEN go to
enable a disabled mailbox	page 8-91.
change a user's password	page 8-93.
reassign a mailbox to another user	page 8-96

Procedure

To modify a local voice user, follow these steps.

Starting Point: The View/Modify Local Voice User screen

Step	Action
1	Look up the type of change(s) you need to make in the table on page 8-84, and go to the page that is indicated for instructions.
2	Make the necessary changes.
3	Press the [Save] softkey.

Checking a user's status

Introduction

The View/Modify Local Voice Users screen contains a number of status fields that are not displayed in the Add Local Voice Users screen. These are read-only information fields.

MMUI user status fields

The dotted box highlights the status fields that are displayed in the MMUI version of the screen.

```
                          User Administration                    MORE ABOVE
View/Modify Local Voice User


Logon Status:                              Disabled Enabled

Preferred Language:                        American_English
                                           Latin_American_Spanish
Invalid Logon Attempts:                    0

Time of Last Logon:                        1/04/00 15:12

Internal Personal Greeting Recorded:       No

External Personal Greeting Recorded:       No

Temporary Absence Greeting Recorded:       No

Password Last Changed:                     1/04/00 15:11

 Save    Cancel    More Detail    Change Password    Voice
```

VMUIF user status fields

The dotted box highlights the status fields that are displayed in the VMUIF version of the screen.

```
User Administration                                    MORE ABOVE
View/Modify Local Voice User

Volume Level                                Normal Loud Louder Loudest

Preferred Language:                         American_English Canadian_French

Invalid Logon Attempts:                     0

Time of Last Logon:                         **/**/** **:**

Time of Last Mailbox Lockout:               **/**/** **:**

Calls were Rejected after Mailbox Full:     No

Personal Greeting Recorded:                 No

Password Last Changed:                      **/**/** **:**

Save   Cancel   More Detail   Change Password   Voice
```

Field descriptions

The following are descriptions of the status fields that are displayed in the View/Modify Local Voice Users screen.

Invalid Logon Attempts	
Description	This is the number of successive logon attempts that have been made using an incorrect password. This field is reset to 0 when • a valid password is entered and the user is allowed to log in • you reenable the mailbox (if it has been disabled due to too many invalid logon attempts)
Potential security risk	A high number in this field can indicate that a hacker has been trying to get into this mailbox.
More information	See the section "Controlling access to Meridian Mail mailboxes" on page 6-123.

Time of Last Logon	
Description	This is the time at which the user last logged in to his or her mailbox. A series of asterisks indicates that the user has not logged in.
Potential security risk	If a considerable amount of time has passed since the user's last logon, you may want to investigate why this is the case. It could be that • the user is on holiday or extended leave • the user has forgotten his or her password and has not notified you • the user has left the organization (in which case the mailbox should be deleted for security reasons)

Time of Last Mailbox Lockout	
Description	If the user has been locked out of his or her mailbox, this is the time at which the last lockout occurred.
Interface	VMUIF only
Potential security risk	VMUIF users are locked out of their mailboxes after an excessive number of invalid logon attempts. Lockout could indicate that a hacker has been trying to get into this mailbox.
More information	See the section "Controlling access to Meridian Mail mailboxes" on page 6-123.

Calls Rejected after Mailbox Full	
Description	*Yes* indicates that the user's mailbox became full and that call answering messages were rejected as a consequence. *No* indicates that calls have not been rejected.
Interface	VMUIF only
Voice storage limit	If a user complains of many lost messages, consider reassigning him or her to another class of service that has a higher voice storage limit. This will allow more messages to be deposited in the mailbox before becoming full.

Personal Greeting Recorded	
Description	This field indicates whether the user has recorded a personal greeting.
Interface	VMUIF only

Internal Greeting Recorded	
Description	This field indicates whether the user has recorded an internal greeting. This greeting is played to internal callers when they are transferred to Meridian Mail to leave a message.
Interface	MMUI only
Interaction with external greeting	This table indicates which greeting is played to internal callers.

WHEN	THEN
there is an internal greeting	the internal greeting is played.
there is no internal greeting but there is an external greeting	the external greeting is played.
there is no internal greeting and no external greeting	a standard system greeting is played.

External Personal Greeting Recorded	
Description	This field indicates whether the user has recorded an external greeting. The external greeting is played to external callers (or internal callers if no internal greeting is recorded) when they are transferred to Meridian Mail.
Interface	MMUI only

Temporary Absence Greeting Recorded	
Description	This field indicates whether the user has recorded a temporary absence greeting. If this greeting is recorded, it is played to internal and external callers until the expiry date.
Interface	MMUI only

Temporary Absence Greeting Expiry Date	
Description	If a temporary absence greeting has been recorded, this field is displayed to indicate when that greeting will expire.
Interface	MMUI only
Possible Values	A date and time indicate that the user has defined an expiry date for the greeting. *Indefinite* indicates that the user has not defined an expiry date for the greeting.
Expired greetings	If the current date has passed the expiry date, the field will be followed by the word "Expired."

Password Last Changed	
Description	This field indicates when the user last changed his or her password. Both the date and time are displayed.
MMUI versus VMUIF	When a new VMUIF user is added, this field is set to Nil. For users who were added a while ago, Nil indicates that they have not changed their default passwords. When a new MMUI user is added, this field is set to the time at which the user was added.

Enabling a disabled mailbox

Introduction

If too many invalid logon attempts are made to a mailbox and the Maximum Invalid Logon Attempts Permitted per Mailbox (as defined in the Voice Security Options screen) is reached, that user's mailbox is disabled.

What happens: MMUI users

When there are too many invalid logon attempts to the mailbox, the mailbox is disabled.

The MMUI user cannot log on to his or her mailbox, but messages are still recorded. When the user's mailbox is reenabled, he or she will be able to listen to the messages that were received while the mailbox was disabled.

What happens: VMUIF users

When there are too many invalid logon attempts on a VMUIF user's mailbox, the following happens:

- The mailbox is disabled.
- The Time of Last Mailbox Lockout field in the View/ Modify Local Voice User screen displays the time at which the mailbox was disabled.
- Meridian Mail checks the Lockout Duration field in the user's class of service to see how long the user should be locked out.

While a VMUIF user's mailbox is disabled, the user can logon, but calls are rejected and new messages are not recorded.

Deciding if action is needed for VMUIF users

For VMUIF users who have been locked out of their mailbox, you may or may not have to manually reenable the mailbox.

IF the Lockout Duration is	THEN
00.00	you must manually reenable the user's mailbox.
not 00.00	you do not have to manually reenable the mailbox. The mailbox is automatically reenabled after the lockout period has passed.

Potential security risk

A high number of invalid logon attempts could be an indicator that a hacker has been attempting to get into your system through this user's mailbox.

Contact the user and investigate why so many invalid logon attempts were made. If the user does not think he or she was responsible for these attempts, you should monitor this user's mailbox for future logon attempts.

Procedure

To enable a disabled mailbox, follow these steps.

Starting Point: The View/Modify Local Voice User screen

Step	Action
1	Go to the Logon Status field and set it to Enabled.
2	Do you suspect hacker activity? • If yes, set the Monitor Mailbox during Monitoring Period field to Yes. • If no, go to step 3. **Note:** See "Monitoring mailbox logins for suspected hacker activity" on page 8-94.
3	Press [Save]. **Result:** The mailbox is reenabled and the Invalid Logon Attempts field is reset to 0.
4	Notify the user that his or her mailbox has been reenabled.

Changing a user's password

When to use

If a local voice user has forgotten his or her password, you will have to change it at the administration terminal.

Procedure

To change a user's password, follow these steps.

Starting Point: The View/Modify Local Voice User screen

Step	Action
1	Press the [Change User Password] softkey. **Result:** You are prompted for a new password.
2	Enter the new password and press <Return>. **Note:** This password must contain numbers only. It can be up to 16 digits in length. **Result:** You are prompted to reenter the password for verification.
3	Enter the same password and press <Return>.
4	Did you get a message indicating a mismatch between the two passwords you entered? • If yes, repeat steps 2 to 3 until there is no mismatch. • If no, go to step 5.
5	Press [Save].
6	Inform the user of the new password.

Monitoring mailbox logins for suspected hacker activity

Introduction

Hacker Monitor is a new feature that flags hacker activity by issuing information SEERs to bring your attention to suspicious activity. Since mailboxes are a potential security risk, mailbox logins are one type of activity that you should check using Hacker Monitor.

When to use

Typically, you do not need to turn mailbox monitoring on for new users. Turn it on only if you suspect that a hacker has been using a particular mailbox. You may, for example, get complaints of abusive messages being sent from a particular mailbox. This is an indication of potential hacker abuse.

How it works

A monitoring period is defined in the Voice Security Options screen. This is the time period during which logins will be monitored.

If mailbox monitoring is enabled, every time someone logs in to the mailbox during the monitoring period, a SEER will be issued. For MMUI users, SEER 2262 will be issued, whereas for VMUIF users, SEER 5662 will be issued.

Procedure

To enable mailbox monitoring, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Obtain the times when the suspected hacker uses the system. ***Note:*** You can do this from Meridian 1 CDR records, or from Meridian Mail Reporter.
2	Is the monitoring period set up to reflect these times? • If yes, go to step 5. • If no, go to step 3.
3	Select Voice Administration and then Voice Security Options.
4	Enter the time period in the System Access Monitoring Period field, save your change, and return to the Main Menu.
5	Select User Administration.

Step	Action
6	Select Local Voice User and press the [View/Modify] softkey. **Result:** You are prompted for a mailbox number.
7	Enter the user's mailbox number.
8	Go to the Monitor Mailbox during Monitoring Period field and set it to Yes.
9	Press the [Save] softkey. **Result:** Whenever the mailbox is logged into during the monitoring period, SEER 2262 for MMUI users or SEER 5662 for VMUIF users will be generated.

Immediate notification of login

If you (or a support person) want to be notified immediately of an occurrence of these SEERs, you can set up a SEER message trigger mailbox and then enable remote notification for that mailbox. To do this you must do the following.

1. Enable mailbox monitoring as described above.
2. Set up a message trigger for SEER 2262 or 5662, or both, so that an urgent SEER message is deposited in a designated mailbox when the mailbox is logged into.

   See "Using SEER triggering" on page 29-35.
3. Set up remote notification for the designated mailbox so that you (or a support person) will be paged or phoned as soon as the urgent message is deposited.

   Refer to the *Outcalling Application Guide* (NTP 555-7001-320) for more information.

Reassigning a mailbox to another user

Two methods

There are two methods for reassigning a mailbox from one user to another. They are:

- modify the mailbox, changing the appropriate fields (Name, Title, Department, etc.) from the old user's data to the new user's data
- delete the mailbox, then re-add it, filling in the new user's data as you configure the mailbox

First method: modify the mailbox

If you use this method, Operational Measurements will not differentiate between traffic/usage associated with the old user and traffic/usage associated with the new user. The reports will supply statistics for that mailbox as if no change had been made.

To use this method, see "Viewing and modifying a local voice user" on page 8-84 for details on how to modify the mailbox.

Second method: delete and add the mailbox

If you use this method, Operational Measurements reports will present the statistics for the old user separately from the statistics for the new user, even though the mailbox number is the same for both.

To use this method, follow the steps below.

1. Contact the current owner of the mailbox and make sure he or she has listened to all of his or her messages.
2. Access the Delete Local Voice User screen and delete the local voice user.

   See "Deleting a local voice user" on page 8-97.
3. Add a new local voice user, using the same mailbox number, and enter the new user's information.

   See "Accessing the Add Local Voice User screen" on page 8-10.

Deleting a local voice user

When to use

You will have to delete a local voice user when

- reassigning the mailbox to another user
- a user leaves the company

Potential security risk

When a user leaves the company, be sure to delete the mailbox immediately. An unused mailbox is a security risk since it is forgotten about and suspicious activity often goes unnoticed.

Choosing the correct procedure

You may or may not know the mailbox number of the user you want to delete. Use this table to decide which procedure to follow to access the Delete Local Voice User screen and then delete a user.

IF	THEN follow
you know the user's mailbox number	the procedure on page 8-98.
you do not know the user's mailbox number	the procedure on page 8-99.

Deleting a local voice user when you know the mailbox number

To delete a local voice user when you know the user's mailbox number, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select User Administration.
2	Select Local Voice User.
3	Press the [Delete] softkey. **Result:** You are prompted for the mailbox number.
4	Enter the mailbox number and press <Return>. **Result:** The Delete Local Voice User screen is displayed.

```
                              User Administration
Delete Local Voice User

Mailbox Number:      7556                    Volume ID:  202

Storage Used:        3

Last Name:           Roberts

First Name:          Erica                   Initials: E

Department:          Hardware Eng

Class of Service:    Personal       001_ptt_load   013_Guest_Clas
(Use More Detail Key)

Primary DN:                                 7556

Extension DNs:                              4142
                                                                    MORE BELOW

 OK to Delete     Cancel     More Detail
```

5	Is this the user you want to delete? • If yes, go to step 6. • If no, press [Cancel] and abandon the procedure. Obtain the correct mailbox number or use the next procedure on page 8-99 to find the user.
6	Press the [OK to Delete] softkey. **Result:** The user is deleted and you are prompted for another mailbox number.
7	Do you want to delete another local voice user? • If yes, repeat steps 4 to 6 until you have deleted all local voice users that you need to delete at this time. • If no, press the [Cancel] softkey.

Finding and deleting a local voice user

To find a local voice user you want to delete when you do not know the mailbox number, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select User Administration.
2	Select Local Voice User.
3	Press [Find]. **Result:** The Find Local Voice Users screen is displayed.

```
                              User Administration
Find Local Voice Users

Status:          Any Enabled Disabled Expired Violation
Mailbox Number:                                  Volume ID:    COS:
Last Name:
First Name:
Department:
Extension Number (DN):
Message Waiting Indication DN:
Revert DN:
Voice Storage Limit (minutes):
Read Message Retention (days):
Minimum Number of Invalid Logon Attempts:
Minimum Number of Days since Last Logon:
Minimum Number of Days since Pswd Changed:
Maximum Message Length (mm:ss):
Maximum CA Message Length (mm:ss):
Receive Composed Messages:                Any No Yes
                                                                    MORE BELOW
Select a softkey >

   Exit      Assign to COS      List      Print
```

Step	Action
4	Enter the information you know about the user. **Examples:** Last Name, First Name, Department
5	Press [List].

Step	Action
6	Select the user you want to view or modify by moving your cursor to the user's name and pressing the spacebar.
7	Press [Delete]. **Result:** The Delete Local Voice User screen is displayed.

```
                          User Administration
Delete Local Voice User

Mailbox Number:      7556                    Volume ID:  202

Storage Used:        3

Last Name:           Roberts

First Name:          Erica                   Initials: E

Department:          Hardware Eng

Class of Service:    Personal       001_ptt_load   013_Guest_Clas
(Use More Detail Key)

Primary DN:                                 7556

Extension DNs:                              4142
                                                                MORE BELOW

 OK to Delete      Cancel      More Detail
```

8	Press the [OK to Delete] softkey. **Result:** The user is deleted and you are prompted for another mailbox number.

Chapter 9

Remote voice users

In this chapter

Section A: Introduction	9-3
Section B: Adding remote voice users	9-11
Section C: Finding remote voice users	9-27
Section D: Modifying and deleting remote voice users	9-39

Section A: Introduction

In this section

What is a remote voice user? 9-4
Remote voice user changes and enhancements 9-6
Permanent remote voice users 9-8
Temporary remote voice users 9-9

What is a remote voice user?

Definition

A remote voice user (RVU) is a Meridian Mail user whose mailbox resides on a remote networking site and who has been added to the local site's user database.

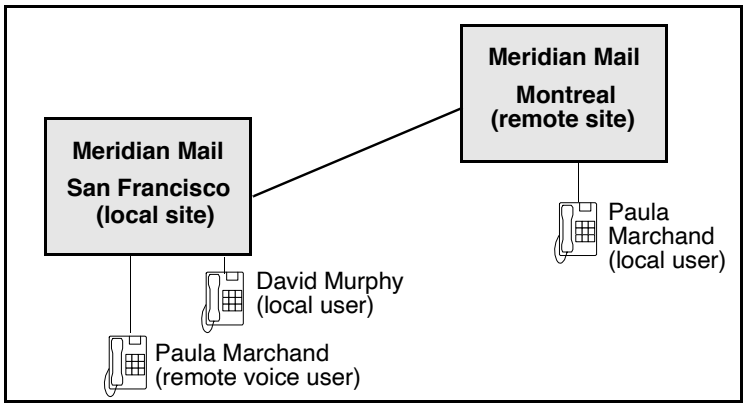
Benefits

The benefits of adding users from remote sites as remote voice users in the local site are as follows.

- Whenever 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 (press 9 on the keypad) to immediately call back the originator of the message.
- 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

David Murphy is a local user at your San Francisco Meridian Mail site. Paula Marchand is a user at the remote Montreal Meridian Mail site. Paula has been added to your local site as a remote voice user.



Example (cont'd)

David Murphy can use name addressing when composing a voice message to Paula Marchand. During message addressing, David will hear Paula's spoken name as a verification of the mailbox number he has entered.

When David listens to a voice message received from Paula, he presses 9 (call sender) to call Paula back.

Remote voice user changes and enhancements

Introduction

In recent Meridian Mail releases, a number of enhancements have been made to the administration of remote voice users to

- provide support for remote voice user propagation to other sites
- to simplify the management of the remote voice user database

New type of remote voice user

In Meridian Mail Releases 11 and 12, you can add remote voice users as temporary users. In the past, users at remote sites could only be added as permanent remote voice users. They had to be added and deleted manually, one at a time.

Temporary users can be added and deleted automatically by the system.

Simplified addition of remote voice users

Prior to Meridian Mail 11, you had to enter each remote voice user to your local site one user at a time.

Now, you can quickly and easily add remote voice users in one of two ways.

- RVU Propagation via Enterprise Networking automatically adds remote voice users to your local site whenever a user at a remote site addresses a voice message to a user at your local site. These users are added as temporary users.
- RVU Propagation via Bulk Provisioning allows you to copy all (or a subset of) users at a remote site to tape and then copy them into your local database as remote voice users. These users can be added as temporary or permanent.

Personal verification in user's voice

Prior to Meridian Mail 11, personal verifications (spoken names) for remote voice users could only be recorded by the local administrator, and, therefore, in a voice other than the user's.

In Meridian Mail Releases 11 and 12, when temporary remote voice users are added to the system using RVU Propagation, the personal verification of each user is added in that user's voice, provided that the user has recorded a personal verification.

When the personal verification is played for remote voice users

A personal verification is played for remote voice users in the following situations:

- A local user composes a message to a remote voice user. When the user enters the remote user's mailbox (or name if using name addressing), he or she will hear the remote voice user's personal verification in the user's voice.
- A local user name dials a remote voice user.
- A local user uses the call sender feature on a message from a remote voice user.
- The envelope of a message received from a remote voice user is played.

When no personal verification has been recorded for a remote voice user

When no personal verification has been recorded, the system plays the remote site's spoken name and the mailbox number (for example, *"Maidenhead, mailbox 1334."*)

If there is no spoken name recorded for the remote site, the system plays the mailbox number in network format (for example, *"Mailbox 64441334."*)

Permanent remote voice users

Introduction

All remote voice users that existed prior to Meridian Mail Release 11 were permanent remote voice users. As of Meridian Mail 11, remote voice users can still be added as permanent remote voice users.

Adding permanent users

Permanent remote voice users can be added in one of two ways.

User Administration

They can be added one at a time through User Administration. This is the way you had to enter them prior to Release 11.

See “Adding remote voice users through User Administration” on page 9-17.

Bulk Provisioning

You can use the Bulk Provisioning feature to copy users from a remote site to your local site’s database as permanent remote voice users.

See “Adding remote voice users using RVU Propagation via Bulk Provisioning” on page 9-24.

Deleting permanent users

Permanent remote voice users remain on the system until you delete them. Permanent users must be deleted one at a time through the User Administration menu.

See “Manually deleting remote voice users” on page 9-45.

Making permanent users temporary

You can convert permanent remote voice users who have not been active for a long time to temporary remote voice users and allow the system to take care of deleting inactive users.

You can verify when a user was last active in one of two ways.

- Check the Last Access Time field in the View/Modify Remote Voice User screen.
- Use the Find function and list all permanent remote voice users. You can then select and modify users from the List screen.

Temporary remote voice users

Introduction

Temporary remote voice users were also introduced in Meridian Mail 11. Temporary remote voice users make administration of remote voice users much easier since they can be both added and deleted automatically by the system.

Adding temporary users

Temporary remote voice users can be added in one of three ways.

User Administration

You can add temporary remote voice users one at a time through User Administration in the same way that you add permanent users.

See "Adding remote voice users through User Administration" on page 9-17.

RVU Propagation via Enterprise Networking

You can have remote voice users automatically added to your system when they send network messages to the local site.

When temporary users are added this way, the personal verifications that users have recorded in their own voices are used.

See "Adding temporary remote voice users using RVU Propagation via Enterprise Networking" on page 9-21.

RVU Propagation via Bulk Provisioning

You can also use the Bulk Provisioning feature to copy users from a remote site to tape and then to your local site's database as temporary or permanent remote voice users. This method is not automatic, but it does allow you to quickly add all users (or a subset of users) from a remote site to your local database.

When remote voice users are added this way, the personal verifications that users have recorded in their voice are used.

See "Adding remote voice users using RVU Propagation via Bulk Provisioning" on page 9-24.

Deleting temporary users

Temporary remote voice users can be deleted in one of two ways.

Manual deletion

If you want to delete a particular remote voice user, you can do so through the User Administration menu in the same way that you delete permanent remote voice users.

See “Manually deleting remote voice users” on page 9-45.

Automatic deletion during nightly audits

Nightly audits are performed on the database of temporary remote voice users in order to keep it from getting too large.

Whenever the number of temporary remote voice users exceeds a threshold, the nightly audit removes the oldest temporary remote voice users in the system. If the number of temporary remote voice users reaches the maximum number allowed on the system, no more temporary users will be added by Remote Voice User Propagation until after the nightly audit is run.

See “How temporary remote voice users are automatically deleted from the system” on page 9-49.

Making temporary users permanent

If you do not want a particular temporary user to be deleted during a nightly audit, you can change that user to a permanent user. Permanent users are not deleted during the nightly audit.

See “Viewing and modifying remote voice users” on page 9-40.

Section B: Adding remote voice users

In this section

The Add Remote Voice User screen	9-12
Adding remote voice users through User Administration	9-17
Recording a personal verification for a remote voice user	9-19
Adding temporary remote voice users using RVU Propagation via Enterprise Networking	9-21
Adding remote voice users using RVU Propagation via Bulk Provisioning	9-24

The Add Remote Voice User screen

Introduction

Permanent and temporary remote voice users can be added to the system one at a time from this screen.

The screen

This is the Add Remote Voice User screen.

Part 1

```
                          User Administration
Add Remote Voice User

Mailbox Number:      8998071

Last Name:           Glass

First Name:          Fred              Initials: ____

Department:          Marketing

Extension DNs:       8998071
                     8999071

Personal Verification Recorded (Voice):      No

Name Dialable by External Callers:           No Yes

                                                                MORE BELOW

 Save      Cancel                                    Voice
```

Part 2

```
                          User Administration                    MORE ABOVE
Add Remote Voice User

First Name:          Fred                 Initials: ____

Department:          Marketing

Extension DNs:       8998071
                     8999071

Personal Verification Recorded (Voice):      No

Name Dialable by External Callers:           No Yes

User Type:                                   Permanent Temporary

Last Access Time:                            **/**/** **:**

   Save      Cancel                                      Voice
```

Field descriptions

This table describes the fields in the Add Remote Voice User screen.

Mailbox Number	
Description	The remote voice user's mailbox number.
Format	The mailbox number must be in network format. It must include the network prefix or steering code of the remote site.
Example	If the dialing plan is ESN, a valid mailbox number is 6233 4433, where 6233 is the network prefix and 4433 is the mailbox number. If the dialing plan is CDP, a valid mailbox number is 54433, where 54 is the steering code.
Default	The number you entered to access the Add Remote Voice User screen.
Maximum length	28 digits (including network prefix)
Mandatory	This field is mandatory. The user cannot be saved if this field is blank.

Last Name and First Name	
Description	The remote voice user's last and first names.
Maximum length	You can enter up to 41 characters for the last name and 21 characters for the first name.
Restricted characters	Do not use the following characters in these fields: plus sign (+), underscore (_), or question mark (?).
Attention	Make sure the spelling is correct. These fields are used by the name dialing and name addressing features. For this reason, it is recommended that you use only alphanumeric characters.
Initials	
Description	Initials can be used to distinguish users with identical first and last names. They are not used by the name dialing or name addressing features.
Default	If you leave this field blank, Meridian Mail will automatically insert the first letter of the user's first name when you save the user.
Maximum length	5 characters
Department	
Description	The remote voice user's department.
Default	This field is blank for the first user you add. For subsequent users, this field defaults to the department entered for the last user you added (as the [Cancel] softkey was not pressed).
Maximum length	31 characters
Restricted characters	Do not use the following characters in these fields: plus sign (+), underscore (_), or question mark (?).

Extension DNs	
Description	A user can have up to three extensions. This means that a caller can dial any one of these numbers and reach the user. The first field is for the primary DN.
Format	These DNs must be in network format. They must include the network prefix or steering code of the remote site.
Maximum length	30 digits
Default	The first DN field is typically filled in with the mailbox number you entered to access the Add Remote Voice User screen.
See Also	See “Primary DN and extension DNs” on page 8-24.

Personal Verification Recorded (Voice)	
Description	This read-only field indicates whether a spoken name has been recorded for this user (either by the user or by the administrator).
Default	This field is set to No when you first add a user.

Name Dialable by External Callers	
Description	This field determines whether this user can be name dialed by external callers. An external caller is anyone who is calling in from a phone that is not on your PBX.
Default	This field uses the setting for the Name Dialable by External Callers field in the Networking Configuration screen under the Network Administration menu.
Valid Options	Yes, No

User Type	
Description	This field identifies the type of remote voice user.
Default	Permanent
Valid Options	Permanent, Temporary
See Also	See “Permanent remote voice users” on page 9-8 and “Temporary remote voice users” on page 9-9.

Last Access Time	
Description	This is a read-only field that indicates the last time • the user was modified via User Administration • the user’s personal verification was played • an Enterprise Networking message was received from this user • the user was updated using bulk provisioning
Default	This field is set to the date and time at which the user is added.
Usage	This time-stamp is used by the nightly audit to determine which temporary remote voice users should be deleted when there are too many temporary users on the system.

Adding remote voice users through User Administration

When to use

Use this procedure to add either permanent or temporary remote voice users one at a time.

Procedure

To add a remote voice user, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select User Administration. **Result:** The User Administration menu is displayed.
2	Select Remote Voice User.
3	Press the [Add] softkey. **Result:** You are prompted for a mailbox number.
4	Enter the mailbox number of the remote voice user. **Requirement:** Enter the necessary network prefix or steering code as part of the mailbox number. **Result:** The Add Remote Voice User screen is displayed.

```
                    User Administration
Add Remote Voice User

Mailbox Number:      8998075

Last Name:           _

First Name:          ____________________   Initials: ____

Department:          ____________________________

Extension DNs:       8998075 ____________________
                     ____________________________
                     ____________________________

Personal Verification Recorded (Voice):      No

Name Dialable by External Callers:           No Yes
                                                          MORE BELOW

 Save      Cancel                                  Voice
```

Note: Field descriptions begin on page 9-13.

5	Enter the user's last name and first name.
6	Enter the user's initials.
7	Enter the user's department.

Step	Action
8	Does the user have a phone and can he or she be dialed directly from the local site? • If yes, go to step 9. • If no, make all Extension DN fields blank and go to step 11.
9	Does the user have more than one extension DN? • If yes, go to step 10. • If no, go to step 11.
10	Enter the user's other DN(s) in the remaining Extension DN fields.
11	Do you want to record a personal verification (spoken name) for the user? • If yes, see "Recording a personal verification for a remote voice user" on page 9-19. • If no, go to step 12.
12	Do you want external callers to be able to name dial this user? • If yes, set the Name Dialable by External Callers field to Yes. • If no, set the Name Dialable by External Callers field to No.
13	Is this a permanent user? • If yes, select Permanent. • If no, select Temporary.
14	Do you want to save the user with the information you have entered? • If yes, press the [Save] softkey. • If no, press the [Cancel] softkey or make the necessary changes and then press [Save].

Recording a personal verification for a remote voice user

Introduction

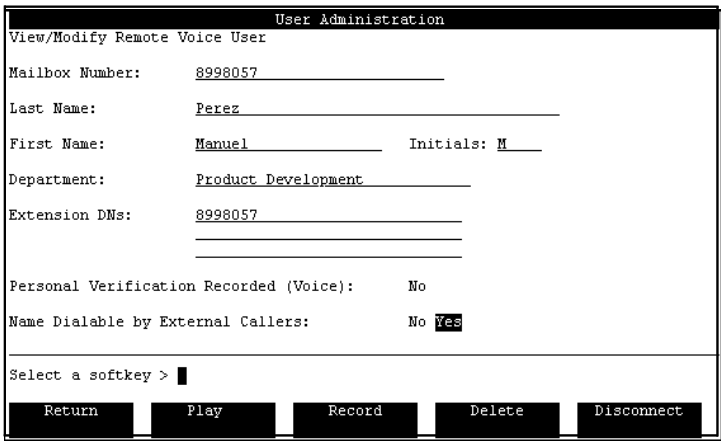
Ideally, users should record personal verifications (spoken names) in their own voice. However, as administrator, you can record personal verifications from the administration terminal on behalf of users.

Procedure

To record a personal verification, follow these steps.

Starting Point: The Add Remote Voice User screen

Step	Action
1	Put the cursor on the Personal Verification Recorded (Voice) field.
2	Press the [Voice] softkey. **Result:** You are prompted to enter the extension of the phone you want to use to record the verification.
3	Enter the extension of the phone and press <Return>. **Result:** The phone rings.
4	Pick up the receiver. **Result:** The recording softkeys are displayed.



Step	Action
5	Press the [Record] softkey. **Result:** The [Stop] softkey is displayed.

Step	Action
6	At the sound of the beep, speak the user's name (and, optionally, the user's extension). **Example:** *"Heather McGee at extension 8523."*
7	Press the [Stop] key to stop recording.
8	Do you want to verify the recording? • If yes, press the [Play] softkey. • If no, go to step 10.
9	Do you want to rerecord the verification? • If yes, repeat steps 5 to 8 to rerecord the verification. • If no, go to step 10.
10	Do you need to record personal verifications for any other users? • If yes, press the [Return] softkey and do not hang up the receiver. The next time you press [Voice] to record another verification, you will not have to reenter the phone extension since the line has not been disconnected. • If no, press the [Disconnect] softkey and hang up the receiver.

Adding temporary remote voice users using RVU Propagation via Enterprise Networking

Introduction

The RVU Propagation via Enterprise Networking feature can be used to add temporary remote voice users.

When this feature is enabled, temporary remote voice users are added automatically.

Requirement

Enterprise Networking must be enabled on both sites: your local site *and* the remote site from which you want to add users to your system.

Enabling RVU Propagation via Enterprise Networking

To automatically add temporary remote voice users to your system, you must enable the RVU Propagation via Enterprise Networking feature. It is disabled by default.

This feature is enabled through Network Administration.

1. Enable RVU Propagation via Enterprise Networking for the local site.

   In the Networking Configuration screen of the local Meridian Mail site, set the Add/Update Remote Voice Users field to Yes.

   This informs Meridian Mail that you want to receive remote voice user information at the local site.

2. Choose the sites whose users you want added as remote voice users to your system. The sites you choose must be Enterprise Networking sites.

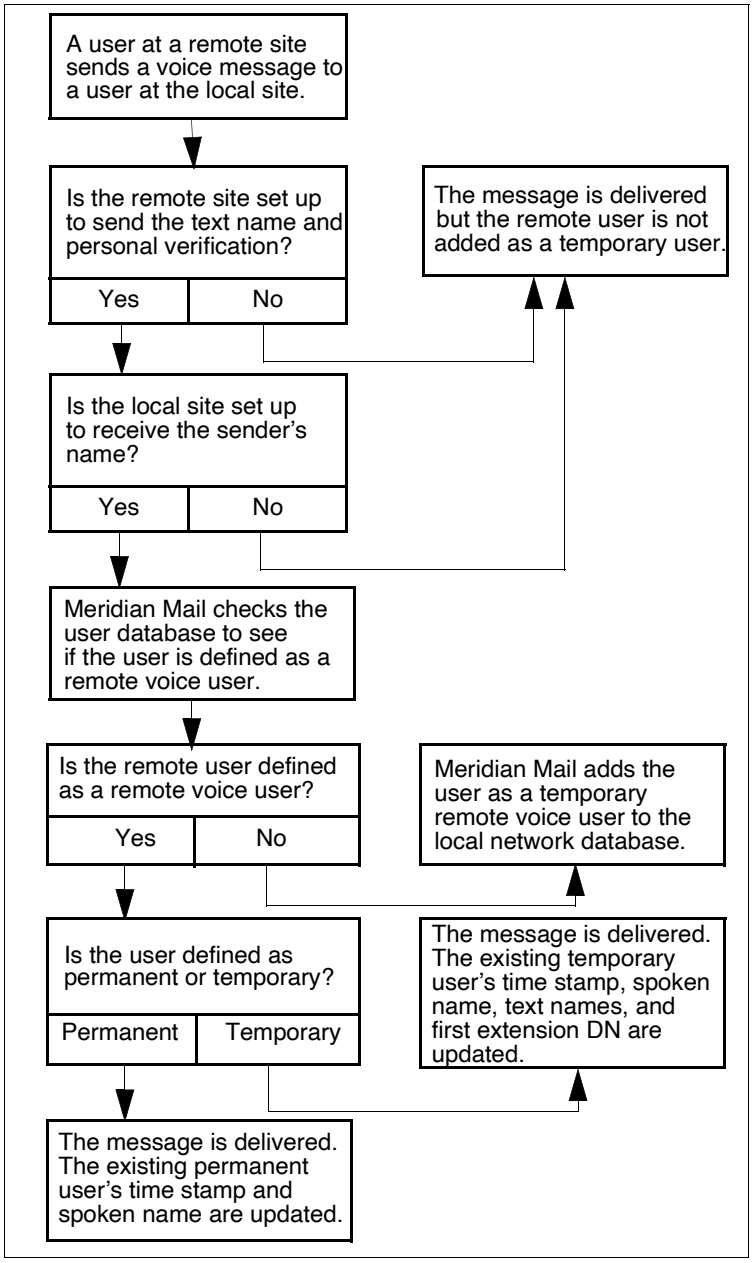
3. To enable the sending of RVU information from each remote site, you must set the Send the Sender's text name and personal verification field to Yes in the Remote Site Maintenance screen at the *remote* Meridian Mail system (not the local system).

See also

For detailed instructions on enabling this feature, refer to the *Enterprise Networking Guide* NTP (555-7001-246), "Maintaining the network" chapter.

When users are added/updated

A temporary remote voice user is added to the local site when a user at a remote site sends a network message to a user at the local site. Remote voice user information is taken from the header of the Enterprise network message that is received.



Limitations

The following are limitations of the RVU Propagation via Enterprise Networking feature:

- Users at remote sites are added to your system as temporary remote voice users only when messages are received from them.

  Remote voice users who do not send network messages will not be added as remote voice users even if they are regularly name-dialed or have a lot of messages sent to them.

  For a description of how to work around this limitation, see "Application 2: Seeding temporary users" on page 9-25.
- No operational measurements are collected for remote voice 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.
- Additions and updates of temporary remote voice users is blocked during the nightly audit.
- Only 18 characters of the remote voice users text name will be sent.

WHEN	THEN
the first and last names are 18 characters or less	the first and last names of the user are sent.
the last name and initials are 18 characters or less	the last name and initials of the user are sent.
the last name only is 18 characters or less	only the last name is sent.
the last name is more than 18 characters long	only the last name is sent and is truncated to 18 characters.

Adding remote voice users using RVU Propagation via Bulk Provisioning

Introduction

Bulk Provisioning is a Meridian Mail 12 feature that allows you to transfer data between Meridian Mail systems using tapes. One of the ways in which you can use this feature is to copy local users from a remote site to tape and then to your local user database as temporary or permanent remote voice users.

Information that is added/updated

The following user information is added to the local system:

- the user's entire name
- the user's mailbox
- the user's primary DN
- the user's personal verification (spoken name)
- the user's department

Application 1: Provisioning permanent users

You can use this feature to add a large number of permanent remote voice users to your local user database. This eliminates the need to add each user manually.

The other benefit over adding each user manually, is that the personal verifications (spoken names) that users have recorded in their own voice will be used. This means that you no longer have to record users' personal verifications at the administration terminal.

Application 2: Seeding temporary users

RVU Propagation via Bulk provisioning

You can use bulk provisioning to initially add temporary remote voice users in a batch as the network is set up. In this way, all the users at a remote site could be made available at one time.

RVU Propagation via Enterprise Networking

Once users have been added using bulk provisioning, you can use RVU Propagation via Enterprise Networking to maintain the database of temporary users.

This means that any additional temporary remote voice users will automatically be added on an as-needed basis. Over time, the less frequently used temporary remote voice users will be deleted during the nightly audit to lessen the system load. Only regularly accessed temporary users will be kept on the system.

Application 3: Selective seeding of temporary users

In Application 2, you use RVU Propagation via Bulk Provisioning to seed a large number of temporary remote voice users.

If you want to add a selective (smaller) subset of remote voice users to your system, you can do the following.

1. Compose a voice message to the users you want to add as remote voice users to your system.
2. Tag the message for acknowledgment.
3. Send the message.

   When the read message acknowledgment comes back, the users are added as temporary remote voice users.

See also

For information about how to use the bulk provisioning feature, see Chapter 34, “Bulk provisioning”.

Section C: Finding remote voice users

In this section

Accessing the Find Remote Voice Users screen 9-28
The Find Remote Voice Users screen 9-29
Wildcard characters 9-32
Finding, listing, and printing remote voice users 9-34

Accessing the Find Remote Voice Users screen

Introduction

You fill in your search criteria in the Find Remote Voice Users screen. You can then choose to print or list (on screen) the users that are found. If you choose to view the list on screen, you can then select a user in order to view, modify, or delete the user.

Procedure

To access the Find Local Voice Users screen, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select User Administration.
2	Select Remote Voice User.
3	Press the [Find] softkey. **Result:** The Find Remote Voice Users screen is displayed.

```
                          User Administration
Find Remote Voice Users

If a specific location is desired, include the location code prefix
in the mailbox number field.

Mailbox Number: _____________________

Last Name:      ____________________________________

First Name:     ___________________

Department:     ____________________________

Extension Number (DN):          ____________________________

Personal Verification Status:   Any Not_Recorded Recorded

User Type:                      Any Permanent Temporary

Select a softkey >

   Exit          List          Print
```

The Find Remote Voice Users screen

Introduction

By entering what you know about the user or subset of users you want to find, Meridian Mail will search the database and return a list of remote voice users that meet the criteria you have specified.

The screen

This is the Find Remote Voice Users screen.

```
                          User Administration
Find Remote Voice Users

If a specific location is desired, include the location code prefix
in the mailbox number field.

Mailbox Number: _____________________

Last Name:      ____________________________________

First Name:     ___________________

Department:     ____________________________

Extension Number (DN):          ___________________________

Personal Verification Status:   Any Not_Recorded Recorded

User Type:                      Any Permanent Temporary

Select a softkey >

   Exit          List        Print
```

Field descriptions

This table describes the fields in the Find Remote Voice Users screen.

Mailbox Number	
Description	Use this field to find users within a certain range of consecutive mailbox numbers or a particular user. To find a range of mailbox numbers, use the appropriate wildcards. The mailbox number must include the network prefix of the remote site.
Maximum Length	You can enter up to 28 characters.

Last Name	
Description	Use this field (in combination with the first name field) if you want to find a particular user, or alone to find all users with a particular last name. Use wildcards if you are unsure of the exact spelling.
Default	Blank (finds users with any last name)

First Name	
Description	Use this field (in combination with the last name field) to find a particular user, or alone to find all remote voice users with a particular first name. Use wildcards if you are unsure of the spelling.
Default	Blank (finds users with any first name)

Department	
Description	Use this field to find users that belong to a particular department. Use wildcard characters if you are unsure of the exact name or spelling, or if you want to find users in a number of similarly named departments.
Default	Blank (finds users in any department)

Extension Number (DN)	
Description	Use this field if you want to find users with a particular primary extension DN. Use wildcards to find users within a range of DNs.
Default	Blank (finds users with any extension DN)

Personal Verification Status	
Description	Use this field to find users who do not have, or have, a recorded personal verification.
Default	Any
Valid Options	Any, Not Recorded, Recorded

User Type	
Description	Use this field to find either temporary users or permanent users.
Default	Any
Valid Options	Any, Permanent, Temporary

Wildcard characters

Introduction

You can use wildcards in most of the fields in the Find Remote Voice Users screen in order to find a subset of users.

Definition: wildcard

A wildcard is a character that is used in a search string to represent an unknown or variable character or string of characters.

Types of wildcards

There are two wildcards that you can use.

Wildcard	Description
_	The underscore (_) replaces a single character.
+	The plus sign (+) replaces a string of characters.

Where you can use wildcards

You can enter wildcards in the following fields:

- Mailbox Number
- Last Name
- First Name
- Department
- Extension Number (DN)

Examples

The following examples show how wildcards can be used to find a range of users.

You enter	Result
“6321210_” in the Mailbox Number field (6321 is the ESN prefix of the remote site).	All mailboxes in the range 63212100 to 63212109 are found.
“7_99” in the Extension Number field.	Users with the following extension DNs are found: 7099, 7199, 7299, 7399, 7499, 7599, 7699, 7799, 7899, 7999.
“3213+” in the Mailbox Number field.	All mailboxes beginning with 3213 are found.
“+Engineering” in the Department field.	Users belonging to all engineering departments are found (such as Software Engineering, Hardware Engineering, Information Engineering).

Finding, listing, and printing remote voice users

Purpose

Use the find function to

- list (on screen) or print the found users
- view or modify any of the found users
- delete any of the found users

Specifying search criteria

You only need to change a field if that field is part of your search criteria. All other fields should be left so that they display their default setting (blank or Any).

Network format

The mailbox numbers and DNs that are listed or printed are displayed in network format.

This means that any necessary network prefixes or steering codes are included as part of the DN or mailbox number.

Examples

If the dialing plan is ESN, you would see DNs like 62334433 where 6233 is the ESN prefix of the remote site and 4433 is the local DN.

If the dialing plan is CDP, you would see DNs like 54433, where 54 is the steering code of the site to which the user belongs.

Examples of use

Here are some examples of how you can use the Find function. You can

- find Cameron in the Technology department
- find an employee by last name only when you are not sure whether they go under Elizabeth, Liz, or Beth as a first name
- find any users who have not yet recorded a personal verification
- find all users in the Documentation department, so that they can be reassigned to the new Information Products department

Procedure

To find a remote voice user (or subset of users), follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select User Administration.
2	Select Remote Voice User.
3	Press the [Find] softkey. **Result:** The Find Remote Voice Users screen is displayed.

```
                          User Administration
Find Remote Voice Users

If a specific location is desired, include the location code prefix
in the mailbox number field.

Mailbox Number: _____________________

Last Name:      ____________________________________

First Name:     ___________________

Department:     ____________________________

Extension Number (DN):        ____________________________

Personal Verification Status: Any Not_Recorded Recorded

User Type:                    Any Permanent Temporary

Select a softkey >

   Exit                        List      Print
```

Step	Action
4	Fill in the necessary fields in order to define your search criteria. **Note:** Field descriptions begin on page 9-29.
5	List or print the users that match the search criteria.

IF you want to	THEN
list the users that match the search criteria	go to step 6.
print the users that match the search criteria	go to step 9.
cancel the search	press [Exit].

Step	Action
6	Press the [List] softkey. **Result:** The List of Remote Voice Users screen is displayed.

```
                              User Administration
List of Remote Voice Users
                                                                          Personal
                                                                User  Last    Verific.
Name           Mailbox                        Department       Type  Access  Recorded
Calhoun,Gavin  8998051                        Public Relatio   Perm  6/11/96 Yes
Campbell,Dave  843309                         Reporting        Temp  6/10/96 No
Cathgart,Dr C  843307                         Reporting        Perm  6/13/96 Yes
Defago,Jacque  843306                         Reporting        Temp  6/15/96 Yes
Douglas,Joe    8998055                        Maintenance      Temp  6/11/96 No
Fedora,Alex    8998052                        Public Relatio   Perm  6/19/96 Yes
Glass,Fred     8998071                        Marketing        Perm  6/20/96 No
Humber,Carol   8998053                        Public Relatio   Perm  6/10/96 Yes
Lebar,Tammy    8998054                        Maintenance      Temp  6/11/96 No
Lee,Wen Mai    8998056                        Product Develo   Temp  6/16/96 Yes
Nero,Giuseppe  843305                         Reporting        Perm  6/11/96 Yes
Nova,Louis     8998050                        Marketing        Temp  6/10/96 No
Perez,Manuel   8998057                        Product Develo   Perm  6/11/96 Yes
Rowe,Colin     8998058                        Product Develo   Perm  6/14/96 Yes

Select a softkey >

   Exit          View/Modify      Delete          Voice
```

7 Do you want to view, modify, or delete a local voice user or record a personal verification?

- If yes, go to step 8.
- If no, press [Exit] to return to the Find Remote Voice Users screen.

8 Select the user by moving your cursor to the user's name and pressing the Spacebar.

IF you want to	THEN press	AND go to
view or modify a user	[View/Modify]	page 9-40.
delete a user	[Delete]	page 9-45.
record a personal verification for the user	[Voice]	page 9-19.

Step	Action
9	Press the [Print] softkey. **Result:** The Printing softkeys are displayed.

```
                    User Administration
Find Remote Voice Users

If a specific location is desired, include the location code prefix
in the mailbox number field.

Mailbox Number: ____________________________

Last Name:      ______________________________________

First Name:     ____________________

Department:     ______________________________

Extension Number (DN):          ____________________________

Personal Verification Status:   Any Not_Recorded Recorded

User Type:                      Any Permanent Temporary

[ ]

[      ] [Cancel Printing] [      ] [Continue Printing] [      ]
```

10	Do you want to continue printing? • If yes, press the [Continue Printing] softkey. **Note:** Once printing has started, you can stop it at any time by pressing the [Cancel Printing] softkey. • If no, press the [Cancel Printing] softkey.

Section D: Modifying and deleting remote voice users

In this section

Viewing and modifying remote voice users 9-40

Manually deleting remote voice users 9-45

How temporary remote voice users are automatically deleted from the system 9-49

Viewing and modifying remote voice users

Introduction

You may or may not know the mailbox number of the user you want to view or modify. Use this table to decide which procedure to follow to access the View/Modify Remote Voice User screen.

IF you	THEN follow
know the user's mailbox number	the procedure on this page.
do not know the users's mailbox number	the procedure on page 9-41.

When to use

Use this procedure when you need to

- modify user information (such as last name or department)
- make a temporary user permanent
- make a permanent user temporary

Accessing the screen when you know the mailbox number

To access the View/Modify Remote Voice User screen directly, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select User Administration.
2	Select Remote Voice User.
3	Press the [View/Modify] softkey. **Result:** You are prompted for a mailbox number.
4	Enter the user's mailbox number (including the access code and network prefix) and press Return. **Result:** The View/Modify Remote Voice User screen is displayed. See page 9-43.

Finding a remote voice user and accessing the screen

To find the remote voice user you want to modify when you do not know the mailbox number, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select User Administration.
2	Select Remote Voice User.
3	Press [Find]. **Result:** The Find Remote Voice Users screen is displayed.

```
                          User Administration
Find Remote Voice Users

If a specific location is desired, include the location code prefix
in the mailbox number field.

Mailbox Number: _____________________

Last Name:      ____________________________________

First Name:     ___________________

Department:     ____________________________

Extension Number (DN):          ___________________________

Personal Verification Status:   Any Not_Recorded Recorded

User Type:                      Any Permanent Temporary

Select a softkey >

   Exit          List        Print
```

4	Enter the information you know about the user. **Examples:** Last Name, First Name, Department If you are not sure of your information, or want to see all the remote voice users listed, go to step 7.

Step	Action
5	Press [List]. **Result:** The List of Remote Voice Users screen is displayed.

```
                              User Administration
List of Remote Voice Users
                                                                    Personal
                                                          User  Last    Verific.
Name           Mailbox                      Department    Type  Access  Recorded
Calhoun,Gavin  8998051                      Public Relatio Perm 6/11/96 Yes
Campbell,Dave  843309                       Reporting      Temp 6/10/96 No
Cathgart,Dr C  843307                       Reporting      Perm 6/13/96 Yes
Defago,Jacque  843306                       Reporting      Temp 6/15/96 Yes
Douglas,Joe    8998055                      Maintenance    Temp 6/11/96 No
Fedora,Alex    8998052                      Public Relatio Perm 6/19/96 Yes
Glass,Fred     8998071                      Marketing      Perm 6/20/96 No
Humber,Carol   8998053                      Public Relatio Perm 6/10/96 Yes
Lebar,Tammy    8998054                      Maintenance    Temp 6/11/96 No
Lee,Wen Mai    8998056                      Product Develo Temp 6/16/96 Yes
Nero,Giuseppe  843305                       Reporting      Perm 6/11/96 Yes
Nova,Louis     8998050                      Marketing      Temp 6/10/96 No
Perez,Manuel   8998057                      Product Develo Perm 6/11/96 Yes
Rowe,Colin     8998058                      Product Develo Perm 6/14/96 Yes

Select a softkey >

   Exit          View/Modify      Delete        Voice
```

6	If you do not see the user you are looking for, scroll down using the down arrow key or the Page Down key to see more users.
7	Select the user you want to view or modify by moving your cursor to the user's name and pressing the Spacebar.
8	Press [View/Modify]. **Result:** The View/Modify Remote Voice User screen is displayed. See page 9-43.

The View/Modify Remote Voice User screen

This is the View/Modify Remote Voice User screen.

Part 1

```
                          User Administration
View/Modify Remote Voice User

Mailbox Number:      8998051

Last Name:           Calhoun

First Name:          Gavin              Initials: G

Department:          Public Relations

Extension DNs:       8998051

Personal Verification Recorded (Voice):      No

Name Dialable by External Callers:           No Yes
                                                                    MORE BELOW

   Save      Cancel                                        Voice
```

Part 2

```
                          User Administration                       MORE ABOVE
View/Modify Remote Voice User

First Name:          Gavin              Initials: G

Department:          Public Relations

Extension DNs:       8998051

Personal Verification Recorded (Voice):      No

Name Dialable by External Callers:           No Yes

User Type:                                   Permanent Temporary

Last Access Time:                            6/11/96 10:21

   Save      Cancel                                        Voice
```

Field descriptions

The fields in this screen are the same as in the Add Remote Voice User screen. For field descriptions, see “The Add Remote Voice User screen” on page 9-12.

Procedure

To view or modify a remote voice user, follow these steps.

Starting Point: The View/Modify Remote Voice User screen

Step	Action
1	Change the user's last name if necessary.
2	Change the user's department if necessary.
3	Change the extension DNs associated with the user if necessary.
4	Do you want to record a personal verification for the user? • If yes, see "Recording a personal verification for a remote voice user" on page 9-19. • If no, go to step 5.
5	Do you want to allow name dialing by external callers? • If yes, select Yes in the Name Dialable by External Callers field. • If no, select No in the Name Dialable by External Callers field.
6	Change the user type if necessary.

IF you want to	THEN select
make a temporary user permanent	Permanent in the User Type field.
make a permanent user temporary	Temporary in the User Type field.

7	Do you want to save the user with the current information? • If yes, press [Save]. • If no, press [Cancel] or make any necessary changes and press [Save].

Manually deleting remote voice users

Introduction

You may or may not know the mailbox number of the user you want to delete. Use this table to decide which procedure to follow to access the Delete Remote Voice User screen and then delete a user.

IF you	THEN follow
know the user's mailbox number	the procedure on this page.
do not know the users's mailbox number	the procedure on page 9-46.

Deleting a user when you know the mailbox number

To access the Delete Remote Voice User screen directly, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select User Administration.
2	Select Remote Voice User.
3	Press the [Delete] softkey. **Result:** You are prompted for a mailbox number.

Step	Action
4	Enter the user's mailbox number (including the access code and network prefix) and press Return. **Result:** The Delete Remote Voice User screen is displayed.

```
                          User Administration
Delete Remote Voice User

Mailbox Number:      8998055

Last Name:           Douglas

First Name:          Joe                    Initials: J

Department:          Maintenance

Extension DNs:       8998055


Personal Verification Recorded (Voice):      No

Name Dialable by External Callers:           No Yes
____________________________________________________________________MORE BELOW

 OK to Delete      Cancel
```

5	Is this the user you want to delete? • If yes, go to step 6. • If no, press [Cancel]. Obtain the correct mailbox number or use the next procedure on page 9-46 to find the user.
6	Press the [OK to Delete] softkey. **Result:** The user is deleted and you are prompted for another mailbox number.
7	Do you want to delete another remote voice user? • If yes, repeat steps 5 to 6 until you have deleted all remote voice users that you need to delete at this time. • If no, press the [Cancel] softkey.

Deleting a remote voice user when you do not know the mailbox number

To find the remote voice user you want to delete when you do not know the mailbox number, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select User Administration.
2	Select Remote Voice User.

Step	Action
3	Press [Find]. **Result:** The Find Remote Voice Users screen is displayed.

```
                          User Administration
Find Remote Voice Users

If a specific location is desired, include the location code prefix
in the mailbox number field.

Mailbox Number: _____________________

Last Name:      ____________________________________

First Name:     ___________________

Department:     ____________________________

Extension Number (DN):          ___________________________

Personal Verification Status:   Any Not_Recorded Recorded

User Type:                      Any Permanent Temporary

Select a softkey >

   Exit          List        Print
```

4 Enter the information you know about the user.

Examples: Last Name, First Name, Department

If you are not sure of your information, or want to see all the remote voice users listed, go to step 5.

5 Press [List].

Result: The List of Remote Voice Users screen is displayed.

```
                          User Administration
List of Remote Voice Users
                                                                  Personal
                                                       User  Last  Verific.
Name          Mailbox                    Department    Type  Access  Recorded
Calhoun,Gavin 8998051                    Public Relatio Perm 6/11/96 Yes
Campbell,Dave 843309                     Reporting      Temp 6/10/96 No
Cathgart,Dr C 843307                     Reporting      Perm 6/13/96 Yes
Defago,Jacque 843306                     Reporting      Temp 6/15/96 Yes
Douglas,Joe   8998055                    Maintenance    Temp 6/11/96 No
Fedora,Alex   8998052                    Public Relatio Perm 6/19/96 Yes
Glass,Fred    8998071                    Marketing      Perm 6/20/96 No
Humber,Carol  8998053                    Public Relatio Perm 6/10/96 Yes
Lebar,Tammy   8998054                    Maintenance    Temp 6/11/96 No
Lee,Wen Mai   8998056                    Product Develo Temp 6/16/96 Yes
Nero,Giuseppe 843305                     Reporting      Perm 6/11/96 Yes
Nova,Louis    8998050                    Marketing      Temp 6/10/96 No
Perez,Manuel  8998057                    Product Develo Perm 6/11/96 Yes
Rowe,Colin    8998058                    Product Develo Perm 6/14/96 Yes

Select a softkey >

   Exit        View/Modify    Delete      Voice
```

6 Select the user you want to delete by moving your cursor to the user's name and pressing the Spacebar.

Step	Action
7	Press [Delete]. **Result:** The Delete Remote Voice User screen is displayed.

```
                          User Administration
Delete Remote Voice User

Mailbox Number:      8998055

Last Name:           Douglas

First Name:          Joe                    Initials: J

Department:          Maintenance

Extension DNs:       8998055


Personal Verification Recorded (Voice):      No

Name Dialable by External Callers:           No Yes
                                                                    MORE BELOW

 OK to Delete    Cancel
```

8	Is this the user you want to delete? • If yes, go to step 9. • If no, press [Cancel].
9	Press the [OK to Delete] softkey. **Result:** The user is deleted and you are prompted for another mailbox number.

How temporary remote voice users are automatically deleted from the system

Introduction

Temporary remote voice users are automatically deleted by the system during nightly audits.

Timestamps

When a temporary remote voice user is added, the date and time at which the user was added is recorded. This is the timestamp.

When the timestamp is updated

This timestamp is updated whenever

- the user is modified via User Administration
- an Enterprise Networking message is received from the remote voice user
- a remote voice user's personal verification or mailbox number (when no verification is recorded) is played

The remote notification is played whenever

- the header of a message from the remote voice user is played
- a message is composed to the remote voice user
- the envelope of a message received from a remote voice user is played (when the local user presses 7-2)
- the remote voice user is name-dialed or name-addressed
- the recipient of a network message uses call sender to call the remote voice user back

Where timestamp information is displayed

The timestamp is displayed in the View/Modify Remote Voice User screen and the List of Remote Voice Users screen in the Last Access Time field.

The cutoff limit

There is a maximum number of temporary remote voice users that can be added to the system. Up to 1000 temporary remote voice users can be added to 1 and 2 node systems. For systems that have 3 or more nodes, up to 10 000 temporary remote voice users can be added. This value can be modified in the Network Configuration screen. The default maximum is 1000.

Whenever the total number of temporary remote voice users exceeds 75% of the cutoff limit, the nightly audit is run to delete some remote voice users.

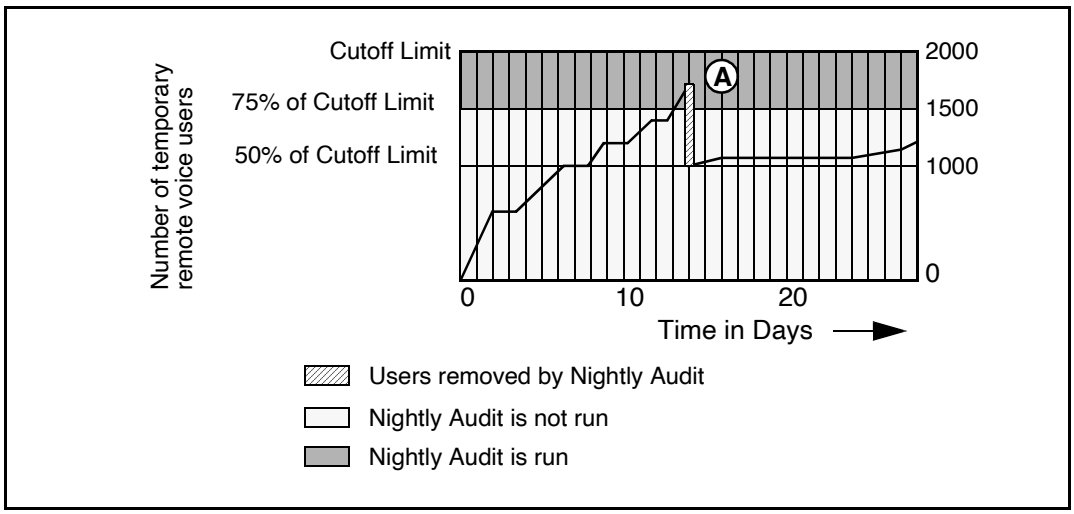
However, temporary remote voice users can still be added (using any method) up to the 100% mark. If this 100% limit is reached, no more remote voice users can be added to the system until after some temporary users are deleted by the audit.

The nightly audit

During the nightly audit, the least recently used users (those with the oldest timestamps) are deleted until the number of remaining temporary voice users equals 50% of the cutoff limit.

Example

The cutoff limit is 2000 temporary remote voice users. On the 14th day (as marked by point A), the number of temporary remote voice users reaches the 75% mark (1500). That night the nightly audit is run and the number of temporary remote voice users is reduced to 1000 (50%).



Chapter 10

Directory entry users

In this chapter

Overview	10-2
What is a directory entry user?	10-3
The Add Directory Entry User screen	10-4
Adding directory entry users	10-7
Recording a personal verification	10-8
The Find Directory Entry Users screen	10-10
Finding directory entry users	10-12
The List of Directory Entry Users screen	10-13
Printing directory entry users	10-15
Viewing or modifying directory entry users	10-16
Deleting directory entry users	10-18

Overview

Introduction

The User Administration screens provide the administrator with the facilities to add, find, view/modify, and delete directory entry users.

This chapter explains who directory entry users are and how to administer them.

User interface

Directory entry users are available in the VMUIF interface but lack name-dial capability (which is specific to the MMUI interface).

What is a directory entry user?

Concept

Directory entry users are users registered in the Meridian Mail directory who do not have mailboxes and, therefore, do not have access to voice messaging functions. They can, however, be referenced by such features as name dialing and automated attendant functions such as voice menus (if they are installed on your system).

Who should be a directory entry user

There are several reasons why users might not have a mailbox associated with their extensions.

- The user may not require or want a mailbox, or perhaps the user is not authorized to have a mailbox.
- Another common reason is that a user shares the same phone with other users. (In other words, you can associate a number of directory entry users with the same DN. This is unlike local voice users in that each local voice user must have a unique primary DN and mailbox number.)

Feature implications

Because directory entry users do not have mailboxes, they do not have access to voice messaging functions (such as compose and send) or other features such as Outcalling, AMIS Networking, and so on.

Directory entry users are included in the Meridian Mail directory. Therefore, you can dial those users using Thru-Dial features such as name dialing and automated attendant.

For example, if three people (say Tom, Dick, and Harriet) share the same phone, then another user can call Tom using the name dialing feature instead of dialing their extension number.

Similarly, an external caller can ring a directory entry user's phone through a voice menu or automated attendant. If the external caller does not remember Tom's extension, the caller can still dial the phone by entering Tom's name.

The Add Directory Entry User screen

Introduction

You may add directory entry users through the Add Directory Entry User screen.

The screen

Following is an example of the Add Directory Entry User screen.

```
                          User Administration
Add Directory Entry User

Last Name:          Adam

First Name:         Patricia            Initials: ____

Department:         EV28

Extension DNs:      7505

Personal Verification Recorded (Voice):      No

Name Dialable by External Callers:           No Yes

Save    Cancel                              Voice
```

Field descriptions

The following table describes the fields in the Add Directory User screen.

Last Name	
Description	This is the last name of the directory entry user. Be sure to fill in this field and ensure correct spelling because the name dialing feature uses this information.
Default	Blank
Maximum length	41 alphanumeric characters
Special characters	This field accepts any characters with the exception of the restricted characters “+”, “#”, and “?”. You should limit yourself to alphanumeric characters for name dialing to work properly.

First Name	
Description	This is the first name of the directory entry user.
Default	Blank
Maximum length	21 alphanumeric characters
Special characters	Same as Last Name

Initials	
Description	These are the initials of the directory entry user. You may use initials to distinguish users with identical first and last names. These initials, however, cannot be used in name dialing. If you do not enter any initials, the system will automatically fill in this field with the first initial of the user's first name.
Maximum length	5 alphanumeric characters

Department	
Description	This is the department of the directory entry user. You can retrieve users on the basis of their department when using the Find Directory Entry Users function (described later in this chapter). Only the first 26 characters of the department are displayed in the List of Directory Entry Users screen. Therefore, make sure that department names are unique based on the first 26 characters of their names.
Note	This field is not available in the VMUIF interface.
Default	Initially blank. After the first user, this field defaults to the department entered for the last user added.
Maximum length	31 alphanumeric characters
Special characters	Same as Last Name

Extension DNs

Description	This is the user's extension number(s). A user can be associated with up to three extensions.
Default	This field defaults to the primary extension.

ATTENTION

Make sure that none of these DNs conflict with any distribution list numbers. If a distribution list and a directory entry user share the same number, the distribution list number will take precedence over a directory entry user number during compose. The message will not be sent to the directory entry user.

Personal Verification Recorded (Voice)

Description	If a personal verification has been recorded for this user, this field displays Yes. No indicates that no verification is currently recorded. The setting in this field changes when the [Voice] softkey is used to record a verification. The personal verification is played when the user's phone is dialed using Thru-Dial service (including name dialing). It informs callers that they have reached the correct phone.

Name Dialable by External Callers

Description	When the field is set to Yes, external callers can reach the user through the name dialing feature. This may occur when a caller reaches a voice menu and is prompted to enter an extension or the name of the person they want to speak to. (Internal callers can always use name dialing to call directory entry users.)
Note	This field is not available in the VMUIF interface.
Default	Yes

Adding directory entry users

Introduction

Use the following procedure to add new directory entry users.

Up to three extensions

Like local voice users, each directory entry user can be associated with up to three different extensions. Primary extension numbers do not have to be unique. A number of users can share the same extension.

Procedure

To add a new directory entry user, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Choose User Administration.
2	Choose Directory Entry User.
3	Press the [Add] softkey.
4	Enter the extension number and press <Return>.
5	Enter the Last Name of the new user.
6	Enter the First Name of the new user.
7	If the interface is MMUI, enter the Department of the new user.
8	Enter the Extension Number(s) of the new user.
9	Do you want to record a personal verification? • If yes, see “Recording a personal verification” on page 10-8. • If no, go to step 10.
10	If the interface is MMUI, do you want external callers to be able to name dial this user? • If yes, set the Name dialable by external callers field to Yes. • If no, set the Name dialable by external callers field to No.
11	Do you want to save the user? • If yes, press [Save]. • If no, press [Cancel].

Recording a personal verification

Introduction

The administrator can use this procedure to record a personal verification on behalf of a directory entry user.

Procedure

To record a personal verification, follow these steps.

Starting Point: The Add Directory Entry User screen, or the View/ Modify Directory Entry User screen

Step	Action
1	Put the cursor on the Personal Verification Recorded (Voice) field.
2	Press the [Voice] softkey.
3	Enter the extension of the phone you will use to record the verification and press <Return>. **Result:** The phone rings.
4	Pick up the receiver. **Result:** The recording softkeys are displayed.
5	Press the [Record] softkey.
6	At the sound of the beep, speak the user's (and, optionally, the user's extension). **Example:** "Billy McGee at extension 8123."
7	Press the [Stop] key to stop recording.

Step	Action
8	Do you want to verify the recording? • If yes, press the [Play] softkey. • If no, go to step 10.
9	Do you want to rerecord the verification? • If yes, press the [Delete] softkey to delete the current recording and repeat steps 5 to 8. • If no, go to step 10.
10	Do you need to record personal verifications for any other users? • If yes, press the [Return] softkey and do not hang up the receiver. The next time you press [Voice] to record another verification, you will not have to reenter the phone extension since the line has not been disconnected. • If no, press the [Disconnect] softkey and hang up the receiver.

The Find Directory Entry Users screen

Introduction

You can locate a directory entry user by extension number or name using the Find function.

The screen

Following is an example of the Find Directory Entry Users screen.

```
                    User Administration
Find Directory Entry Users

Last Name:        Adam

First Name:       Patricia

Department:

Extension Number (DN):

Personal Verification Status:  Any Not_Recorded Recorded

Select a softkey >

Exit        List        Print
```

Field descriptions

The following table describes the fields in the Find Directory Users screen.

Last Name	
Description	Fill in this field if you want to retrieve a particular user and remember only the last name. Use wildcard characters (“+”, “?”, and”_”) if you are unsure of the spelling.

First Name	
Description	Fill in this field if you want to retrieve a particular user and you remember only the first name. If you also know the last name, the first name will narrow the search (if a number of users have the same last name). Use wildcard characters (“+”, “?”, and”_”) if you are unsure of the spelling.

Department	
Description	This field can help you narrow down a search even further if, for example, you can remember only the first or last name of the user you want to find. You can also use this field if you want to retrieve all users that belong to a particular department. Use wildcard characters if you are unsure of the spelling or the exact name of the department.
Extension DNs	
Description	This is the user's primary extension DN. Enter the user's DN if it is known. Use wildcard characters ("+", "?", and"_") to retrieve a subset of users in a particular range of DNs.
Personal Verification Recorded (Voice)	
Description	Set this field to Not_Recorded to retrieve all directory users who do not have a recorded personal verification. Since it is a good idea for all users to have a personal verification, you should record a verification for the user. If the personal verification status is not important, make sure that this field is set to Any (the default).

Finding directory entry users

Introduction

The [Find] softkey can be used to search for a directory entry user, depending upon your search parameters.

Procedure

To access the Find Directory Entry User screen, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Choose User Administration.
2	Choose Directory Entry User.
3	Press the [Find] softkey. **Result:** The Find Directory Entry User screen is displayed.

The List of Directory Entry Users screen

Introduction

The List of Directory Entry Users screen appears when the [List] softkey on the Find Directory Entry Users screen is used. It provides a list of user names matching the search parameters entered in the Find Directory Entry Users screen.

Screen

Following is an example of the List of Directory Entry Users screen.

```
                          User Administration
List of Directory Entry Users
                                                                Personal
                                                                Verific.
Name                                        Department          Recorded
Adam,Patricia                               EU28                   No
Argent,Crystal                              EU28                   No
Babatunde,John Adewale                                             No
Cleveland,Gordon                            EU15                   No
Kimball,Stephanie                           EU28                   No
Locke,Claire                                EU15                   No
Miller,Roy                                  EU28                   No
Ricci,Mario                                                        No
Smith,John                                  EU15                   No
Stash,Joe                                   EU28                   No

Select a softkey >

   Exit          View/Modify      Delete        Voice
```

Field descriptions

The following table describes the fields in the List of Directory Entry Users screen.

Name	
Description	This is the user's last name followed by the first name.
Department	
Description	This is the name of the department to which the user belongs.
Personal Verific. Recorded	
Description	This field indicates whether or not a spoken name (personal verification) has been recorded for this user.

Viewing a list of directory entry users

To view a list of directory entry users from your search, follow this procedure.

Starting Point: The Find Directory Entry Users screen

Step	Action
1	Fill in the screen with the required search parameters.
2	Press [List] to display the results of the search on the screen.
3	To view or modify a directory entry user, move to the user's line and press the <spacebar> to select it.

Printing directory entry users

Introduction

The results of your search for an individual or list of directory entry users can also be printed. Instead of using the [List] softkey on the Find Directory Entry Users screen, use the [Print] softkey.

Screen

Following is an example of the Find Directory Entry Users screen, after being filled out for an individual user.

```
                    User Administration
Find Directory Entry Users

Last Name:      adam

First Name:     patricia

Department:     eu28

Extension Number (DN):          4581

Personal Verification Status:   Any Not_Recorded Recorded

Please ensure that the printer is ready.

                Cancel          Continue
                Printing        Printing
```

Procedure

To print out a list of directory entry users from your search, follow this procedure.

Starting Point: The Find Directory Entry Users screen

Step	Action
1	Do you want to print a list of all directory entry users? • If yes, leave all fields blank. • If no, fill in the screen with the required search parameters.
2	Press the [Print] softkey.
3	Ensure the printer is working and press the [Continue Printing] softkey.

Viewing or modifying directory entry users

Introduction

This procedure explains how to view or modify a directory entry user. Initially, you are prompted for an extension number.

WHEN	THEN
more than one directory entry user is associated with that extension	you will see the List of Directory Entry Users screen (see page 10-13).
only one directory entry user is associated with the extension	the View/Modify Directory Entry User screen is displayed.

Field descriptions

The fields in the View/Modify Directory Entry User screen are identical to those on the Add Directory Entry User screen, described on page 10-4.

Procedure

To view or modify a directory entry user, follow this procedure.

Starting Point: The Main Menu

Step	Action
1	Choose User Administration
2	Choose Directory Entry User.
3	Do you know the user's extension number? • If yes, press the [View/Modify] softkey. Go to step 4. • If no, press, the [Find] softkey.
4	Enter the extension number.

IF	THEN
more than one user shares the extension only	the List of Directory Entry Users screen appears. Go to step 5.
one user is assigned to the extension number	the View/Modify Directory Entry User screen appears. Go to step 6.

Step	Action
5	Choose a user by placing the cursor on the user you want to view or modify. Press the <spacebar> to select the user and press [View/Modify].
6	Modify the fields as needed.
7	Do you want to record a personal verification? • If yes, go to “Recording a personal verification” on page 10-8. • If no, go to step 8.
8	Do you want to save the modified user? • If yes, press [Save]. **Result:** The system saves the modified directory entry user. You are prompted for another extension number. (Go to step 4 to modify another user.) • If no, press [Cancel]. **Result:** Any changes will be discarded. The Directory Entry User Administration softkeys screen or the List of Directory Entry Users screen is displayed.

Deleting directory entry users

Introduction

This procedure explains how to delete a directory entry user.

The Delete Directory Enter User screen

Following is an example of the Delete Directory Entry User screen.

```
                          User Administration
Delete Directory Entry User

Last Name:          Adam

First Name:         Patricia                Initials: P

Department:         EV28

Extension DNs:      7505


Personal Verification Recorded (Voice):     No

Name Dialable by External Callers:          No Yes


OK to Delete    Cancel
```

Procedure

To delete a directory entry user once you have selected the user from the list of users, follow this procedure.

Starting Point: The Main Menu

Step	Action
1	Choose User Administration.
2	Choose Directory Entry User.
3	Do you know the user's extension DN? • If yes, press the [Delete] softkey and go to step 6. • If no, press the [Find] softkey. **Result:** The Find Directory Entry Users screen is displayed.

Step	Action
4	Enter the extension number.

IF	THEN
more than one user shares the extension only	the List of Directory Entry Users screen appears. Go to step 5.
one user is assigned to the extension number	the View/Modify Directory Entry Users screen appears. Go to step 6.

5	Choose a user by placing the cursor on the user you want to delete. Press the <spacebar> to select the user and press [Delete].
6	Do you want to delete the user? • If yes, press [OK to Delete]. • If no, press [Cancel].

Chapter 11

Distribution lists

In this chapter

Overview	11-2
Understanding distribution lists	11-3
Limitations on distribution lists	11-4
Accessing the Distribution Lists softkeys screen	11-7
Adding a system distribution list	11-9
Finding and viewing a system distribution list	11-17
Modifying a system distribution list	11-22
Printing a system distribution list	11-24
Deleting a system distribution list	11-26

Overview

Introduction

This chapter provides an overview of distribution lists. It explains what a distribution list is and briefly sets out the differences between system and personal distribution lists.

It also provides information and procedures for administering system distribution lists:

- adding a system distribution list
- finding an existing system distribution list
- viewing a system distribution list
- modifying a system distribution list
- printing a system distribution list
- deleting a system distribution list

Understanding distribution lists

Introduction

A distribution list is a mailing list that enables you to send the same message to a number of people. After you add and save a distribution list, you can reuse it whenever you need to send messages to the same group or groups of people.

Adding a distribution list involves assigning a unique number and title to the list and specifying the mailbox numbers that you want to include on it. If you choose to, you can also make a voice recording of the list's title.

When you compose a message, you specify the distribution list number as you would any other mailbox number. Then when you send your message, it is deposited in every mailbox included in the list.

There are two types of distribution lists: system distribution lists and personal distribution lists.

This chapter contains information about administering system distribution lists. Personal distribution lists are explained in the *Meridian Mail Voice Messaging User Guide* (P0839942).

Definition: system distribution list

You add a system distribution list through Meridian Mail User Administration.

You can add any number of system distribution lists, each containing up to 120 entries.

Definition: personal distribution list

Meridian Mail users create personal distribution lists from their telephone sets.

A user can create up to 9 personal distribution lists, each containing up to 99 entries.

Limitations on distribution lists

Introduction

This topic presents an overview of factors that affect the creation and use of distribution lists.

Message number and size

The number of addresses to which a user can successfully send a message simultaneously depends on the size of the message, as shown in the following table.

Length of message	Number of addresses
90 minutes voice	up to 290 addresses
60 minutes voice	up to 350 addresses
10 minutes voice	up to 425 addresses
1 minute voice	up to 440 addresses

Note: Each system distribution list is one address, regardless of the number of entries on the list, while each entry on a personal distribution list is one address. Therefore, a system distribution list with 10 entries is 1 address, while a personal distribution list with 10 entries is 10 addresses.

Restrictions on distribution list numbers

The following restrictions are placed on distribution list numbers:

- A system distribution list cannot be assigned a number between 1 and 9. These numbers are reserved for personal distribution lists.
- Each distribution list must have a unique distribution list number.
- A distribution list number must not conflict with any dialing plan prefixes or codes. (These are explained further in the description of the List Number field on page 11-12.) This includes the Network Wide Broadcast Prefix, defined in the Network Configuration screen.
- A distribution list number cannot be the same as any mailbox number, including the broadcast mailbox number. The default broadcast mailbox number is 5555.

- A distribution list number cannot share a directory entry user's DN. If a distribution list number and a directory entry user number are the same, the distribution list number takes precedence over the directory entry user number when a list is composed.

MMUI restrictions

Distribution lists can include the following types of numbers:

- mailbox numbers of local voice users (including users at any location in an NMS network)
- mailbox numbers of remote voice users
- broadcast mailbox numbers for particular Networking sites and NMS locations (personal distribution lists only)

To include a mailbox number at an AMIS site, you must have Meridian Networking installed. You must also define the AMIS site as a virtual node in the Meridian network. For more information, refer to the *Virtual Node AMIS Installation and Administration Guide* (NTP 555-7001-245).

To include individual users at remote sites in a Meridian network, you must define them as remote voice users in the local database.

The following types of numbers do not have mailboxes associated with them and, therefore, cannot be included in a distribution list:

- numbers of directory entry users
- remote notification targets
- delivery to non-user targets

Restrictions on personal distribution lists

A personal distribution list can contain up to 99 entries. There are, however, some limitations on the total number of addresses to which an outgoing message can be sent using personal distribution lists. If a user tries to send a message to a number of distribution lists, he or she may get the following message if the maximum address size of the message is exceeded: *"Your command cannot be completed at this time. Please try again, or contact your administrator."* The message is deleted, and the user is positioned at the next message in the mailbox (or at the end of the mailbox) and can use other commands normally.

Note: If VMUIF is installed and you want VMUIF subscribers to be able to address messages to personal distribution lists, you must define a personal distribution list prefix in the Voice Messaging Options screen. By default, no prefix is defined.

Accessing the Distribution Lists softkeys screen

Introduction

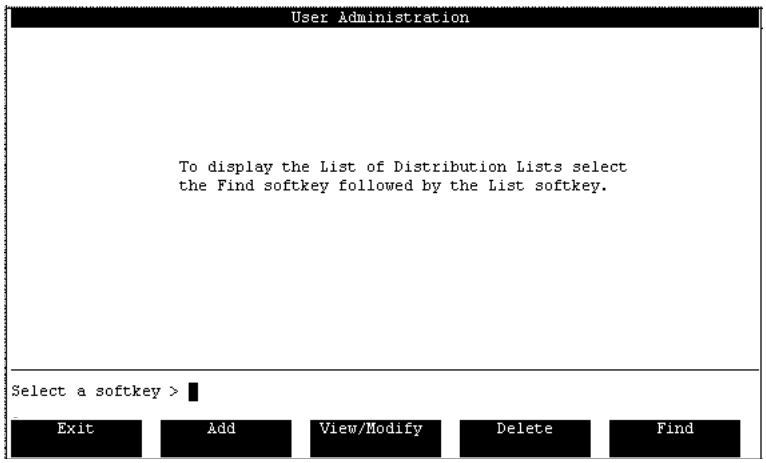
Many of the administration tasks concerned with distribution lists begin with the Distribution Lists softkeys screen. These tasks include the following:

- adding a distribution list by using the [Add] softkey
- adding mailboxes to or removing mailboxes from an existing distribution list by using the [View/Modify] softkey
- deleting a distribution list by using the [Delete] softkey
- finding a distribution list by using the [Find] softkey followed by the [List] softkey

This topic explains how to get to the Distribution Lists screen.

The Distribution Lists softkeys screen

The following shows an example of the Distribution Lists softkeys screen.



Procedure

To go to the Distribution Lists softkeys screen, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select User Administration.
2	Select Distribution Lists. **Result:** The system displays the Distribution Lists softkeys screen.

Adding a system distribution list

Introduction

You add a distribution list using the Add Distribution List screen. Adding a distribution list involves assigning a unique number and title to the list and specifying the mailbox numbers that you want to include on it. If you choose to, you can also make a voice recording of the list's title.

When you compose a message, you specify the distribution list number as you would any other mailbox number. Then when you send your message, it is deposited in every mailbox included in the list.

If you assign numbers to distribution lists that are of a different length from those you use as mailbox numbers, you are able to avoid confusion or conflict with your mailbox numbers.

Although making a voice recording of the list title is optional, the voice recording has the same purpose as a personal verification. That is, it is played when a distribution list number is entered when addressing messages. The list title describes who is included in the list or the purpose of the list. This makes it easier to identify whether you have entered the correct list number when you address messages.

The Add Distribution List screen

The following shows an example of the Add Distribution List screen.

```
                          User Administration
Add Distribution List

List Number:        6011
List Title:         Management Operations
List Title Recorded (Voice):  No
Mailbox Numbers:
2001                2002
2003                2004
2005                2006
2007                2008
2009                2010

Save    Cancel    More Fields    Voice
```

Field descriptions

The following table describes the fields in the Add Distribution List screen.

Location Prefix	
Description	This number identifies the location where the mailboxes on the list (or those to be added to the list) reside. ***Note:*** The system displays this field only if Network Message Service (NMS) is installed. If you do not specify a location prefix, the system defaults to your current administration context. See "Setting the default administration context for NMS" on page 8-8.
Default	There is no default.
Valid range	There is no default range.

Location Name	
Description	This field indicates the name of the location that corresponds to the location prefix. (See the description above for the Location Prefix field.)
Default	There is no default.
Valid range	There is no default range.

List Number	
Description	This value uniquely identifies the distribution list. The list number cannot be the same as the following numbers: • personal distribution list numbers The single digits 1 to 9 are reserved for personal distribution lists. • any mailbox number, including the broadcast mailbox number The default broadcast mailbox number is 5555. • a directory entry user's DN If a distribution list and a directory entry user share a number, the distribution list number takes precedence over the directory entry user number when a list is composed. • the name dialing prefix The default name dialing prefix is 11. Do not use 11 to number a list unless you have changed the name dialing prefix in the Voice Messaging Options screen. • the Delivery to Non-User prefix • another distribution list number • any dialing plan access code prefixes • the Network-Wide Broadcast prefix
Default	There is no default. You can use any valid number.
Valid range	from 10 to 999999999999999999 (there are 18 9s; only digits are allowed)

List Title	
Description	This is the title of the distribution list. It can be up to 41 characters in length. Do not use “?”, “+”, or “_” (underscore) which are wildcard characters. The title can be used to address the distribution list by name when you are composing and sending a message to mailboxes on the distribution list.
Default	There is no default value.
Valid range	There is no default range.

List Title Recorded (Voice)	
Description	This read-only field indicates whether a voice recording of the list title has been made. It is a good idea to record a title for each distribution list. This helps you to identify the list after you have entered its number when composing a message. Choose a name that uniquely identifies this list. This field changes only when you use the [Voice] softkey to record or delete a list title.
Default	No
Valid range	There is no default range.

Mailbox Numbers	
Description	In these fields, you type the mailbox numbers of the users you want to include on the distribution list. Mailbox numbers can be up to 18 digits in length. If Meridian Networking is installed and enabled, you can enter up to 28 characters in each of these fields. You can include up to 120 mailbox numbers in a system distribution list. To add more mailbox fields, use the [More Fields] softkey.
Default	These fields are blank.
Valid range	from 10 to 999999999999999999 (there are 18 9s) ***Note:*** These must be valid local and remote voice users.

Adding a system distribution list

To add a system distribution list, follow these steps.

Starting Point: The Distribution Lists softkeys screen

Step	Action
1	Select the [Add] softkey. **Result:** The system prompts for a distribution list number.
2	Type a valid number. **Note:** For information about valid distribution list numbers, see the description of the List Number field on page 11-12. **Result:** The system displays the Add Distribution List screen.
3	Type a name for the list in the List Title field.
4	Type the mailbox numbers of the users you want to include in the distribution list. **Note:** If you are including the mailbox number of a remote voice user, type the network prefix (ESN prefix or CDP steering code), followed by the mailbox number. The system informs you if any of the numbers are not valid.
5	To add more mailboxes, use the [More Fields] softkey. **Note:** The system draws one row of fields each time you use this softkey. You can include up to 120 mailboxes in a system distribution list.
6	Make a voice recording of the title of the distribution list. **Note:** This step is optional. For more information, see “Recording a distribution list title” on page 11-15.

Step	Action
7	Use the following table to determine the next step.

IF you want to	THEN
save your distribution list	go to step 8.
add another distribution list	go to step 8.
exit without saving your distribution list	go to step 9.

Step	Action
8	To save your distribution list, use the [Save] softkey. **Result:** The system saves your distribution list. If your distribution list is long, it may take a few moments to save. The system then prompts you to enter a number for a new distribution list. To add another distribution list, type a valid number, and go to step 3. **Note:** For information about valid distribution list numbers, see the description of the List Number field on page 11-12.
9	To exit without saving your distribution list, use the [Cancel] softkey. **Result:** The system does not save the distribution list, and you are returned to the Distribution Lists softkeys screen.

Recording a distribution list title

To make a voice recording of the title of a distribution list, follow these steps.

Note: This procedure is optional.

Starting Point: The Distribution Lists softkeys screen

Step	Action
1	Select the [View/Modify] softkey. **Result:** The system prompts for a distribution list number.
2	Type the number of the distribution list for which you are recording a title.
3	Select the [Voice] softkey. **Result:** The system prompts for an extension number.
4	Type the extension number of the telephone set you are going to use to record the title, and press <Return>. **Result:** The phone rings.

Step	Action
5	Pick up the telephone handset. **Result:** The system displays the recording softkeys.
6	Select the [Record] softkey. **Result:** The system displays a message on the console requesting you to make the recording. The system displays the [Stop] softkey in place of the [Record] softkey. You hear a beep through the telephone receiver.
7	At the beep, say the list title into the telephone handset.
8	To stop recording, use the [Stop] softkey. **Result:** The recording stops automatically, and the system again displays the recording softkeys.
9	If you are satisfied with the recording, select either the [Disconnect] softkey or the [Return] softkey. **Note:** When you use the [Return] softkey, the line is not disconnected unless you hang up the receiver. This means that if you decide to rerecord or listen to the recording, you do not have to type the telephone extension again after selecting the [Voice] softkey. When you use the [Disconnect] softkey, the line is disconnected, and if you select the [Voice] softkey to access the recording softkeys again, you must again type the telephone extension.

Finding and viewing a system distribution list

Introduction

The Find function generates a list of distribution lists. Use this function to locate a particular distribution list or a subset of lists.

Use the List function to view onscreen the distribution lists that you retrieve. You can then view, modify, or delete these distribution lists.

The Find Distribution Lists screen

The following shows an example of the Find Distribution Lists screen. In this example, the user is searching for a list by name.

```
                          User Administration
Find Distribution Lists

List Number:      ________________

List Name:        Management Operations_________________


Select a softkey >

 Exit |          | List | Print Titles | Print Entries
```

Field descriptions

For explanations of the fields in the Find Distribution Lists screen, see “Field descriptions” on page 11-11.

The fields are identical to those in the Add Distribution List screen, except that you can use the wildcards “ +”, “_”, and “?” to retrieve subsets of lists.

Using wildcards

If you do not know the name or number of a list you want to retrieve but do not want to retrieve all available distribution lists, you can use wildcards to narrow your search.

Types of wildcards

There are three wildcards that you can use.

Wildcard	Description
_	The underscore (_) replaces a single character.
+	The plus sign (+) replaces a string of characters.
?	The question mark (?) produces a “sound match”. It finds distribution lists with names that sound alike.

Examples

The following examples show how wildcards can be used to find a subset of distribution lists.

You enter	Result
“2_” in the List Number field	All lists in the range 20 to 29 are found.
“3+” in the List Number field	All distribution lists beginning with 3 are found.
“+Engineering” in the List Name field	All distribution lists that end in “Engineering” are found (such as Software Engineering, Hardware Engineering, Information Engineering).
Braymore?	All distribution lists with names that sound like Braymore (Breymore, Braemore), are found.

Finding and viewing a distribution list

To find a distribution list or a subset of a distribution list, follow these steps.

Starting Point: The Distribution Lists softkeys screen

Step	Action
1	Select the [Find] softkey. **Result:** The system displays the Find Distribution Lists screen.
2	Use the following table to determine the next step.

IF you want to	THEN
find a distribution list	type the complete number or name of the list.
find a subset of a distribution list	use wildcard characters to create a search pattern. **Example:** To retrieve all lists beginning with 1, type **1+** in the List Number field. **Note:** For more information about wildcards, See “Using wildcards” on page 11-18.
retrieve a distribution list whose name you do not know	leave both fields blank.

Step	Action
3	To view a list of the retrieved distribution lists, use the [List] softkey. **Result:** The system displays the List of Distribution Lists screen. **Note:** The system displays only the first 20 characters of the name of each retrieved list.
4	Use the following table to determine the next step.

IF you want to	THEN
print the retrieved list title or list entries	go to step 5.
modify a retrieved list	see “Modifying a system distribution list” on page 11-22.
delete a retrieved list	see “Deleting a system distribution list” on page 11-26.

Step	Action
5	Use the [Print Titles] softkey or the [Print Entries] softkey, depending on what you want to print.

IF you want to print	THEN
the titles and list numbers only	select the [Print Titles] softkey.
the mailboxes associated with the retrieved list or lists	select the [Print Entries] softkey.

Result: The system displays the [Continue Printing] softkey and the [Cancel Printing] softkey.

It also prompts you to check that the printer is ready.

6 Use the following table to determine the next step.

IF you want to	THEN
print the list	go to step 7.
cancel printing	go to step 8.

7 Select the [Continue Printing] softkey.

Result: The system begins to print the distribution list titles or entries.

When printing is complete, the system again displays the Find Distribution Lists screen.

Note: To stop printing at any time, select [Cancel Printing].

8 Select the [Cancel Printing] softkey.

Result: The system cancels the print operation, and you are returned to the List of Distribution Lists screen.

Note: There may be some delay before control is returned to the screen because the system waits for the printer to stop.

The List of Distribution Lists screen

The following shows an example of the List of Distribution Lists screen with two retrieved lists.

```
                          User Administration
List of Distribution Lists

                      List Number          List Title
                      6011                 Management Operation
                      6012                 Mngt Ops Subgroup

Select a softkey >

   Exit                 View/Modify        Delete
```

Field descriptions

For explanations of the fields in the List of Distribution Lists screen, see “Field descriptions” on page 11-11. The fields are identical to those in the Add Distribution List screen.

Modifying a system distribution list

Introduction

This topic explains how to make changes to an existing distribution list. From the View/Modify Distribution List screen, you can add one or more mailbox numbers to a distribution list. You can change the mailboxes that you include on a list, or you can delete one or more mailboxes.

Note: To delete an entire distribution list, see "Deleting a system distribution list" on page 11-26.

The View/Modify Distribution List screen

The following shows an example of the View/Modify Distribution List screen.

```
                          User Administration
View/Modify Distribution List

List Number:        6012
List Title:         Mngt Ops Subgroup
List Title Recorded (Voice):  No
Mailbox Numbers:
2001                          2005
2006                          2009
2002

   Save      Cancel                More Fields     Voice
```

Field descriptions

For explanations of the fields in the View/Modify Distribution List screen, see "Field descriptions" on page 11-11. The fields are identical to those in the Add Distribution List screen.

Procedure

To modify a distribution list, follow these steps.

Starting Point: The Distribution Lists softkeys screen

Step	Action
1	Do you know the number of the distribution list you want to modify? **IF** — **THEN** yes — go to step 2. no — see “Finding and viewing a system distribution list” on page 11-17.
2	Select the [View/Modify] softkey. **Result:** The system prompts for a distribution list number.
3	Type the number of the list you want to modify, and press <Return>. **Result:** The system displays the View/Modify Distribution List screen.
4	Make your changes to your list. **Note:** Use the [More Fields] softkey if you reach the last available mailbox number and wish to add more mailboxes to the list. You can include up to 120 mailboxes in a system distribution list.
5	Use the following table to determine the next step. **IF you want to** — **THEN** save your distribution list — go to step 6. exit without saving your distribution list — go to step 7.
6	To save your modified distribution list, use the [Save] softkey. **Result:** The system saves your changes. It then prompts you for another distribution list number. To modify another list, go to step 3.
7	To exit without saving your changes, use the [Cancel] softkey. **Result:** The system returns you to the Distribution Lists softkeys screen.

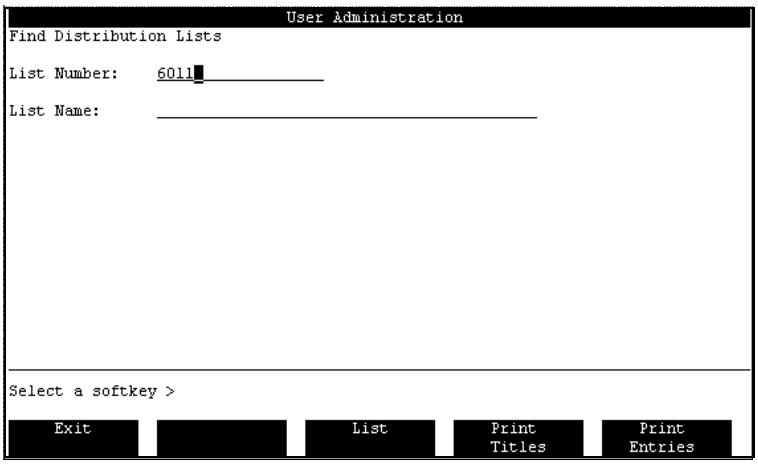
Printing a system distribution list

Introduction

This topic explains how to print information in a system distribution list using the softkeys in the Find Distribution Lists screen.

The Find Distribution Lists screen

The following shows the position of the print keys on the Find Distribution Lists screen.



Field descriptions

For explanations of the fields in the Find Distribution List screen, see “Field descriptions” on page 11-11. The fields are identical to those in the Add Distribution List screen.

Procedure

To print distribution list information, follow these steps.

Starting Point: The Find Distribution Lists screen

Step	Action
1	Use the [Print Titles] softkey or the [Print Entries] softkey, depending on what you want to print. **IF you want to print** — **THEN** the titles and list numbers only — select the [Print Titles] softkey. the mailboxes associated with the retrieved list or lists — select the [Print Entries] softkey. **Result:** The system displays the [Continue Printing] softkey and the [Cancel Printing] softkey. It also prompts you to check that the printer is ready.
2	Use the following table to determine the next step. **IF you want to** — **THEN** print the list — go to step 3. cancel printing — go to step 4.
3	Select the [Continue Printing] softkey. **Result:** The system begins to print the distribution list titles or entries. When printing is complete, the system again displays the Find Distribution Lists screen. **Note:** To stop printing at any time, go to step 4.
4	Select the [Cancel Printing] softkey. **Result:** The system cancels the print operation, and you are returned to the List of Distribution Lists screen. **Note:** There may be some delay before control is returned to the screen because the system waits for the printer to stop.

Deleting a system distribution list

Introduction

This topic explains how to delete a system distribution list using the Delete Distribution List screen. This screen enables you to view a distribution list before you delete it.

To delete mailbox numbers from a distribution list but not the entire list, see “Modifying a system distribution list” on page 11-22.

The Delete Distribution List screen

The following shows an example of the Delete Distribution List screen.

```
                          User Administration
Delete Distribution List

List Number:       6012
List Title:        Mngt Ops Subgroup
List Title Recorded (Voice):  No
Mailbox Numbers:
2001                          2002
2005                          2006
2009

OK to Delete   Cancel
Entire List
```

Field descriptions

For explanations of the fields in the Delete Distribution List screen, see “Field descriptions” on page 11-11. The fields are identical to those in the Add Distribution List screen.

Note: In the Delete Distribution List screen, these fields are read-only.

Procedure

To delete a system distribution list, follow these steps.

Starting Point: The Distribution Lists softkeys screen

Step	Action
1	Do you know the number of the distribution list you want to delete? **IF** — **THEN** yes — go to step 2. no — see “Finding and viewing a system distribution list” on page 11-17.
2	Select the [Delete] softkey. **Result:** The system prompts for a distribution list number.
3	Type the number of the list you want to delete, and press <Return>. **Result:** The system displays the Delete Distribution List screen.
4	Use the following table to determine the next step. **IF you want to** — **THEN** delete your distribution list — go to step 5. exit without deleting your distribution list — go to step 6.
5	To delete your distribution list, use the [Delete] softkey. **Note:** The system deletes the list. It then prompts you for another distribution list number. To delete another list, go to step 3.
6	To exit without deleting the list, use the [Cancel] softkey. **Result:** The system returns you to the Distribution Lists softkeys screen.

Chapter 12

General administration–an overview

In this chapter

General Administration 12-2

General Administration

Introduction

This chapter provides an overview of the General Administration menu and related screens.

The General Administration menu

When you select the General Administration option from the main menu, the General Administration menu appears.

```
General Administration

        1  General Options
        2  Volume and Selective Backup
        3  Restore from Selective Backup
        4  Change System Administrator Password
        5  Change Customer Administrator Password
        6  Change AdminPlus Download Password
        7  Change System Time
        8  Dialing Translation

Select an item >

   Exit
```

General Options

The General Options option allows you to

- view installed features
- assign Classes of Service to the system
- configure the following:
  - — attendant DN
  - — date formats for reports
  - — SEER printer

Volume and Selective Backup

The Volume and Selective Backup option allows you to make backup copies of some or all of the data stored on your hard disk. You can perform the following types of backups:

- full backup to tape
- partial backup to tape or disk

Note: Partial backup to disk can only be done if the Disk-to-Disk Backup feature is installed.

- selective backup of users
- selective backup of services

Restore from Selective Backup

The Restore from Selective Backup option allows you to restore data that was selectively backed up to tape.

Note: If you want to restore your system using the data from a full or partial backup, you must use the Restore from backup utility available on the Install/data tape. For more information on this utility, refer to the *System Installation and Modification Guide* (NTP 555-7001-215).

Change System Administrator Password

The Change System Administrator Password option allows you to change the password for the administration terminal. Your password should be changed on a regular basis to ensure maximum security.

Change Customer Administrator Password

The Change Customer Administrator Password option allows you to change the password for Multiple Administration Terminals (MATs). Your password should be changed on a regular basis to ensure maximum security.

Change AdminPlus Download Password

The Change AdminPlus Download Password option allows you to change the password used by Meridian Mail Reporter (MMR) to download data from the system. The same password must be set up on the MMR side before data can be downloaded. This password must be set up when the system is installed as the default value will not allow the download to take place.

Note: This option only appears if the AdminPlus feature is installed.

Change System Time

The Change System Time option allows you to change your system time.

Dialing Translation

If Fax on Demand or AMIS Networking, or both, are installed, you must set up translation tables. These tables tell Meridian Mail how to translate collected digits (from an AMIS message

header or a fax callback number entered by a caller) into a number that Meridian Mail can dial.

Note: In Meridian Mail 12, this option appears for all Meridian 1 systems.

Related chapters

The following table describes which chapter you should refer to when using one of the General Administration menu options.

For the following option	See
General Options	Chapter 13, “General options.”
Volume and Selective Backup	Chapter 15, “Back up and restore Meridian Mail data.”
Restore from Selective Backup	Chapter 15, “Back up and restore Meridian Mail data.”
Change System Administrator Password	Chapter 16, “Password and system time changes.”
Set Minimum Length for Administrator Passwords	Chapter 16, “Password and system time changes.”
Change AdminPlus Download Password	Chapter 16, “Password and system time changes.” For more information on Meridian Mail Reporter, refer to the MMR document (P0847870).
Change System Time	Chapter 16, “Password and system time changes.”
Dialing Translation	Chapter 17, “Dialing translations.”

Chapter 13

General options

In this chapter

Overview	13-2
Accessing the General Options screen	13-3
Modifying the system name and system number	13-5
Defining the system addressing length and the supervised transfer delay	13-8
Verifying installed features	13-11
Assigning classes of service to the system	13-13
Setting the attendant DN	13-15
Setting the date format for reports	13-18
Setting printer port names	13-20

Overview

Introduction

Defining general system options involves the following:

- assigning classes of service to the system
- defining the attendant DN
- setting the date format for reports
- specifying the SEER printer and Reports printer port names

Modifying general options

Review the default settings in the General Options screen to see which fields you need to modify in order to customize the system to satisfy your requirements.

Accessing the General Options screen

Introduction

All of the procedures in this chapter are performed from the General Options screen.

Procedure

To access the General Options screen, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration and press <Return>. **Result:** The General Administration menu appears.

```
                    General Administration

          1  General Options

          2  Volume and Selective Backup

          3  Restore from Selective Backup

          4  Change System Administrator Password

          5  Change Customer Administrator Password

          6  Change System Time

          7  Dialing Translation

Select an item >

     Exit
```

Step	Action
2	Select General Options and press <Return>. **Result:** The General Options screen appears.

```
                    General Administration
General Options

System Name:                    MeridianMail

System Number:                  0

System Addressing Length:       0

Supervised Transfer Delay (CS): 200

Minimum Admin Password Length:  6

Allow Duplicate User DNs:       No Yes

Available Features:
                                Integrated Mailbox Administration
                                Dual Language Prompting
                                Outcalling
                                                                MORE BELOW
Select a softkey >

   Save        Cancel
```

Modifying the system name and system number

Introduction

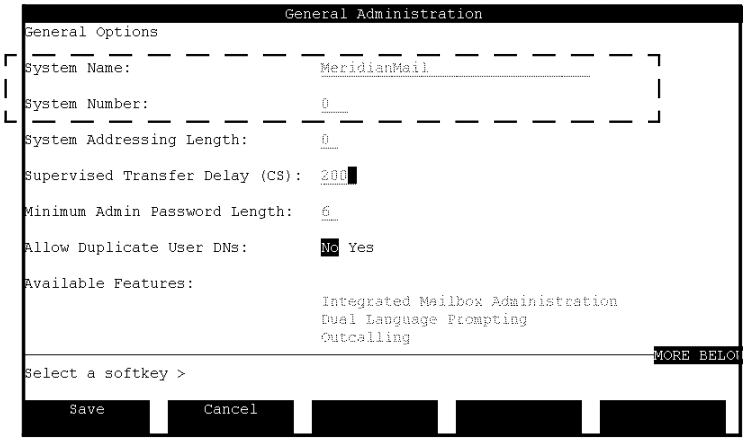
The system name and system number are defined during installation.

When to use

Use this procedure if you need to modify the system name or number, or both, from the values defined during installation.

The General Options screen

The dotted box highlights the fields in the General Options screen in which you define the system name and number.



Field descriptions

This table describes the fields used to define the system name and number.

System Name	
Description	This is the name by which Meridian Mail is identified. This name is printed on all reports and lists in Meridian Mail.
Default	The name supplied during installation.
Maximum length	You can enter up to 30 alphanumeric characters.

System Number	
Description	This field is prefilled with the number supplied during system installation. The system number must match the Meridian 1's customer number.
Attention	Because this number is entered during installation, you should not have to change it. If there is a mismatch with the Meridian 1's customer number, certain Meridian Mail features that dial out (such as call sender and thru-dial) will not work.
Default	The value supplied during installation.

Procedure

To change the system name or number, follow these steps.

Starting Point: The General Options screen

Step	Action
1	Delete the current name and enter the new name in the System Name field.
2	Change the system number, if necessary. **Attention:** The system number must equal the Meridian 1 customer number. **Note:** If you modify the system number, you must reboot the system for the change to take effect.
3	Have you finished modifying general options? • If yes, press [Save] to save your changes and return to the General Administration menu. • If no, go to the next procedure to continue modifying general options, or press [Cancel] to return to the General Administration menu without saving your changes.

Defining the system addressing length and the supervised transfer delay

System addressing length

The system addressing length is intended for Meridian Mail systems connected to DMS-family and SL-100 switches. When set to a non-zero value, the address expansion feature is enabled.

Address expansion is used on systems where the local addressing lengths are shorter than the system addressing lengths.

Meridian 1

For systems connected to Meridian 1 PBXs, the system addressing length should be set to 0 to disable address expansion. This is the default.

Supervised transfer delay

Usage

This transfer delay is used by ACCESS applications when transferring a call to a non-local telset. It is important in cases where the telset to which the call is transferred is busy.

Meridian Mail 11 and 12 versus prior releases

In releases prior to Meridian Mail 11, this delay was set to 200 centi-seconds (2 seconds) and could not be modified.

Default and range

200 centi-seconds is now the default, but it can be modified (to a value between 100 and 1000 centi-seconds, or 1 to 10 seconds).

Centi-seconds

A centi-second is 1/100th of a second. Therefore, 100 centi-seconds equals 1 second.

Do you need to change the default?

If you get reports of callers hearing busy signals when transferred from an ACCESS application to a telset, you need to increase this value.

Finding the right value for your system may take some trial and error. Try incrementing this value by 50 or 100 centi-seconds until you find a setting that works for your system.

How it works

When an ACCESS application transfers a call off-switch, it waits for the amount of time specified in the delay field. If the telset is busy, a certain amount of time is required to detect the busy signal.

If the delay is not long enough, the busy signal is not detected, the call is transferred to the telset, and the caller hears the busy signal. When the busy signal is detected, the transfer is denied.

The General Options screen

The dotted box highlights the fields in the General Options screen in which you define the system addressing length and supervised transfer delay.

```
                    General Administration
General Options

System Name:                    MeridianMail

System Number:                  0

System Addressing Length:       0

Supervised Transfer Delay (CS): 200

Minimum Admin Password Length:  6

Allow Duplicate User DNs:       No Yes

Available Features:
                                Integrated Mailbox Administration
                                Dual Language Prompting
                                Outcalling
                                                                MORE BELOW
Select a softkey >

   Save        Cancel
```

Procedure

To change the system addressing length and supervised transfer delay, follow these steps.

Starting Point: The General Options screen

Step	Action
1	Leave the system addressing length as 0.
2	If the current delay is too short to detect busy signals, then increase the value in the Supervised Transfer Delay field.
3	Have you finished modifying general options? • If yes, press [Save] to save your changes and return to the General Administration menu. • If no, go to the next procedure to continue modifying general options, or press [Cancel] to return to the General Administration menu without saving your changes.

Verifying installed features

When to use

Use this procedure if you need to verify the features that are installed on your system.

The General Options screen

View the list of Available Features in the General Options screen.

```
                    General Administration                    MORE ABOVE
General Options


Available Features:
                                Multiple Administration Terminals
                                Meridian ACCESS
                                AdminPlus
                                Voice Messaging (MMUI)
                                Voice Messaging (VMUIF)
                                AMIS
                                Dual Language Prompting
                                Outcalling
                                Voice Menus & Announcements
                                Voice Forms
                                Meridian Mail Networking

                                                                MORE BELOW
Select a softkey >

   Save        Cancel
```

Possible features

These are the features that may be installed on your system:

- Multiple Administration Terminals
- Disk To Disk Backup
- Meridian ACCESS (Unix Access)
- AdminPlus
- Meridian Mail AutoAdmin
- Integrated Mailbox Administration
- Voice Messaging (MMUI)
- Voice Messaging (VMUIF)
- Hospitality

  Note: Voice Messaging (MMUI), Voice Messaging (VMUIF), and Hospitality are mutually exclusive and cannot be installed on the same system.
- Network Message Services (NMS)

- Voice Menus and Announcements

  This feature allows you to create the following voice services: Voice Menus, Announcements, Thru-Dial services, Time-of-Day Controllers, Prompt Maintenance, and Remote Activation.
- Voice Forms
- Fax on Demand

  This enables a number of fax-related services: Fax Information Service, Fax Item Maintenance Service, Fax Call Back Delivery, and Fax Same Call Delivery.
- Meridian Mail Networking (not available for VMUIF customer groups)

To make the following features available to users, certain fields must be enabled in the user's class of service:

- AMIS
- Dual Language Prompting (MMUI only)
- Outcalling (includes Remote Notification and Delivery to Non-User)

Assigning classes of service to the system

Introduction

Once you have created Meridian Mail classes of service (through Class of Service Administration), you must assign them to the system. Otherwise, they will not be available when you add local voice users.

The General Options screen

The dotted box highlights the fields in which you assign classes of service to the system.

```
                          General Administration                MORE ABOVE
General Options

                                Voice Menus & Announcements
                                Voice Forms
                                Fax On Demand
                                Meridian Mail Networking

Class of Service Selection:     __ __ __ __ __ __ __ __
                                __ __ __ __ __ __ __ __

Attendant DN:                   0_____________________

Date Format for Administration
and Maintenance Reports:        mm/dd/yy yy/mm/dd dd/mm/yy

Valid printer port/device names can be viewed by selecting View/Modify for
each printer from Data Port Configuration in the Hardware Administration menu.
                                                                MORE BELOW
Select a softkey >

   Save        Cancel
```

Field description

You enter the classes of service that you want to assign to the system in the Class of Service Selection fields.

When adding local voice users, you will assign them to one of the COSs specified here.

Default
All fields are blank.

Maximum number of classes of service
You can enter up to 15 classes of service in these fields.

Procedure

To assign classes of service, follow these steps.

Starting Point: The General Options screen

Step	Action
1	Use the cursor keys to move to the Class of Service Selection field.
2	Enter up to 15 classes of service in the Class of Service Selection fields.
3	Have you finished modifying general options? • If yes, press [Save] to save your changes and return to the General Administration menu. • If no, go to the next procedure to continue modifying general options, or press [Cancel] to return to the General Administration menu without saving your changes.

Setting the attendant DN

The attendant DN

The Attendant DN is the extension number to which a caller is transferred when the user's revert DN is unsuccessful or undefined.

The revert DN

When adding users, you can define a unique revert DN for each user. If the Custom Revert DN feature is enabled, users can define their own revert DNs from their telsets.

When the attendant DN is used

The Attendant DN that is defined in General Options is used if the revert DN is not defined or the call is not successfully transferred to the user's revert DN.

The revert DN and attendant DN are used under two conditions.

Call answering
A caller can press "0" during a call answering session in order to transfer to another number (such as that of an attendant or secretary). This gives callers the chance to transfer to a person for assistance.

Mailbox thru-dial (extension dialing)
Mailbox thru-dial allows MMUI users to dial a number while they are logged into their mailbox. The user enters "0" followed by the number. If the user waits for more than 2 seconds after entering "0", he or she is transferred to the revert DN.

See also

For more information, see "The revert DN" on page 8-26.

The General Options screen

The dotted box highlights the field in which you define the Attendant DN.

```
                          General Administration                MORE ABOVE
General Options

                                  Voice Menus & Announcements
                                  Voice Forms
                                  Fax On Demand
                                  Meridian Mail Networking
                                  Network Message Services

Class of Service Selection:       __ __ __ __ __ __ __ __
                                  __ __ __ __ __ __ __

Attendant DN:                     0

Date Format for Administration
and Maintenance Reports:          mm/dd/yy yy/mm/dd dd/mm/yy

Valid printer port/device names can be viewed by selecting View/Modify for
each printer from Data Port Configuration in the Hardware Administration menu.
                                                                MORE BELOW
Select a softkey >

   Save        Cancel
```

Field description

This field may be left blank. However, it is recommended that you define this DN so that it can serve as a backup if the user's revert DN is not defined or unsuccessful.

Maximum length

You can enter a DN that is up to 30 digits in length. This DN can begin with 0.

Default

0

Procedure

To change the attendant DN, follow these steps.

Starting Point: General Options screen

Step	Action
1	Use the cursor keys to move to the Attendant DN field.
2	Do you want to revert callers to a DN other than 0? • If yes, delete the current DN and enter the new DN in the Attendant DN field. • If no, leave the Attendant DN field set to 0.
3	Have you finished modifying general options? • If yes, press [Save] to save your changes and return to the General Administration menu. • If no, go to the next procedure to continue modifying general options, or press [Cancel] to return to the General Administration menu without saving your changes.

Setting the date format for reports

Introduction

The date format that is selected in General Options is used on administration and maintenance reports.

The General Options screen

The dotted box highlights the field in which you specify the date format.

```
                          General Administration                    MORE ABOVE
General Options


Class of Service Selection:      _ _ _ _ _ _ _ _
                                 _ _ _ _ _ _ _

Attendant DN:                    0_________________________

Date Format for Administration
and Maintenance Reports:         mm/dd/yy yy/mm/dd dd/mm/yy

Valid printer port/device names can be viewed by selecting View/Modify for
each printer from Data Port Configuration in the Hardware Administration menu.

SEER Printer Port Name:          ___________   (Blank implies the console port)

Reports Printer Port Name:       ___________   (Blank implies the console port)

Select a softkey >

 Save      Cancel
```

Field description

The date format selected in the Date Format for Administration and Maintenance Reports field affects the following:

- reports generated by Meridian Mail (including operational measurements)
- SEERs
- the format for inputting dates in Meridian Mail screens

Default

The default is mm/dd/yy.

Valid options

You can choose from the following date formats:

- mm/dd/yy (default)
- yy/mm/dd
- dd/mm/yy

Procedure

To change the date format, follow these steps.

Starting Point: The General Options screen

Step	Action
1	Use the cursor keys to move to the date format field.
2	Select the date format you want used on reports and in screens.
3	Have you finished modifying general options? • If yes, press [Save] to save your changes and return to the General Administration menu. • If no, go to the next procedure to continue modifying general options, or press [Cancel] to return to the General Administration menu without saving your changes.

Setting printer port names

Introduction

You can define separate printer port names for a SEER printer and a reports printer.

If you do not define these printer port names, SEERs or reports, or both, are printed to the console printer port.

The General Options screen

The dotted box highlights the fields in which printer port names are defined.

```
                          General Administration                MORE ABOVE
General Options

                                  Network Message Services

Class of Service Selection:       __ __ __ __ __ __ __ __
                                  __ __ __ __ __ __ __

Attendant DN:                     0_________________________

Date Format for Administration
and Maintenance Reports:          mm/dd/yy yy/mm/dd dd/mm/yy

Valid printer port/device names can be viewed by selecting View/Modify for
each printer from Data Port Configuration in the Hardware Administration menu.

SEER Printer Port Name:           ___________   (Blank implies the console port)

Reports Printer Port Name: __ __ __________  (Blank implies the console port)

Select a softkey >

   Save        Cancel
```

Field descriptions

This table describes the printer port name fields.

SEER Printer Port Name	
Description	This is the printer port to which the SEER printer is connected.
Requirement	You must have additional data ports on an RSM card to support a SEER printer. They must be defined as printer ports in the hardware database.
Default	Blank If this field is left blank, the SEERs will print to the console printer port.
Maximum length	The printer port name may be up to 12 alphanumeric characters long.

Reports Printer Port Name	
Description	This is the printer port to which the Reports printer is connected. Operational measurements and general print jobs from the administration terminal are sent to this printer.
Requirement	Additional data ports on an RSM card are required. The data ports must be defined as printer ports in the hardware database.
Default	Blank If this field is left blank, the reports will print to the console printer port.
Maximum length	You can enter a printer port name up to 12 alphanumeric characters long.

Procedure

To set or change the printer port names, follow these steps.

Starting Point: The General Options screen

Step	Action
1	Use the cursor keys to move to the printer name field to be modified.
2	Have you set up a special printer for SEERs? • If Yes, enter its port name in the SEER Printer Port Name field. • If No, leave this field blank and proceed to the next step.
3	Have you set up a special printer for printing reports? • If Yes, enter its port name in the Reports Printer Port Name field. • If No, leave this field blank and proceed to the next step.
4	You are finished defining general options. Do you want to save your changes? • If yes, press [Save]. **Result:** The changes are saved, and you are returned to the General Administration screen. • If no, press [Cancel]. **Result:** The changes are not saved, and you are returned to the General Administration screen.

Chapter 14

Volume administration

In this chapter

Overview	14-2
Volume names	14-3
Volume contents	14-5
Volume distribution on single- and multi-node systems	14-7
Voice storage capacity in single- and multi-node systems	14-8
Checking volume capacity and usage levels for your system	14-10

Overview

Introduction

Meridian Mail systems can have from one to five nodes, each of which contains a hard disk drive for data storage. The hard disk drives are partitioned into volumes. Volumes are storage areas for system and user-related information.

Volume administration involves making backup copies of some or all of the data stored on a hard disk. If a disk fails, data can be restored from the backup so that the system can be brought back into service quickly with minimal loss of information.

Volume names

Introduction

Volume names are used to identify volume partitions on hard disk drives. The volumes are already set up when your Meridian Mail system is installed.

Definition

Each hard disk on each node is partitioned into two volume types: system and user. Volume names follow specific formats to ensure easy identification when backing up the system.

In the first node, the system volume is named VS1 and the user volume is named VS2.

In three-node, four-node, and five-node configurations, the disk drive on the first node contains no user volume. Volumes on nodes other than the first node are named VStnnX.

Components

Volume names consist of four components. These four components are listed in the following table.

Component	Description
VS	Volume server
t	The first digit in the volume name indicates the type of information stored on the volume. Possible digits are 1 system information 2 user information 9 disk-to-disk backup (if installed, for partial backup)
nn	The last two digits in the volume number indicate the node number.
X	The region on the volume, either T for text data, or V for voice data.

Example

VS205T refers to the text region (T) of a user volume (2) on node 5 (05).

Name exceptions

There are some special cases where volume names differ from the standard volume name format.

These are the exceptions:

- User volume on node 1 is labeled VS2.
- System volume on node 1 is labeled VS1.
- Full backup of VS1 creates volume backup labels B102V and B102T.

Volume contents

Introduction

The two types of volumes, system and user, contain different sets of information. For backup purposes, it is important to be aware of the type of information stored on each volume type.

System volume

The system volume VS1 contains the user information listed below:

- each user's personal verification
- system profile
- corporate directory
- operation measurement traffic and billing data
- program software
- network database*
- voice menus and announcements*
- voice forms*
- fax items*
- network message queues
- voice prompts for third and fourth languages*

Items marked with an asterisk (*) may not be installed and stored on VS1, depending on how your system was set up.

Note: Voice services (voice menus, voice forms, fax items) are stored on VS1 by default. However, they can be moved to another volume if there is not enough space on VS1.

User volumes

The user volumes (VS2, VS202, VS203, VS204, VS205) can contain the following information:

- messages
- greetings
- voice services (voice menus, voice forms, fax items) which may be moved from VS1 to VS2 or VS202 if voice services require more space than is available on VS1
- user information
- voice prompts for first and second languages (on VS2 only)
- voice form responses

Volume distribution on single- and multi-node systems

Introduction

Single-node and multi-node systems contain different volume configurations.

Node contents

The following table shows the possible volume configuration for each node.

System	Node 1	Node 2	Node 3	Node 4	Node 5
Single-node	VS1 - system VS2 - user				
Two-node	VS1 - system VS2 - user VS901- backup	VS202 - user VS902 - backup			
Three-node	VS1 - system VS2 - system VS901 - backup	VS202 - user	VS203 - user		
Four-node	VS1 - system VS2 - system VS901 - backup	VS202 - user	VS203 - user	VS204 - user	
Five-node	VS1 - system VS2 - system VS901- backup	VS202 - user	VS203 - user	VS204 - user	VS205 - user

Voice storage capacity in single- and multi-node systems

Voice storage capacity The following table shows the voice storage capacity for single-node and multi-node systems.

Voice Storage capacity		Maximum hours available for voice storage (per disk volume)						
System Size	**Total hours per volume**	**VS1**	**VS2**	**VS202**		**VS203**	**VS204**	**VS205**
1-node 1.2 Gbyte disk (EC and ModOp)	5 11 24 36 54 100 200*	2 2 3.5 3.5 3.5 5.5 10.2	5 11 24 36 54 100 200					
2-node 1.2 Gbyte disk (EC and ModOp)	26 54 84 114 200 400*	2 3.5 3.5 3.5 5.5 10.2	11 24 24 54 100 200	15 30 60 60 100 200	n/a 22.2 52.2 52.2 90.1 184.8			
3-node 1.2 Gbyte disk (EC and ModOp)	30 60 90 120 200 400*	18.4 18.4 18.4 18.4 18.4 51.9		15 30 60 60 100 200	n/a 6.3 36.3 36.3 76.3 142.4	15 30 30 60 100 200		
4-node 1.2 Gbyte disk (EC and ModOp)	45 90 120 180 300 600*	18.4 18.4 18.4 18.4 18.4 68.6		15 30 60 60 100 200	n/a 5.3 35.3 35.3 75.3 124.5	15 30 30 60 100 200	15 30 30 60 100 200	

Voice Storage capacity		Maximum hours available for voice storage (per disk volume)						
System Size	**Total hours per volume**	**VS1**	**VS2**	**VS202**		**VS203**	**VS204**	**VS205**
5-node 1.2 Gbyte disk (EC and ModOp)	60 120 180 240 400 800*	19.6 19.6 19.6 19.6 19.6 86.6		15 30 60 60 100 200	— 2.4 32.4 32.4 72.4 104.6	15 30 30 60 100 200	15 30 30 60 100 200	15 30 60 60 100 200
Note: VS202 lists two columns of figures. The first column is without disk-to-disk backup. The second column is with disk-to-disk backup.								
* — A 2.0 Gbyte disk is required for each of these configurations.								

Additional language exceptions

The number of languages your system uses has an impact on the available volume capacity for each hard disk.

If your system has three or more nodes and a second language installed, subtract three hours from the volume capacity of VS2. If your system only has one or two nodes, then subtract three hours from the volume capacity of VS1.

If your system has a third language installed, subtract three hours from VS1, and an additional three hours for the fourth language.

Checking volume capacity and usage levels for your system

Description

The Volume and Selective Backup screen displays all the volumes on your system, their designated use, their capacity in kbytes and equivalent hours and minutes, and the percentage of voice and data storage currently used.

Accessing the Volume and Selective Backup screen

To access the Volume and Selective Backup screen, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen is displayed.

Volume and Selective Backup screen

The following shows the Volume and Selective Backup screen.

```
                          General Administration
  Volume and Selective Backup


  Volume     Use                Volume Size            Usage(%Full) Number of
  Name                        Data          Voice       Data Voice  Mailboxes
                            (KBytes)  (KBytes) (hh:mm)
  VS1        System           52720    155520    19:04     33    16        0
  VS202      Users            21488    526080    64:29      1     0       20
  VS203      Users             9856    271360    33:16      1     0        0
  VS204      Users             9856    271360    33:16      1     0        0
  Selective  Messages&PDLs
  Selective  Services
                            Total number of mailboxes on the system       20


Move the cursor to the desired items and press the space bar to select.

   Exit        Backup        |          Backup Status    View/Delete
               To Tape       |                           Schedule
```

Field descriptions

This table describes the fields in the Volume and Selective Backup screen.

Volume Name	
Description	Displays the name of the volume. The volume name indicates the type of data contained on the volume, and the node on which it resides.
Format	Volume names are in the format VSTnn. The region of the volume (x) is not displayed.
Valid options	Any of the listed volumes.

Use	
Description	Describes the type of volume, either system or user.

Volume Size Data (kbytes)	
Description	Displays the amount of storage allocated for blocks of data on the volume.
Measurement	Storage is expressed in thousands of bytes (kbytes).

Volume Size Voice (kbytes)	
Description	Displays the amount of storage allocated for blocks of voice data on the volume.
Measurement	Storage is expressed in thousands of bytes (kbytes).

Volume Size Voice (hh:mm)	
Description	Displays the amount of storage allocated for blocks of voice data on the volume.
Measurement	Storage is expressed in hours and minutes.

Usage (% Full) Data	
Description	Displays the percentage of allocated data storage currently in use.

Usage (% Full) Voice	
Description	Displays the percentage of allocated voice storage currently in use.

Number of Mailboxes	
Description	Displays the number of local voice users on the volume.
Dependency	This number is dependent on the number of voice users configured for your system.

Total number of mailboxes on the system	
Description	Displays the total number of mailboxes on the system.

Checking disk capacity and usage levels

For information on checking disk capacity and usage levels for your system, see “Disk Usage Detail report” on page 31-52.

Chapter 15

Back up and restore Meridian Mail data

In this chapter

Overview	15-2
Section A: Preparing for backups	15-3
Section B: Full and partial backups to tape	15-15
Section C: Selective backup of users and services	15-23
Section D: Partial backups to disk	15-39
Section E: Scheduled backups	15-41
Section F: Backup maintenance	15-47
Section G: Restoring information from a Selective backup	15-53

Overview

Description

This chapter

- explains the importance of Meridian Mail system backups
- suggests which volumes to back up, and how frequently
- describes selective backup of mailboxes and services
- describes the two available backup media, and how to perform a backup with either one
- describes the procedures for scheduling a backup to occur automatically at a later time, and for checking on the status of a backup in progress
- describes procedures for restoring selective backup data from backup media (disk or tape) back to the Meridian Mail system

Section A: Preparing for backups

In this section

Overview	15-4
The three types of backups	15-5
Selective backup	15-6
Partial backup	15-8
Full backup	15-9
Volumes to back up	15-10
How often to do backups	15-11
Disk backup or tape backup	15-13
Before you perform a backup	15-14

Overview

Introduction

This section describes the three types of backups: selective, partial, and full.

It is important to perform backups regularly as they provide a safeguard against disk failure. Recovery from a system where no backups have been made entails a complete reentry of all user and site-specific information.

Nightly audits

Nightly VS audits have been modified to permit an overnight full backup. If a backup is running, the VS audit will be repeatedly delayed until either the backup completes or a specified time limit, set upon installation, is reached, (around 4:30 a.m.). If the time limit is reached, the VS audit will force the backup to be aborted. Previously, overnight full backups were likely to fail due to a conflict with one of the automatic nightly VS audits.

The Volume and Selective Backup screen

The following is an example of the Volume and Selective Backup screen where backup options are accessed.

```
                          General Administration
  Volume and Selective Backup


  Volume     Use                Volume Size            Usage(%Full) Number of
  Name                        Data          Voice       Data Voice  Mailboxes
                            (KBytes)  (KBytes) (hh:mm)
  VS1        System           52720    155520    19:04     33    16       0
  VS202      Users            21488    526080    64:29      1     0      20
  VS203      Users             9856    271360    33:16      1     0       0
  VS204      Users             9856    271360    33:16      1     0       0
  Selective  Messages&PDLs
  Selective  Services
                          Total number of mailboxes on the system      20



Move the cursor to the desired items and press the space bar to select.

    Exit        Backup        |          Backup Status    View/Delete
                To Tape       |                           Schedule
```

The three types of backups

Introduction

There are three types of backups that can be performed:

- selective
- partial
- full

Description

The three backup options allow you to select the appropriate type for your backup without always having to perform a full backup.

Selective backup

Selective backups allow you to back up user messages, personal distribution lists, and multimedia services. Selective backup also enables you to back up mailboxes by specific criteria (such as volume or department).

Partial backup

Partial backups save the administration configuration of the system, including the system volume and user profiles. This type of backup saves user data only, not voice.

Full backup

Full backups back up all volumes on your system, including voice and data from system and user volumes.

Selective backup

Introduction

The selective backup option provides online backups for user messages, personal distribution lists (PDLs), and multimedia services.

Description

The selective backup feature provides you with considerable flexibility in backing up data. User messages, PDLs, and multimedia services may be backed up at any time or as part of the regular backup schedule.

Backup criteria for messages and PDLs

To use the selective backup option, you must select a criteria by which to back up from the list below. You can select only one criteria per selective backup, and this criteria defines the content to be backed up:

- all messages and PDLs of all users on the system
- by volume, up to the total number of volumes on the system
- by classes of service, up to 15
- by departments, up to five input areas. The wildcards '+' and '_' are permitted so that more than five departments may be backed up.
- by individually specified mailboxes, up to 10 input areas. The wildcards '+' and '_' are permitted so that more than 10 mailboxes may be backed up.

Note: Only one wildcard can be used per input field, and it should be the last character.

Example

Valid	Invalid
805+	80+1
805_	80_1

Backup criteria for voice services

One of the following criteria must be selected for the selective backup of voice services:

- all voice services on the system
- by service ID, up to 30 input areas. The wildcards '+' and '_' are permitted so that more than 30 services may be backed up.

Note: Only one wildcard can be used per input field, and it should be the last character.

Example

Valid	Invalid
805+	80+1
805_	80_1

Backup order

If a selective backup is chosen together with a regular backup, the volume backups will always be done first. The selective backup will always be the last backup on the tape.

Partial backup

Introduction

Partial backups allow you to back up and save the administration configuration of your system. It will back up the system volume and user profiles. During a restore, this avoids having to reenter user information; however, all voice messages and user greetings will be lost.

Data that is backed up

When you perform a partial backup, you save the administration configuration of the system including the following:

- the user database
- spoken names (personal verification)
- voice services (voice menus, voice forms, fax items) if stored on VS1

Volumes that are backed up

A partial backup saves the following volumes:

- VS1T
- VS1V
- VS1B
- VS901T

Exceptions

Partial backups do not back up the following information:

- users' voice data (including voice messages and greetings)
- voice services (voice menus, voice forms, fax items) if stored on a volume other than VS1

Full backup

Introduction

A full backup is used to back up all system and user voice and data on the entire system. A full backup is not normally done unless significant changes have been made to your system.

Data that is backed up

A full backup backs up all system data including

- the user database
- spoken names (personal verification)
- voice services (voice menus, voice forms, fax items)
- users' voice data (including voice messages and greetings)

Volumes that are backed up

A full backup saves the following volumes:

- VS1T
- VS1V
- VS1B
- all VSxT, VSxV, and VSxB, where x is 2 or 202 through 205, depending on the number of nodes in your system.

VS1B

VS1B is a temporary volume that is created during backup and is copied to tape. It is automatically deleted from disk once the backup is complete.

Exceptions

Normally, full backups are not done because user messages and greetings are transitory and do not warrant the extra time required to back them up.

> **CAUTION**
>
> **Risk of data loss**
>
> If the loss of messages carries financial or legal implications, weekly or even daily backups of voice data may be warrranted.

Volumes to back up

Introduction

Backups are essential to safeguard your system against disk failure. It is important to back up volumes with all necessary system and user voice and data information.

Volumes recommended for regular backup

The following table shows the recommended volumes for backup on single-node, two-node, three-node, four-node, and five-node systems.

Volumes marked with * store data unless voice services are installed there, in which case you select Voice and Data, rather than Data.

Single-node system	Two-node system	Three-node system	Four-node system	Five-node system
VS1 - Voice and Data	VS1 - Voice and Data	VS1 - Voice and Data	VS1 - Voice and Data	VS1 - Voice and Data
VS2 - Data *	VS2 - Data *	VS202 - Data *	VS202 - Data *	VS202 - Data
	VS202 - Data *	VS203 - Data *	VS203 - Data *	VS203 - Data *
			VS204 - Data *	VS204 - Data *
				VS205 - Data *

How often to do backups

Introduction

Backups should be performed regularly. Recovery from a system where no backups have been made entails a complete reentry of all user and site-specific information.

Nightly audits

Nightly VS audits have been modified to permit an overnight full backup. If a backup is running, the VS audit will be repeatedly delayed until either the backup completes, or a specified time limit, set upon installation, is reached (around 4:30 a.m.). If the time limit is reached, the VS audit will force the backup to be aborted.

Backup considerations

Keep the following in mind when determining how often and when to do backups:

- Backups should be carried out at a time when the system is relatively quiet, or outside the regular business hours for your organization.
- Do not back up the system while it is being actively used (more than half the ports or channels are active). The system may not have enough resources to complete the backup.
- Backups to disk can be done frequently with relatively little effort, and reduce the need for frequent and time-consuming backups to tape. However, disk-to-disk backups do not eliminate the need for tape backups.

Location of voice services

Verify where voice services (such as voice menus, thru-dialers, and voice forms) are stored.

ATTENTION

If voice services are stored on a volume other than VS1, be sure to do a full backup of that volume, selecting the Voice and Data option.

Verifying the location of voice services

To verify where voice services are stored, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Services Administration.
3	Select Voice Services Profile.
4	Check the Voice Services Volume field. This is where voice services are stored.

System backup requirements

A field support representative can restore a system to the state it was in at the time of the last backup. To ensure that this recovery process is complete, you should make certain that you have on hand a complete set of backup tapes.

If no backups have been kept, a complete reentry of all user and site-specific information will be required. How often you back up your data is influenced by how often changes are made to user and system information. If you make important changes to the system daily, then daily backups may be in order.

Disk backup or tape backup

Introduction

Meridian Mail offers two types of backups, disk and tape.

Disk backup

Backup to disk can be either partial or selective. To use the backup-to-disk feature, the disk-to-disk option must be installed. Full backups cannot be done to disk and must be backed up using tape.

On multi-node systems, the backup-to-disk option copies selected information from the first hard disk to the second hard disk on the system. This allows for data to be copied from one disk to another in order to allow for recovery after a single disk failure. Backup to disk can be done frequently with relatively little effort, and reduces the need for frequent and time-consuming backups to tape.

Backups to disk do not completely eliminate the need for tape backups.

> **CAUTION**
>
> **Risk of data loss**
>
> If a disk failure occurs in the middle of a disk-to-disk backup, the copy will not be consistent and recovery from this backup copy will not be possible. For this reason, disk-to-tape backups should also be performed periodically.

Tape backup

Backup to tape allows for the backup of the entire Meridian Mail system including voice and data on all volumes. This provides you with a full backup copy of all information needed to restore your system to full working order in case of failure.

All Meridian Mail systems have a tape drive capable of reading and writing industry-standard 1/4-inch data cartridges.

Before you perform a backup

Overview

There are many considerations that need to be taken into account before performing a backup.

Timing

Avoid backing up the system between the hours of 1:00 a.m. and 5:00 a.m. since important system audits take place during these hours.

Do not back up the system when it is operating above 50% of the rated capacity for call answering, voice messaging, and port usage. Try to choose the lowest traffic time outside of the audit hours.

Storage

Backup tapes should be stored in a secure area free of electromagnetic fields. Important backups should be stored off-site for added security.

Store tapes in their cases, label them clearly, and set the write protection tab (turn the rotating knob until the arrow points to Safe).

Other backup considerations

Consider the following before backing up:

- Restoring from a full or partial backup from tape involves downtime as the system is booted from tape and data is restored onto disks one at a time.
- Do not schedule a backup to tape that requires multiple tapes unless you will be around during the backup to switch tapes.
- Do not use Nortel software distribution tapes for backing up your system; these tapes are important for recovering from disk failures.
- Do not reuse the same tapes for consecutive backups. It is recommended that you maintain at least two sets of backup tapes and that you use these sets in rotation.

Section B: Full and partial backups to tape

In this section

Overview 15-16
Performing a full backup to tape 15-18
Performing a partial backup to tape 15-20

Overview

Introduction

This section details information on full and partial backups to tape.

Types of tape drives

Meridian Mail supports two tape drives: the Tandberg TDC4220 drive, and the Archive Viper drive.

The Tandberg TDC4220 drive reads and writes tapes with a capacity up to 2.5 Gbytes and is backwards compatible with all existing Meridian Mail tapes.

The Archive Viper drive supports a maximum storage capacity of 250 Mbytes, and should be used only with DC6250 tapes.

CAUTION

Risk of tape load failure

Use of 6150 tapes may cause tape load failures. 6150 tapes are no longer supported.

Using the Archive Viper tape drive

When using a Viper tape drive, insert the tape with the metal side facing the left side of the drive and the opening on the tape facing up. Once the tape is inserted, secure it by pressing down on the lever on top of the opening until the latch catches. To remove a tape, slide the latch up and the tape will be ejected.

Using the Tandberg tape drive

When using a Tandberg tape drive, press the Release button to open the door. (If there is a tape in the drive already, remove it.) Gently push the tape into the drive and close the door. To remove a tape, press the Release button to open the door and remove the tape.

Write-protection

Tape cartridges can be write-protected by turning the rotating knob on the cartridge until the arrow points to the Safe indicator. Any attempt to write on a write-protected cartridge will generate an error.

Tape errors

If a tape error occurs during backup, you do not have to restart the backup process from tape 1. Follow the instructions as they appear on your screen. In some instances, you are required to keep the tape, as the data that was recorded is not corrupt; in other instances, you will be required to discard the tape. At this stage, you should clean the tape heads before inserting another tape. See “Cleaning/maintaining the tape drive” on page 15-52.

Performing a full backup to tape

Introduction

A full backup to tape backs up all of your system and user voice and data.

Labeling backup tapes

During every backup, all tapes should be labeled and numbered as they are removed from the tape drive.

Backup tape requirements and time estimates

The following table lists the backup tape requirements for a full backup for each system.

One full backup (250 Mbyte tapes)					
System	**# Tapes**	**System**	**# Tapes**	**System**	**# Tapes**
1 node		2 node		3 node	
5 h	1	26 h	2	30 h	2
11 h	1	54 h	3	60 h	4
24h	2	84 h	4	90 h	5
36 h	2	114 h	5	120 h	6
54 h	3	200 h	8	200 h	9
100 h	5				
4 node		5 node			
45 h	3	60 h	3		
90 h	5	120 h	5		
120 h	6	180 h	8		
180 h	8	240 h	10		
300 h	12	400 h	16		

Procedure

To perform a full backup to tape, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Position the cursor on the volume you want to back up, and press <Space Bar> to select it. **Note:** It is recommended that you back up only one volume at a time. However, you can select more than one volume.
4	Press [Backup to Tape]. **Result:** The Disk to Tape Backup screen appears.
5	Enter an appropriate label for this backup.
6	Use the arrow keys to move to the Backup Options column. Select Voice and Data for a full backup.
7	Do you want to back up now? • If yes, then press [Immediate Backup] and go to step 8. **Result:** If you select Immediate Backup, the softkeys change to [OK to Start Backup] and [Cancel]. The system also displays how much data (in Mbytes) will be backed up. • If no, go to “Scheduling the backup for a later time” on page 15-42.
8	Insert the tape for backup into the tape drive. See “Overview” on page 15-16 for information on inserting tapes.
9	Do you want to continue with the backup? • If yes, press [OK to Start Backup] to initiate the backup. **Result:** The tape is automatically retensioned. • If no, press [Cancel] to return to the Disk to Tape backup screen.
10	If the tape becomes full, you are prompted to insert the next tape. **Note:** Do not remove the tape from the tape drive until it has finished rewinding.
11	Repeat this procedure until all volumes have been backed up.

Performing a partial backup to tape

Introduction

A partial backup to tape backs up your system configuration and user information. This backup backs up only user data, and not voice.

Labeling backup tapes

During every backup, all tapes should be labeled and numbered as they are removed from the tape drive.

Backup tape requirements and time estimates

The following table lists the backup tape requirement estimates for a partial backup for each system.

One partial backup (250 Mbyte tapes)					
System	# Tapes	System	# Tapes	System	# Tapes
1 node		**2 node**		**3 node**	
5 h	1	26 h	1	30 h	1
11 h	1	54 h	1	60 h	1
24h	1	84 h	1	90 h	1
36 h	1	114 h	1	120 h	1
54 h	1	200 h	1	200 h	1
100 h	1				
4 node		**5 node**			
45 h	1	60 h	1		
90 h	1	120 h	1		
120 h	1	180 h	1		
180 h	1	240 h	1		
300 h	1	400 h	2		

Procedure

To perform a partial backup to tape, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume Administration and Selective Backup. **Result:** The Volume Administration and Selective Backup screen appears.
3	Position the cursor on the volumes you want to back up, and press <Space bar> to select them.
4	Press [Backup to Tape]. **Result:** The Disk to Tape Backup screen appears.
5	Enter an appropriate label for this backup.
6	Use the arrow keys to move to the Backup Options column.
7	Are you backing up the system volume? • If yes, select Voice and Data. • If no (you are backing up a user volume), select Data.
8	Do you want to back up now? • If yes, then press [Immediate Backup]. **Result:** The [OK to Start Backup] and [Cancel] softkeys are displayed. • If no, go to “Scheduling the backup for a later time” on page 15-42.
9	Insert the tape for backup into the tape drive. See “Overview” on page 15-16 for information on inserting tapes.
10	Do you want to continue with the backup? • If yes, press [OK to Start Backup]. **Result:** The tape is automatically retensioned. • If no, press [Cancel] to return to the Disk to Tape Backup screen.
11	If the tape becomes full, you are prompted to insert the next tape. **Note:** Do not remove the tape from the tape drive until it has finished rewinding.

Section C: Selective backup of users and services

In this section

Overview	15-24
Backing up all users	15-25
Backing up individual users	15-27
Backing up all users in a specified volume	15-29
Backing up all users assigned to a particular class of service	15-31
Backing up all users in a specific department	15-33
Backing up all multimedia services	15-35
Backing up selected individual multimedia services	15-37

Overview

Introduction

The selective backup feature allows for the selective backup of user messages, personal distribution lists (PDLs), and multimedia services. Selective backups can be performed as immediate backups or scheduled on a regular basis.

Example

The Selective Backup and Restore feature allows users to request a backup of their messages and PDLs for safekeeping, and can have them restored at any time. If scheduled daily selective backups are being done, the user can request the restore of an accidentally deleted message or PDL and have it restored from the previous day's backup.

Flexibility

The selective backup feature offers new flexibility in backing up and restoring data. User messages, PDLs, and multimedia services may be backed up at any time or as part of the regular backup schedule.

Selective backup criteria

When specifying which data to back up, there are a number of criteria from which to choose. To back up messages and PDLs, one (and only one) of the following criteria may be used:

- all the messages and PDLs of all users on the system
- by volume, up to the total number of volumes on the system
- by classes of service, up to 15
- by departments, up to five input areas
- by individually specified mailboxes, up to 10 input areas (more can be backed up using the wildcards '+' and '_')

For services, one of the following criteria may be used:

- all services on the system
- by service ID, up to 30 input areas (more can be backed up using the wildcards '+' and '_')

Backing up all users

Introduction

The selective backup All option backs up all mailboxes on the system.

Labeling backup tapes

During every backup, all tapes should be labeled and numbered as they are removed from the tape drive.

Procedure

To perform a selective backup of all users, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Use the arrow keys to move to SELECTIVE BACKUP Messages and PDLs, press the Space Bar, and then press [Backup To Tape]. **Result:** The Disk to Tape Backup window appears.
4	Enter an appropriate label for this selective backup.
5	Use the Space Bar or arrow keys to select All, and press the Tab key.
6	Enter the appropriate label for this selective backup.
7	Do you want to back up now? • If yes, then press [Immediate Backup]. **Result:** The softkeys change to [OK to Start Backup] and [Cancel]. • If no, go to “Scheduling the backup for a later time” on page 15-42.
8	Insert the tape for backup into the tape drive. See “Overview” on page 15-16 for information on inserting tapes.

Step	Action
9	Do you want to continue with the backup? • If yes, press [OK to Start Backup]. **Result:** The tape is automatically retensioned. • If no, press [Cancel] to return to the Disk to Tape Backup screen.
10	If the tape becomes full, you are prompted to insert the next tape. **Note:** Do not remove the tape from the tape drive until it has finished rewinding.

Backing up individual users

Introduction

The selective backup Individual option allows you to select specific mailboxes for backup by mailbox number.

Up to 10 individual mailbox input areas are provided, but the actual number of mailboxes may be much larger with the use of wildcards ('+' and '_').

Labeling backup tapes

During every backup, all tapes should be labeled and numbered as they are removed from the tape drive.

Procedure

To perform a selective backup of specified individual users, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Use the arrow keys to move to SELECTIVE BACKUP Messages and PDLs, press the Space Bar to select it, and then press [Backup To Tape]. **Result:** The Disk to Tape Backup window appears.
4	Enter an appropriate label for this selective backup.
5	Use the Space Bar or arrow keys to select Individual, and press the Tab key.
6	Enter the mailbox numbers for all individual mailboxes to back up. Use wildcards '+' and '_' to specify more than 10 mailboxes. **Note:** Wildcards are only permitted as the last character of an input, and only one wildcard is allowed per input field.

Step	Action
7	Do you want to back up now? • If yes, then press [Immediate Backup]. **Result:** The softkeys change to [OK to Start Backup] and [Cancel]. • If no, go to “Scheduling the backup for a later time” on page 15-42.
8	Insert the tape for backup into the tape drive. See “Overview” on page 15-16 for information on inserting tapes.
9	Do you want to continue with the backup? • If yes, press [OK to Start Backup]. **Result:** The tape is automatically retensioned. • If no, press [Cancel] to return to the Disk to Tape Backup screen.
10	If the tape becomes full, you are prompted to insert the next tape. **Note:** Do not remove the tape from the tape drive until it has finished rewinding.

Backing up all users in a specified volume

Introduction

The selective backup volume option backs up all users in the specified volume. As many volumes may be specified as are on the system.

Recommendation

It is recommended that you perform selective backups on a different tape from other backups (such a volume backups.)

Labeling backup tapes

During every backup, all tapes should be labeled and numbered as they are removed from the tape drive.

Procedure

To perform a selective backup of specified volumes, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Use the arrow keys to move to SELECTIVE BACKUP Messages and PDLs, press Space Bar to select it, and then press [Backup To Tape]. **Result:** The Disk to Tape Backup window appears.
4	Enter an appropriate label for this selective backup.
5	Use the Space Bar or arrow keys to select Volume, and press the Tab key.
6	Enter the volume numbers to be backed up.
7	Do you want to back up now? • If yes, then press [Immediate Backup]. **Result:** The softkeys change to [OK to Start Backup] and [Cancel]. • If no, go to “Scheduling the backup for a later time” on page 15-42.

Step	Action
8	Insert the tape for backup into the tape drive. See “Overview” on page 15-16 for information on inserting tapes.
9	Do you want to continue with the backup? • If yes, press [OK to Start Backup]. **Result:** The tape is automatically retensioned. • If no, press [Cancel] to return to the Disk to Tape Backup screen.
10	If the tape becomes full, you are prompted to insert the next tape. **Note:** Do not remove the tape from the tape drive until it has finished rewinding.

Backing up all users assigned to a particular class of service

Introduction

The selective backup Class of Service option backs up selected classes of service. Up to 15 classes of service may be specified.

Recommendation

It is recommended that you perform selective backups on a different tape from other backups (such a volume backups.)

Labeling backup tapes

During every backup, all tapes should be labeled and numbered as they are removed from the tape drive.

Procedure

To perform a selective backup of selected classes of service, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Use the arrow keys to move to SELECTIVE BACKUP Messages and PDLs, press Space Bar to select it, and press [Backup To Tape]. **Result:** The Disk to Tape Backup window appears.
4	Enter an appropriate label for this backup.
5	Use the arrow keys or space bar to move to COS (class of service) and press Tab.
6	Enter a list of class of service numbers to be backed up.
7	Do you want to back up now? • If yes, then press [Immediate Backup]. **Result:** The softkeys change to [OK to Start Backup] and [Cancel]. • If no, go to “Scheduling the backup for a later time” on page 15-42.

Step	Action
8	Insert the tape for backup into the tape drive. See “Overview” on page 15-16 for information on inserting tapes.
9	Do you want to continue with the backup? • If yes, press [OK to Start Backup]. **Result:** The tape is automatically retensioned. • If no, press [Cancel] to return to the Disk to Tape Backup screen.
10	If the tape becomes full, you are prompted to insert the next tape. **Note:** Do not remove the tape from the tape drive until it has finished rewinding.

Backing up all users in a specific department

Introduction

The selective backup Department option backs up all specified departments. Up to five departments may be specified, but the actual number of specified departments may be much larger with the use of wildcards ('+' and '_').

Recommendation

It is recommended that you perform selective backups on a different tape from other backups (such a volume backups.)

Labeling backup tapes

During every backup, all tapes should be labeled and numbered as they are removed from the tape drive.

Procedure

To perform a selective backup of selected departments, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Use the arrow keys to move to SELECTIVE BACKUP Messages and PDLs, press Space Bar to select it, and press [Backup To Tape]. **Result:** The Disk to Tape Backup window appears.
4	Enter an appropriate label for this backup.
5	Use the arrow keys or Space Bar to select Dept, and press Tab.
6	Enter the department numbers to be backed up. Use wildcards '+' and '_' to specify more than 10 wildcards. **Note:** Wildcards are only permitted as the last character of an input, and only one wildcard is allowed per input field.

Step	Action
7	Do you want to back up now? • If yes, then press [Immediate Backup]. **Result:** The softkeys change to [OK to Start Backup] and [Cancel]. • If no, go to “Scheduling the backup for a later time” on page 15-42.
8	Insert the tape for backup into the tape drive. See “Overview” on page 15-16 for information on inserting tapes.
9	Do you want to continue with the backup? • If yes, press [OK to Start Backup]. **Result:** The tape is automatically retensioned. • If no, press [Cancel] to return to the Disk to Tape Backup screen.
10	If the tape becomes full, you are prompted to insert the next tape. **Note:** Do not remove the tape from the tape drive until it has finished rewinding.

Backing up all multimedia services

Introduction

The selective backup All option backs up all multimedia services.

Recommendation

It is recommended that you perform selective backups on a different tape from other backups (such a volume backups.)

Labeling backup tapes

During every backup, all tapes should be labeled and numbered as they are removed from the tape drive.

Procedure

To perform a selective backup of all multimedia services, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Use the arrow keys to move to SELECTIVE BACKUP Services, press the Space Bar to select it, and press [Backup To Tape]. **Result:** The Disk to Tape Backup window appears.
4	Enter an appropriate label for this selective backup.
5	Use the arrow keys or Space Bar to move to All.
6	Do you want to back up now? • If yes, then press [Immediate Backup]. **Result:** The softkeys change to [OK to Start Backup] and [Cancel]. • If no, go to “Scheduling the backup for a later time” on page 15-42.
7	Insert the tape for backup into the tape drive. See “Overview” on page 15-16 for information on inserting tapes.

Step	Action
8	Do you want to continue with the backup? • If yes, press [OK to Start Backup]. **Result:** The tape is automatically retensioned. • If no, press [Cancel] to return to the Disk to Tape Backup screen.
9	If the tape becomes full, you are prompted to insert the next tape. **Note:** Do not remove the tape from the tape drive until it has finished rewinding.

Backing up selected individual multimedia services

Introduction

The selective backup Individual option backs up all specified multimedia services. Services are specified by service ID. There are 30 input areas for specified services, which can be expanded with the use of '+' and '_' wildcards.

Recommendation

It is recommended that you perform selective backups on a different tape from other backups (such a volume backups.)

Procedure

To perform a selective backup of all multimedia services, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Use the arrow keys to move to SELECTIVE BACKUP Services, press the Space Bar to select it, and press [Backup To Tape]. **Result:** The Disk to Tape Backup window appears.
4	Enter an appropriate label for this selective backup.
5	Use the arrow keys or space bar to select Individual, and press Tab.
6	Enter the numbers for service ID for all services to be backed up. Use wildcards '+' and '_' to specify more than 10 wildcards. **Note:** Wildcards are only permitted as the last character of an input, and only one wildcard is allowed per input field.
7	Do you want to back up now? • If yes, then press [Immediate Backup]. **Result:** The softkeys change to [OK to Start Backup] and [Cancel]. • If no, go to "Scheduling the backup for a later time" on page 15-42.

Step	Action
8	Insert the tape for backup into the tape drive. See “Overview” on page 15-16 for information on inserting tapes.
9	Do you want to continue with the backup? • If yes, press [OK to Start Backup]. **Result:** The tape is automatically retensioned. • If no, press [Cancel] to return to the Disk to Tape Backup screen.
10	If the tape becomes full, you are prompted to insert the next tape. **Note:** Do not remove the tape from the tape drive until it has finished rewinding.

Section D: Partial backups to disk

In this section

Performing a partial backup to disk 15-40

Performing a partial backup to disk

Introduction

Backups to disk are only partial backups as the Voice and Data backup option is not allowed for user volumes. The backups options are Voice and Data for the system volume, and Data for user volumes.

Procedure

To perform a partial backup to disk, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Position the arrow on the volume you want to backup and press <Space bar> to select it.
4	Enter an appropriate label for this backup.
5	Press [Backup to Disk]. **Result:** The Disk to Disk Backup screen appears.
6	Do you want to back up now? • If yes, then press [Immediate Backup]. **Result:** The softkeys change to [OK to Start Backup] and [Cancel]. • If no, go to “Scheduling the backup for a later time” on page 15-42.
7	Do you want to continue with the backup? • If yes, press [OK to Start Backup] to initiate the backup. **Result:** The Backup status screen appears. • If no, press [Cancel] to return to the Disk to Disk backup screen.

Section E: Scheduled backups

In this section

Scheduling the backup for a later time 15-42
Deleting a scheduled backup 15-45

Scheduling the backup for a later time

Introduction

The Schedule Backup screen allows you to schedule the backup frequency (daily, weekly, or monthly) and start time for your backup to occur. This allows you to schedule a backup for which you do not need to be present.

> **ATTENTION**
>
> Do not schedule important backups between 1:00 a.m. and 5:00 a.m. when important system audits occur. Do not schedule a backup if more than one tape is required.

The Schedule Backup screen

This is the Schedule Backup screen.

```
                          General Administration
Schedule Backup to Tape

Backup frequency:       Daily Weekly Monthly

Backup start time:      00:00

Tape Label:             Tape 15

Information to backup:  VS1                     Backup Voice & Data
                        VS202                   Backup Data
                        VS203                   Backup Data

Select a softkey>

 Save      Cancel                                                    *L
 Schedule
```

Field descriptions

This table describes fields in the Schedule Backup screen.

Backup frequency	
Description	This field determines how often scheduled backups occur.
Default	Weekly
Valid options	Daily, Weekly, Monthly
Weekly	
Description	This field determines on which day of the week weekly backups occur.
Conditions of display	This field is displayed if the backup frequency is Weekly.
Default	Sun
Valid options	Sun, Mon, Tue, Wed, Thu, Fri, Sat
Day of Month	
Description	This field determines on which day of the month monthly backups occur.
Conditions of display	This field is displayed only if the backup frequency is Monthly.
Default	1
Valid range	0 to 31
Backup start time	
Description	This is the time of day at which scheduled backups begin.
Default	00:00
Valid range	00:00 to 23:59

Tape label	
Description	This is the label that is given to the backup tape.
Default	Blank

Information to backup	
Description	This field displays the volumes you have selected to back up, or the criteria specified for a selective backup.

Procedure

To schedule a backup, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Position the cursor on the volumes and selective backups you want to back up and press <Space Bar> to select them.
4	Press [Backup to Tape] or [Backup to Disk].
5	Press [Schedule Backup].
6	Move the cursor to the required backup frequency (daily, weekly, or monthly) and press Return. **Result:** For weekly backups, the screen displays the days of the week; for monthly backups, the screen displays a prompt for the date on which the backups will occur.
7	For weekly backups, choose the day on which the backup will occur. For monthly backups, enter the required date.
8	Enter the backup start time.
9	Do you want to save the schedule? • If yes, press [Save Schedule]. • If no, press [Cancel] to return to the Volume and Selective Backup screen.

Deleting a scheduled backup

Introduction

The View/Delete Backup Schedule screen displays the currently scheduled backups. The screen is read-only and displays the current settings of the backup schedule, including the type of backup (to disk or tape), frequency of backup, start time, backup selection, and backup options.

Procedure

To delete a previously scheduled backup, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Press [View/Delete Schedule]. **Result:** The View/Delete Backup Schedule screen appears.
4	Press [Cancel Schedule]. **Result:** The schedule is deleted and you are returned to the Volume and Selective Backup screen.

Section F: Backup maintenance

In this section

Checking the status of a backup 15-48
Cleaning/maintaining the tape drive 15-52

Checking the status of a backup

Introduction

The Backup Status screen displays the current status of a backup, if one is in progress. The screen displays the time at which the backup started, time remaining for backup completion, volumes being backed up, selective backup criteria, and current progress of the backup. Time remaining will not be shown if selective backup was chosen.

Exceptions

If you are performing a partial backup (Data) of a volume, there is an intermediate step in the backup process that will be reported in the status screen.

VS901T is used as a partial backup of VS202T, VS203T, VS204T, and VS205T. Text files are first copied to VS901T and then copied from VS901T to tape. While files are being copied to VS901T, the tape drive will be inactive. The status of VS901T will be reported on the Backup status screen while the backup is occurring.

The Backup Status screen: partial backup

This is the Backup Status screen for a partial backup.

```
                          General Administration
  Backup Status

  Backup Started:      0/02/08 18:55        Time Remaining (hh:mm):  00:07
  Backup Completed:    Immediate backup in progress
  Tape Label:          Tape 2
  Backing Up Volumes:  VS1

    VS1T      15% done

Select a softkey>

    Exit                                                   Abort Backup
```

The Backup Status screen: selective backup

This is the Backup Status screen for a selective backup. There is no Time Remaining field.

```
                          General Administration
  Backup Status

  Backup Started:      7/30/96 15:41
  Backup Completed:    Immediate backup in progress
  Tape Label:          Tape 24
  Backing Up Volumes:  VS1
  Backing Up Selected: Messages&PDLs:  All

    VS1T       3% done

Select a softkey>

    Exit                                                   Abort Backup
```

Field descriptions

The following table provides field descriptions for the Backup Status screen.

Backup Started	
Description	The date and time the current backup started.
Date format	The date format is determined by the Date Format for Administration and Maintenance Reports field in the General Options screen.
Time Remaining	
Description	This is the time remaining to complete the backup, displayed in hh:mm.
Conditions of display	This field is not displayed if selective backup is chosen.
Backup Completed	
Description	This is the date and time at which the backup was completed. If the backup is still in progress, this field displays "Immediate backup in progress."
Tape Label	
Description	This is the label that was assigned to the tape.
Backup Volumes	
Description	If a full or partial backup is being performed, this field displays the list of volumes that are being backed up.
Backup Selected	
Description	If a selective backup is being performed, this field displays the criteria chosen to selected users and/or services for backup.

Procedure

To check the status of a current backup, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Volume and Selective Backup. **Result:** The Volume and Selective Backup screen appears.
3	Press [Backup Status]. **Result:** The Backup Status screen appears displaying information about the backup in progress, or about the last backup that was completed.
4	When you are finished viewing the status, you can exit the screen or abort the backup. • To exit the Backup Status screen, press [Exit]. • To abort a current backup, press [Abort Backup]. **Result:** You are returned to the Volume and Selective Backup screen.

Cleaning/maintaining the tape drive

Guidelines

Preventive maintenance of the tape drive involves periodic cleaning after every four to six hours of use.

Precautions

To ensure reliable tape drive performance, you should establish a regular cleaning schedule and observe the following precautions:

- Maintain a clean, dust-free environment within the temperature and humidity limits listed in the specifications of the Meridian Mail system.
- Keep all liquids away from the drive and tapes to prevent spills into the equipment.
- Exercise reasonable care when using and storing tape cartridges. Do not place cartridges on the Meridian Mail or Meridian 1 cabinets, or on the monitor of the system administrator's terminal.
- When a stored tape is moved to an environment with a greatly different temperature, allow the tape to slowly reach room temperature before using it.
- Do not touch the tape surface.

Reference

For detailed procedures on cleaning and maintaining the tape drive, see the *Meridian Mail Installation and Maintenance Guide* (NTP 555-70x1-250).

Section G: Restoring information from a Selective backup

In this section

Overview 15-54
Restore from Selective backup 15-56

Overview

Introduction

This section provides information on restoring from a Selective backup.

Description

The Selective Restore feature allows for an online restore of users' messages, individually specified Personal Distribution Lists (PDLs), or multimedia services. An entire mailbox is not restored, only the messages and PDLs for an existing mailbox. When restoring a user's messages and PDLs, the user is locked out of his or her mailbox until the restore is complete.

Restoring messages and PDLs

In restoring both messages and PDLs, if one already exists, it is not overwritten. For VMUIF users, no message will be restored to a mailbox once it is full. For MMUIF users, all messages are restored unless the Call Answering Blocking Factor is set.

Call Answering Blocking Factor limits the number of call answering messages that can be deposited in a mailbox once the number of messages in the mailbox exceeds the mailbox storage limit.

Restoring multimedia services

Restoring multimedia services can be done by service ID, or by restoring all services.

Restore exceptions

Data not restored from a selective backup includes mailbox configuration such as passwords, auto-login, storage limits, login status, and other data kept in the user's profile.

The More Detail screen

The Restore from Selective Backup More Detail screen provides a summary of the data backed up on a backup tape. The More Detail screen is accessed by the [More Detail] softkey in the Selective Backup and Restore screen.

```
                          General Administration
Restore from Selective Backup More Detail

This Selective Backup Contains:
Tape Label: JulysMessages&PDLs&ServicesBkup        Date: 07/24/96 Time: 11:36

Messages&PDLs  Individual
               COS:
               4   1   3   5   8   6

Services       All

     Exit
```

Reference

For information on Full and Partial restores, see Chapter 6, “Restore system from backup,” in the *System Installation and Modifications Guide* (NTP 555-7001-215).

Restore from Selective backup

Introduction

The Selective backup option allows you to restore messages, PDLs, and multimedia services. This procedure allows you to select to restore none, all, or individual messages, PDLs, and multimedia services.

If you choose None, then nothing for that option will be restored. If you choose All, then everything for that option will be restored. If you choose Individual, then the system displays a list of the available Individual options from which to select. If you require more information about your restore tape, when in the Selective Restore screen, press [More Detail].

Procedure

To restore from a selective backup, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Restore from Selective Backup. **Result:** The Restore from Selective Backup screen appears and prompts you to insert the restore tape in the tape drive.
3	Insert the tape in the tape drive, and press [OK to Read Tape]. **Result:** The tape drive retensions the tape. This takes approximately three to four minutes. Once the tape is retensioned, the screen displays the tape label and creation date. **Note:** If you require more information about the restore tape that you are using, press [More Detail] which will present a more detailed summary of the criteria used to perform the initial backup.
4	Use the arrow keys or space bar to select one of None, All, or Individual for Messages and PDLs, and press Tab. If you choose Individual, enter the mailbox(es), then select Yes or No for each of the Mailboxes, to restore messages or not respectively, and enter the PDL numbers you want to be restored.

Step	Action
5	Use the arrow keys or Space Bar to select one of None, All, or Individual for Services, and press Tab. If you choose Individual, then enter the Service IDs that you want restored.
6	Once you have selected all the required restore options, press [Restore]. **Result:** The system begins to read the requested data from the tape and transfer it to disk. Status information is displayed as % complete in the Status field. **Note:** When the restore is finished, a summary line will show the number of successes and failures for both mailboxes and services.
7	Do you want to perform another restore? • If yes, repeat steps 3 to 7. • If no, go to step 9.
8	Press [Exit] to return to the General Administration screen.

Chapter 16

Password and system time changes

In this chapter

Overview	16-2
Changing the system administrator password	16-3
Changing the customer administrator password for MATs and Meridian Mail AutoAdmin	16-5
Setting the minimum password length for all administrator passwords	16-7
The AdminPlus Download password	16-8
Changing the system time	16-10

Overview

Introduction

This chapter describes

- how and how often to change the Administrator password and the AdminPlus Download password
- how to set the minimum length for the System and Customer Administrator passwords
- how to change Meridian Mail's system time setting

Changing the system administrator password

Introduction

When the Meridian Mail system is first installed, you are given a default system administrator password (adminpwd). When you log on for the first time using this default password, you are prompted for a new password.

Password requirements

Passwords are not case sensitive; any capitalization used in defining the password need not be used when entering the password. The password can contain both alpha and numeric characters.

The minimum password length is set in the General Options screen. See "Setting the minimum password length for all administrator passwords" on page 16-7. The default length is six characters. It is recommended that your administration password be at least seven characters for added security. The longer the password, the better.

Frequency of password changes

Once you have initially changed your password, you should continue to change it on a regular basis.

Procedure

To change the system administrator password, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Change System Administrator Password. **Result:** You are prompted to enter the existing system administrator password.
3	Enter the existing password. **Note:** The passwords are not displayed on the screen as you enter them. **Result:** You are prompted to enter the new administrator password.

Step	Action
4	Enter the new password. **Result:** You are prompted to enter the new password again for verification purposes.
5	Reenter the new password. **Result:** The new password is recorded and you are returned to the General Administration menu.

Changing the customer administrator password for MATs and Meridian Mail AutoAdmin

Introduction

If the Multiple Administration Terminals (MATs) feature or the Meridian Mail AutoAdmin feature is installed, the password you use to log on is called the Customer Administrator Password. The default password is custpwd.

The first time you log on with this password, you are forced to change it for security purposes.

However, any subsequent password changes must be done from the General Administration menu.

Password requirements

Passwords are not case sensitive; any capitalization used in defining the password need not be used when entering the password. The password can contain both alpha and numeric characters.

The minimum password length is set in the General Options screen. See "Setting the minimum password length for all administrator passwords" on page 16-7. The default length is six characters. It is recommended that your administration password be at least seven characters for added security. The longer the password, the better.

Frequency of password changes

Once you have initially changed your password, you should continue to change it on a regular basis.

Procedure

To change the customer administrator password, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Change Customer Administrator Password. **Result:** You are prompted to enter the existing customer administrator password.
3	Enter the existing password. **Note:** The passwords are not displayed on the screen as you enter them. **Result:** You are prompted to enter the new administrator password.
4	Enter the new password. **Result:** You are prompted to enter the new password again for verification purposes.
5	Enter the new password. **Result:** The new password is recorded and you are returned to the General Administration menu.

Setting the minimum password length for all administrator passwords

Introduction

Longer passwords generally offer higher system security. At least seven characters in length is a minimum recommendation. The minimum length you set here will be applied when system administrator and customer administrator passwords are changed.

Default minimum password length

The default minimum password length is 6 characters, and the maximum length is 16 characters.

Procedure

To check or change the current minimum administration password length setting, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select General Options. **Result:** The General Options screen appears.
3	Cursor down to the Minimum Admin Password Length field.
4	Enter the new Minimum Admin Password Length, and press <Return>. The number must be a value between 6 and 16.
5	When you have entered the new value, press <Save>. **Result:** The new Minimum Admin Password Length is recorded and you are returned to the General Options menu.

The AdminPlus Download password

Introduction

The AdminPlus Download password allows Meridian Mail Reporter to download data from the system. This password must match the OM password on the Meridian Mail Reporter side before data can be downloaded. Both passwords must be set up when the system is installed as the default values will not allow the download to take place.

Note: This capability is only available if AdminPlus is an installed feature.

Password requirements

Passwords are not case sensitive; any capitalization used in defining the password need not be used when entering the password. The password can contain both alpha and numeric characters.

The minimum password length is 1 character, and the maximum length is 16 characters. It is recommended that your AdminPlus password be at least seven characters for added security. The longer the password, the better.

Frequency of password changes

Once you have initially changed your password, you should continue to change it on a regular basis.

Procedure

To change the AdminPlus password, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Change AdminPlus Password. **Result:** You are prompted to enter the existing system administrator password.

Step	Action
3	Enter the existing password. **Note:** The passwords are not displayed on the screen as you enter them. **Result:** You are prompted to enter the new AdminPlus password.
4	Enter the new password. **Result:** You are prompted to enter the new password again for verification purposes.
5	Enter the new password. **Result:** The new password is recorded and you are returned to the General Administration menu.

Changing the system time

Introduction

The Meridian Mail system gets its time from the Meridian 1. It receives time stamps passed from the switch at regular intervals. However, you can set up your Meridian Mail database while the link to the switch is down. If you will be configuring the database when the link is not operational, you will have to set the system time on the Meridian Mail side. Then, once the link is up, the switch time will override the Meridian Mail time.

Procedure

To change the system time, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select General Administration. **Result:** The General Administration screen appears.
2	Select Change System Time. **Result:** You are prompted to enter the date and time.
3	Enter the date and time, and press <Return>. **Result:** The clock is synchronized to the clocking signals from the network, the time is recorded, and the General Administration screen is redisplayed.
4	When you have set the system time, press <Exit>.

Chapter 17

Dialing translations

In this chapter

Overview	17-2
Section A: Introduction to dialing translations	17-3
Section B: How dialing translations work	17-17
Section C: Setting up network dialing prefixes and local defaults	17-29
Section D: Setting up translation tables	17-43
Section E: Sample datafills	17-69
Section F: Troubleshooting dialing translations	17-75

Overview

Introduction

This chapter introduces dialing translations as a concept and the ways that you, as the system administrator, can plan and set up dialing translation defaults and translation tables, if necessary.

Meridian Mail users do not directly access dialing translations. Taking the features and requirements of the system into consideration, the administrator needs to examine how private or public network numbers are dialed. Various features then use dialing translations to produce dialable numbers.

In the chapter, you will find explanations of what translations are, how they function, and when they are required. In addition, this chapter contains procedures that guide you through the administration of dialing translations.

Section A: Introduction to dialing translations

In this section

Overview	17-4
Dialing translations	17-5
Default dialing prefixes and local system defaults	17-7
When default dialing translations defaults are required	17-10
Translation tables	17-12
When translation tables are required	17-14

Overview

Introduction

This section introduces the concept of dialing translations and the ways in which they are implemented.

This section discusses the two main parts of dialing translations: dialing translation defaults and translation tables.

Dialing translations

Description

Dialing translations are the means by which Meridian Mail transforms a number into a dialable directory number (DN). For instance, translation determines how to dial a DN depending on whether a number is a local, national, international, or ESN.

How translations are used

Users of Meridian Mail do not directly use translation. Rather, certain features use dialing translations in order to generate a dialable DN to call back:

- The system administrator uses default dialing prefixes to handle normal situations for local, national, international and (if they exist) ESN calls.
- Exceptional situations, such as calls to other area codes that are still considered local calls, use translation tables.

Example

For example, if a caller requests that a fax be sent to 214-555-1234 (a long distance number), this number must be translated into a DN that can be dialed from your system. In this case, the dialable DN must include the long distance dialing prefix. If your system dials “91” to place long distance calls, then the resulting DN will be 91-214-555-1234.

Features that use dialing translations

The following features use dialing translations:

- Fax on Demand
  - For example, a user calls Meridian Mail, enter a fax number without a prefix and wait for the fax to call back.
- AMIS Networking
  - For example, a user receives a message from a remote AMIS site and the number is included in the message header. The number must be translated to use the Reply feature to call back.

- External CLID
  - For example, CLID collects the caller's number from the switch. Meridian Mail translates the number, and it is announced in a message to you with the prefixes included, ready to dial out.

Outcalling does *not* use translations

Default dialing prefixes are not required for outcalling (remote notification and delivery to non-user.) The numbers entered are already in a dialable format and, therefore, do not need to be translated for a callback.

Default dialing prefixes and local system defaults

Introduction

There are two levels to the translation process. The first level involves dialing translation defaults, which include default dialing prefixes and local system defaults. Both are used only under normal dialing conditions.

Default dialing prefixes

The system administrator must define four default dialing prefixes:

- local
- long distance
- international
- ESN

These prefixes are the dialing digits that are used to dial out of the switch to place local, long distance, international, and ESN calls using either the public network, the ESN network, or a combination of both.

Meridian Mail uses these prefixes to generate a DN that is understandable to the switch.

Local dialing prefix

This is the prefix that is used by the system to dial out of the switch and access the public network or a private network in order to place a local call.

Format

The prefix you enter will depend on whether you use a private network or a public network to place local calls. Typical examples of network dialing prefixes are 9 or 8 to access the public network.

To access a private ESN network is a little more complicated. You would typically dial 6 plus the digits needed to make a national call to the same local site. For instance, the area/city code of Manhattan is 212, so the prefix would be 61212.

Long distance dialing prefix

This is the prefix that is used by the system to dial out of the switch and access the public network or a private network in order to place a long distance call.

Format

The prefix you enter will depend on whether you use a private network or a public network to place long distance calls. Typical examples of long distance dialing prefixes are 91 or 81 in North America, or 90 or 80 in Germany, to access the public network, or 6 to access a private ESN network.

International dialing prefix

This is the prefix that is used by the system to dial out of the switch and access the public network or a private network in order to place an international call.

Format

The prefix you enter will depend on whether you use a private network or a public network to place international calls. Typical examples of international dialing prefixes in North America are 9011 or 8011 to access the public network, or 6011 to access a private ESN network.

An international dialing prefix in England, for example, is 900.

ESN dialing prefix

This is the prefix that is used by the system to access the private ESN network.

Local system defaults

Local system defaults identify the country and the area/city codes of the switch connected to your Meridian Mail.

You will fill out these fields to inform Meridian Mail of its location within the public network. This information is used by dialing translations to determine how to translate a number.

Country code

Identify the country code for your system. (For instance, it is 1 for the U.S.A. and Canada. It is 44 for England, 61 for Austria, and 86 for China.)

Local system defaults (cont'd)

Area/city code

Identify the area/city code for the local system.

The term "area/city code" is used to define either area code or city code. The two terms are used interchangeably.

Countries that use city codes should use this field for city codes, and countries that use area codes should use the field for area codes. However, if a country uses *both* area and city code for its dialing plan, the field should be used for *either* the area or city codes for the site in which the Meridian Mail is located.

When a number that includes an area/city code is provided by a caller for a fax callback delivery or by a user when replying to an AMIS message, it will be stripped out if it matches the code entered in the field.

Example

A caller requests that a fax item be sent (using callback delivery) to the DN 416-555-9911. The local system's area/city code is also 416. Therefore, the area code will be stripped out and the dialable DN will be 9-555-9911, where 9 is the network dialing prefix (for local calls).

When default dialing translations defaults are required

Description

The dialing translation defaults must be filled in before features like AMIS networking, Fax on Demand, and External CLID can be used.

The dialing translation defaults consist of

- default dialing prefixes

  This is where you specify the network access codes that are used by your system for placing local calls, long distance calls, international calls and ESN calls. These prefixes are needed to generate dialable DNs from
  - fax callback numbers
  - numbers contained in the headers of AMIS messages (so that local users can reply to AMIS messages)
  - numbers of external callers who left messages with users on your system
- local system defaults

  This is where you enter the country code and the area/city code of your Meridian Mail site. These codes are used to determine if the country or area/city code entered by a caller needs to be stripped out.

Scenario

In a Fax on Demand application, for example, a caller includes the country code and area/city code in the callback number he or she has entered.

Meridian Mail checks the values defined to see if the country and area/city codes specified in the callback number match the codes of the Meridian Mail system. If there is a match, the country and area/city codes which are not required, if any, for dialing purposes and are stripped out.

Example of the scenario

A caller enters 1-214-555-2222 as a callback number for a fax. The country code (1) and the area/city code (214) are the same as the one for the Meridian Mail system. Therefore these codes are not needed to dial the number.

Meridian Mail strips out the 1214, gets the network dialing prefix for local dialing (9), and generates the following dialable DN: 9-555-2222.

Translation tables

Concept

Translation tables are the second level of the translation process, after the dialing translation defaults.

These tables handle certain dialing exceptions that may not arise in your system. Therefore, translation tables will not be required by all systems.

For example, in a normal local dialing scenario, the area/city code (in North America, it is called the Numbering Plan Area or NPA) of the calling site is the same as the called site. A call in this situation would be handled by the dialing defaults.

However, there may be a dialing scenario where the area/city codes are different but the call is still considered local. A translation table would have to handle this case in order to determine that the call in question could be handled as local rather than as long distance.

The exceptional cases that require translation tables are outlined in “When translation tables are required” on page 17-14.

Restriction/ permission lists

Meridian Mail applies translation tables before checking restriction/permission lists.

Example

For example, a call to another area/city code is considered local, and the restriction/permission list applied to a Fax on Demand application allows only local calls.

If a translation table is not set up for this exceptional dialing scenario, the system will assume that the callback number is long distance (because the area/city code is different from the local site) and Meridian Mail will not deliver the fax (since the restriction/permission list does not allow delivery to long distance numbers).

Restrictions for AMIS and Fax on Demand

For more information on how restrictions and permissions interact with Fax on Demand and AMIS Networking, refer to the following NTPs: *Fax on Demand Application Guide* (NTP 555-7001-327) and the *AMIS Networking Installation and Administration Guide* (NTP 555-7001-242).

When translation tables are required

Description

Translation tables need only be defined if

1. some calls placed to the same area/city code as the local site are dialed differently than local (for example, long distance)
2. calls placed to different area codes are not dialed long distance

For example, if calls to some numbers in an area/city code are long distance, while calls to other numbers in that same area/city code are local, a translation table would be used to determine dialable DNs. This situation is normally dictated by the dialing plan of the local public network.

Translation tables for four exemplary cases

If any of the following situations occur in your system, you will have to define a translation table for each area/city code.

Type of dialing	To what area/city code?	Is the area/city code required in the DN?
Local dialing	Different	Required
Local dialing	Different	Not required
Long distance dialing	Same	Required
Long distance dialing	Same	Not required

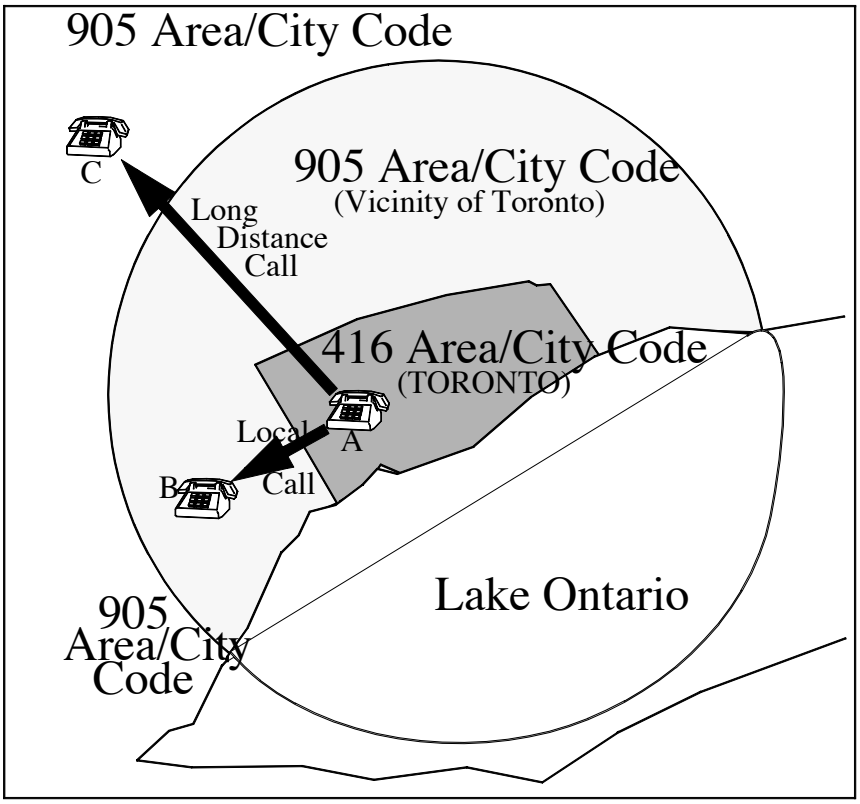
In all other dialing scenarios (such as long distance dialing to a different area/city code and local dialing to the same area/city code), the network dialing prefixes are used instead.

Example 1

For example, if a neighboring area code (905) contains both local and long-distance numbers, and a call to a local number in the 905 area needs a different number format than a call to a long-distance number in the 905 area, at least one translation table will be required.

The table determines on the basis of the local prefix which calls are local, and which are long distance.

Example 1 (cont'd) Consider the following example which shows the dialing plan of Toronto, Ontario, Canada.



You can see that both local (A→B) and long-distance (A→C) dialing is used depending on the location of the destination call.

A translation table must be defined to tell Meridian Mail which 905 numbers must be dialed as long distance and which ones must be dialed as local.

Section B: How dialing translations work

In this section

Overview 17-18
How Meridian Mail collects digits 17-19
How dialing translations translate numbers 17-22
How Meridian Mail uses the dialable number 17-27

Overview

Introduction

The dialing translation process occurs in three stages:

- input to the translation process (how DN digits are collected)
- the translation itself (how the collected DN is translated)
- output from the translation process (what happens to the translated DN)

This section will discuss each stage.

How Meridian Mail collects digits

Description

The format in which Meridian Mail requires a DN depends on the feature using dialing translations.

The three features using dialing translations are

- Fax on Demand
- AMIS Networking
- External Calling Line Identification (External CLID)

The following descriptions explain how each feature collects digits for translation.

Fax on Demand

When users call the Meridian Mail Fax on Demand service (VSDN), Meridian Mail prompts users for the number of their fax machine to which the fax will be sent.

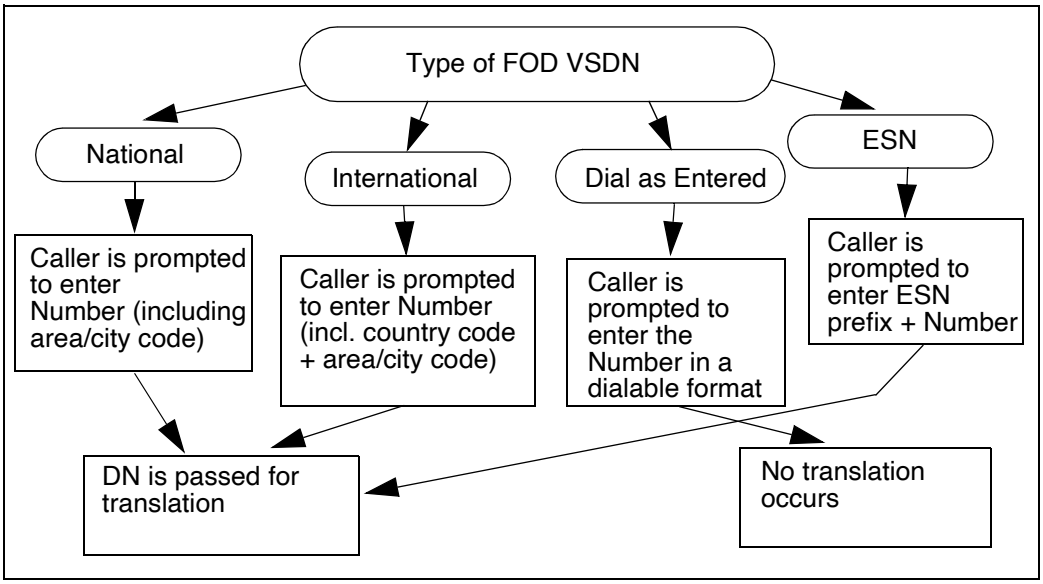
A session profile sets up the operational characteristics of the Fax on Demand service. Using the session profile, the Fax on Demand VSDN can be set up as national, international, dial-as-entered, or ESN.

This setup is done in the Treat Callback Number As field in the Session Profile screen for that VSDN.

Different prompts exist for each type of service. The prompts ask the user to enter the fax number in a particular format (national, international, dial-as-entered, or ESN.)

Digit collection for fax callback

The following diagram illustrates the different types of the Fax on Demand VSDN and what the caller is prompted for each type.



After the DN is passed for translation, the translation type depends on the type of FOD VSDN.

For more information about VSDNs, see Chapter 24, “The VSDN table” under Section E: Session profiles.

AMIS

AMIS collects digits for translation in two ways:

- When an AMIS message is received from a remote AMIS site, the number from that site (in an international, nondialable format) is included in the message.

  When the user replies to this message, or when the Meridian Mail system determines that the message cannot be delivered and generates a Non-Delivery Notification (NDN) to that remote system, the number must be translated into dialable DN before the remote system can be reached.

  Refer to the *AMIS Networking Installation and Administration Guide* (NTP 555-7001-242) for more details.

- When a message is sent to a Virtual Node AMIS site, the connection DN defined for that site must be translated into a dialable DN.

  Refer to the *Virtual Node AMIS Networking Installation and Administration Guide* (NTP 555-7001-245) for more details.

In both AMIS cases, the number is translated as an international number.

External CLID

External CLID collects digits from the switch. When an external caller calls a user at the local system and leaves a message for the local user, the caller's number is passed to Meridian Mail by the switch. The *type* of this number (national, international, ESN, and so on) is also passed to Meridian Mail from the switch.

In order to make this number dialable, the External CLID feature translates the number to a dialable format using dialing translations. The type of translation depends on the number type received from the switch.

Suggestions for CLID

This feature must set the translation of the unknown calling number type to one of the following: local, long distance, international, or ESN. It means that the system administrator must be confident that all the unknown incoming calls are the same type (because all the unknown calls will be translated as though they were the same type).

If those unknown calls are of more than one type, the system administrator must either decide not to translate the number (to treat it as dialed), or not to collect the unknown numbers.

How dialing translations translate numbers

Introduction

Once the number has been captured (as explained in the previous section), dialing translations is applied to it.

The following flowcharts illustrate the way in which the translation is achieved by individual type.

Five translation types are available:

- international
- national
- local
- ESN
- dial-as-entered

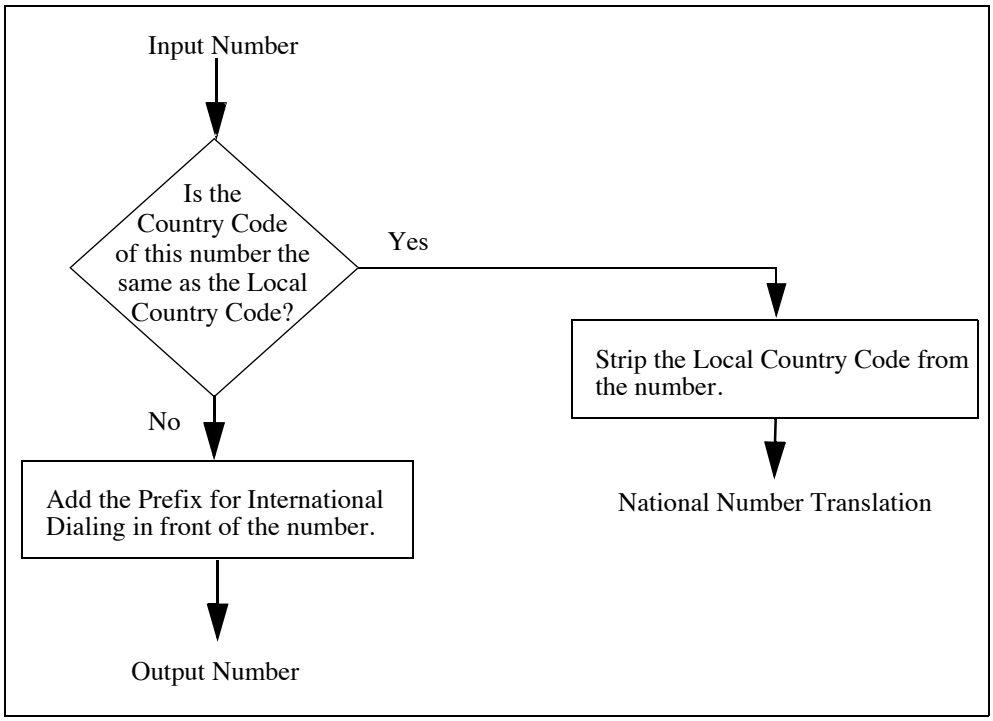
The translation type used depends on the type of number collected by the Fax on Demand, AMIS, or External CLID features. For instance, an international number will undergo an international translation, and so on.

International number translation

An international number is always in the format of

- country code + national significant number

It is translated in the following manner:

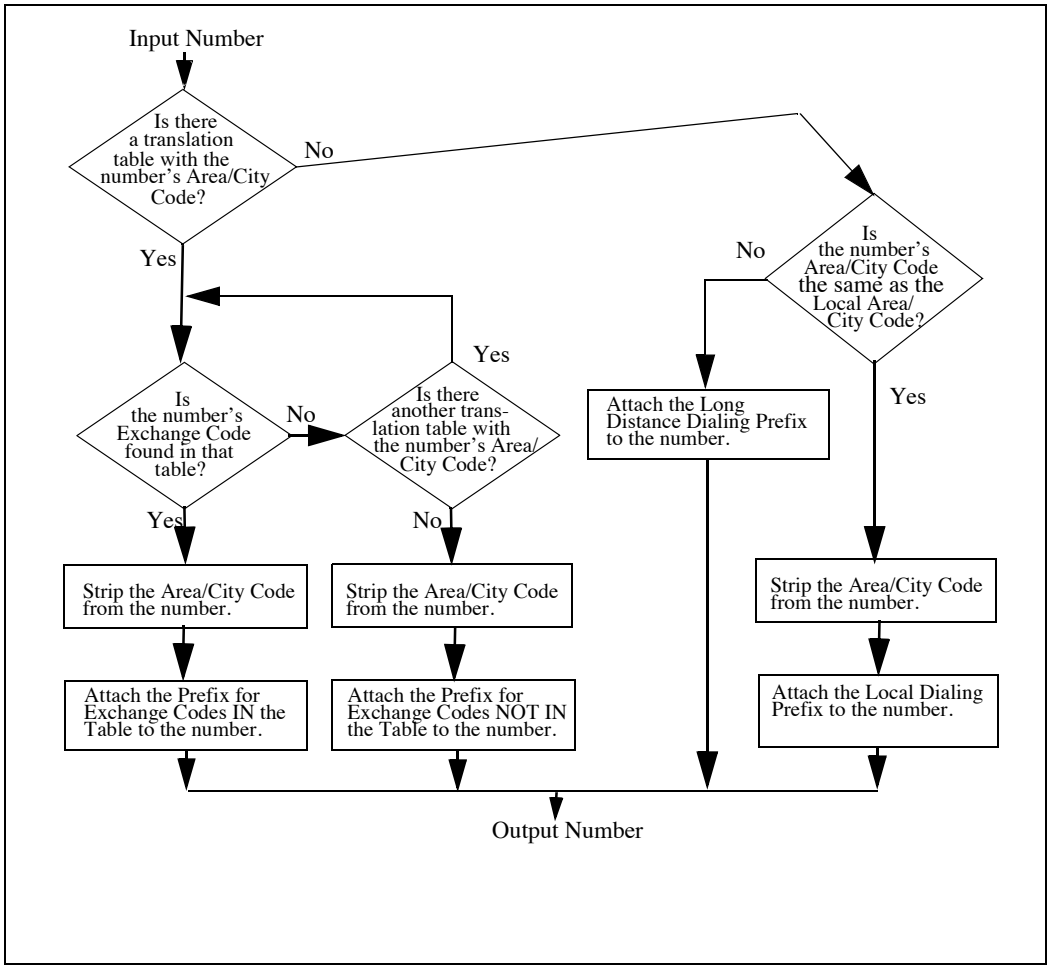


National number translation

A national number is always in the following format:

- area/city code + exchange code + station number

It is translated in the following manner:

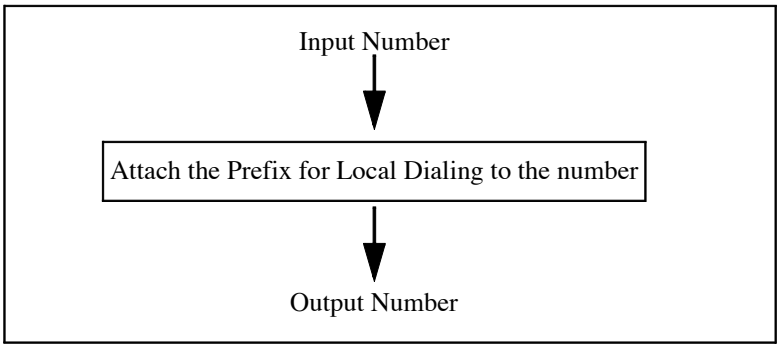


Local number translation

The local number is always in the following format:

- Local subscriber number (*without* country code or area/city code)

The translation proceeds as follows:



ESN number translation

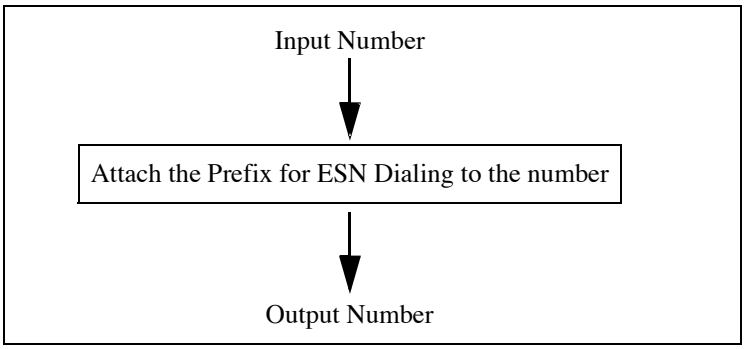
The ESN number can be in one of the following formats:

- a number on the ESN network
  - for example, 444-1000

    where 444 is the location code of the ESN switch, and 1000 is the DN at the ESN location
- any number dialable via the ESN network
  - for example, 1-212-555-1234

    where the entire number can be dialed via the ESN network by adding the prefix for ESN dialing in front of it

In both cases, the translation proceeds as follows:



Dial-as-Entered translation

The dial-as-entered number is always in the following format:

- Any string of digits

A dial-as-entered number is *not* translated. The number is assumed to be dialable exactly as it is specified (that is, containing all required prefixes and codes).

How Meridian Mail uses the dialable number

Introduction

Once the number is translated, it is returned to the feature that required the translation.

Fax on Demand

For Fax on Demand, the translated number will be checked against restriction/permissions for that VSDN.

If the number passes the check, Meridian Mail dials the number so that the requested fax can be delivered to the user. If the fax fails the restriction/permission check, the user requesting the fax will be informed that the number cannot be reached from that service and asked to enter another number.

AMIS

In AMIS, the translated, dialable number will be checked against AMIS restriction/permission lists. If the number passes the check, Meridian Mail uses the number to call the remote AMIS system so that AMIS Networking messages can be delivered to the system.

If the number fails the check (that is, it is restricted and Meridian Mail cannot dial the number), the AMIS message will not be delivered and a Non-Delivery Notification (NDN) will be sent to the sender of the message.

External CLID

In External CLID, the translated number is used for

- call sender

  The user places a call to the number.
- announcing the sender's number

  In the message header, or when the user uses call sender, or call reply.

When the user listens to a message from an external caller, the user will hear

- "From phone number: <digits>"

  where "digits" is the translated number

External CLID (cont'd) When the user requests a reply or call-sender to the caller, the number will be announced. When the user requests call sender, this translated number will be dialed so that the caller who left the number can be reached.

Note: Before being dialed, the number will also be checked against the restriction/permission list. Call sender will only continue if the number passes this check (that is, it is not restricted.)

Section C: Setting up network dialing prefixes and local defaults

In this section

Overview	17-30
Worksheet for default dialing prefixes and local system defaults	17-31
Dialing translation defaults screen	17-33
Configuring the default dialing prefixes and local system defaults	17-37
Sample datafills for dialing translation defaults	17-40

Overview

Introduction

This section explains how to set up and maintain dialing translation defaults for your system.

In addition to explanatory concepts and procedures, there are sample datafills to which you may compare your system and a worksheet to help you plan your dialing translations.

Worksheet for default dialing prefixes and local system defaults

Worksheet

You can use the following worksheet to plan default dialing prefixes and local system defaults.

Dialing Translation Defaults worksheet

Default Dialing Prefixes

Local Dialing: _____

Long Distance Dialing: _____

International Dialing: _____

ESN Dialing: _____

Local System Defaults

Local Country Code: _____

Local Area/City Code: _____

Dialing translation defaults screen

Introduction

When you are ready to configure the default dialing prefixes and the local system defaults, you will need to access the dialing translation defaults.

The screen

The following shows an example of the Dialing Translation Defaults screen.

```
                          Dialing Translation
Dialing Translation Defaults

Default Dialing Prefixes
   Local Dialing:            9
   Long Distance Dialing:    91
   International Dialing:    9011
   ESN Dialing:              6

Local System Defaults
   Local Country Code:       1
   Local Area/City Code:     416

Capture External CLID with Unknown Format:        No Yes

Select a softkey >

   Save        Cancel
```

Field descriptions

The following table describes the fields in the Dialing Translation Defaults screen.

Local Dialing	
Description	This field specifies the prefix needed in front of a number when dialing it (and the number dialed is in the same area/city as the Meridian Mail system).
Minimum length	0 (zero characters)
Maximum length	10 characters
Valid characters	0-9, * (where * is a pause)

Long Distance Dialing	
Description	This field specifies the prefix used for long-distance dialing of public network numbers. Meridian Mail places this prefix in front on long distance DNs before placing a call (for example, National numbers with a different area/city code)
Minimum length	Zero characters
Maximum length	10 characters
Valid characters	0-9, * (* is a 3-second pause)

International Dialing	
Description	This field specifies the prefix used for international dialing of public network numbers. Meridian Mail places this prefix in front of international DNs (for example, DNs with a different country code)
Minimum length	Zero characters
Maximum length	10 characters
Valid characters	0-9, * (* is a 3-second pause)

ESN Dialing	
Description	This field specifies the prefix that needs to be attached to a number to access the ESN network. Meridian Mail places this prefix in front of ESN DNs.
Minimum length	Zero characters
Maximum length	Three characters
Valid characters	0-9, * (* is a 3-second pause)

Local Country Code	
Description	This field defines the country code of the local system.
Minimum length	Zero characters
Maximum length	Four characters
Valid characters	0-9, * (* is a 3-second pause)

Local Area/City Code	
Description	This field defines the area/city code of the local system.
Minimum length	0
Maximum length	Eight characters
Valid characters	0-9

Capture External CLID with Unknown Format	
Description	This field specifies whether to capture an external caller's number (External CLID) if that caller's format is unknown. This capability may be necessary in the case where the numbers received by Meridian Mail from the switch are in an unknown format.
Default	No
Feature dependency	This field appears only on systems with either AML or DIAL.

Default Translation for CLID with Unknown Format	
Description	This field specifies how the external caller's number (External CLID) of unknown type is translated if it is captured. Setting this field to Local, National, International, or ESN results in the External CLID being translated as though the DN were Local, National, International, or ESN, respectively.
Default	None (that is, no translation is performed on the number)
Field status	This field appears only if Capture External CLID with Unknown Format is set to Yes.

Configuring the default dialing prefixes and local system defaults

Introduction

Once you have identified the ways that your system makes external calls through a private or public network, or a combination of both, you are ready to configure your dialing translation defaults which include the default dialing prefixes and the local system defaults.

Procedure

To configure the default dialing prefixes and the local system defaults, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Choose General Administration. **Result:** The General Administration menu is displayed.
2	Choose Dialing Translation. **Result:** The Dialing Translation menu is displayed.
3	Choose Dialing Translation Defaults. **Result:** The Dialing Translation Defaults screen is displayed.
4	Define the Prefix for Local Dialing. **Note:** For more information, see “Local dialing prefix” on page 17-7.
5	Define the Prefix for Long Distance Dialing. **Note:** For more information, see “Long distance dialing prefix” on page 17-8.
6	Define the Prefix for International Dialing. **Note:** For more information, see “International dialing prefix” on page 17-8.

Step	Action

7 Define the Prefix for ESN Dialing.

IF your system is	THEN
connected to an ESN network	define the prefix.
not connected to an ESN network	leave the field blank.

Note: For more information, see “ESN dialing prefix” on page 17-8.

8 Define the local Country Code.

Note: For more information, see “Local system defaults” on page 17-8.

9 Define the local Area/City Code.

IF	THEN
your MM system is located in an area code	enter that area code.
your MM system is located in a city code	enter that city code.
your country does not have either area or city codes	leave this field blank.

Note: For more information, see “Local system defaults” on page 17-8.

10 Does your system have AML or DIAL?

- If yes, continue with the next step.
- If no, go to step 13.

Step	Action
11	Do you want to capture External CLIDs that are of an unknown type? • If yes, set the “Capture External CLID with Unknown Format” field to Yes. • If no, set the “Capture External CLID with Unknown Format” field to No. Go to step 13.
12	Set the “Default Translation for CLID with Unknown Format” field so that all numbers with an unknown call type will be translated as though they were all of one format.

IF all numbers of unknown format are	THEN set the field to
international	International.
national	National.
ESN	ESN.
not to be translated	None.
of various different formats	Nothing. Do not use this field. Return to step 11, and select No.

13	Do you want to save the screen? • If yes, press the [Save] softkey. • If no, press the [Cancel] softkey.

Sample datafills for dialing translation defaults

Introduction

You may compare the following sample datafills of dialing translation defaults to handle different methods of dialing (private versus public network).

Defaults screen for North America

The screen below illustrates a standard dialing plan situation in Toronto, Ontario, Canada, where the country code is 1and the area code is 416. In this example, the digit 6 accesses the ESN network.

```
                          Dialing Translation
Dialing Translation Defaults

Default Dialing Prefixes
   Local Dialing:            9
   Long Distance Dialing:    91
   International Dialing:    9011
   ESN Dialing:              6

Local System Defaults
   Local Country Code:       1
   Local Area/City Code:     416

Capture External CLID with Unknown Format:        No Yes

Select a softkey >

   Save        Cancel
```

Defaults screen for England

The screen below illustrates a standard dialing plan situation in England where the country code is 44. In this example, the digit 6 accesses the ESN network.

```
                          Dialing Translation
Dialing Translation Defaults

Default Dialing Prefixes
   Local Dialing:            9
   Long Distance Dialing:    9
   International Dialing:    900
   ESN Dialing:              6

Local System Defaults
   Local Country Code:       44
   Local Area/City Code:     0171

Capture External CLID with Unknown Format:        No Yes

Select a softkey >

   Save        Cancel
```

All ESN screen

If your system makes all calls though a private network, then your network dialing prefixes would all begin with the access to the ESN network. In this example, the digit 6 accesses the ESN network.

```
                          Dialing Translation
Dialing Translation Defaults

Default Dialing Prefixes
   Local Dialing:            61509
   Long Distance Dialing:    61
   International Dialing:    6011
   ESN Dialing:              6

Local System Defaults
   Local Country Code:       1
   Local Area/City Code:     509

Capture External CLID with Unknown Format:        No Yes

Select a softkey >

   Save        Cancel
```

Mixture of ESN and public screen

If your system makes calls through a combination of private and public networks, then you may use a combination of access prefixes.

This example illustrates the datafill for a system in which the local calls are dialed on the public network, but long distance and international calls are dialed on the ESN network.

```
                              Dialing Translation
Dialing Translation Defaults

Default Dialing Prefixes
   Local Dialing:            9
   Long Distance Dialing:    6
   International Dialing:    6011
   ESN Dialing:              6

Local System Defaults
   Local Country Code:       1
   Local Area/City Code:     416

Capture External CLID with Unknown Format:        No Yes

Select a softkey >

     Save        Cancel
```

Section D: Setting up translation tables

In this section

Overview	17-44
Identifying translation table requirements	17-45
Identifying translation tables required on your system	17-48
Local dialing to a different area/city code (area/city code required)	17-52
Local dialing to a different area/city code (no area/city code required)	17-56
Long distance dialing to the same area/city code (area/city code required)	17-59
Long distance dialing to the same area/city code (area/city code not required)	17-61
The View/Modify Translation Table screen	17-62
Configuring translation tables	17-64
Deleting translation tables	17-67

Overview

Introduction

This section guides the system administrator through all aspects of translation tables.

First, this section explains and illustrates the differences between normal dialing scenarios (ones that do not require translation tables) and exceptional dialing scenarios (ones that require translation tables). In so doing, this section demonstrates when translation tables are needed.

Second, this section explains in detail some of the exceptional dialing scenarios to provide you with a better idea of what each scenario is, how to handle each one, and how to handle any other exceptions that may occur.

Finally, this section contains procedures for adding, modifying, and deleting translation tables on the Meridian Mail, as well as field descriptions for those tables.

Identifying translation table requirements

Introduction

Not all systems require translation tables, so you must first identify if there is a need for a table on your system.

If the following cases are the only local and long distance scenarios that take place, you will not have to create any translation tables. Meridian Mail will use the prefixes that are defined in the Dialing Translation Defaults screen to perform all the translations required.

Normal dialing cases

All DNs with the same area/city code as the local site are treated as local calls.

All DNs with a different area/city code to the local site, are treated as long-distance.

Meridian Mail assumes that all the numbers in the local area/city code are dialed with the local dialing prefix and *without* the local area/city code (in other words, with a format such as 9-xxx-xxxx).

Meridian Mail also assumes that all numbers in area/cities other than the local area/city are dialed with the long distance dialing prefix and with the area/city code of the number (in other words, with a format such as 6 [xxx]-xxx-xxxx).

If these two statements are true for your system, you do not need to define any translation tables. Otherwise, if either or both of these statements are not always true for your system, then translation tables will have to be defined for the exceptional cases.

Dialing cases requiring translation tables

The following table shows examples of the exceptional dialing scenarios that require translation tables.

Case	Is area/city code in called DN same as or different than the local site's area/city code?	Called Area Is	DN Format needs to be
1	Different	Local	Local dialing prefix + area/city code + local number
2	Different	Local	Local dialing prefix + local number
3	Same	Long Distance	Long distance dialing prefix + area/city code + local number
4	Same	Long Distance	Long distance dialing prefix + local number

Cases 1 and 2

Local dialing to another area/city code

For cases 1 and 2, you need to define those instances in which calls to certain exchanges in *another* area/city code (other than your system's) are considered local.

These are exceptional scenarios and require translation tables.

In the translation table, specify either the exchange codes to which a call is considered local or the exchange codes to which a call is considered long distance.

Use the method that results in entering the smaller number of exchange codes. For example, if 200 exchange codes in the area/city code are considered local and 12 are long distance, enter the exchange codes to which dialing is considered long distance.

Cases 3 and 4

Long distance dialing to the same area/city code

For cases 3 and 4, define those instances in which a call to certain exchanges in the *same* area/city code as your system's area/city code are considered long distance.

These cases are also exceptional scenarios, and require translation tables. A translation table allows you to define which exchanges in your area/city are considered local and which exchange codes are considered long distance.

In the translation table, enter either the exchange code to which calls are considered long distance or local (depending on which method results in entering the lesser number of exchange codes).

Creating multiple tables

If more than 120 exchange codes are required for one area/city code, create another table for the area/city code. A number of tables that are created for the same area/city code can be considered a "joint" table. If this is the case, the Prefix for exchange codes *not* in the table field must be identical for all tables that are created for the same area/city code.

Other dialing exceptions

Other dialing exceptions may exist, for example, dialing to the local area/city with a local dialing prefix *and* with the local area/city code in the number dialed. You would also need to define translation tables for these exceptions.

Identifying translation tables required on your system

Introduction

A translation table is needed for an area/city code if calls placed from your system to that area/city code are made in one of the ways that are not supported by the dialing translation defaults. (The scenario where defaults alone support dialing translation is described in "Identifying translation table requirements" on page 17-45.)

Area/city code

A translation table is defined for an area/city code. You should have a good idea of the exchange codes and the two prefixes for the table before you define the table.

Exchange codes

You should identify the exchange codes for the translation table before you identify the prefix for the exchange codes in the table and the prefix for the exchange codes not in the table. This is because depending on which exchange codes you define in the table (they may be considered local or long distance), these prefixes will change.

Prefix for exchange codes in the table

For those exchange codes that are defined in the table, this prefix will be used by the system to dial out of the switch and place the call. Therefore, depending on the scenario, this prefix will either be for local dialing or long distance dialing. The prefix is needed to generate a dialable DN that is understood by the switch.

Prefix for exchange codes *not* in the table

For those exchange codes *not* defined in the table (or any other table for this area/city code) that belong to the area code to which the table applies, this prefix will either be for local dialing or long distance dialing. This prefix is needed to generate a dialable DN that is understood by the switch.

Prefixes for exchange codes - North American example

This table illustrates the format of the prefixes for exchange codes in, and *not* in, the translation table of a North American dialing plan. Remember that you can find these same examples in the scenarios described in more detail on the following pages.

Dialing scenario	Prefix for exchange codes in table	Prefix for exchange codes NOT in table
1. Local dialing to a different area/city code (area/city code required in DN).		
Exchange codes defined in table are considered local.	Y-NPA (9-905)	P-NPA (9-1-905)
Exchange codes defined in table are considered long distance.	P-NPA (9-1-905)	Y-NPA (9-905)
2. Local dialing to a different area/city code (no area/city code).		
Exchange codes defined in table are considered local.	Y (9)	P (9-1)
Exchange codes defined in table are considered long distance.	P (9-1)	Y (9)
3. Long distance dialing to same area/city code (area/city code required in dialing).		
Exchange codes defined in table are considered long distance.	P-NPA (9-1-214)	Y (9)
Exchange codes defined in table are considered local.	Y (9)	P-NPA (9-1-214)
4. Long distance dialing to same area/city code (area/city code required in dialing).		
Exchange codes defined in table are considered long distance.	P (9-1)	Y (9)
Exchange codes defined in table are considered local.	Y (9)	P (9-1)

- Y is the local dialing prefix (9, 8, or 6).
- P is the long distance dialing prefix (91).
- NPA is the Numbering Plan Area (area code).

Translation table worksheet

You can use the following worksheet to plan the exchange codes in your translation table. Remember that each translation table may contain up to 120 exchange codes.

Translation table worksheet

Table ID: _____ **Area/City Code:** _____

Prefix for exchange codes in the table: _____

Prefix for exchange codes NOT in the table: _____

Exchange codes:

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____

_____ _____ _____ _____ _____ _____ _____ _____ _____ _____

Compiling a list of required translation tables

To prepare the data for translation tables, follow these steps.

Step	Action
1	Does your system need a translation for any of the four exceptional dialing situations? • If yes, continue with this procedure. • If no, you do not need this procedure.
2	Select the area code and the two prefixes for exchange codes in, and not in, the translation table.
3	Fill in the associated exchange codes. **Note:** It is recommended that you configure a table that requires fewer exchange codes for the prefix with exchange codes *in* the table than for the prefix with exchange codes *not in* the table.
4	Repeat steps 2 and 3 if there are more exceptional dialing cases requiring a table.

Local dialing to a different area/city code (area/city code required)

Introduction

The area/city code of the dialed DN is different from your local system's area/city code, but no long distance charges apply and a local dialing prefix is required *instead* of a long distance prefix. The area/city code is required as part of the dialable DN.

Scenario

This scenario may occur in larger metropolitan areas that are serviced by a number of area codes. For instance, a large city may have two or three area/city codes (like 416 and 905) to cover the entire metropolitan area.

When a call is placed from the 416 area/city code to some exchange codes in the 905 area/city code, the call may be local. However, for other exchanges, the call may be considered long distance. For those exchanges that are considered local, the long distance prefix must not be inserted in the dialed DN.

In this scenario, the area/city code of the dialed DN is different than your local system's area/city code. However, the local dialing prefix must be included in the dialed number, *not* the long distance prefix. (Charges do not apply to certain calls to the destination area/city code, and the long distance dialing prefix need not be used.) The area/city code *must* be part of the dialable DN.

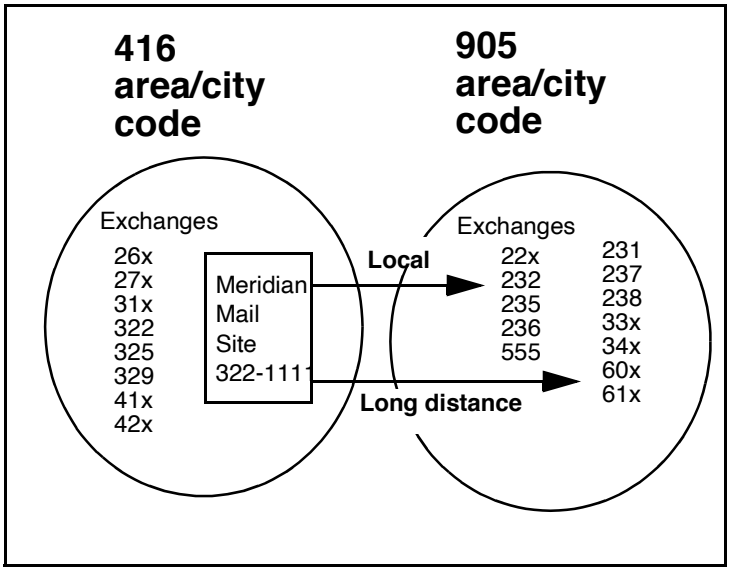
A translation table is required for each area/city code that has *both* local and long distance exchanges, and is dialed from your local system.

Area/city code required for local call

As you can see in the following diagram, in the 905 area code, the exchange codes 22x (which means from 220 to 229), 232, 235, 236, and 555 are local from the 416 area/city code.

Exchanges 231, 237, 238, 33x, 34x, 60x, 61x are all long distance from the 416 area/city code

.



Example

Your Meridian Mail system is located in area/city code 416. The network dialing prefix is 9 and the long distance prefix is 91. A caller phones your system and requests a fax item. Your Fax on Demand service is configured for callback delivery, so the caller is prompted for a callback number in national format. The caller enters 1-905-555-2121 (the 1 is the country code).

If you look at the exchange code diagram above, you will notice that calls to the 555 exchange are considered local. The dialable DN is therefore 9-905-555-2121, and not 91-905-555-2121.

Translation table setup (version 1)

The screen example on page 17-54 shows the translation table that you would have to create to handle the above scenario. This screen example assumes that the local dialing prefix is 9 and that the long distance dialing prefix is 91.

Screen (version 1)

The following screen illustrates the version 1 translation table.

```
                          Dialing Translation
View/Modify Translation Table
                                Prefix for exchange    Prefixes for exchange
Table ID  Area/City Code        codes in the table     codes NOT in the table
    1         905                  9905                   91905

The following exchange codes are defined:
22      232     235     236     555

Select a softkey >

Save    Cancel                                         More Fields
```

Logic of version 1

This example selects those exchange codes in area/city code 905 that require only a local call to area/city code 416. The example shows that the exchange codes (22x, 232, 235, 236, and 555) are local and, therefore, they are assigned the Prefix for exchange codes in the table.

Any other exchange code will be considered long distance by consequence and will be assigned the long distance prefix (91-905), which is defined in the Prefix for exchange codes *not* in the table field.

Translation table setup (version 2)

You could also define the translation in the inverse manner from version 1. That is, you could define the exchange codes that require the long distance prefix, while the remaining exchange codes would be assigned the local prefix by default.

Screen (version 2)

The following screen illustrates the version 2 translation table.

```
                          Dialing Translation
View/Modify Translation Table
                                Prefix for exchange    Prefixes for exchange
Table ID  Area/City Code        codes in the table     codes NOT in the table
    2         905                  91905                    9905

The following exchange codes are defined:
231     237     238     33      34      60      61      [ ]

Select a softkey >

   Save      Cancel                                   More Fields
```

Logic of version 2

The exchange codes that are long distance within the 905 area/city code are explicitly defined in the table instead of the local codes. (Note that the two prefixes for exchange codes in the table and exchange codes *not* in the table fields are reversed from version 1).

Hint for planning translation tables

The way in which you define the table will depend on how many exchange codes within the area/city code are considered local and how many are considered long distance. If, for example, 100 exchange codes in the 905 area/city code are long distance and ten are local, the version 1 translation table would be easier to create since you would have to define only ten codes. However, if there were more local exchange codes than long distance codes, you would create a table similar to that in version 2.

Local dialing to a different area/city code (no area/city code required)

Introduction

This scenario is almost identical to the first scenario because there is local dialing from one area/city code to a different area/city code. However, the difference is that no area/city code is required in the dialable DN. Using the example from page 17-52, the dialable DN would be 9-555-2121 instead of 9-905-555-2121.

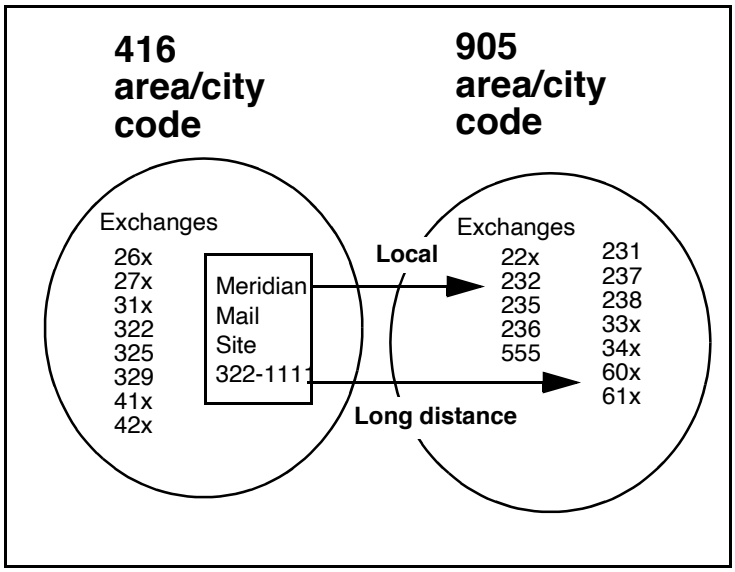
Scenario

This situation may occur if, for example, a metropolitan area is in the process of adopting a new area code in which certain exchanges will be considered local (as described in the previous example).

Therefore, in the exchange code diagram that follows, the first column of exchange codes in the 905 area code are local if dialed from the 416 area code. In order to make the transition easier for people in the area, the service provider will allow calls to the local exchanges in the 905 area code to be placed without the area/city code since this is what people are accustomed to dialing. However, after a certain specified date (when the phone company ends the transition period), the new area code will have to be entered and the translation table prefixes updated (to those in the previous example).

Area/city code not required for local call

This diagram shows the same relationship between 416 and 905 area/city codes as in the previous example except that this time an area/city code is not required to make a local or a long distance call.



Example

If you had to create a translation table to handle the instance in the exchange code diagram above (which does not require area/city codes in a dialable DN), it would look like the View/Modify Translation Table screen that follows.

Translation Table screen–different area/ city code

This example assumes that the default translation prefix for local calls is 9 and for long distance calls is 91.

```
                          Dialing Translation
View/Modify Translation Table
                                Prefix for exchange    Prefixes for exchange
Table ID  Area/City Code        codes in the table     codes NOT in the table
    1         905                   9                       91

The following exchange codes are defined:
22      232     235     236     555

Select a softkey >

   Save      Cancel                                    More Fields
```

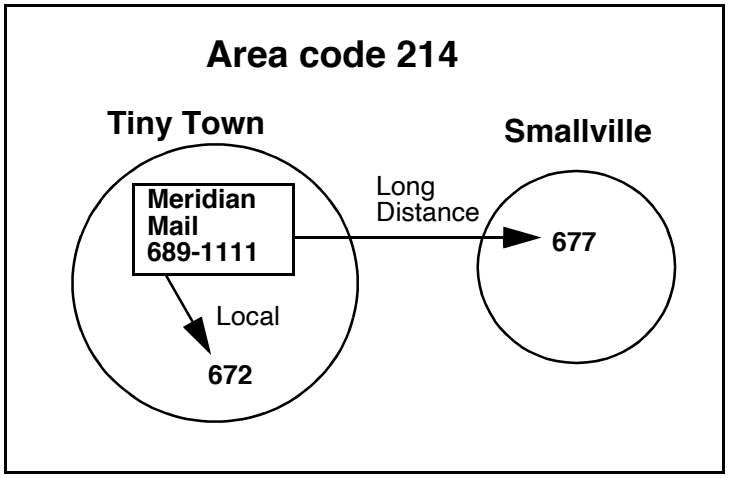
Long distance dialing to the same area/city code (area/city code required)

Introduction

This scenario describes toll call (long distance) dialing within the same area/city code. Calls involve the long distance dialing prefix even though both the calling party and the called party are under the same area code. In this scenario, the area/city code is also required as part of the dialable DN.

Scenario

This sort of dialing scenario may occur when a number of smaller rural areas or towns share an area/city code, yet calls from one town to another are considered long distance.



Example

A caller from Smallville calls into the Meridian Mail system located in Tiny Town and requests that a fax be delivered to DN 214-677-1133. Exchange 677 is in the 214 area code, however, so this is considered long distance because it is in a different town.

Meridian Mail must convert this DN to the dialable DN 91-214-677-1133, where 91 is the long distance dialing prefix.

Translation table

The following translation table illustrates long distance dialing to the same area/city code where the area/city code is not required to make a dialable DN.

```
                              Dialing Translation
Delete Translation Table
                                Prefix for exchange    Prefixes for exchange
Table ID  Area/City Code        codes in the table     codes NOT in the table
    5         416                   91416                     9

The following exchange codes are defined:
592

Select a softkey >

 OK to Delete      Cancel
```

Long distance dialing to the same area/city code (area/city code not required)

Introduction

This scenario is almost identical to the preceding scenario because there is long distance dialing from one area/city code to the same area/city code. The only difference is that no area/city code is required in the dialable DN. Using the previous example, the dialable DN in this case would be 91-677-1133 instead of 91-214-677-1133.

Translation table

The following translation table illustrates long distance dialing to the same area/city code where the area/city code is not required to make a dialable DN.

```
                              Dialing Translation
Delete Translation Table
                              Prefix for exchange    Prefixes for exchange
Table ID  Area/City Code      codes in the table     codes NOT in the table
    5         416                 91416                     9

The following exchange codes are defined:
592

Select a softkey >

 OK to Delete      Cancel
```

The View/Modify Translation Table screen

Introduction

A translation table is defined on the View/Modify Translation Table screen. This subsection explains this screen and the contents of each field in the screen.

How to access the screen

See “Configuring translation tables” on page 17-64.

View/Modify Translation Table screen

The following is an example of the View/Modify Translation Table screen.

```
                          Dialing Translation
View/Modify Translation Table
                                Prefix for exchange    Prefixes for exchange
Table ID  Area/City Code        codes in the table     codes NOT in the table
    1        905                   9905                   91905

The following exchange codes are defined:
427      428      619      684      685      686      687      688
689

Select a softkey >

   Save      Cancel                                      More Fields
```

Field descriptions

The following table describes the fields in the View/Modify Translation Table screen.

Table ID	
Description	This field contains the number of the translation table.
Field status	Read-only. There are 15 tables, numbered 1-15. This is the ID of the selected table. This field cannot be changed. (Once the table is deleted, the table ID can be reused.)

Area/City Code	
Description	This field contains the area/city code of the translation table. A translation table is defined for an area/city code.
Valid characters	0-9
Valid length	1-8 characters

Prefix for exchange codes in the table	
Description	This field contains the prefix used for dialing telephone numbers in the area/city of this table, whose exchange codes are defined in the translation table.
Valid characters	0-9, * (where * means pause)
Valid length	0-12 characters

Prefixes for exchange codes NOT in the table	
Description	This field contains the prefix used for dialing telephone numbers in the area/city of this table and whose exchange codes are *not* defined in the translation table. If more than one table is defined for one area/city code, this field is enforced to be the same in every table (so that there is only one set of exchange codes *not* in any table).
Valid characters	0-9, * (where * means pause)
Valid length	0-12 characters

The following exchange codes are defined:	
Description	These fields contain the exchange codes defined in the translation table. Up to 120 exchange codes may be defined for one table. (To display more empty rows of exchange codes, press the [More Fields] softkey.)
Valid length	0-8 characters If the length of a given exchange code is 0, then that field is empty.

Configuring translation tables

Procedure To configure a translation table, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Choose General Administration.
2	Choose Dialing Translation.
3	Choose Translation Tables. **Result:** The Translation Tables screen appears listing the existing and empty tables.

```
                              Dialing Translation
Translation Tables
                                   Prefix for exchange    Prefixes for exchange
Table ID  Area/City Code           codes in the table     codes NOT in the table
      1     905                        9905                   9905
      2     905                        91905                  9905
      3     214                        91214                  9
      4     214                        91                     9
      5     Empty
      6     Empty
      7     Empty
      8     Empty
      9     Empty
     10     Empty
     11     Empty
     12     Empty
     13     Empty
     14     Empty
     15     Empty

Move the cursor to the item and press the space bar to select.
The Network Database has been updated.
     Exit                          View/Modify        Delete
```

Step	Action
4	If you want to add a new table, move the cursor to an empty table. To modify an existing table, move the cursor to that table.
5	Press the <Space Bar> to select it.

Step	Action
6	Press the [View/Modify] softkey. **Result:** You are prompted for an area/city code.

```
                              Dialing Translation
View/Modify Translation Table
                              Prefix for exchange    Prefixes for exchange
Table ID  Area/City Code      codes in the table     codes NOT in the table
    1         213                 _____                  _____

The following exchange codes are defined:
_______  _______  _______  _______  _______  _______  _______  _______

                                                                _______
Select a softkey >

   Save        Cancel                                   More Fields
```

7	Enter the area/city code for the translation table that you want to create and press <Return>. **Result:** The View/Modify Translation Table screen is displayed.
8	Specify the prefix for the exchange codes that are defined in the table. This prefix is applied to DNs entered by callers/ users in order to generate the appropriate dialable DN.
9	Specify the prefix for exchange codes that are *not* defined in the table. This prefix is applied to DNs entered by callers/ users in order to generate the appropriate dialable DN.

Step	Action
10	Enter the appropriate exchange codes. To display more empty fields, press the [More Fields] softkey. Up to 120 exchange codes can be defined for a table. **Note:** All entries will be validated to avoid duplication.
11	Do you want to save the screen? • If yes, press the [Save] softkey to save the table. **Result:** The updated Translation Tables screen is displayed. **Note:** If you run out of exchange code fields for an area/city code, create another table for that area/city code. Return to step 4. The values you enter in the Area/City Code and the Prefix for exchange codes *not* in the table fields of the second table must match those of the first table. • If no, press the [Cancel] softkey.

Deleting translation tables

Introduction

You can use the following procedure if you want to remove a translation table in its entirety.

Procedure

To delete the data from a translation table, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Choose General Administration.
2	Choose Dialing Translation.
3	Choose Translation Tables.
4	Move the cursor to the (non-empty) table that you want to delete.
5	Press <Space Bar> to select it.
6	Press the [Delete] softkey. **Result:** The Delete Translation Table screen is displayed. All fields in this screen are read-only.

```
                                Dialing Translation
Delete Translation Table
                                Prefix for exchange    Prefixes for exchange
Table ID  Area/City Code        codes in the table     codes NOT in the table
    5        416                   91416                    9

The following exchange codes are defined:
592

Select a softkey >

OK to Delete    Cancel
```

7	Do you want to delete the table? • If yes, press the [OK to Delete] softkey. • If no, press the [Cancel] softkey.

Section E: Sample datafills

In this section

Overview 17-70
Datafill for countries without area/city codes 17-71
Datafill for a case where the switch handles dialing translation 17-72

Overview

Introduction

This section illustrates two special cases for dialing translation which require a slightly different setup.

The two cases are

- countries without area/city codes in their dialing plans
- the switch is already handling the dialing translations

Datafill for countries without area/city codes

Introduction

Some countries, such as Costa Rica, do not require area/city codes for national calls in their dialing plans.

For example, the following Dialing Translation Defaults screen leaves the area/city code field blank. The other field as defined as usual.

No area/city codes screen

The following shows an example of the Dialing Translation Defaults screen defined for a location without an area/city code.

```
                          Dialing Translation
Dialing Translation Defaults

Default Dialing Prefixes
   Local Dialing:            9
   Long Distance Dialing:    9
   International Dialing:    9011
   ESN Dialing:              6

Local System Defaults
   Local Country Code:       852
   Local Area/City Code:

Capture External CLID with Unknown Format:        No Yes



Select a softkey >

     Save        Cancel
```

Description

When the Local Area/City Code is not entered, the system will treat *all* numbers undergoing translations as having no area/city code.

This eliminates the difference between local and long distance calls, and all national numbers will be treated in the same fashion as local numbers.

Datafill for a case where the switch handles dialing translation

Introduction

In the case where the switch is already set up and used to handle dialing translations, you may choose to *bypass* the definition of any translation tables on Meridian Mail.

In order to allow the switch to take over dialing translations, all calls must be handled by the switch.

On the M1, this can be accomplished using ESN. To implement this, all numbers dialed by the Meridian Mail must be in the same format (for example, 6-1-area/city code - local number). The switch will use its ESN software to correctly dial and route the call.

Defaults screen for switch handling translation

The following shows an example of the Dialing Translation Defaults screen with fields set so that the number passed to the switch by Meridian Mail is always in the same format so that on-switch dialing translations are used.

```
                          Dialing Translation
Dialing Translation Defaults

Default Dialing Prefixes
   Local Dialing:            61509
   Long Distance Dialing:    61
   International Dialing:    6011
   ESN Dialing:              6

Local System Defaults
   Local Country Code:       1
   Local Area/City Code:     509

Capture External CLID with Unknown Format:        No Yes



Select a softkey >

     Save        Cancel
```

Scenario: International number

Company X publishes a Fax On Demand number set up for international callback for callers outside of North America. A caller from England enters the number of her fax machine as 44-628-812810 in response to the prompt “Please enter the fax

number, including country code and area or city code, followed by number sign."

The system translates the number according to the defaults in the example screen:

- The service is set up for international callback and, therefore, the system performs an international number translation on the entered number. First the system checks for the local country code (in this case, 1) at the start of the number. However, the callers country code is different.
- The caller's country code is 44 and the city code is 628, so the system attaches 6011 to create the number 6011-44-628-812810.

Scenario: Local number

The new External CLID feature has been installed on the system and allows the system to recognize the type of a number based on the information received from the switch.

An external caller leaves a message in the Meridian Mail user's mailbox. The CLID received is 795 9851, and the switch indicates that this is a local subscriber number.

To reply to this number, the number must be translated by the system as follows:

- Since this is a local subscriber number, the system knows that the number should be dialed for a local call. The system adds the local dialing prefix to the beginning of the number.
- The final number is 6 1 509 795 9851, where 6 1 509 is the added prefix.

Section F: Troubleshooting dialing translations

In this section

Overview 17-76
Diagnosing and tracing problems in a dialing translation 17-77

Overview

Introduction

This section provides you with a procedure to diagnose problems with dialing translations. It should be used in conjunction with the NTP of the feature (like the *Fax on Demand Application Guide* [NTP 555-7001-327] or *AMIS Networking Installation and Administration Guide* [NTP 555-7001-242] that uses dialing translations).

Diagnosing and tracing problems in a dialing translation

Introduction

Dialing translation problems show up as an inability to reach a number specified in the AMIS, External CLID, or Fax on Demand services. Diagnosis of such problems is best accomplished by collecting all setup information and then following the flowcharts of the translation process to determine the translated number.

Procedure

To troubleshoot the translation process, follow these steps.

Step	Action
1	Collect all relevant information. **Note:** This includes the dialing translation defaults and translation table settings.

IF the problem occurred in	THEN go to
Fax on Demand	the Fax on Demand VSDN definition and session profile.
AMIS	local AMIS VSDN definition.
Virtual Node AMIS	local AMIS VSDN definition and the VSDN definition of the Virtual Node AMIS remote site.
External CLID	the External CLID (the caller's number) to which the user listened or to which the user tried to send a message.

2	Is the translated number already dialable? • If yes, go to step 5. • If no, the dialing translation setup is likely incorrect. Continue with the following steps.

Step	Action
3	Determine the translated dialable number that was found to be invalid.

IF the invalid number used	THEN
Fax on Demand	the Fax Audit Trail will contain the translated DN that the system is attempting to dial. For more information about the Fax Audit Trail, see Chapter 33, “Audit Trail reports” under Section C: Fax Audit Trail reports.
AMIS	SEER 4211 is generated. (The SEER text is “The number XXXXXXX cannot be reached,” where XXXXXXX is the translated number).
External CLID	ask the user for the number that is announced by Meridian Mail when listening to the message from which the error was reported.

4 Pick a particular scenario that is causing problems and walk through the translation process flowcharts from page 17-23 to 17-26 to determine the translated number.

This method will help you determine if the problem is caused by dialing translations.

Step	Action
5	If the translated number is dialable on the system, then the problem may not be related to dialing translations. In this case, the problem is likely to be one of the following: • The fax callback number, AMIS number, or External CLID number is restricted in the Meridian Mail restriction/ permission lists and cannot be dialed. • For External CLID, the number that is passed from the switch to Meridian Mail may be incorrect. Use the Session Trace feature from the Tools level to determine the number and call type that was received from the switch when the external caller left the user a message in the user's mailbox. • For External CLID, refer to *System Administration Tools* (NTP 555-7001-305.) • For Fax on Demand, check the session profile and ensure that it is set up correctly. • For AMIS, check the class of service to which the user belongs and ensure that it allows the user to send or receive Open Network (AMIS) messages. • The area/city code of the callback number or AMIS number may be restricted on the switch. Check LD 90 in the Meridian 1. • Alternatively, the entire number may be restricted because it is considered a "special number" (also check LD 90 in the Meridian 1). • The agent is restricted in the switch. Check NCOS and FCAS in LD 87.

Chapter 18

Routine maintenance

In this chapter

Overview	18-2
Monitoring Meridian Mail operation	18-3
Monitoring Meridian Mail hardware	18-5
Backing up the system	18-7
Cleaning the tape drive	18-9

Overview

Introduction

This chapter identifies the routine maintenance tasks recommended for optimum operation of your Meridian Mail system. It then refers you to the chapters or manuals that contain the information and procedures you need to perform these tasks.

Purpose

These tasks are carried out regularly to ensure efficient operation of your system and to anticipate future capacity needs or necessary services available to users.

Monitoring Meridian Mail operation

Introduction

Operational Measurement (OM) reports enable you to monitor your system usage. You can study which features are being used on your system and how heavily they are being used.

OM reports can reveal potential technical problems with your system, such as low disk space (which affects the ability of the Meridian Mail system to store messages and perform its functions).

Operational measurements

The following provides an overview of OM reports.

OM traffic reports

The OM traffic reports show both how the system is being used and how much the system is being used. That is, they identify the number of calls processed, and the number of times a user logs in to Meridian Mail or accesses particular features. If a feature is not being used, this may indicate that users are not aware of it or do not know how to use it. It may also reveal that the feature is not required.

These reports also help you to ensure the security of your system. If certain features are being accessed frequently during off-hours, this may indicate that hackers are attempting to use your system to place unauthorized long distance calls.

OM user usage reports

The OM user usage reports monitor how specific users employ features such as Voice Messaging or networking, if they are installed.

User usage reports display daily summary statistics about each user, including the following:

- the number of times a user has logged on
- the number and total length of times that callers have connected to a user's mailbox
- the number and total length of messages created and received
- the disk space used by the user's messages and greetings

Operational measurements (cont'd)

Disk Usage Detail report

This report shows the voice space used on a disk volume. If the voice space is consistently greater than your disk usage warning level, then disk space is getting low, and you should take steps to reduce the voice space used.

Channel Usage Detail report

This report shows the number of calls and voice mail usage per channel. If the number of calls is high or the average message length is exceptionally long, the channels may be too busy to handle all incoming calls. As a result, users may not be able to access the Meridian Mail system.

Frequency

Check the performance of your Meridian Mail system periodically to ensure that efficient use is made of the voice services provided on your system.

Procedure

For information and procedures required for monitoring the operation of your Meridian Mail system, see Chapter 30, "Operational Measurements".

For information and procedures required for helping to ensure the security of your Meridian Mail system, see Chapter 6, "Setting up Meridian Mail security".

Monitoring Meridian Mail hardware

Introduction

The System Status and Maintenance menu provides monitoring and control screens through which you obtain views of the operational state of the system at four levels:

- system status
- card status
- DSP port status
- disk status

Description

The System Status and Maintenance functions are used in the course of routine maintenance and enable you to take any component of the system out of service while performing maintenance. A component can be taken out of service by disabling it (forcing it out of its operational state), or by performing a courtesy disable, which progressively disables active DSP ports as they become idle. The Courtesy Disable feature avoids any disruption of calls in progress.

What to check

The System Status and Maintenance menu provides options for viewing the system status, card status, and DSP port and disk status. From this menu, you can also manipulate the Channel Allocation Table, perform Disk Maintenance, and view System Event and Error Reports.

The Hardware Administration screens allow you to view the contents of the hardware database in your Meridian Mail system. The hardware database is a system utility that maintains a current listing and description of all nodes, cards, and ports in your system.

Modifying the hardware database

To modify the hardware database, you must use the “modify hardware” tool. Refer to *Meridian Mail System Administration Tools* (NTP 555-7001-305).

Frequency

Check the operation of Meridian Mail hardware periodically and when a problem is reported by the system.

Procedure

For information and procedures required for checking the operation of your Meridian Mail hardware, see Chapter 27, “Hardware administration” and Chapter 28, “System status and maintenance”.

Backing up the system

Introduction

If a disk drive fails, the system can be restored to a working state by copying the data back from tape onto a replacement disk. Backup copies of the system data are fundamental to restoring the system with as little disruption and data loss as possible.

Backups to tape

All Meridian Mail systems have a tape drive capable of reading and writing industry-standard quarter-inch data cartridges (QIC). Backups to tape can be either full or partial. You can also selectively back up users or services to tape, or both.

Backups to disk

If the Disk-to-Disk Backup feature is installed, you can copy data from one disk to another. This allows you to recover data if a disk fails.

Backups to disk can be done frequently, with relatively little effort, and reduce the need for frequent and time-consuming backups to tape. However, disk-to-disk backups do not completely eliminate the need for tape backups.

Storage impact

Disk-to-disk backup reduces the voice message storage somewhat and sets aside some of the disk space for backup copies.

Scheduling a backup

Schedule backups for a time when your system is relatively quiet or outside the regular business hours for your organization. Do not back up the system if it is operating above 50% of the rated capacity or between the hours of 1:00 a.m. and 5:00 a.m., since important system audits take place during these hours. These audits are activated automatically at the same time every day and ensure the continued operation of your system. Do not schedule a backup if more than one tape is required for it unless you are going to be available to switch tapes when you are prompted to do so.

Frequency

Back up your system on a regular schedule. You can set the frequency as daily, weekly, or monthly in the Schedule Backup screen under the General Administration menu. You should also back up your system whenever you make changes to it.

Procedure

For information and procedures required for backing up your Meridian Mail system, see Chapter 15, “Back up and restore Meridian Mail data”.

Cleaning the tape drive

Introduction

As occurs with any high-capacity removable media such as tapes or floppy drives, debris collects on the tape heads each time a tape drive is used. If too much debris collects, the tape drive is unable to write or read data correctly, and the tape head must be cleaned.

Frequency

Most tape drive manufacturers recommend cleaning the tape heads after a brand-new tape has been used for the first time, and after every eight hours of tape drive operation. If media (parity) errors occur when reading or writing tapes, it is an indication of either a faulty tape or dirty tape heads.

Procedure

For information and procedures required for cleaning your tape drive, refer to the *Meridian Mail Installation and Maintenance Guide* (NTP 555-70x1-250) appropriate for your system.

Chapter 19

Voice administration—an overview

In this chapter

Voice Administration 19-2

Voice Administration

Introduction

This chapter describes the use of the Voice Administration menu and the related chapters.

Voice administration comprises all facilities related to processing voice information. These facilities offer a range of functions from the playback of a recorded announcement to the automated attendant service.

The Voice Administration menu

When you select Voice Administration from the main menu, the following screen appears.

```
                    Voice Administration

          1  Voice Messaging Options

          2  Voice Security Options

          3  Restriction/Permission Lists

          4  Voice Services Administration

          5  Outcalling Administration

          6  Voice Form Definitions

Select an item >

     Exit
```

Voice Messaging Options

Voice Messaging Options determine the general characteristics of the voice messaging service.

Voice Security Options

Voice Security Options allow you to control the level of security and access provided to Meridian Mail users.

Restriction/ Permission Lists

The Restriction/Permission Lists option allow you to set up the restriction/permission codes to be used by your system. These codes are applied to various features and are intended to protect your system by preventing users and callers from placing unauthorized calls while connected to your Meridian Mail system.

Voice Services Administration

The Voice Services Administration option allows you to

- add service DNs to the system and maintain existing DN information
- create a Voice Services profile
- create and maintain services such as
  - Announcements
  - Thru-Dial services
  - Voice Menus
  - Time-of-Day controllers
  - Fax item definitions (if Fax on Demand is installed)

These services offer a range of functions from the simple playback of a recorded announcement to the more sophisticated voice menus which allow callers to make choices by pressing keys on their telephone keypads.

Outcalling Administration

The Outcalling Administration option allows you to specify outcalling parameters which affect the Remote Notification and Delivery to Non-user feature.

This option is displayed only if the outcalling feature is installed.

Voice Form Definitions

The Voice Form Definitions option allows you to develop custom applications that ask specific questions of callers and collect their responses. These applications can be thought of as the electronic equivalent of a survey or questionnaire.

This option is displayed only if the voice forms feature is installed.

Related chapters

The following table describes which chapter or document you should refer to when using one of the Voice Administration menu options.

For the following option	See
Voice Messaging Options	Chapter 20, "Voice messaging options".
Voice Security Options	Chapter 6, "Setting up Meridian Mail security".
Restriction/Permission Lists	Section H: Restriction/ Permission lists in Chapter 6, "Setting up Meridian Mail security".
Voice Services Administration	Chapter 21, "Display options".
Outcalling Administration	*Outcalling Application Guide* (NTP 555-7001-320).
Voice Form Definitions	*Voice Services Application Guide* (NTP 555-7001-325).

Related information

Display options

The [Display Options] softkey is available from Voice Services Administration. The Display Options screen allows you to customize the Voice Services Administration screens.

See Chapter 21, “Display options. ”

Finding VSDNs and services

Within Voice Administration, you can use the find function to find a specific VSDN or voice or fax service, or a subset of VSDNs or voice and fax services.

See Chapter 22, “Finding and printing VSDNs and service definitions. ”

Configuring Meridian Mail services

Configuring Meridian Mail services involves setup on the Meridian 1 and in Meridian Mail.

For information about how to configure the Meridian 1 to support Meridian Mail services, see Chapter 23, “Configuring Meridian Mail services”.

Chapter 20

Voice messaging options

In this chapter

Section A: Introduction	20-3
Section B: Languages on multilingual systems	20-11
Section C: Customizing recordings	20-27
Section D: Defining operational characteristics for voice messaging	20-37

Section A: Introduction

In this section

Overview 20-4
Accessing the Voice Messaging Options screen 20-5
The Voice Messaging Options screen 20-6
Defining voice messaging options 20-9

Overview

Introduction

Setting up voice messaging options for your system involves the following tasks.

Setting up languages

If you have more than one language installed, you must set up certain language parameters. This is described in Section B: Languages on multilingual systems.

Customizing recordings

You can customize the following recordings:

- the call answering greeting (for MMUI)
- the VMUIF introductory tutorial (for VMUIF)
- the VMUIF login greeting

This is described in Section C: Customizing recordings.

Enabling features

You can enable/disable certain voice messaging features such as timed delivery, name dialing/name addressing, and external call sender. This is described in Section D: Defining operational characteristics for voice messaging.

Setting up the broadcast mailbox

The broadcast mailbox is set up in the Voice Messaging Options screen. This involves assigning a mailbox number and recording a personal verification (the verification is optional). This is described in Section D: Defining operational characteristics for voice messaging.

Defining operational characteristics

You can define operational characteristics for voice messaging such as

- the maximum number of days that read messages are kept before being deleted
- whether a warning message is played to users when their mailbox is almost full, and when this message is played
- the billing DN

This is described in Section D: Defining operational characteristics for voice messaging.

Accessing the Voice Messaging Options screen

Introduction

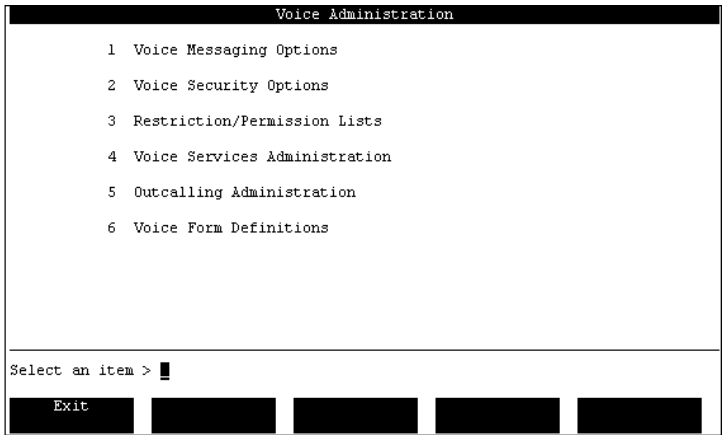
All of the procedures in this chapter are carried out in the Voice Messaging Options screen. Use this procedure to access this screen.

Procedure

To access the Voice Messaging Options screen, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Voice Administration. **Result:** The Voice Administration menu is displayed.



2	Select Voice Messaging Options. **Result:** The Voice Messaging Options screen is displayed.

The Voice Messaging Options screen

Introduction

The fields in the Voice Messaging Options screen vary somewhat depending on the interface (MMUI or VMUIF).

MMUI version

This is the MMUI version of the Voice Messaging Options screen.

Part 1

```
                          Voice Administration
Voice Messaging Options

Default Language:                              American_English
                                               Canadian_French

Secondary Default Language                     American_English
                                               Canadian_French

Default Language Overrides User's
Preferred Language for Call Answering:         No Yes

Customized recording for American_English

  Call Answering Greeting (Voice):             No

Customized recording for Canadian_French

  Call Answering Greeting (Voice):             No
                                                                MORE BELOW

   Save        Cancel                                   Voice
```

Part 2

```
                          Voice Administration                  MORE ABOVE
Voice Messaging Options

Maximum Delay for Timed Delivery (days):       31

Name Dialing and Name Addressing:              Disabled Enabled

Prefix for Name Dialing and Name Addressing:   11

Broadcast Mailbox Number:                      5555

Broadcast Mailbox Personal Verification (Voice): No

Billing DN:

Local Addressing Lengths:                      0  0

Default Message Delivery Priority:             Standard Economy
                                                                MORE BELOW

   Save        Cancel                                   Voice
```

Part 3

```
MMUI VM                        Voice Administration                    MORE ABOVE
Voice Messaging Options

Local Addressing Lengths:                                  0  0

Mailbox Full Warning Threshold (percentage):               85

Maximum Read Message Retention (days):                     7
("0" implies that there is no organization
 maximum limit. Read Message Retention will
 be determined from each user's profile.)

External Call-Sender Allowed:                              No Yes

Voice Message Playback Speed                               Percentage Increase
        Normal     :                                       None
        Increment 1:                                       None 25 33 50 67 75 100
        Increment 2:                                       None 25 33 50 67 75 100
        Increment 3:                                       None 25 33 50 67 75 100

      Save        Cancel                                        Voice
```

VMUIF version

This is the VMUIF version of the Voice Messaging Options screen.

Part 1

```
                              Voice Administration
Voice Messaging Options

Default Language:                                  American_English
                                                   Canadian_French

Default Language Overrides User's
Preferred Language for Call Answering:             No Yes

Customized recordings and Recording Selections for American_English

  VMUIF Introductory Tutorial (Voice): No        Type: None Default Custom

  VMUIF Introductory Tutorial for
  Dial Pulse (Voice):                  No        Type: None Default Custom

  Login Greeting (Voice):              No        Type: None Default Custom

Customized recordings and Recording Selections for Canadian_French
                                                                   MORE BELOW

      Save        Cancel                                        Voice
```

Part 2

```
                    Voice Administration                    MORE ABOVE
Voice Messaging Options


Customized recordings and Recording Selections for Canadian_French

  VMUIF Introductory Tutorial (Voice): No        Type: None Default Custom

  VMUIF Introductory Tutorial for
  Dial Pulse (Voice):                  No        Type: None Default Custom

  Login Greeting (Voice):              No        Type: None Default Custom

Lockout Revert DN:                                _____________________
(Blank implies no revert)

Personal Distribution List Prefix:                __

Broadcast Mailbox Number:                         5555_____________
                                                                MORE BELOW

   Save        Cancel                                   Voice
```

Part 3

```
                    Voice Administration                    MORE ABOVE
Voice Messaging Options

Personal Distribution List Prefix:                __

Broadcast Mailbox Number:                         5555_____________

Broadcast Mailbox Personal Verification (Voice): No

Billing DN:                                       _____________________

Local Addressing Lengths:                         0_ 0_

Maximum Read Message Retention (days):            7_
("0" implies that there is no organization
 maximum limit. Read Message Retention will
 be determined from each user's profile.)

External Call-Sender Allowed:                     No Yes

   Save        Cancel                                   Voice
```

Defining voice messaging options

Procedure

This is a high-level procedure for setting up your voice messaging options. Detailed step-by-step procedures are provided in the following sections in this chapter.

Step	Action
1	Do you have more than one language installed on your system? • If yes, see the section "Languages on multilingual systems" on page 20-11. • If no, go to step 2.
2	Do you want to customize or disable any greetings or tutorials? • If yes, see the section "Customizing recordings" on page 20-27. • If no, go to step 3.
3	Set up operational characteristics for voice messaging. See the section “Defining operational characteristics for voice messaging” on page 20-37.

Section B: Languages on multilingual systems

In this section

Overview	20-12
The default language and the user's preferred language	20-13
Setting up languages on systems without dual language prompting	20-15
Setting up languages on systems with dual language prompting	20-19

Overview

Introduction

The language parameters you need to define depend on whether the Dual Language Prompting feature is installed.

Choosing the correct procedure

Use this table to identify which procedure to follow to set up languages on your system.

IF Dual Language Prompting	THEN follow the procedure
is not installed	on page 20-15.
is installed	on page 20-19.

The default language and the user's preferred language

The default language

The first language that was installed becomes the default language. You can change the default language in the Voice Messaging Options screen.

The default language is also known as the primary language.

When the default language is used

The default language is the language in which prompts are played to callers

- during call answering and express messaging sessions
- during initial logon (before the mailbox number is identified) if they are calling from a phone that does not have a mailbox. This could either be an external phone or an internal phone that does not have an associated mailbox.

The user's preferred language

When multiple languages are installed on the system, local voice users can have a preferred language that is different from the default language. A user's preferred language is specified when you add a mailbox in the Add Local Voice User screen.

Affected prompts

If the user has a preferred language that is different from the primary default language, the following prompts are played in the user's preferred language:

- prompts that are played to the user while the user is logged on to Meridian Mail
- prompts that are played to callers during call answering and express messaging sessions

Overriding the user's preferred language

You may not want internal or external callers, or both, who are transferred to Meridian Mail to hear prompts in the user's preferred language. Instead, you might want them to hear prompts in the (primary) default language.

To ensure that callers who are forwarded to Meridian Mail hear prompts in your system's primary language, the Default Language Overrides User's Preferred Language field in the Voice Messaging Options screen must be set to Yes. Users, however, still hear prompts in their preferred language when they log in to retrieve messages.

Example

Your office is located in Vancouver, British Columbia. Many of your employees speak Mandarin as their first language and, therefore, prefer to hear prompts in Mandarin while using Meridian Mail.

However, most of your customers and external callers are English-speaking and you want them to hear Meridian Mail prompts in English.

You, therefore, set the Default Language Overrides User's Preferred Language field to Yes.

Setting up languages on systems without dual language prompting

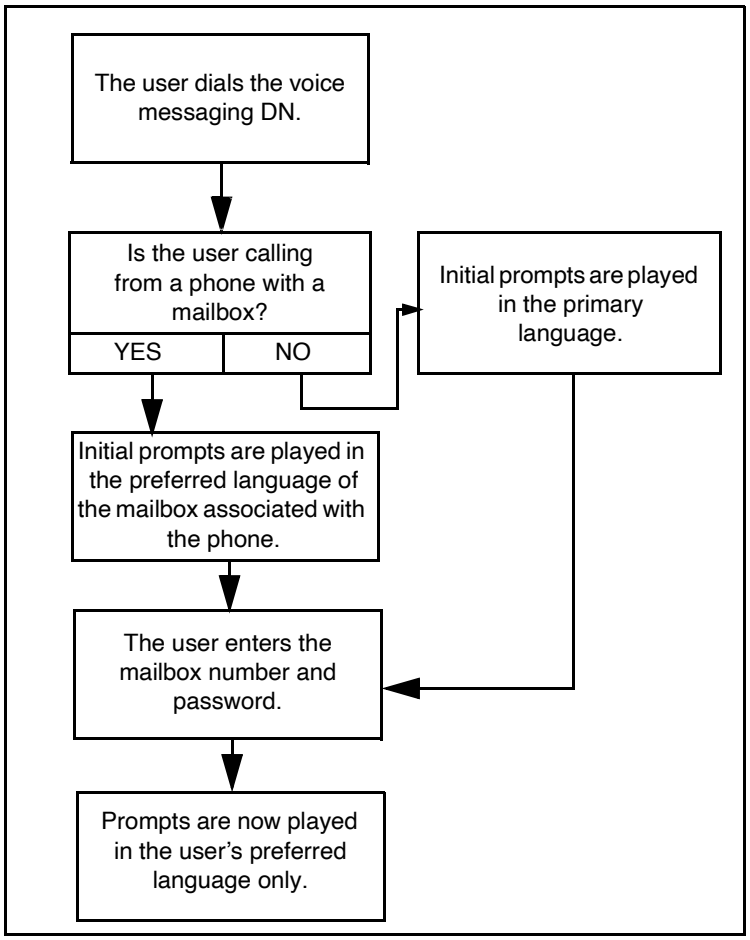
Introduction

To set up languages when Dual Language Prompting is not installed, you must specify

- the default language (also known as the primary language)
- whether the default language overrides the user's preferred language

Mailbox logon

This flowchart shows the language in which prompts are played during mailbox logon.



Express messaging

The language in which prompts are played depends on whether the caller is calling from a phone that has a mailbox.

WHEN the caller calls	THEN prompts are played
from a phone with a mailbox	in the preferred language of the mailbox associated with the phone.
from a phone that does not have a mailbox	in the primary default language.

Call answering

Prompts are played in the user's preferred language unless the system default language overrides the user's preferred language.

Procedure

To set up languages on a multilingual system, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Messaging Options. **Result:** The Voice Messaging Options screen is displayed.

```
                              Voice Administration
Voice Messaging Options

Default Language:                                Latin_American_Spanish Japanese

Default Language Overrides User's
Preferred Language for Call Answering:           No Yes

Customized recordings and Recording Selections for Latin_American_Spanish

  VMUIF Introductory Tutorial (Voice): No        Type: None Default Custom

  VMUIF Introductory Tutorial for
  Dial Pulse (Voice):                  No        Type: None Default Custom

  Login Greeting (Voice):              No        Type: None Default Custom

Customized recordings and Recording Selections for Japanese
                                                                    MORE BELOW

   Save        Cancel                                               Voice
```

3	Select the language in which you want Meridian Mail prompts to be played in the Default Language field.

Step	Action
4	Do you want the (primary) default language to override users' preferred languages? • If yes, select Yes in the Default Language Overrides User's Preferred Language field. • If no, select No.
5	Do you want to continue defining voice messaging options?

IF you want to	THEN
customize or disable recordings	see the section "Customizing recordings" on page 20-27.
modify other voice messaging options	see the section "Defining operational characteristics for voice messaging" on page 20-37.
save what you have done and quit	press [Save].
quit without saving	press [Cancel].

Setting up languages on systems with dual language prompting

Description: dual language prompting

Dual Language Prompting is an optional Meridian Mail feature that is intended for bilingual environments. When installed, prompts are played in two languages:

- the primary language followed by the secondary language or
- the primary language followed by the user's preferred language

Configuration requirements

If Dual Language Prompting is installed on your system, you must specify

- the default language (also known as the primary language)
- the secondary language
- whether the default language overrides the user's preferred language

The secondary default language

When Dual Language Prompting is installed, you can choose a secondary default language in which to play prompts for call answering, express messaging, and mailbox login.

How this secondary language is used depends on other factors as described in more detail on the following pages.

Default

By default, the secondary language is set to the first language that was installed. After installation, the secondary default language is, therefore, the same as the (primary) default language.

How it works

Dual language prompting affects how prompts are played during express messaging, logon, and call answering. However, for each of these features, different factors affect how it works as described on the following pages.

Known versus unknown callers

For express messaging, whether the caller to the service is known affects how dual language prompting works. What is really meant by a "known caller" is a caller whose preferred language is known. In the case of an "unknown caller," the caller's preferred language is not known.

Known callers

A caller is known when calling from an internal phone that has a mailbox associated with it. When calling from his or her own phone, the caller's preferred language is known. When the caller is calling from another internal phone that has a mailbox, the caller's preferred language is not known. However, the preferred language for the associated mailbox is known and, therefore, the caller is considered to be known.

Unknown callers

A caller is unknown when calling from a phone that does not have an associated mailbox (and, therefore, no preferred language associated with it).

An unknown caller could be calling from an external phone or an internal phone that does not have an associated mailbox.

How it works for Express Messaging

Stage 1: express messaging DN is dialed

This is how dual language prompting works when a caller has dialed the express messaging DN but has not yet identified the mailbox number.

WHEN the caller	THEN prompts are played
is known	in the caller's preferred language.
is not known	in the primary language followed by the secondary language.

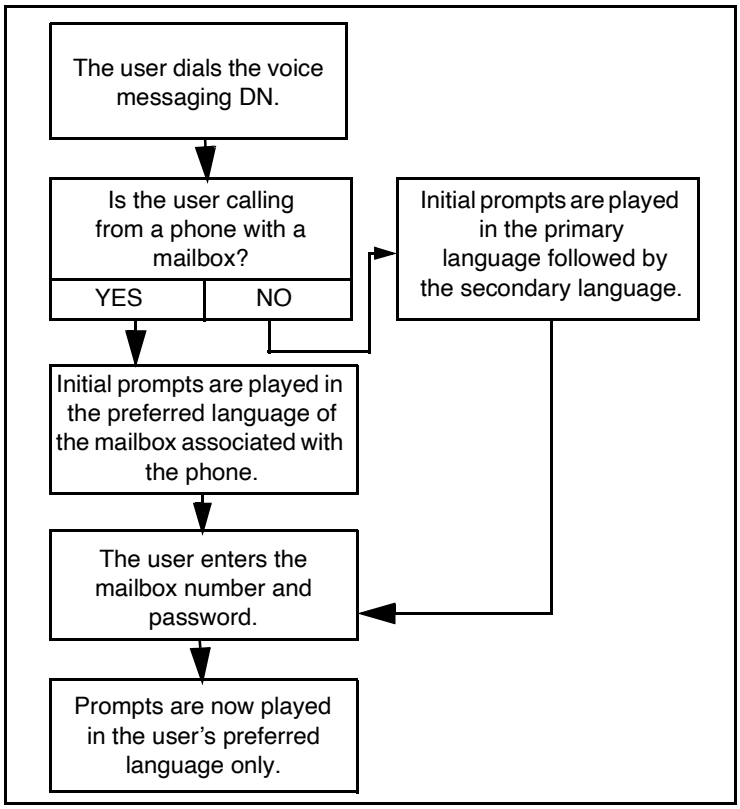
Stage 2: mailbox number is specified

This is how dual language prompting works once the caller has identified the mailbox number.

WHEN the default language	AND the caller	THEN prompts are played in the
does not override the user's preferred language	is known	user's preferred language.
	is not known	primary and then secondary language.
overrides the user's preferred language	is known	primary language only.
	is not known	primary and then secondary language.

How it works for logon

This is how dual language prompting works when a user is logging on to his or her mailbox. The setting in the Default Language Overrides User's Preferred Language field does not affect how dual prompting works in this case.



Configuring dual language prompting for call answering

The following factors affect how dual language prompting works during call answering sessions:

- whether the system default language overrides the user's preferred language
- whether dual language prompting is enabled in the user's class of service

Use this table to help you decide how to configure dual language prompting.

IF you want prompts	THEN set	AND
to be played in the primary language followed by the user's preferred language	the Default Language Overrides User's Preferred Language to No	enable dual language prompting in the user's class of service.
to be played in the user's preferred language only	the Default Language Overrides User's Preferred Language to No	disable dual language prompting in the user's class of service.
to be played in the primary language followed by the secondary language	the Default Language Overrides User's Preferred Language to Yes	enable dual language prompting in the user's class of service.
to be played in the primary language only	the Default Language Overrides User's Preferred Language to Yes	disable dual language prompting in the user's class of service.

Setting up languages for dual language prompting

To set up languages on a system that has dual language prompting, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Messaging Options. **Result:** The Voice Messaging Options screen is displayed.

```
                    Voice Administration
Voice Messaging Options

Default Language:                          American_English
                                           Canadian_French

Secondary Default Language                 American_English
                                           Canadian_French

Default Language Overrides User's
Preferred Language for Call Answering:     No Yes

Customized recording for American_English

  Call Answering Greeting (Voice):         No

Customized recording for Canadian_French

  Call Answering Greeting (Voice):         No
                                                          MORE BELOW

   Save        Cancel                                      Voice
```

3	Select the language in which you want Meridian Mail prompts to be played in the Default Language field.
4	Select the secondary default language.
5	Do you want the (primary) default language to override users' preferred languages? • If yes, select Yes in the Default Language Overrides User's Preferred Language field. • If no, select No.

Step	Action
6	What do you want to do next?

IF you want to	THEN
customize or disable recordings	see the section "Customizing recordings" on page 20-27.
modify other voice messaging options	see the section "Defining operational characteristics for voice messaging" on page 20-37.
save what you have done and quit	press [Save].
quit without saving	press [Cancel].

Section C: Customizing recordings

In this section

Overview 20-28
Recording a customized call answering greeting 20-29
VMUIF introductory tutorials and the VMUIF login greeting 20-32
Recording or disabling VMUIF tutorials and login greeting 20-34

Overview

Introduction

The recordings that you can customize differ depending on the interface type (MMUI or VMUIF).

MMUI call answering greeting

If the interface is MMUI, you can record a custom call answering greeting that identifies your organization.

See “Recording a customized call answering greeting” on page 20-29.

VMUIF tutorials and greeting

If the interface is VMUIF, there are three associated recordings:

- an introductory tutorial for touch-tone phone users
- an introductory tutorial for dial pulse phone users
- a greeting that is played to users when they log in to Meridian Mail

There are prerecorded (“canned”) recordings of these tutorials and the login greeting that are enabled by default.

You can either use these default recordings, customize them, or disable them altogether.

See “VMUIF introductory tutorials and the VMUIF login greeting” on page 20-32.

Recording a customized call answering greeting

Description

The call answering greeting is an optional greeting for the MMUI interface. It typically consists of the spoken name of an organization and is used to identify an organization to callers and users.

Default

By default, there is no call answering greeting. There is no generic call answering greeting. A custom greeting must be recorded if you want to use this greeting.

When the greeting is played

The call answering greeting is played when

- an external caller is transferred to Meridian Mail to leave a message (call answering)
- a user answers a remote notification call

Multilingual systems

If more than one language is installed on your Meridian Mail system and you want to record a call answering greeting, you need to record one greeting for each language.

Before you begin

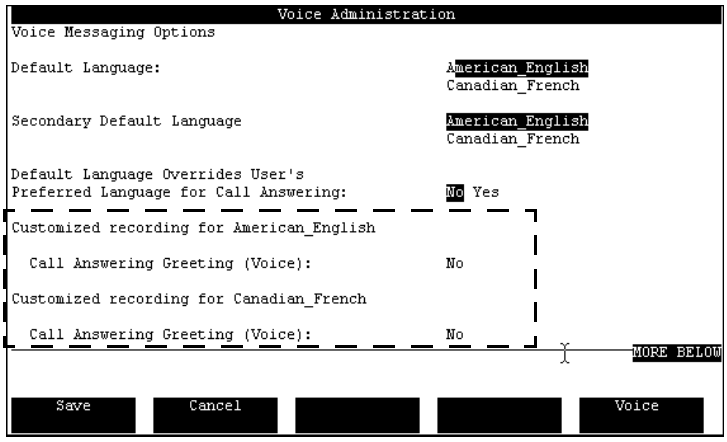
You must access the Voice Messaging Options screen before beginning the following procedure. The procedure for accessing this screen is on page 20-5.

Procedure

To record a call answering greeting, follow these steps.

Starting Point: The Voice Messaging Options screen

Step	Action
1	Move the cursor to the (first) Call Answering Greeting (Voice) field.



2 Press the [Voice] softkey.

Result: The recording softkeys are displayed, and you are prompted for an extension number.

3 Enter the extension of the phone you will use to make the recording.

Result: The phone rings.

4 Pick up the handset.

5 Press the [Record] softkey.

Result: The [Stop] softkey is displayed.

6 Speak the call answering greeting and press [Stop] when you are done.

Note: Recording stops automatically if the greeting exceeds the Maximum Prompt Size or the Record Timeout set in the Voice Services Profile.

7 Do you want to verify the recording?

- If yes, press the [Play] softkey.
- If no, go to step 9.

Step	Action
8	Do you want to rerecord the greeting? • If yes, repeat steps 5 to 7 until you are satisfied with the greeting. **Note:** The old recording will be recorded over. • If no, go to step 9.
9	Do you have more than one language installed? • If yes, press the [Return] softkey to return to the Voice Messaging Options screen and go to step 10. **Note:** Do not hang up the phone. • If no, go to step 11.
10	Move your cursor to the next Call Answering Greeting field (for the next language), and repeat steps 2 to 7 until a greeting has been recorded for each language.
11	Press the [Disconnect] softkey and hang up the phone.
12	Do you want to change any other voice messaging options? • If yes, see the section "Defining operational characteristics for voice messaging" on page 20-37. • If no, press the [Save] softkey.

VMUIF introductory tutorials and the VMUIF login greeting

Introduction

There are three recordings for the VMUIF interface:

- the introductory tutorial (for touch-tone users)
- the introductory tutorial (for dial-pulse users)
- the login greeting

Prerecorded ("canned") versions of these recordings are provided. These default recordings are enabled by default.

You can either use these default canned recordings, customize them, or disable them altogether.

The VMUIF introductory tutorials

When the tutorial is played

This introductory tutorial is played to users when they log on for the first time to familiarize them with the service.

The default (touch-tone) tutorial

This is the prerecorded tutorial (for touch-tone users) that is enabled by default:

"You are about to hear an introduction to call answering. This service will allow your callers to leave you recorded messages. You can play back your messages from your home phone or, if you create a password, from any touch-tone phone outside your home. You can also record a personalized greeting that will be played to your callers, and you can erase your messages right away or store them temporarily in your mailbox. Step-by-step instructions will guide you through your sessions. And remember, for help at any time, just press zero."

The VMUIF introductory tutorials (cont'd)

The default dial-pulse tutorial

This is the prerecorded tutorial for dial pulse users that is enabled by default:

"*You are about to hear an introduction to call answering. This service will allow your callers to leave you recorded messages. You can listen to your messages from your home phone at any time. You can also play your messages from any touch-tone phone. And by calling the Greeting Change Service, you can record a personalized greeting that will be played to your callers. Step-by-step instructions will guide you through your sessions. Consult the brochure for more information.*"

The login greeting

When the greeting is played

The login greeting is played to users when they log in to Meridian Mail.

The default login greeting

This is the prerecorded login greeting that is enabled by default:

"Welcome to call answering."

Multilingual systems

If more than one language is installed on your Meridian Mail system, you need to record a separate version of the tutorials and login greeting for each installed language.

Recording or disabling VMUIF tutorials and login greeting

When to use

Follow this procedure if you want to customize or disable one or more of the following:

- the VMUIF introductory tutorial
- the VMUIF introductory tutorial (dial-pulse version)
- the login greeting

Before you begin

You must access the Voice Messaging Options screen before beginning the following procedure. The procedure for accessing this screen is on page 20-5.

Procedure

To record or disable a tutorial or greeting, follow these steps.

Starting Point: The Voice Messaging Options screen

Step	Action
1	Select what you want to record or disable by moving your cursor to the “Type” field associated with one of the following fields: • VMUIF Introductory Tutorial • VMUIF Introductory Tutorial for Dial Pulse • Login Greeting

```
                          Voice Administration                    MORE ABOVE
Voice Messaging Options


Customized recordings and Recording Selections for American_English

  VMUIF Introductory Tutorial (Voice): No        Type: None Default Custom

  VMUIF Introductory Tutorial for
  Dial Pulse (Voice):                  No        Type: None Default Custom

  Login Greeting (Voice):              No        Type: None Default Custom

Customized recordings and Recording Selections for Canadian_French

  VMUIF Introductory Tutorial (Voice): No        Type: None Default Custom

  VMUIF Introductory Tutorial for
  Dial Pulse (Voice):                  No        Type: None Default Custom
                                                                 MORE BELOW

     Save        Cancel                                          Voice
```

Step	Action
2	Do you want to disable the tutorial or greeting? • If yes, select None. Do this for each tutorial or greeting you want to disable. • If no, go to step 3.
3	Do you want to record a custom tutorial or greeting? • If yes, go to step 4. • If no, go to step 14.
4	Press the [Voice] softkey. **Result:** You are prompted for the extension of the phone you want to use to make the recording.
5	Enter the extension and press <Return>. **Result:** The phone rings.
6	Pick up the receiver. **Result:** The recording softkeys are displayed.
7	Press the [Record] softkey.
8	At the sound of the beep, speak the greeting or tutorial.
9	Press the [Stop] softkey to stop recording.
10	Do you want to verify the recording? • If yes, press the [Play] softkey, listen to the recording, and then go to step 11. • If no, go to step 12.
11	Do you want to rerecord? • If yes, press the [Record] softkey to rerecord the current recording until you are satisfied with the recording. • If no, go to step 12.
12	Select Custom to enable the tutorial or greeting you recorded.
13	Do you want to record another tutorial or greeting? • If yes, move the cursor to the appropriate tutorial or greeting field, and repeat steps 7 to 12 for each additional recording. • If no, go to step 14.
14	Do you want to modify any other voice messaging options? • If yes, see the section "Defining operational characteristics for voice messaging" on page 20-37. • If no, press [Save].

Section D: Defining operational characteristics for voice messaging

In this section

Overview	20-38
Enabling/disabling timed delivery and name dialing/name addressing	20-40
Defining the lockout revert DN and personal distribution list prefix	20-45
Setting up the broadcast mailbox	20-47
Defining the billing DN	20-51
Specifying the message delivery priority for networked systems	20-53
Specifying the mailbox full warning threshold	20-55
Specifying the maximum read message retention	20-57
Enabling/disabling external call sender	20-60
Enabling and configuring speed control	20-62

Overview

Introduction

This section describes

- how to enable or disable voice messaging features such as timed delivery, name dialing/addressing, external call sender, and speed control
- how to set up a broadcast mailbox
- how to define voice messaging characteristics such as
  - how long to store read messages
  - whether to play a warning message to users when their mailbox is full
  - when network messages should be deliverered

Defining MMUI voice messaging options

This is a high-level procedure that describes the tasks you can perform if the interface is MMUI. Detailed step-by-step procedures are provided in the rest of this section.

Step	Action	See page
1	Enable or disable timed delivery and name dialing/ name addressing.	20-40
2	Set up the broadcast mailbox.	20-47
3	Define the billing DN.	20-51
4	If Meridian Networking is installed, define the message delivery priority.	20-53
5	Specify the mailbox full warning threshold.	20-55
6	Specify the maximum read message retention.	20-57
7	Enable or disable external call sender.	20-60
8	Enable and configure speed control.	20-62

Defining VMUIF voice messaging options

This is a high-level procedure that describes the tasks you can perform if the interface is VMUIF. Detailed step-by-step procedures are provided in the rest of this section.

Step	Action	Page
1	Define the lockout revert DN and personal distribution list prefix.	20-45
2	Set up the broadcast mailbox.	20-47
3	Define the billing DN.	20-51
4	Specify the maximum read message retention.	20-57
5	Enable or disable external call sender.	20-60

Enabling/disabling timed delivery and name dialing/name addressing

Introduction

Timed delivery, name dialing, and name addressing are applicable to the MMUI interface only.

Timed delivery

The timed delivery feature allows users to record a voice message now, but tag it for delivery at a later date.

The maximum timed delivery delay

In Voice Messaging Options, you can define the maximum number of days that a message can be delayed before being delivered. The default is 31 days.

Example

You have defined the maximum delay as 62 days. A user tries to tag his or her message for a delivery date of 75 days from today. The user hears the following message:

"*The date you have entered is too far into the future. Please reenter the date.*"

Name dialing and name addressing

Name dialing and name addressing allow users and callers to dial or address users when the extension or mailbox number is not known. As long as the caller knows the user's name, the user can be reached.

Name dialing

Name dialing allows users and callers who have accessed a thru-dial service to enter a user's name instead of his or her extension. The digits that the caller enters are interpreted as letters instead of numbers.

Name addressing

Name addressing allows users to enter another user's name instead of a mailbox number when composing a voice message, composing personal distribution lists, or when using express messaging.

The name dialing/ addressing prefix

If name dialing and name addressing are enabled, you must define a prefix. This prefix must be entered by users or callers before they begin entering the user's name. This prefix signals Meridian Mail that the digits that are about to be entered should be interpreted as letters instead of numbers.

Thru-dial services

When defining a thru-dial service, you have the option of specifying the dialing method as Dial by Number, Dial by Name, or Both.

To select Dial by Name or Both, Name Dialing and Name Addressing must be enabled in the Voice Messaging Options screen.

If Both is selected, meaning that the caller has the choice of how he or she dials the user, the caller must enter the prefix.

If you want to give callers this choice, but do not want them to have to enter a prefix, you can use a voice menu as a front end to two thru-dialers (one that is set up for Dial by Name and one that is set up for Dial by Number). This is described in detail in the *Voice Services Application Guide*.

When to disable name dialing/addressing

This feature should be disabled in countries where the telephone keypads do not map to an alphabetical sequence recognizable to Meridian Mail.

The Voice Messaging Options screen

These are the fields you use to enable/disable timed delivery and name dialing/name addressing.

```
                    Voice Administration                    MORE ABOVE
Voice Messaging Options

Maximum Delay for Timed Delivery (days):          31
Name Dialing and Name Addressing:                 Disabled Enabled
Prefix for Name Dialing and Name Addressing:      11
Broadcast Mailbox Number:                         5555
Broadcast Mailbox Personal Verification (Voice): No
Billing DN:
Local Addressing Lengths:                         0  0
Default Message Delivery Priority:                Standard Economy
                                                                MORE BELOW

Save      Cancel                                  Voice
```

Field descriptions

This table describes the fields that are used to enable/disable timed delivery and name dialing/name addressing.

Maximum Delay for Timed Delivery (days)	
Description	The maximum number of days that a message can be delayed before being delivered.
Default	31
Valid range	0 to 365 A setting of 0 disables the Timed Delivery feature.

Name Dialing and Name Addressing	
Description	Enables/disables the name dialing and name addressing feature.
Default	Enabled
Valid options	Enabled, Disabled
Attention	If you disable this feature and then reenable it, the prefix is reset to null and must be redefined.

Prefix for Name Dialing and Name Addressing	
Description	Users must dial this prefix in order to name dial (using thru-dial) or name address (during message or personal distribution list composition, or express messaging).
Default	11
Valid range	1 to 99
Potential conflicts	Make sure this prefix does not conflict with (duplicate) or underlap (begin with the same digits) any of the following: • mailbox numbers • telephone extensions • distribution list numbers • the DNU prefix • network prefixes • the AMIS compose prefix

Procedure

To enable/disable timed delivery or name dialing/name addressing, or both, follow these steps.

Starting Point: The Voice Messaging Options screen

Step	Action
1	Do you want to disable timed delivery? • If yes, enter 0 in the Maximum Delay for Timed Delivery field. • If no, enter the maximum number of days you want users to be able to delay delivery of voice messages.
2	Do you want to disable name dialing and name addressing? • If yes, select Disabled in the Name Dialing and Name Addressing field. • If no, select Enabled.
3	Are name dialing and name addressing enabled? • If yes, change the prefix if necessary. • If no, go to step 4.
4	Do you want to continue defining voice messaging options?

IF you want to	THEN
continue	see page 20-47.
save your changes and quit	press [Save].
quit without saving your changes	press [Cancel].

Defining the lockout revert DN and personal distribution list prefix

Introduction

The lockout revert DN and personal distribution list prefix are applicable to the VMUIF interface only.

The Voice Messaging Options screen

These are the relevant fields in the Voice Messaging Options screen.

```
                    Voice Administration                    MORE ABOVE
Voice Messaging Options

Lockout Revert DN:                          _
(Blank implies no revert)

Personal Distribution List Prefix:          __

Broadcast Mailbox Number:                   5555

Broadcast Mailbox Personal Verification (Voice): No

Billing DN:

Local Addressing Lengths:                   0  0

Maximum Read Message Retention (days):      7
("0" implies that there is no organization
 maximum limit. Read Message Retention will
                                                            MORE BELOW

 Save      Cancel                                   Voice
```

Field descriptions

This table describes the fields in which you define the lockout revert DN and personal distribution list prefix.

Lockout Revert DN	
Description	This is the DN to which users are transferred if the mailbox that they are trying to log in to is disabled.
Default	Blank (no DN) If this field is left blank, a prompt is played to callers asking them to try again at a later time.

Personal Distribution List Prefix	
Description	Users must enter this prefix when composing a message to a distribution list. This prefix informs Meridian Mail that the number about to be entered is a distribution list rather than a mailbox.
Default	Blank If left blank, users cannot create personal distribution lists.
Valid range	1 to 99

Procedure

To define the lockout revert DN and personal distribution list prefix, follow these steps.

Starting Point: The Voice Messaging Options screen

Step	Action
1	Do you want users to be reverted to a particular DN if their mailbox is disabled when they try to log in? • If yes, enter this number in the Lockout Revert DN field. • If no, leave this field blank.
2	Do you want users to be able to create personal distribution lists? • If yes, enter a prefix in the Personal Distribution Prefix field (or use the default prefix). • If no, make this field blank.
3	Do you want to continue defining voice messaging options?

IF you want to	THEN
continue	see page 20-47.
save your changes and quit	press [Save].
quit without saving your changes	press [Cancel].

Setting up the broadcast mailbox

Introduction

Broadcast mailboxes can be set up for both the MMUI and VMUIF interface.

Description

When you compose a message to the broadcast mailbox, the message is sent to all of the users on the system.

To set up a broadcast mailbox, all you have to do is assign a mailbox number to the broadcast mailbox in the Voice Messaging Options screen. You do not need to set up an actual mailbox through User Administration.

The Network Broadcast option

If Meridian Networking has been installed on your system, broadcast messages can also be sent to all users at a particular remote site, to all users at each of a group of remote sites, or to all users at all remote sites.

To enable network broadcast messaging, you must do the following:

- Fill in the required Network Broadcast Administration fields in the Network Configuration screen. See your Network Administration book for details.
- Record a personal verification for the broadcast mailbox.

For details on Network broadcast messages, see “Recording and sending broadcast messages” on page 5-39.

The NMS broadcast message option

If NMS is installed on your system, broadcast messages can also be sent to all users at a particular remote NMS location, to all users at each of a group of locations, or to all users at all remote locations.

If your system also includes Meridian Mail Networking, this can include locations connected to remote sites.

For details, see “Recording and sending broadcast messages” on page 5-39.

The broadcast mailbox personal verification

You can record a personal verification for the broadcast mailbox so that when you enter the mailbox number during message composition, you get a verification that you have entered the correct number.

The personal verification for a broadcast mailbox can say something like this:

"Broadcast mailbox 5555."

The Voice Messaging Options screen

These are the fields in the Voice Messaging Options screen in which you set up the broadcast mailbox.

```
                    Voice Administration                    MORE ABOVE
Voice Messaging Options

Maximum Delay for Timed Delivery (days):          31
Name Dialing and Name Addressing:                 Disabled Enabled
Prefix for Name Dialing and Name Addressing:      11
Broadcast Mailbox Number:                         5555
Broadcast Mailbox Personal Verification (Voice): No
Billing DN:
Local Addressing Lengths:                         0  0
Default Message Delivery Priority:                Standard Economy
                                                                MORE BELOW

 Save      Cancel                                        Voice
```

Field descriptions

This table describes the fields that you use to set up the broadcast mailbox.

Broadcast Mailbox Number	
Description	This is the number of the mailbox that is used to send broadcast messages. This number is specified when you are prompted for a mailbox number while composing the message.
Default	5555
Potential Conflicts	Make sure this number does not conflict with any other numbers in Meridian Mail. If you have network broadcast messaging enabled for your system, this number also must not conflict with any mailboxes at any remote sites. One easy way to avoid conflict is to make the broadcast mailbox number longer than any user mailbox numbers on your network.

Broadcast Mailbox Personal Verification (Voice)	
Description	This is a read-only field that indicates whether a personal verification has been recorded for the broadcast mailbox. The broadcast mailbox personal verification must be recorded for the network broadcast option to work.

Procedure

To set up a broadcast mailbox, follow these steps.

Starting Point: The Voice Messaging Options screen

Step	Action
1	Change the broadcast mailbox number if necessary.
2	Do you want to record a personal verification for the broadcast mailbox? • If yes, go to step 3. • If no, go to step 12.
3	Put the cursor on the Broadcast Mailbox Personal Verification (Voice) field.

Step	Action
4	Press the [Voice] softkey.
5	Enter the extension of the phone you will use to record the verification, and press <Return>. **Result:** The phone rings.
6	Pick up the receiver. **Result:** The recording softkeys are displayed.
7	Press the [Record] softkey.
8	At the sound of the beep, speak the verification. **Example:** *"Broadcast mailbox 5555."*
9	Press the [Stop] softkey to stop recording.
10	Do you want to verify the recording? • If yes, press the [Play] softkey, listen to the recording, and go to step 11. • If no, press [Disconnect] and hang up the phone. Go to step 12.
11	Do you want to rerecord the verification? • If yes, repeat steps 7 to 10. • If no, press [Disconnect] and hang up the phone. Go to step 12.
12	Do you want to continue defining voice messaging options?

IF you want to	THEN
continue	see page 20-51.
save your changes and quit	press [Save].
quit without saving your changes	press [Cancel].

Defining the billing DN

Introduction

A billing DN can be defined for both the MMUI and VMUIF interface.

How the billing DN is used

This DN may be used for billing purposes when an outbound call is made. There are other numbers that are also used for billing.

This table shows which numbers Meridian Mail will try to use for a particular outbound service.

Service	A Used if defined	B Used if A not defined	C Used if A and B not defined
Remote Notification and Delivery to Non-User	Billing DN in Voice Messaging Options	Mailbox Number	Nil. Call is still made.
Thru-Dial service	Billing DN in Voice Messaging Options	VSDN of dialed service	Nil. Call is still made.
Extension dialing (mailbox thru-dial)	Billing DN in Voice Messaging Options	Mailbox Number	Nil. Call is still made.
Fax Item and Fax Item Maintenance (callback delivery)	Billing DN in Session Profile	Billing DN in Voice Messaging Options	VSDN of dialed service
AMIS Networking	Billing DN in Voice Messaging Options	Sender's DN	Nil. Call is still made.

Procedure

To define the billing DN, follow these steps.

Starting Point: The Voice Messaging Options screen

Step	Action
1	Go to the Billing DN field.

```
                    Voice Administration                    MORE ABOVE
Voice Messaging Options

Maximum Delay for Timed Delivery (days):          31
Name Dialing and Name Addressing:                 Disabled Enabled
Prefix for Name Dialing and Name Addressing:      11
Broadcast Mailbox Number:                         5555
Broadcast Mailbox Personal Verification (Voice):  No
Billing DN:
Local Addressing Lengths:                         0  0
Default Message Delivery Priority:                Standard Economy
                                                                MORE BELOW

Save      Cancel                                  Voice
```

2 Enter a DN that is up to 30 digits long.

3 Do you want to continue defining voice messaging options?

IF you want to	THEN
continue	see page 20-53.
save your changes and quit	press [Save].
quit without saving your changes	press [Cancel].

Specifying the message delivery priority for networked systems

When to use

This procedure applies only to systems on which Meridian Networking is installed. Meridian Networking can be installed only if the interface is MMUI.

Message delivery priority

The Default Message Delivery Priority field determines when network messages are delivered. You can choose between Standard and Economy delivery. The default is Standard.

Standard delivery

Messages are retained for a certain period of time before they are sent to remote sites.

This time period is defined in the Standard Holding Time field in the Network Scheduling Parameters screen.

Economy delivery

Messages are sent at a specific time each day, usually during off-hours, when rates are cheaper.

This delivery time is defined in the Economy Initiation Time field in the Network Scheduling Parameters screen.

Procedure

To set the message delivery priority, follow these steps.

Starting Point: The Voice Messaging Options screen

Step	Action
1	Go to the Default Message Delivery Priority field.

```
Voice Administration                                   MORE ABOVE
Voice Messaging Options

Maximum Delay for Timed Delivery (days):          31
Name Dialing and Name Addressing:                 Disabled Enabled
Prefix for Name Dialing and Name Addressing:      11
Broadcast Mailbox Number:                         5555
Broadcast Mailbox Personal Verification (Voice): No
Billing DN:
Local Addressing Lengths:                         0  0
Default Message Delivery Priority:                Standard Economy
                                                                MORE BELOW

Save        Cancel                                        Voice
```

2 Choose when you want network messages to be delivered.

IF you want messages	THEN
to be delivered after a specified holding time	select Standard.
to be delivered at the same time each day (during off-hours)	select Economy.

3 Do you want to continue defining voice message options?

IF you want to	THEN
continue (if the interface is MMUI)	see page 20-55.
continue (if the interface is VMUIF)	see page 20-57.
save your changes and quit	press [Save].
quit without saving your changes	press [Cancel].

Specifying the mailbox full warning threshold

Introduction

This warning threshold is applicable to the MMUI interface only.

Description

When an MMUI user's mailbox starts to get full, a warning message can be played to remind the user that his or her mailbox is almost full and to start deleting messages. This message can be disabled.

The warning threshold

This threshold determines when this message is played. The threshold is based on how full the user's mailbox is.

Default
The default setting is 85%.

Valid range
You can enter a value between 0 and 100%.

Example

The warning threshold is set to 85%. The user's voice storage limit (as defined in the user's class of service) is five minutes.

A caller leaves a message that increases the user's voice storage to 4 minutes 30 seconds. Since this is slightly more than 85% of the total voice storage for the user, the next time the user logs on, the mailbox full warning threshold message is played.

Procedure

To set the mailbox full warning threshold, follow these steps.

Starting Point: The Voice Messaging Options screen

Step	Action
1	Go to the Mailbox Full Warning Threshold field.

```
                          Voice Administration                    MORE ABOVE
Voice Messaging Options

Broadcast Mailbox Personal Verification (Voice): No

Billing DN:                                      ____________________________

Local Addressing Lengths:                        0  0

Default Message Delivery Priority:               Standard Economy

Mailbox Full Warning Threshold (percentage):     85

Maximum Read Message Retention (days):           7
("0" implies that there is no organization
 maximum limit. Read Message Retention will
 be determined from each user's profile.)

External Call-Sender Allowed:                    No Yes

   Save      Cancel                                          Voice
```

2 Do you want to disable the warning threshold message?

- If yes, set the field to 0.
- If no, set the field to a non-zero value that represents how full the mailbox must be before the warning message is played.

3 Do you want to continue defining voice message options?

IF you want to	THEN
continue	see page 20-57.
save your changes and quit	press [Save].
quit without saving your changes	press [Cancel].

Specifying the maximum read message retention

Introduction

The maximum read message retention applies to both the MMUI and VMUIF interfaces.

Description

Once a user listens to a message, that message is still stored on the system. A message that has been listened to is known as a read message.

The system will begin to fill up with read messages over time. You can either have Meridian Mail delete any read messages every certain number of days, or you can leave it up to users to delete read messages on their own.

Maximum read message retention

The Maximum Read Message Retention (days) field determines how long read messages are stored before being deleted.

WHEN this field	THEN read messages are
is set to 0	not automatically deleted. They are retained until deleted by the user.
is set to 1 or more	deleted every X days as specified in this field.

Default

The default maximum read message retention is seven days.

Valid range

You can enter a value between 0 and 31 (days).

ATTENTION

It is recommended that you set the read message retention to a non-zero value to avoid filling up the disk with read messages.

Class of service setting

This field also exists in the Add and View/Modify Class of Service screens. This table describes which setting is used under different conditions.

WHEN the Voice Messaging Options setting is	AND the Class of Service setting is	THEN read messages are kept
0 (zero)	0 (zero)	until the user deletes them.
0 (zero)	1 or more	for the time specified in the Class of Service screen.
1 or more	0 (zero)	for the time specified in the Voice Messaging Options screen.
1 or more	1 or more	for the lesser of the two values.

Procedure

To define the maximum read message retention, follow these steps.

Starting Point: The Voice Messaging Options screen

Step	Action
1	Go to the Maximum Read Message Retention field.

```
                          Voice Administration                    MORE ABOVE
Voice Messaging Options

Broadcast Mailbox Personal Verification (Voice): No

Billing DN:                                      ____________________________

Local Addressing Lengths:                        0  0

Default Message Delivery Priority:               Standard Economy

Mailbox Full Warning Threshold (percentage):     85

Maximum Read Message Retention (days):           7
("0" implies that there is no organization
 maximum limit. Read Message Retention will
 be determined from each user's profile.)

External Call-Sender Allowed:                    No Yes

 Save      Cancel                                          Voice
```

Step	Action
2	Do you want read messages to be stored until deleted by users? • If yes, set the field to 0. • If no, set the field to a non-zero value that represents how often you want read messages to be automatically deleted.
3	Do you want to continue defining voice message options?

IF you want to	THEN
continue	see page 20-60.
save your changes and quit	press [Save].
quit without saving your changes	press [Cancel].

Enabling/disabling external call sender

Introduction

External Call Sender is available in both the MMUI and VMUIF interfaces.

Description

When a user is listening to a voice message left by another Meridian Mail user, the user can press 9 on the keypad to immediately call back the originator of the message. This is the call sender feature.

The External Call Sender feature allows users to press 9 to call back external callers who leave voice messages.

Default

This feature is enabled by default.

VMUIF interface

For the VMUIF interface, this field interacts with the Call Sender field in the user's class of service. Both fields must be set to Yes for External Call Sender to work.

Restricting External Call Sender

If you enable External Call Sender, apply the appropriate restrictions to the numbers that users are allowed to call back.

Restrictions are applied to external call sender in classes of service. See "The Add Class of Service screen (MMUI)" on page 26-13.

Procedure

To enable or disable external call sender, follow these steps.

Starting Point: The Voice Messaging Options screen

Step	Action
1	Go to the External Call-Sender Allowed field.

```
                          Voice Administration                    MORE ABOVE
Voice Messaging Options

Broadcast Mailbox Personal Verification (Voice): No

Billing DN:                                      ____________________________

Local Addressing Lengths:                        0  0

Default Message Delivery Priority:               Standard Economy

Mailbox Full Warning Threshold (percentage):     85

Maximum Read Message Retention (days):           7
("0" implies that there is no organization
 maximum limit. Read Message Retention will
 be determined from each user's profile.)

External Call-Sender Allowed:                    No Yes

 Save      Cancel                                          Voice
```

2 Do you want to allow users to use the call sender feature to call back external callers?
- If yes, set the field to Yes.
- If no, set the field to No.

3 Do you want to save the Voice Messaging Options screen with the current information?
- If yes, press [Save].
- If no, press [Cancel], or make any necessary changes and then press [Save].

Enabling and configuring speed control

Introduction

This feature is available to MMUI users only.

Description

The speed control feature lets mailbox users control the playback speed of a voice mail message. As Administrator, you can specify up to three speed increases for a user to apply during message playback (for example, 25% faster than normal, 50% faster, and 100% faster.)

User perspective

During message playback, the user can press 2-3 to increase the playback speed by one level, and 2-1 to decrease it by one level.

A 1.5-second time-out applies; the user must press 2, then either 1 or 3 immediately afterwards to use this feature. After 1.5 seconds, the 1 and 3 keys resume their usual message playback roles (skipping the message back/forwards by 5 seconds.)

When a user reaches the highest speed level, the system ignores any further speed increase commands.

This feature can be applied to the following:

- new messages
- previously read messages
- composed messages
- sent messages
- unsent messages
- deleted messages

Meridian Mail prompts, system-generated messages, and personal greetings and personal verifications will not be affected by this feature.

Procedure

To enable/configure the speed control feature, follow these steps.

Starting Point: The Voice Messaging Options screen

Step	Action
1	Go to the Voice Message Playback Speed fields in the Voice Messaging Options screen.

```
VMUI VM                    Voice Administration                    MORE ABOVE
Voice Messaging Options

Local Addressing Lengths:                          0  0

Mailbox Full Warning Threshold (percentage):       85

Maximum Read Message Retention (days):             7
("0" implies that there is no organization
 maximum limit. Read Message Retention will
 be determined from each user's profile.)

External Call-Sender Allowed:                      No Yes

Voice Message Playback Speed                       Percentage Increase
       Normal     :                                None
       Increment 1:                                None 25 33 50 67 75 100
       Increment 2:                                None 25 33 50 67 75 100
       Increment 3:                                None 25 33 50 67 75 100

   Save        Cancel                                          Voice
```

Step	Action
2	For each of the three increments, select the desired speed increase for that level (for example, Increment 1 at 50%, Increment 2 at 75%, and Increment 3 at 100%).

IF you want	THEN set
three levels of increased speed	each increment to a higher number than the one before it.
two levels of increased speed	Increment 3 at the same number as Increment 2.
one level of increased speed	Increments 2 and 3 at the same level as Increment 1.

Note: If two Increments are set to the same speed, there will be no speed change when the user moves up or down from one to the other.

3 Do you want to save the Voice Messaging Options screen with the current information?

- If yes, press [Save].
- If no, press [Cancel], or make any necessary changes and then press [Save].

Chapter 21

Display options

In this chapter

Overview	21-2
Different ways of sorting the VSDN table	21-3
Different ways of sorting the service definitions tables	21-5
Different ways of sorting the Choice of Services and Menu Actions list	21-7
Changing the display options	21-9

Overview

Introduction

This chapter describes the different ways information can be displayed on the Voice Services Administration screens. You can control two basic options:

- how information is sorted (for example, sort VSDN table by DN or by Comment)
- whether or not the Choice of Services and Menu Actions lists are displayed

This chapter presents screen examples that show the different ways the Voice Services Administration screens appear according to the options you select. The section “Changing the display options” on page 21-9 explains how to change the display options.

Different ways of sorting the VSDN table

Introduction

This section provides screen examples that show how the VSDN table looks when it is

- sorted by DN (see “Example 1”)
- sorted by Comment (see “Example 2”)

Example 1

The following example shows how the VSDN table looks when you choose to have the information sorted by the DNs.

```
                    Voice Services Administration
Voice Services-DN Table

            DN                              Service        Comment
            7000                            VM             Voice Messaging
            7001                            MS  100        Services menu
            7002                            EM             Express Messaging
            7003                            PM             Prompt Maintenance
            7004                            MS  105        Off hours menu
            7005                            MS  110        Sales menu

Move the cursor to the item and press the space bar to select.

   Exit        Add        View/Modify        Delete        Find
```

Example 2

The following example shows how the VSDN table looks when you choose to have the information sorted by the Comment.

```
                    Voice Services Administration
Voice Services-DN Table

            DN                          Service        Comment
            7002                        EM             Express Messaging
            7004                        MS  105        Off hours menu
            7003                        PM             Prompt Maintenance
            7005                        MS  110        Sales menu
            7001                        MS  100        Services menu
            7000                        VM             Voice Messaging

Move the cursor to the item and press the space bar to select.

   Exit        Add        View/Modify      Delete        Find
```

Different ways of sorting the service definitions tables

Introduction

This section provides screen examples that show how the service definition tables (for example, the Voice Menu Definitions table) look when they are

- sorted by ID (see “Example 1”)
- sorted by Title (see “Example 2”)

Example 1

The following example shows how the Voice Menu Definitions table looks when you choose to have the information sorted by ID.

```
                    Voice Services Administration
Voice Menu Definitions

            ID          Title
            100         Services menu
            105         Off hours menu
            110         Sales menu

Move the cursor to the item and press the space bar to select.

 Exit      Add      View/Modify      Delete      Find
```

Example 2

The following example shows how the Voice Menu Definitions table looks when you choose to have the information sorted by Title.

```
                    Voice Services Administration
Voice Menu Definitions

            ID          Title
            105         Off hours menu
            110         Sales menu
            100         Services menu

Move the cursor to the item and press the space bar to select.

   Exit      Add      View/Modify      Delete      Find
```

Different ways of sorting the Choice of Services and Menu Actions list

Introduction

This section provides screen examples that show how the Choice of Services list looks when it is

- sorted by acronym (see “Example 1”)
- sorted by description (see “Example 2”)

The effect on how the Menu Actions list appears would be the same.

Definition: Menu Actions

“Menu Actions” refers to the default menu actions that you can choose from when you define a voice menu. Refer to the *Voice Services Application Guide* for more details.

Example 1

The following example shows how the choice of services are listed in the Find Subset of VSDNs/Services screen when you choose to have the choice of services sorted by the acronym.

```
                    Voice Services Administration
Find Subset of VSDNs/Services

Choice of Services:
AS  Announcement Service  CA  Call Answering        EM  Express Messaging
FI  Fax Info Service      FIM Fax Item Maintenance  MS  Voice Menu Service
PM  Prompt Maintenance    RA  Remote Activation     TD  Time-of-Day Control
TR  Transcription Service TS  Thru-Dial Service     VF  Voice Forms Service
VM  Voice Messaging

Type:    VSDN_Entry Announcement Thru_Dial TOD_Control Voice_Menu Fax_Item

DN:      ______________________________

Service: ___

Comment: ___________________

Select a softkey >

[          ] [ Cancel ] [ Find Selection ] [ Print Selection ] [          ]
```

Example 2

The following example shows how the choice of services are listed in the Find Subset of VSDNs/Services screen when you choose to have the choice of services sorted by the description.

```
                    Voice Services Administration
Find Subset of VSDNs/Services

Choice of Services:
AS  Announcement Service  CA  Call Answering        EM  Express Messaging
FI  Fax Info Service      FIM Fax Item Maintenance  PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Type:    VSDN_Entry Announcement Thru_Dial TOD_Control Voice_Menu Fax_Item

DN:      ____________________________

Service: ___

Comment: _________________

Select a softkey >

[          ] [ Cancel ] [ Find Selection ] [ Print Selection ] [          ]
```

Changing the display options

Introduction

The display options are controlled by the Set Display Options screen.

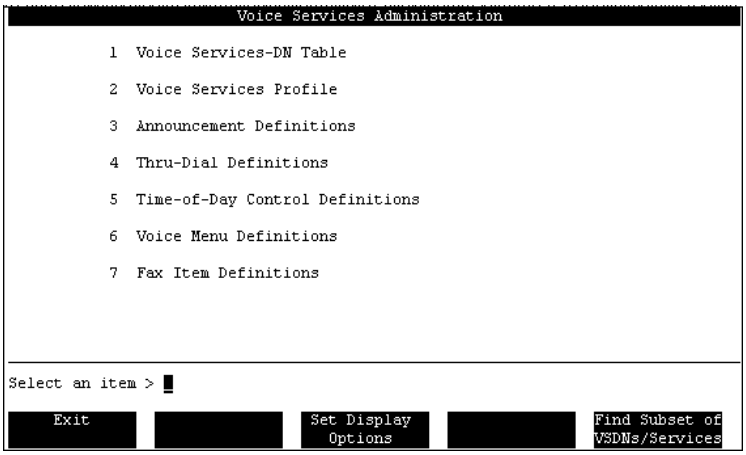
The Set Display Options screen allows you to specify how information is sorted on the Voice Services Administration screens. For example, you can decide if the Choice of Services list is sorted in alphabetical order according to service acronym (“ms,” for example) or service description (“voice menu service,” for example), or whether the Choice of Services list is displayed at all.

Procedure

To change the display options, follow these steps.

Starting Point: Main Menu

Step	Action
1	Select Voice Administration. **Result:** The Voice Administration menu is displayed.
2	Select Voice Services Administration. **Result:** The Voice Services Administration menu is displayed and the [Set Display Options] softkey also appears.



Step	Action
3	Press the [Set Display Options] softkey. **Result:** The Set Display Options screen appears.

```
                    Voice Services Administration
Set Display Options

Default sort order for:                    by:
        VSDN Table data menu:              DN Comment
        Service Definitions data menu:     ID Title

Sort Choice of Services/Menu Actions by:   Acronym Description

Display Choice of Services/Menu Actions in:
        VSDN Table DN Information form:    No Yes
        Voice Menu Definition form:        No Yes
        Find form:                         No Yes

Select a softkey >

   Save        Cancel
```

4	Make your selections according to how you want information to be sorted or displayed in the Voice Services Administration screens.
5	If you are satisfied with the changes, press [Save]. Otherwise, press [Cancel] to discard the changes. **Result:** Whether you save or cancel, you are returned to the Voice Services Administration menu.

Field descriptions

The following fields and options appear on the Set Display Options screen.

Default sort order for VSDN Table data menus	
Description	The selection you make affects how information is sorted in the VSDN table.
Default	DN
Valid options	DN, Comment • ***DN*** sorts entries numerically by DN. • ***Comment*** sorts entries alphabetically by comment.

Default sort order for Service Definition data menus	
Description	The selection you make affects how information is sorted in the service definitions tables (for example, in the Voice Menu Definitions screen).
Default	ID
Valid options	ID, Title • ***ID*** sorts entries numerically by service IDs. • ***Title*** sorts entries alphabetically by title.

Sort Choice of Services/Menu Actions by	
Description	The selection you make affects how the Choice of Services list and the Menu Actions list are sorted. The Choice of Services list appears on many screens including the Find subset of VSDNs/ Services screen. The Menu Actions list is displayed in the Add, View/Modify, and Delete a Voice Menu Definition screens.
Default	Description
Valid options	Description, Acronym • ***Description*** sorts entries alphabetically by description. • ***Title*** sorts entries alphabetically by title.

Display Choice of Services/Menu Actions in	
Description	You can turn the display of the Choice of Services or Menu Actions list on or off for the following: • VSDN Table DN Information screens (Add, View/Modify, Delete DN Information) • Voice Menu Definition screens (Add, View/ Modify, Delete a Voice Menu Definition) • Find Subset of VSDNs/Services screen
Default	Yes
Valid options	Yes, No • ***Yes*** shows the choice of services/menu actions. • ***No*** hides the choice of services/menu actions.

Chapter 22

Finding and printing VSDNs and service definitions

In this chapter

Overview	22-2
Wildcards	22-5
The Find Subset of VSDNs/Services screen	22-7
Finding and printing VSDNs	22-9
Finding and printing service definitions	22-11

Overview

Introduction

Use the find feature if you want to modify, delete, print, or simply view any of the following:

- a specific VSDN
- a range of VSDNs
- all VSDNs for a certain kind of service (such as announcements, voice menus, or fax items)
- a specific service definition
- a range of service definitions that have similar titles

Location of Find softkeys

Find softkeys are located on the following screens.

- the VSDN table
- service definition selection menus (such as the Announcement Definitions screen)
- the Voice Services Administration menu

Using Find as a shortcut

When you are adding a voice or fax service to Meridian Mail, you must go back and forth between the VSDN table and the Add a service definition screen (to add a VSDN for the service and to create a definition for the service). You can use the Find softkey to quickly move back and forth between the VSDN table screen and the service definition screen, as follows.

Starting Point: Any voice services administration screen that has a [Find] or [Find Subset of VSDNs/Services] softkey

Step	Action
1	Press the [Find] softkey.
2	Select the service type that you want to add in the “Type” field and press <Tab>.
3	Press the [Find Selection] softkey. **Result:** The service definition screen is displayed.
4	To return to the VSDN table, press the [Find] softkey, select VSDN_Entry in the Type field and press <Tab>. Then press the [Find Selection] softkey.

Service definitions

Service definitions exist for announcements, thru-dial services, time-of-day controllers, and voice menus, and fax items (if Fax on Demand is installed on your system).

Example: service definition

Here is an example of a voice menu definition.

```
                    Voice Services Administration
View/Modify a Voice Menu Definition

Choice of Menu Actions:
AS  Announcement Service  CL  Call                  CA  Call Answering
RV  Call Revert DN        DS  Disconnect            EM  Express Messaging
PP  Play Prompt           PM  Prompt Maintenance    RP  Repeat Menu Choices
MM  Return to Main Menu   TS  Thru-Dial Service     TD  Time-of-Day Control
MS  Voice Menu Service    VM  Voice Messaging

Voice Menu ID:    105____          Title:  Off hours menu_______________

Revert DN:        7550_____________________________

Access Password:  _______________   Update Password:  _______________

Greeting Recorded (Voice):   No     Menu Choices Recorded (Voice):  No

_____________________________________________________________________MORE BELOW
Select a softkey >

   Save        Cancel                     Voice
```

Wildcards

You do not have to remember exact DNs or service titles. You can use wildcards to fill in the parts you cannot remember.

Wildcards

Definition: wildcard

A wildcard is a character that is used in a search string to represent an unknown or variable character or string of characters.

Purpose

Wildcards have two main purposes. They allow you to find

- a particular VSDN or service definition without having to remember and enter the exact voice service DN or Comment, or service definition ID or title
- a range of VSDNs or service definitions

Types of wildcards

There are three wildcards that you can use.

Wildcard	Description
_	The underscore (_) replaces a single character.
+	The plus sign (+) replaces a string of characters.
?	The question mark (?) means “sounds like.” Meridian Mail will find words that are spelled differently but sound like the word that is entered.

Where wildcards are used

You can enter wildcards in the DN, Comment, and Title fields in the Find Subset of VSDNs/Services screen.

Examples

The following examples show how wildcards can be used when searching for a particular VSDN or service definition, or a range of VSDNs or service definitions.

You enter	Result
“210_” in the DN field	All VSDNs in the range 2100 to 2109 are retrieved.
“7_99” in the DN field	The following VSDNs are retrieved: 7099, 7199, 7299, 7399, 7499, 7599, 7699, 7799, 7899, and 7999.
“3+” in the DN field	All DNs beginning with 3 are retrieved.
“+ holiday” in the Title field (Type is Announcement)	All of the announcements whose titles end with the word “holiday” are retrieved.
“Braymore?” in the Comment field	Meridian Mail retrieves service definitions with Braymore, Braemer, and Breymore in the Comment field.

The Find Subset of VSDNs/Services screen

Accessing the screen

This screen can be accessed from

- the Voice Services Administration menu using the [Find Subset of VSDNs/Services] softkey
- the VSDN table using the [Find] softkey
- any service definition (such as an announcement, thru-dial, time-of-day control, voice menu, or fax item definition) using the [Find] softkey

The screen: Type is VSDN

This is the Find Subset of VSDNs/Services screen when the selected Type is VSDN_Entry.

```
                         Voice Services Administration
Find Subset of VSDNs/Services

Choice of Services:
AN  AMIS Networking       AS  Announcement Service  EN  Enterprise Networking
EM  Express Messaging     FI  Fax Info Service      FIM Fax Item Maintenance
ACC Meridian ACCESS       NW  Meridian Networking   PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Type:    VSDN_Entry Announcement Thru_Dial TOD_Control Voice_Menu Fax_Item

DN:      ______________________________

Service: ___

Comment: ________________

Select a softkey >

[          ] [ Cancel ] [ Find Selection ] [ Print Selection ] [          ]
```

The screen: Type is service

This is the Find Subset of VSDNs/Services screen when the selected Type is a service definition (Announcement, Thru-Dial, TOD Control, Voice Menu, or Fax Item).

```
                    Voice Services Administration
Find Subset of VSDNs/Services

Choice of Services:
AN  AMIS Networking       AS  Announcement Service  EN  Enterprise Networking
EM  Express Messaging     FI  Fax Info Service      FIM Fax Item Maintenance
ACC Meridian ACCESS       NW  Meridian Networking   PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Type:    VSDN_Entry Announcement Thru_Dial TOD_Control Voice_Menu Fax_Item

ID:      _______

Title:   ___________________________


Select a softkey >

          Cancel    Find Selection    Print Selection
```

Note: If you select TOD Control, the Title field will not be displayed in the Find Subset of VSDNs/Services screen.

Finding and printing VSDNs

Procedure

Follow these steps to find or print a particular VSDN or a subset of VSDNs.

Starting Point: The Main Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Services Administration.
3	Press the [Find Subset of VSDNs/Services] softkey. **Result:** The Find Subset of VSDNs/Services screen is displayed.

```
                    Voice Services Administration
Find Subset of VSDNs/Services

Choice of Services:
AN  AMIS Networking       AS  Announcement Service  EN  Enterprise Networking
EM  Express Messaging     FI  Fax Info Service      FIM Fax Item Maintenance
ACC Meridian ACCESS       NW  Meridian Networking   PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Type:    VSDN_Entry Announcement Thru_Dial TOD_Control Voice_Menu Fax_Item

DN:      ____________________________

Service: ___

Comment: _________________

Select a softkey >

[          ] [ Cancel ] [ Find Selection ] [ Print Selection ] [          ]
```

Step	Action
4	Select “VSDN_Entry” in the Type field (this is the default).
5	Specify the DN or range of DNs you want to find in the DN field.

IF you want to find	THEN
a particular VSDN and you know the exact DN	enter the exact DN and go to step 8.
a range of VSDNs	use wildcards to specify a search pattern.
all VSDNs for a particular service type (such as voice menus)	leave the DN field blank and specify the type in the Service field.

Step	Action
6	If you want to retrieve VSDNs of a certain service type only, specify one of the following types.

IF you want to find	THEN enter
announcements only	AS
thru-dial services only	TS
time-of-day controllers only	TD
voice menus only	MS
fax items only	FI

7 Enter a comment if this will help narrow the search.

Note 1: The comment must be exactly as entered in the service definition. If you do not know the exact comment, enter as much as you can and use wildcards for the rest.

Note 2: If the service is TD Time-of-Day Controller, then go to step 8.

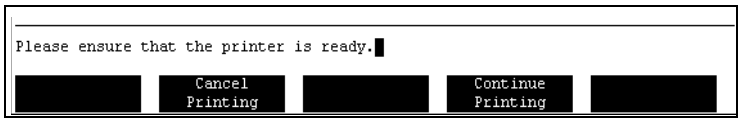
8 Do you want to print the results of the search?

If yes, go to step 9.

If no, go to step 11

9 Press the [Print Selection] softkey.

Result: The following softkeys are displayed.



10 Do you want to go ahead with printing?

If yes, press the [Continue Printing] softkey.

If no, press the [Cancel Printing] softkey and go to step 11.

11 Press the [Find Selection] softkey to view the found VSDNs, or press [Cancel] to cancel the search and exit the screen.

Result: If you pressed the [Find Selection] softkey, the VSDN table is displayed, listing only those VSDNs that met your search criteria. You can use any of the softkeys the same as if you accessed the VSDN table directly from the Voice Services Administration menu.

Finding and printing service definitions

Procedure

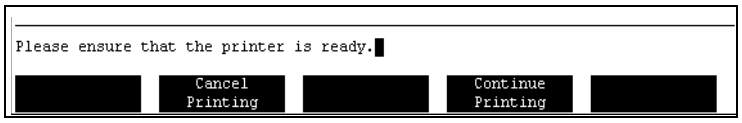
To find or print a particular service definition or a subset of service definitions, follow these steps.

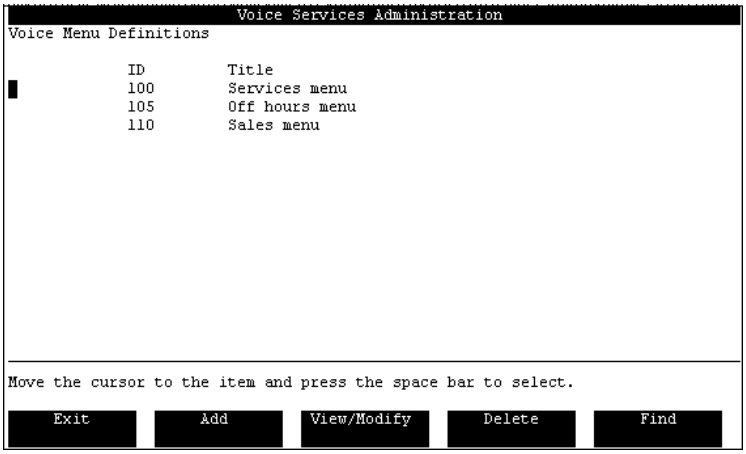
Starting Point: The Main Menu

Step	Action
1	Select Voice Administration.
2	Select Voice Services Administration.
3	Press the [Find Subset of VSDNs/Services] softkey. **Result:** The Find Subset of VSDNs/Services screen is displayed.
4	Select a service type in the Type field.
5	Specify the ID of the service definition you want to find.

IF you want to	THEN
find a service and you know the exact ID	enter the exact ID and go to step 7.
find a service but you do not know the ID	leave the ID field blank and go to step 6 to fill in the Title field.
retrieve all service definitions of the specified type	leave the ID field and the Title field blank, and go to step 7.

Step	Action
6	Enter the exact service title, or part of the title and use wildcards for the rest.
7	Do you want to print the results of the search? If yes, go to step 8. If no, go to step 10.
8	Press the [Print Selection] softkey. **Result:** The following softkeys are displayed.



Step	Action
9	Do you want to go ahead with printing? If yes, press the [Continue Printing] softkey. If no, press the [Cancel Printing] softkey and go to step 10.
10	Press the [Find Selection] softkey to view the list of found service definitions, or press [Cancel] to cancel the search and exit the screen. **Result:** If you pressed the [Find Selection] softkey, the list of service definitions that match your selection criteria is displayed. **Example:** If you selected “Voice_Menu” in the Type field, the Voice Menu Definitions screen is displayed with only the voice menu definitions that match your selection criteria listed. The screen would appear similar to the following example.  **Note:** You can use any of the softkeys the same as if you accessed this screen directly from the Voice Services Administration menu.

Chapter 23

Configuring Meridian Mail services

In this chapter

Overview	23-2
Section A: Introduction	23-3
Section B: Planning your configuration	23-13
Section C: Configuring the Meridian 1 for Meridian Mail services	23-31

Overview

Configuring Meridian Mail services

Each dialable Meridian Mail service needs an ACD queue and a VSDN.

Setting up a Meridian Mail service, therefore, requires configuration on the Meridian 1 and in Meridian Mail.

Meridian 1 setup

Configuration of Meridian Mail services begins on the Meridian 1 where you must

- Set up one or more ACD queues for call handling.
- Set up a dummy queue for each Meridian Mail service that requires an access number.

Meridian Mail setup

In Meridian Mail, you must add the ACD queue DNs of the queues you created on the Meridian 1 to the VSDN Table. This is where you indicate which service a particular DN should start up.

Meridian 1 setup

This chapter describes how to set up the Meridian 1 to support Meridian Mail services.

Section	Description
Section A	This is an introductory section that explains concepts that are necessary to understand how the Meridian 1 must be set up to support Meridian Mail.
Section B	This section discusses the different kinds of Meridian Mail ports, port requirements for services, and planning the Meridian 1 configuration.
Section C	This section contains step-by-step procedures for configuring Meridian 1. This includes procedures for setting up ACD queues and dummy queues.

Meridian Mail setup

Chapter 24, “The VSDN table”, describes how to configure the VSDN Table once you have added the necessary ACD queues on the Meridian 1.

Section A: Introduction

In this section

Automatic Call Distribution (ACD) 23-4
Meridian 1 – Meridian Mail connections 23-6
How Meridian Mail uses ACD 23-7
Types of queues 23-9
Assigning DNs to services in the VSDN table 23-11

Automatic Call Distribution (ACD)

Definition: ACD

Automatic Call Distribution (ACD) is a feature on the Meridian 1 that allows a number of telephones connected to the Meridian 1, known as agents, to share equally in answering incoming calls.

Definition: ACD agent

Agents are programmed on the switch to serve a particular ACD queue. Agents are programmed as SL-1 phones on the Meridian 1.

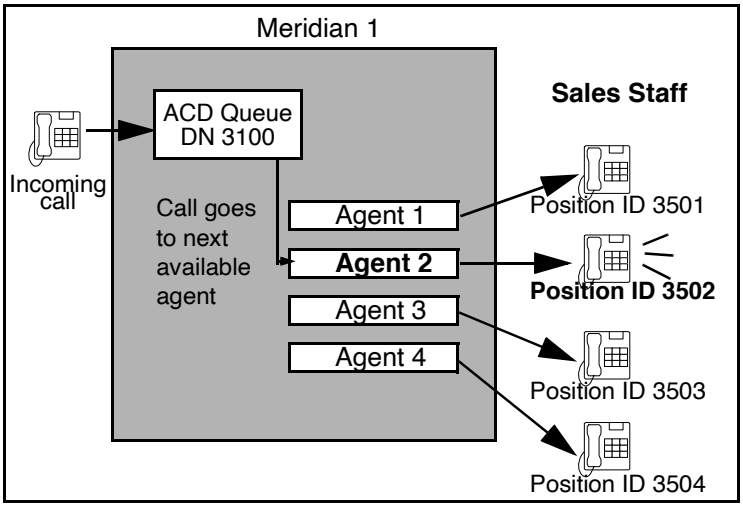
How it works

ACD provides call handling capabilities to the Meridian 1. This table describes how ACD handles an incoming call.

Stage	Description
1	A call comes into the Meridian 1.
2	The call is placed in an ACD queue where it waits to be connected to an agent.
3	The call is passed to the agent that has been idle the longest, or if all agents are busy, the first available agent.
4	The agent answers the call.

Example

When a call comes into the Meridian 1, the DN (directory number) that was dialed determines which ACD queue the call goes to.



Meridian 1 – Meridian Mail connections

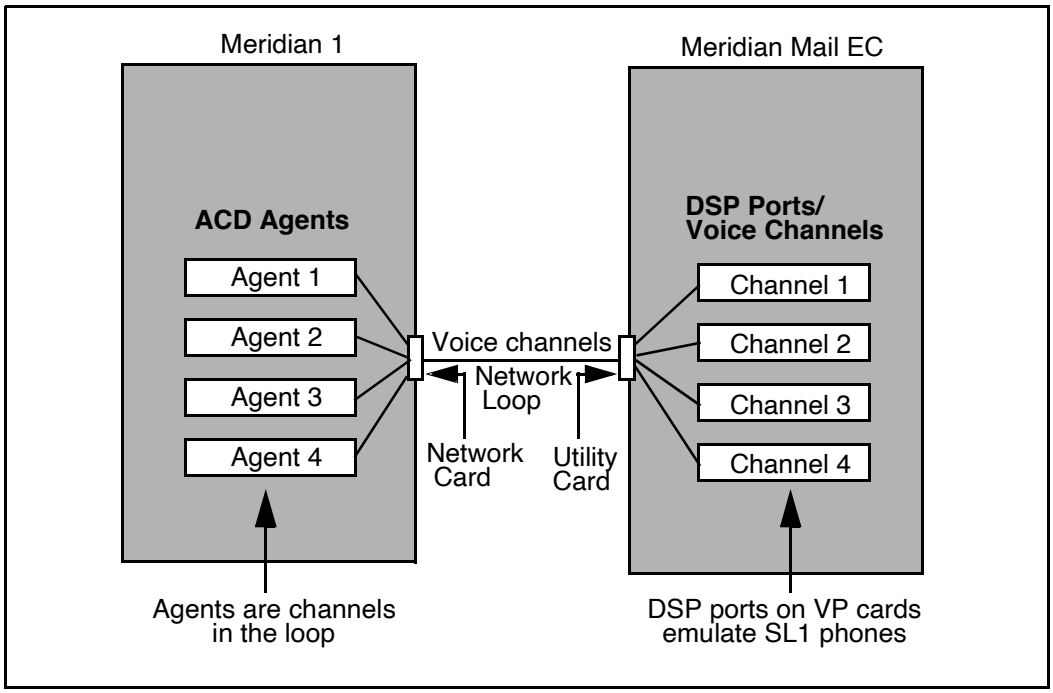
M1 agents and Meridian Mail ports

Each agent in an ACD queue is associated with a specific DSP port in Meridian Mail. These DSP ports physically exist on Meridian Mail voice processor cards.

The terms channel and port are often used interchangeably. They mean the same thing.

Example

This simplified diagram shows how Meridian 1 agents connect to channels in a Meridian Mail Modular Option EC.



How Meridian Mail uses ACD

Virtual agents

In Meridian Mail, there are no “physical” agents or telephones. Instead, “virtual agents” are used. Virtual agents are the DSP ports that are configured in the Meridian Mail software. These ports emulate SL-1 telephone sets.

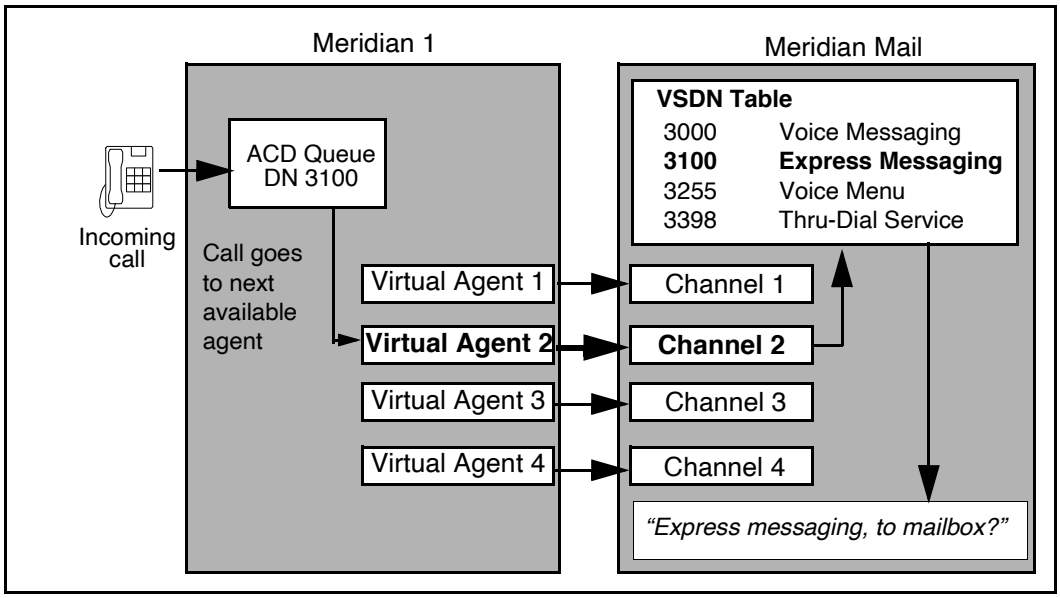
Directing calls to services

Meridian Mail uses ACD to perform its call handling functions. However, instead of being directed to agents or telephones, incoming calls are directed to Meridian Mail services such as Voice Messaging, Express Messaging, or a Voice Menu via the virtual agents.

Example

An incoming call to DN 3100 goes to ACD queue 3100. It gets directed to the first available agent. It is then connected to a Meridian Mail channel (port) and routed to the VSDN Table.

In the VSDN Table, Meridian Mail looks up the DN that was dialed to see which service is associated with it. Meridian Mail then starts the service and plays the appropriate prompts.



Types of queues

Two types of queues

There are two types of queues that you can configure on the Meridian 1 for Meridian Mail:

- ACD agent queues
- dummy queues

Agent queues

Agent queues contain agents and are served by Meridian Mail ports. These queues conduct the actual call handling.

The ACD DNs of agent queues are listed in the Meridian Mail Channel Allocation Table (CAT). The CAT indicates to which queue a particular agent is assigned.

Other terms

Agent queues are sometimes referred to as primary queues or main queues.

Dummy queues

Dummy queues do not have agents. They accept calls and then reroute callers to an agent queue for call handling. A Night Call Forward (NCFW) DN must be defined for all dummy queues. This DN determines the agent queue to which calls are rerouted.

Other terms

Dummy queues are sometimes referred to as secondary queues or service queues.

Why use dummy queues?

Many of the Meridian Mail services that you configure need to be directly accessible. That is, you want callers to be able to dial a number in order to access the service.

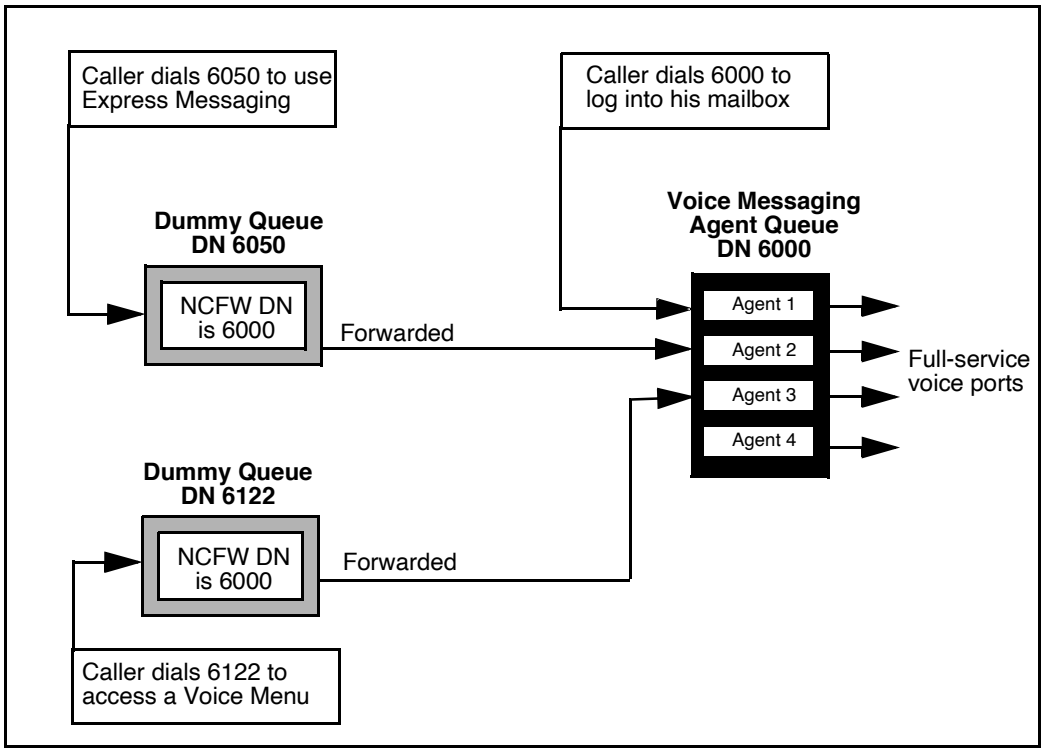
Each directly dialable service needs a unique number, or DN, so that when the DN is dialed, the correct service is started and the appropriate prompts are played.

Why use dummy queues (cont'd)

Creating an agent queue for each service would be very inefficient, even if you had all the necessary ports. Instead, you create a small number of agent queues for call handling, and a dummy queue for each directly dialable service. Since each dummy queue has an ACD DN associated with it, this DN becomes the access number for the service.

Example

Two dummy queues have been set up. One (DN 6050) is for Express Messaging. The other (DN 6122) is for a Voice Menu. They both forward to DN 6000.



Assigning DNs to services in the VSDN table

Introduction

When you create a dummy queue for a Meridian Mail service, the DN assigned to it is the access number for the service.

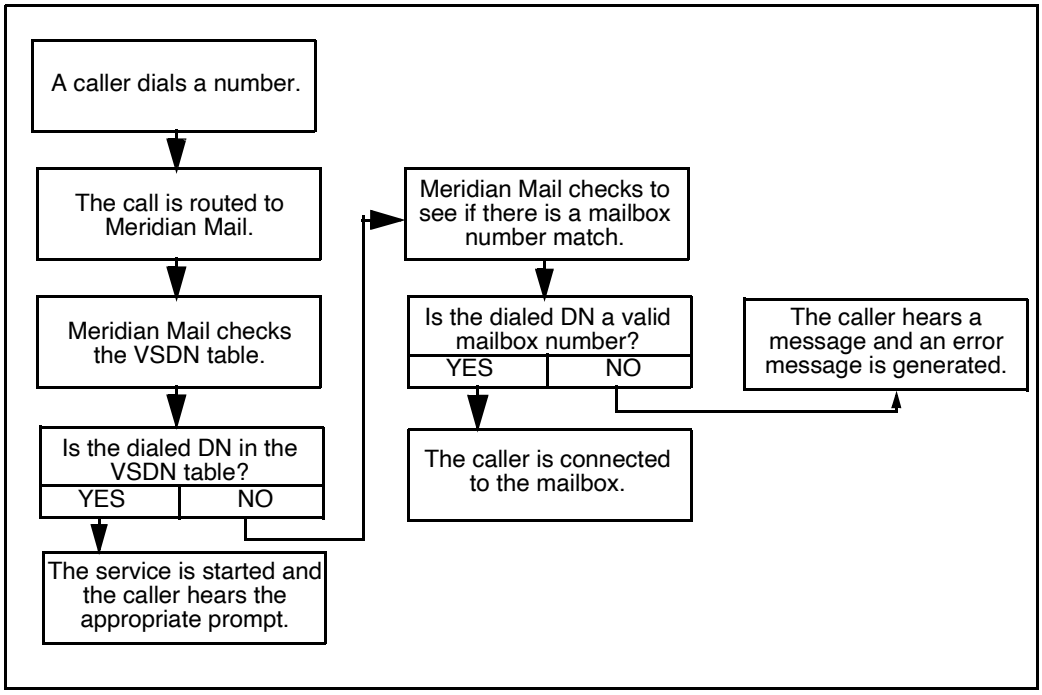
Mapping DNs to services: the VSDN table

These ACD DNs are configured on the Meridian 1. When you create an ACD queue or dummy queue, you cannot specify the associated Meridian Mail service on the Meridian 1. So how does Meridian Mail know which service to start when a particular DN is dialed?

The answer is the VSDN Table. All of the ACD DNs that are configured on the Meridian 1 for Meridian Mail services are entered into the VSDN Table. When you add a VSDN, you define the access DN (this is the ACD DN) and the service. This provides a mapping between ACD DNs and Meridian Mail services.

How DNs are looked up

When a call comes into the system, Meridian Mail looks up the dialed DN in the VSDN Table.



Section B: Planning your configuration

In this section

Overview	23-14
Types of Meridian Mail ports	23-15
Port requirements for Meridian Mail services	23-18
Identifying the ports that are installed on your system	23-20
Should you dedicate ports?	23-23
Dedicating ports because of mixed port types	23-24
Dedicating ports to services	23-26
Determining how many ACD queues you need	23-28
Determining how many dummy queues you need	23-29

Overview

Introduction

Before you begin configuring the Meridian 1 for Meridian Mail services, you need to do some analysis and planning. You will need to determine

- the types of Meridian Mail ports that are installed on your system
- the number of Meridian Mail services that require DNs
- whether you want to dedicate channels to any services
- how many ACD queues you need
- how many dummy queues you need

Types of Meridian Mail ports

Three port types

There are three types of Meridian Mail DSP ports:

- basic service ports
- full-service voice ports
- full-service multimedia ports

Grade of service

These different port types represent different grades of service. Some services can use any of these ports. Others require a certain level of service and can use only one or two kinds of port.

How ports are used for outcalls

Meridian Mail begins by seeking the lowest-grade port required. If those are busy, Meridian Mail searches the next higher grade of port.

Example

Remote Notification requires full voice ports. When there is an attempt to place an outcall, Meridian Mail searches for an idle full voice port. If all voice ports are disabled, Meridian Mail will seek an idle multimedia port and will use it as long as it is not dedicated.

Basic ports

Basic service ports can be used by services that require a very basic grade of service; in other words, services that do not require full service voice or fax capability.

Supported services

Basic service ports can be used to run the following services:

- Meridian ACCESS applications
- Announcement services
- Thru-dial service
- Voice Prompt Maintenance
- Remote Activation
- Voice Menus and Time-of-Day Controllers that do not invoke services requiring full-service voice full-service multimedia ports

Full-service voice ports

Full-service voice ports provide a higher grade of service because they are capable of supporting all voice-related activities such as compression, recording, playback, and tone detection.

Supported services

Full-service voice ports can be used to run the following services in addition to services that need only basic service ports:

- Voice Messaging
- Express Messaging
- Call Answering
- Fax Items with callback fax delivery mode
- Outcalling (Remote Notification and Delivery to Non-User)
- Hospitality Messaging
- Post-Checkout Mailbox (a hospitality feature)
- Voice Forms
- Transcription Service (a voice forms feature)
- Meridian Networking
- AMIS Networking
- Enterprise Networking
- Voice Menus and Time-of-Day Controllers that invoke any of the above services or services that can use basic service voice ports

Full-service multimedia ports

A full-service multimedia port is not a different kind of port. It is the equivalent to approximately two full-service voice ports. A larger number of multimedia ports means a smaller number of total ports on your system.

Supported services

Multimedia ports are required by the following Fax on Demand services. They can also be used by any other service:

- Fax Items with same call or caller choice fax delivery mode
- Fax Item Maintenance
- Voice Menus and Time-of-Day Controllers that invoke any of the above services

Port requirements for Meridian Mail services

Requirements

This table summarizes minimum port requirements.

Meridian Mail service		Type
ACC	Meridian ACCESS	Basic
AN	AMIS Networking	Voice
AS	Announcement Service	Basic
CO	Post-Checkout Mailbox	Voice
EM	Express Messaging	Voice
CA	Call Answering	Voice
EN	Enterprise Networking	Voice
FI	Fax Information Service • callback fax delivery • same call or caller choice fax delivery	 • Voice • Multimedia
FIM	Fax Item Maintenance	Multimedia
HM	Hospitality Messaging	Voice
MS	Voice Menu that invokes • only services requiring basic ports • any services requiring voice ports • any services requiring multimedia ports	 • Basic • Voice • Multimedia
NW	Meridian Networking	Voice
OC	Outcalling	Voice
PM	Voice Prompt Maintenance	Basic
RA	Remote Activation	Basic
TD	Time-of-Day Controller that invokes • only services requiring basic ports • any services requiring voice ports • any services requiring multimedia ports	 • Basic • Voice • Multimedia
TR	Transcription Service	Voice

Meridian Mail service	Type
TS Thru-Dial Service	Basic
VF Voice Forms Service	Voice
VM Voice Messaging	Voice

Identifying the ports that are installed on your system

Introduction

You designate ports as one of the three types during Meridian Mail software installation or expansion.

You can check the types of ports that are installed on your system by viewing the Channel Allocation Table. This table is accessible from the System Status and Maintenance menu.

Multimedia ports

A multimedia port is actually made up of two voice ports. Each multimedia port, therefore, has two terminal numbers (TNs) associated with it.

Procedure

To check the installed ports, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance.
2	Select Channel Allocation Table from the System Status and Maintenance menu. • If you have a single node system, the Channel Allocation Table is displayed. Go to step 4. • If you have a multinode system, go to step 3.

Step	Action
3	Enter the number of the node on which the port resides, followed by <Return>. **Result:** The Channel Allocation Table is displayed.

```
                          System Status and Maintenance
Channel Allocation Table for Node 2 (C=Card D=DSP P=Port)
Choice of Services:
ALL All Services          AN  AMIS Networking       AS  Announcement Service
EM  Express Messaging     FOC Fax Outcalling        GS  Greetings Service
MS  Voice Menu Service    OC  RN/DNU Outcalling     PM  Prompt Maintenance
RA  Remote Activation     TR  Transcription Service TS  Thru-Dial Service
VF  Voice Forms Service   VM  Voice Messaging       VS  Voice Softkey

Limit; MaxVoice MinMulti; MaxFull;            ---------Allocated---------
  72      68        2        68               M/F:  2   V/F: 66   V/B:  2

 #  C-D-P    TN         ACD DN     SCN     Type  Capability Outbound
 1  2-1-1 009-0-02-00 3658      2800      Multi Full       ALL
          009-0-02-01 blocked for Multimedia port 2-1-1.
 2  2-2-1 009-0-02-02 3658      2802      Multi Full       ALL
          009-0-02-03 blocked for Multimedia port 2-2-1.
 3  2-3-1 009-0-02-04 3659      2804      Voice Full Basic ALL
 4  2-3-2 009-0-02-05 3659      2805      Voice Full Basic ALL
                                                                   MORE BELOW
Select a softkey >

     Save        Cancel                                  Hide Choice of
                                                            Services
```

4	Review the Channel Allocation Table. • The TN column lists the terminal numbers (hardware addresses) of the agents. • The Type and Capability columns indicate the port type of each agent (port).

Keeping track of TNs

It will help you later when adding agents to queues if you create a list of all TNs and their port types. A list in the following format is useful.

TN	Port Type	Port Capability	ACD DN
002-0-02-00	Voice	Basic	5470
002-0-02-01	Voice	Basic	5470
002-0-02-02	Voice	Full	5480
002-0-02-03	Voice	Full	5480
002-0-02-04	Multimedia	Full	5490
002-0-02-05	Multimedia	Full	5490
.			
.			
.			

If agent queues have not been created yet, you can decide on the ACD DNs now, and then use them when you actually create the agent queues.

Should you dedicate ports?

Introduction

Agents (ports) can be shared by all services or dedicated to particular services.

There are some conditions under which you must dedicate ports, and others that are good reasons for dedicating ports.

Reasons for dedicating ports

There are two reasons for dedicating ports:

- If there is more than one port type on your system (two or more of basic, voice, and multimedia ports), you must create multiple ACD queues. A separate ACD queue is required for each port type.

  See “Dedicating ports because of mixed port types” on page 23-24.
- You want to dedicate ports to a particular service.

  See “Dedicating ports to services” on page 23-26.

Dedicating ports because of mixed port types

Restriction

An ACD queue can be serviced by only one type of DSP port. For example, the same ACD queue cannot be serviced by both basic service DSP ports and full-service voice DSP ports.

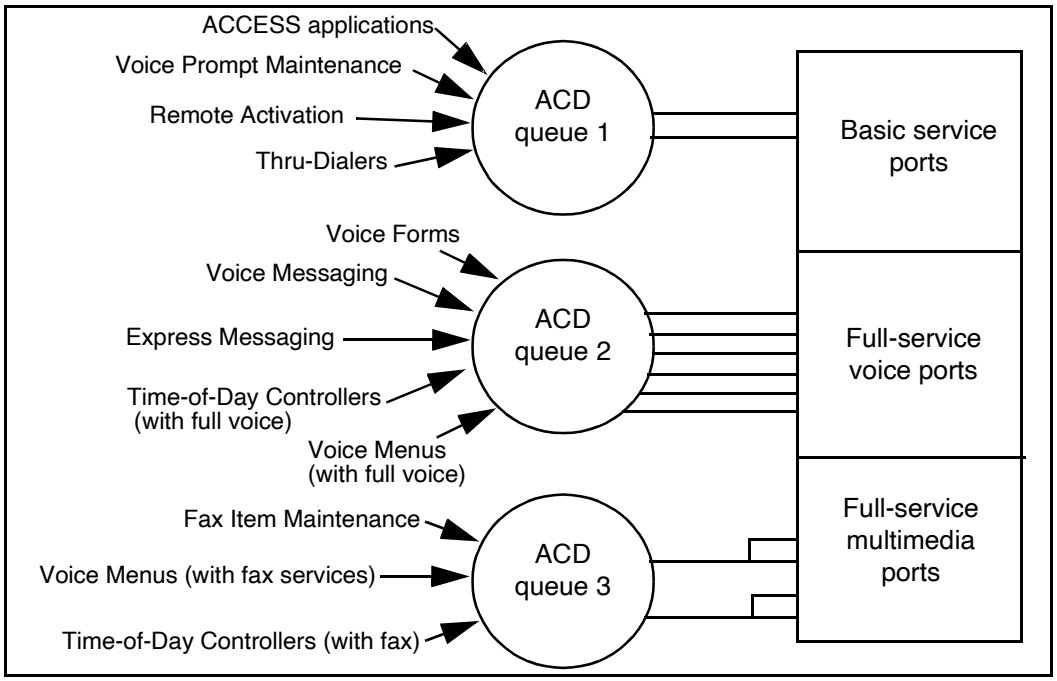
Implication

This means that you must create an ACD queue for each type of port. All agents that are added to it must correspond to Meridian Mail ports of the same type. This ensures that services access ports with an appropriate grade of service.

Example

You have all three port types on your system: basic service, full-service voice, and full-service multimedia.

You, therefore, set up three ACD queues; one for each type. When configuring dummy queues for each Meridian Mail service, you make sure it forwards to the correct ACD queue. The ACD queue to which you forward the dummy queue depends on the port requirements for the Meridian Mail service.



Dedicating ports to services

Reasons for dedicating ports

You may decide to dedicate ports to a particular Meridian Mail service for the following reasons:

- Traffic studies have indicated that a particular inbound service is used heavily and that calls are being lost because the service is competing for ports with other services.
- It is crucial that a particular outbound service (such as Remote Notification or an ACCESS application) always have access to ports.

Reasons not to dedicate ports

Share DSP ports as much as possible because they are used more efficiently when shared.

When ports are dedicated to services, the overall efficiency of the system is reduced for the following reasons:

- A port that is fully dedicated to a particular service cannot be used by any other service, even if idle.
- When ports are dedicated to a particular service, that service can use those ports only. It cannot use other ports if the dedicated ports are in use.

Partially versus fully dedicated ports

When you dedicate ports to services, you are blocking other services from using them. You can either partially or fully dedicate ports, although it is recommended that you fully dedicate them.

Blocking inbound calls

To block other services from using a channel when inbound calls are made, you must create a ACD queue for the service and assign agents to it.

Blocking outbound calls

To block other services from using a channel for placing outbound calls only, you do not need to create a special ACD queue. All you have to do is dedicate the port to the service in the Channel Allocation Table.

Choosing a procedure

Use this table to determine what you need to do, and where to find instructions, based on whether you want to partially or fully dedicate ports to a service.

IF you want to block	THEN	AND follow the
only inbound calls from using the port (partially dedicated)	create an ACD queue for the service	procedure on page 23-40.
only outbound calls from using the port (partially dedicated)	dedicate the port to the service in the CAT	procedure on page 23-43.
both inbound and outbound calls from using the port (fully dedicated)	• create an ACD queue for the service, and • dedicate the port in the CAT	procedure on page 23-49.

Determining how many ACD queues you need

Introduction

For more information about factors that influence how many ACD queues you need, see the following:

- "Should you dedicate ports?" on page 23-23
- "Dedicating ports because of mixed port types" on page 23-24
- "Dedicating ports to services" on page 23-26

Procedure

To determine how many ACD queues you need, follow these steps.

Step	Action
1	Do you know what kinds of ports you have installed on your system? • If yes, go to step 2. • If no, see "Identifying the ports that are installed on your system" on page 23-20 and then return to this procedure.
2	Do you have more than one port type on your system? • If yes, you require one ACD queue per port type. • If no, you require only one ACD queue (for voice ports).
3	Do you want to fully dedicate ports to any services? • If yes, you require one ACD queue for each service to which you want to dedicate ports for inbound and outbound calls. • If no (you do not want to dedicate channels at all, or you only want to dedicate channels for outcalls), you do not need additional ACD queues.
4	Total the numbers that resulted from steps 2 to 3 to determine the total number of ACD queues that you need.

Determining how many dummy queues you need

Procedure: newly installed system

To determine how many dummy queues you need for a newly installed system, follow these steps.

Step	Action
1	Identify how many directly dialable Meridian Mail services you will initially be configuring.
2	If you are likely to add services in the future, identify how many dummy queues you would need to support them. **Note:** You do not have to add extra dummy queues at this point. However, it is convenient to have additional dummy queues already configured if the need for a new service arises.
3	Add the numbers from steps 1 and 2 to get the total number of dummy queues you need to configure.

Procedure: operational system

To determine how many dummy queues you need to add to an operational system, follow these steps.

Step	Action
1	Identify how many services you need to add to your system.
2	Check to see if you have enough dummy queues to support these services.
3	Do you have enough dummy queues? • If yes, gather the available DNs and configure them in the VSDN Table in Meridian Mail. • If no, create enough dummy queues to support the new services and configure the VSDN table.

Section C: Configuring the Meridian 1 for Meridian Mail services

In this section

Overview	23-32
Creating ACD queues for a totally shared configuration	23-33
Creating ACD queues for a combination (shared and dedicated) configuration	23-35
Partially dedicating ports – blocking inbound calls only	23-40
Partially dedicating ports – blocking outbound calls only	23-43
Fully dedicating ports – blocking inbound and outbound calls	23-49
Creating an agent queue	23-52
Adding agents to a queue	23-55
Creating a dummy queue	23-59
Moving agents from one queue to another	23-61
Removing agents from a queue	23-63
Modifying the Channel Allocation Table after moving agents	23-64

Overview

Introduction

This section contains step-by-step procedures for setting up queues on the Meridian 1.

Begin by reviewing the high-level procedure for the configuration you require.

IF	THEN go to
you need only one agent queue	page 23-33.
you need multiple agent queues (because you have mixed port types or need to dedicate ports to services)	page 23-35.

Overlays

The following Meridian 1overlays are used to configure the Meridian 1 for Meridian Mail services.

Overlay	Function
LD 23	This overlay is used to create agent queues and dummy queues.
LD 11	This overlay is used to add agents to an agent queue (or remove them).

Overlay prompts

Procedures in this section instruct you on how to fill in various Meridian 1 overlays.

The procedures tell you which prompts need to be responded to in a certain way for Meridian Mail. For all other prompts, you can simply press Enter to accept the default values as they do not affect Meridian Mail.

Creating ACD queues for a totally shared configuration

Introduction

All agents can be shared by all Meridian Mail services if

- you have only one type of Meridian Mail port (full-service voice ports only) and if
- you do not need to dedicate agents (ports) to any Meridian Mail services

If both of these conditions are not met, see "Creating ACD queues for a combination (shared and dedicated) configuration" on page 23-35.

The primary Voice Messaging queue

You can make the agent queue the primary Voice Messaging queue. This means that you can publish the ACD DN of the agent queue as the Voice Messaging DN.

Alternatively, you can create a dummy queue for Voice Messaging that forwards to the agent queue. In this instance, the DN of the agent queue is not published to users and is never directly dialed.

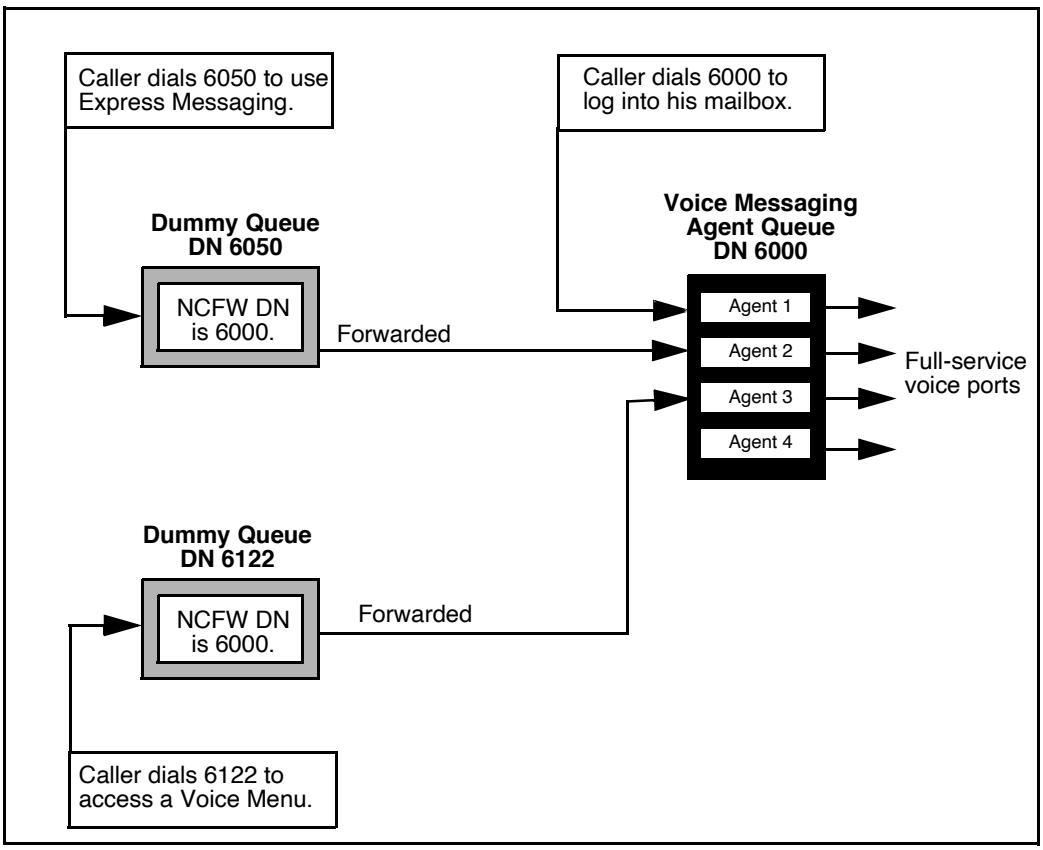
Procedure

This is a high-level procedure for configuring the Meridian 1 and Meridian Mail for services. Detailed step-by-step procedures are on the corresponding pages.

Step	Action	See
Meridian 1 configuration		
1	Create an ACD agent queue.	page 23-52
2	Add all agents to this queue.	page 23-55
3	Create a dummy queue for each Meridian Mail service that needs to be directly dialable. **Note:** Forward (NCFW) all dummy queues to the agent queue you created in step 1.	page 23-59
Meridian Mail configuration		
4	Add the ACD DNs of the agent queue and dummy queues to the VSDN table.	Chapter 24

Example

This is an example of a shared configuration in which there is only one agent queue, which is also the Voice Messaging queue. All other queues are dummy queues that forward to this single agent queue for call handling.



Creating ACD queues for a combination (shared and dedicated) configuration

Introduction

You need a combination shared and dedicated configuration if one or both of these conditions are met:

- There are mixed port types on your system (more than one of basic service, full-service voice, and full-service multimedia ports).

  For more information, see "Dedicating ports because of mixed port types" on page 23-24.
- You need to dedicate ports to one or more Meridian Mail services.

  For more information, see "Dedicating ports to services" on page 23-26.

The primary Voice Messaging queue

You can make the agent queue that contains the full-service voice ports the primary Voice Messaging queue. This means that you can publish the ACD DN of this agent queue as the Voice Messaging DN.

Alternatively, you can create a dummy queue for Voice Messaging that forwards to this agent queue. In this instance, the DN of the agent queue is not published to users and is never directly dialed.

Do not mix port types in one queue

When adding agents to an agent queue, make sure they are all of the same type. An ACD agent queue cannot be serviced by Meridian Mail ports of different types (such as basic service and full-service voice ports).

Forwarding dummy queues

When you specify the NCFW (Night Call Forward) DN for a dummy queue, make sure you enter the DN of the appropriate agent queue. Ensure that the dummy queue terminates on an agent queue that is serviced by ports of the appropriate type.

To identify the minimum port requirements for a Meridian Mail service, see "Port requirements for Meridian Mail services" on page 23-18.

Creating agent queues

This is a high-level procedure for configuring agent queues in a combination shared and dedicated configuration. Detailed step-by-step procedures are on the corresponding pages.

Step	Action	See page
1	Create an ACD agent queue for full-service voice ports.	23-52
2	Add the necessary agents (that correspond to full-service voice ports in Meridian Mail) to this queue.	23-55
3	Do you have basic service ports on your system? • If yes, go to step 4. • If no, go to step 6.	
4	Create an ACD agent queue for basic service ports.	23-52
5	Add the necessary agents (that correspond to basic service ports in Meridian Mail) to this queue.	23-55
6	Do you have full-service multimedia ports on your system? • If yes, go to step 7. • If no, go to step 9.	
7	Create an ACD agent queue for full-service multimedia ports.	23-52
8	Add the necessary agents (that correspond to full-service multimedia ports in Meridian Mail) to this queue.	23-59

Step	Action	See page
9	Do you need to dedicate ports to any Meridian Mail services? • If yes, go to step 10. • If no, go to step 11.	
10	Choose the way in which you want to dedicate ports.	

IF you want to	THEN go to
partially dedicate the ports by blocking only other inbound calls from using the ports	page 23-40.
partially dedicate the ports by blocking only other outbound calls from using the ports	page 23-43.
fully dedicate the ports by blocking all other inbound and outbound calls from using the ports (recommended method)	page 23-49.
Note: When you are done, return to this procedure to define dummy queues and configure the VSDN table in Meridian Mail.	

Step	Action	See page
11	Go to the next procedure for creating dummy queues.	

Creating dummy queues

This is a high-level procedure for configuring dummy queues. Detailed step-by-step procedures are on the corresponding pages.

Step	Action	See page
1	Identify the port requirements of each Meridian Mail service for which you need a dummy queue.	23-18
2	Create a dummy queue for each Meridian Mail service that needs to be directly dialable but that does not need dedicated ports. **Note:** Make sure you forward each dummy queue to the correct agent queue.	23-59
3	Go to the next procedure for configuring Meridian Mail.	23-38

Configuring Meridian Mail

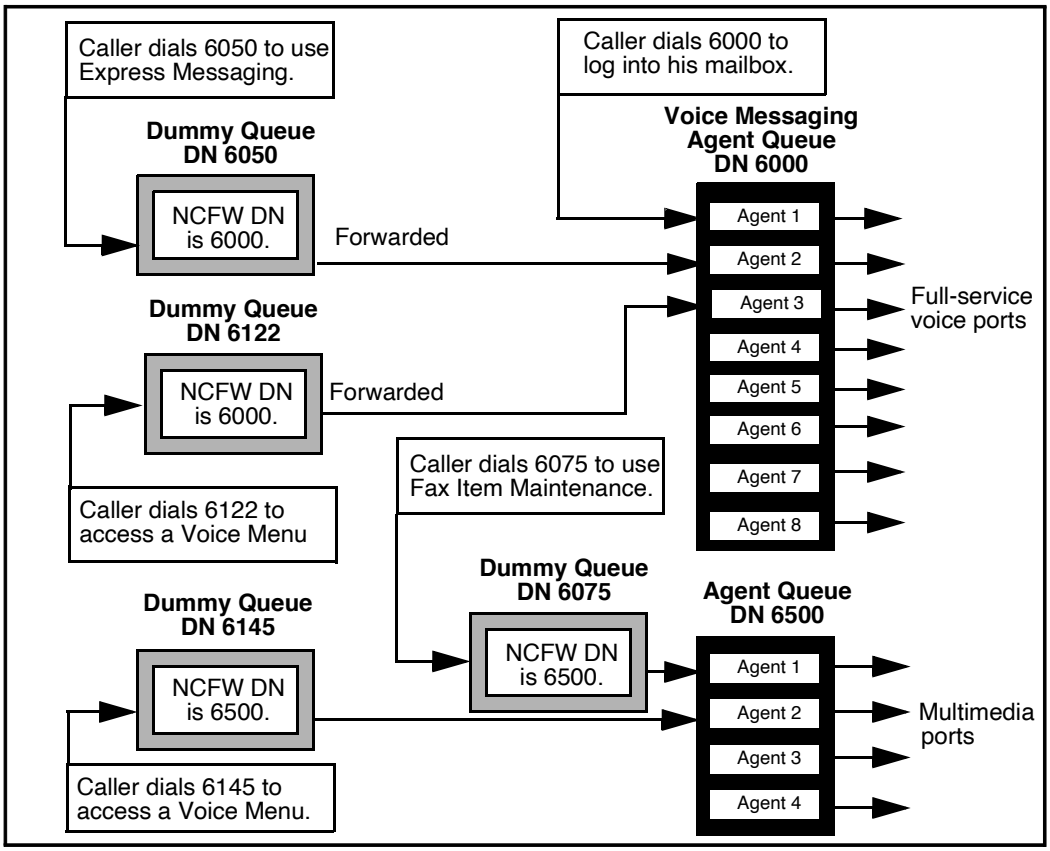
This is a high-level procedure for configuring VSDNs.

Step	Action	See
1	If you moved agents from one queue to another, modify the ACD DN of each moved agent in the Channel Allocation Table.	page 23-64
2	Add ACD DNs of the agent and dummy queues you have created to the VSDN Table.	Chapter 24

Example

In this example, two agent queues have been created. Agents in queue 6000 are connected to Meridian Mail full-service voice ports. Agents in queue 6500 are connected to multimedia ports.

Voice menu 6122 does not contain fax services, whereas menu 6145 contains fax items with same call delivery.



Partially dedicating ports – blocking inbound calls only

Inbound calls

These are calls made to Meridian Mail such as when

- users log in to their mailboxes
- users dial into Express Messaging
- callers dial into a Voice Menu
- callers are transferred to Meridian Mail to leave a message (Call Answering)

When to use

Use this procedure if you want to partially dedicate ports to a service by blocking all other inbound calls, but not outbound calls.

To do this, you must create a separate ACD agent queue for the service.

Procedure

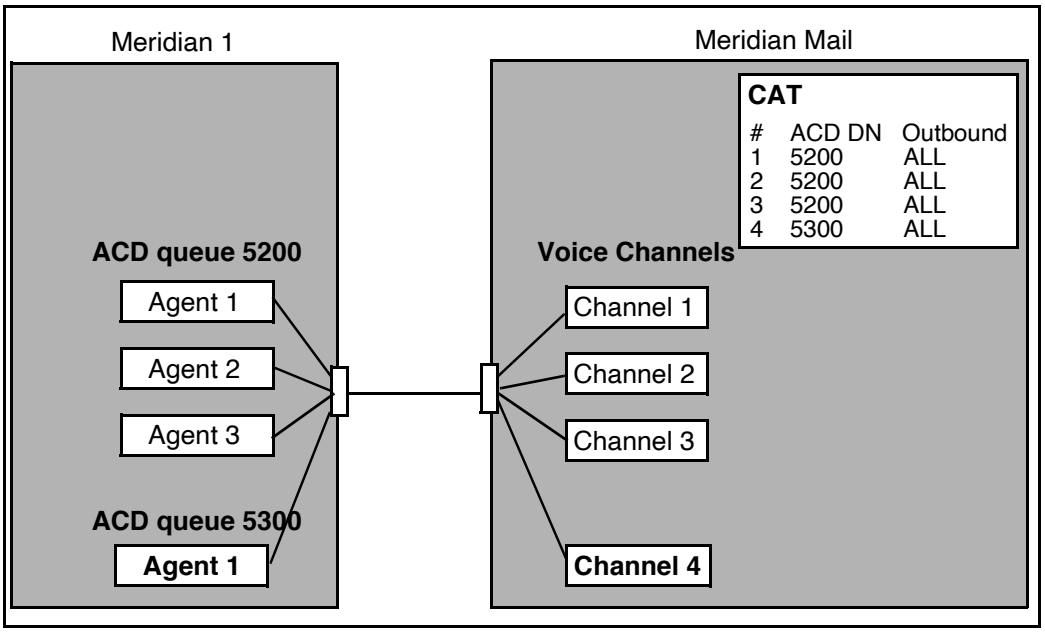
To block inbound calls on a port, follow these steps.

Step	Action	See Page
1	Identify the ports you want to dedicate to the service. **Note:** If you have mixed port types on your system, make sure the ports you dedicate are of the correct type, and all of the same type.	23-26
2	Create an agent queue for the service.	23-52
3	Add or move the agents to the queue.	23-55 (add) 23-61 (move)

Example

In this example, an agent (port) is dedicated to a particular Voice Menu. ACD queue 5300 has been set up for this Voice Menu and it contains one agent.

The port, however, is not dedicated in the Channel Allocation Table. Outbound calls from any Meridian Mail service are allowed on this port.



Scenario A

In this scenario, an inbound call is placed to Voice Messaging (DN 5200).

Stage	Description
1	A caller dials 5200 to log in to her mailbox.
2	The call is routed to ACD queue 5200. • All of the agents in queue 5200 are busy. • The agent in queue 5300 is idle but cannot be used by this call.
3	The call waits for an agent in queue 5200 to become idle.

Example (cont'd)

Scenario B

In this scenario, Meridian Mail makes a remote notification attempt (an outbound call).

Stage	Description
1	A message is left for a user that has remote notification capability.
2	Meridian Mail attempts to place an outbound call to deliver the notification.
3	Meridian Mail looks for an idle port. • Ports 1, 2, and 3 (that belong to ACD queue 5200) are busy. • Port 4 (in ACD queue 5300) is idle.
4	Since the Outbound column in the CAT table is set to ALL for this port, the call is placed.

Partially dedicating ports – blocking outbound calls only

Outbound calls

These are calls made by Meridian Mail. The following Meridian Mail features make outbound calls:

- all networking features
- Outcalling (Remote Notification and Delivery to Non-User)
- Fax on Demand (call back fax delivery)

When to use

Use this procedure if you want to partially dedicate ports to a service by blocking all other outbound calls but not inbound calls.

To do this, you must do the following:

- Disable the ports you want to dedicate.
- Modify the Outbound column in the Channel Allocation Table.
- Reenable the ports.

Disabling ports

Before you can modify the Outbound column in the Channel Allocation Table, you must disable the port(s) you want to dedicate.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance.
2	Select DSP Ports.
3	If you have a multi-node system, enter the number of the node on which the port(s) resides.
4	Press the [Courtesy Disable Port] or [Disable Port] softkey. **Result:** You are prompted for a node number.
5	Enter the node number. **Note:** Wait until the port status is OutofService.
6	Do you want to disable another port? • If yes, repeat steps 4 to 5 until you have disabled all the ports you want to dedicate. • If no, go to step 7.
7	Press [Exit]. **Result:** The System Status and Maintenance menu is displayed.

Modifying the Outbound column in the CAT

To dedicate a port by blocking all other outbound calls, follow these steps.

Starting Point: The System Status and Maintenance menu

Step	Action
1	Select Channel Allocation Table. **Result:** If you have a multi-node system, you are prompted for a node number.
2	If you have a multi-node system, enter the number of the node on which the port resides.
3	Move the cursor to the port you want to dedicate.
4	Go to the Outbound column and enter the service (acronym) to which you want to dedicate the port.

```
                        System Status and Maintenance                MORE ABOVE
Channel Allocation Table for Node 1 (C=Card D=DSP P=Port)
Choice of Services:
ALL All Services          AN  AMIS Networking       AS  Announcement Service
EN  Enterprise Networking EM  Express Messaging     FOC Fax Outcalling
ACC Meridian ACCESS       NW  Meridian Networking   PM  Prompt Maintenance
RA  Remote Activation     OC  RN/DNU Outcalling     TS  Thru-Dial Service
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging       VS  Voice Softkey

Limit; MaxVoice MinMulti; MaxFull;            ---------Allocated---------
  48      40        4        40               M/F:  4   V/F: 36   V/B:  4

 #  C-D-P    TN         ACD DN     SCN     Type  Capability Outbound
 5  4-1-1 032-0-02-08 3650      2808      Voice Full Basic ALL
 6  4-1-2 032-0-02-09 3650      2809      Voice Full Basic ALL
 7  4-2-1 032-0-02-10 3650      2810      Voice Full Basic ALL
 8  4-2-2 032-0-02-11 3650      2811      Voice Full Basic ALL
 9  4-3-1 032-0-02-12 3659      2812      Voice Full Basic ALL
                                                                  MORE BELOW
Select a softkey >

   Save        Cancel                                   Hide Choice of
                                                          Services
```

Step	Action
5	Do you want to dedicate another port? • If yes, repeat steps 3 to 4. • If no, go to step 6.
6	Press the [Save] softkey. **Result:** The System Status and Maintenance menu is displayed.

Reenabling the ports

To reenable the ports you dedicated, follow these steps.

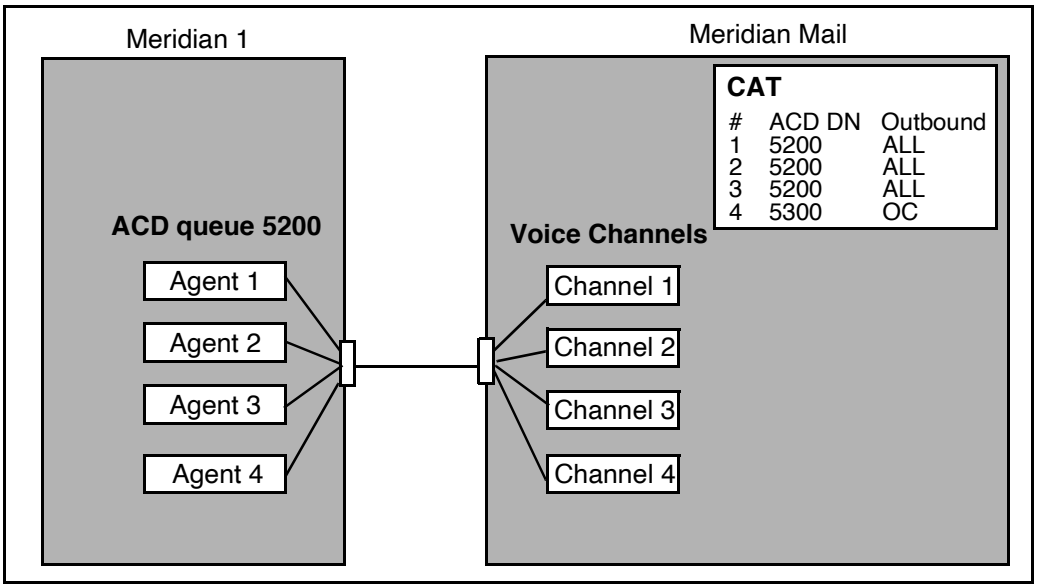
Starting Point: The System Status and Maintenance menu

Step	Action
1	Select DSP Ports. **Result:** If you have a multi-node system, you are prompted for a node number.
2	If you have a multi-node system, enter the number of the node on which the port(s) resides.
3	Press the [Enable Port] softkey. **Result:** You are prompted for the number of the port you want to enable.
4	Enter the port number. **Note:** Wait until the screen indicates that the port is no longer POutof Service.
5	Do you want to enable another port? • If yes, repeat steps 4 to 5 until you have enabled all the ports you dedicated. • If no, go to step 6.
6	Press [Exit]. **Result:** The System Status and Maintenance menu is displayed.

Example

In this example, a separate queue has not been set up on the PBX. All inbound calls can, therefore, use all agents (ports).

In Meridian Mail, however, Channel 4 is dedicated to Outcalling (OC) in the Channel Allocation Table.



Scenario A

In this scenario an inbound call is placed to Voice Messaging (DN 5200).

Stage	Description
1	A caller dials 5200 to log in to her mailbox.
2	The call is routed to ACD queue 5200. • The first three agents in queue 5200 are busy. • Agent 4 is idle.
3	The call is completed using agent 4.

Example (cont'd)

Scenario B

In this scenario, Meridian Mail attempts to make an outbound networking call.

Stage	Description
1	A network message is ready to be delivered.
2	Meridian Mail attempts to place an outbound call to deliver the network message.
3	Meridian Mail looks for an idle port. • Ports 1, 2, and 3 are busy. • Port 4 is idle.
4	Since the Outbound column in the CAT table is set to OC for Port 4 (it is dedicated to Outcalling), the call waits until another agent (port) becomes available.

Fully dedicating ports – blocking inbound and outbound calls

Introduction

If you are considering dedicating ports to a service, it is recommended that you fully dedicate them so that no other services can use the ports.

To do this, you must create an agent queue on the PBX *and* dedicate the port in the Channel Allocation Table in Meridian Mail.

Procedure

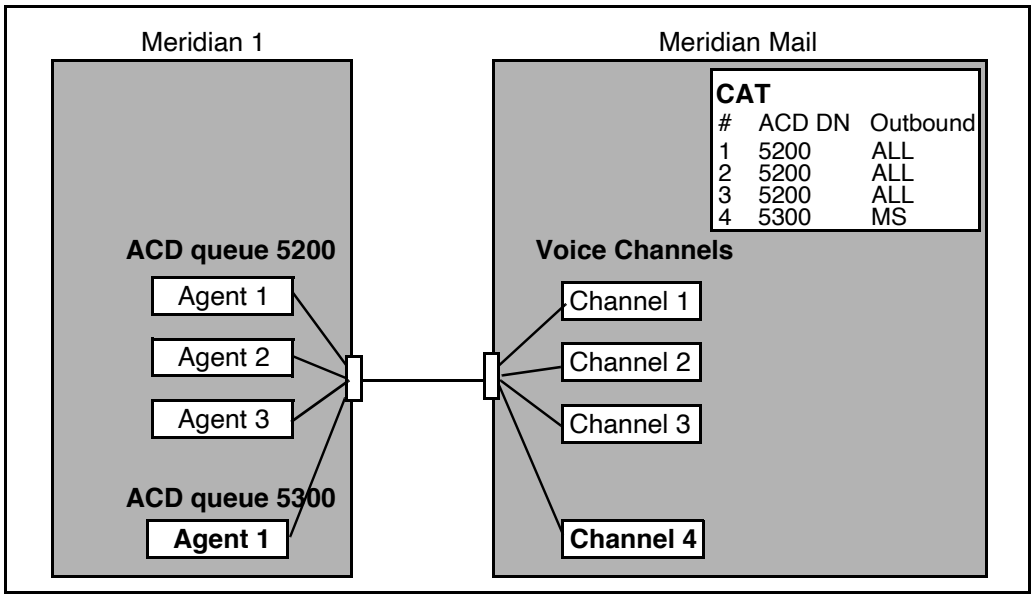
To completely dedicate ports to a service, follow these steps.

Step	Action	See page
	Meridian 1 configuration	
1	Identify the ports you want to dedicate to the service. **Note:** If you have mixed port types on your system, make sure the ports you dedicate are of the correct type, and all of the same type.	23-26
2	Create an agent queue.	23-52
3	Add or move the ports to the queue.	23-55 (add) 23-61 (move)
	Meridian Mail configuration	
4	Disable the ports you want to dedicate.	23-44
5	Modify the Outbound column in the CAT table.	23-45
6	Reenable the ports.	23-46

Example

ACD queue 5300, containing one agent, has been set up for a Voice Menu.

The port is also dedicated to the Voice Menu Service in the Channel Allocation Table. Only calls to the Voice Menu can use Agent (Channel) 4.



Scenario A

In this scenario, an inbound call is placed to Voice Messaging (DN 5200).

Stage	Description
1	A caller dials 5200 to log in to her mailbox.
2	The call is routed to ACD queue 5200. • All of the agents in queue 5200 are busy. • The agent in queue 5300 is idle but cannot be used by this call.
3	The call waits until an agent in queue 5200 becomes idle.

Example (cont'd)

Scenario B

In this scenario, Meridian Mail attempts to make an outbound networking call.

Stage	Description
1	A network message is ready to be delivered.
2	Meridian Mail attempts to place an outbound call to deliver the network message.
3	Meridian Mail looks for an idle port. • Ports 1, 2, and 3 are busy. • Port 4 is idle.
4	Since the Outbound column in the CAT table is set to MS for this port (it is dedicated to the Voice Menu Service), the call waits until another port (agent) becomes available.

Creating an agent queue

Introduction

ACD queues are created using overlay 23. You must set up at least one agent queue on the Meridian 1 to serve as the primary Voice Messaging queue. This queue is usually set up by the install technician.

You may or may not need other agent queues depending on how many port types you have on your system and whether or not you want to dedicate ports to any services.

When to use

Create an agent queue

- as the primary Voice Messaging queue (containing full-service voice ports)
- for each additional port type that is installed on your system (basic and/or full multimedia)
- for each service to which you want to dedicate ports

If you are not sure of how many agent queues you require, see "Determining how many ACD queues you need" on page 23-28.

Procedure

To create an agent queue, follow these steps.

Step	Action
1	Log in.
2	Enter **LD 23** to load overlay 23.
3	Respond to prompts as shown in the following table.

Prompt	Response	Description
REQ	NEW	Indicates you are creating a new queue.
TYPE	ACD	Indicates an ACD data block.
CUST	xx	Enter the SL-1 customer number (00-31).
ACDN	xxxxxxx	Enter the DN of the ACD queue. This is the number you enter in the VSDN table.
MWC	YES	Indicates this is a message center and that the queue has agents.
IMS	YES	Indicates an Integrated Messaging service.
CMS	YES	Command and Status Link Applications Protocol is used.
IMA	YES	Enables IMS attendant.
IVMS	YES	Integrated Voice Messaging. Creates a message center from which messages can be retrieved.
VSID	xx	Enter the VAS ID (0 to 15) from LD 17.
MAXP	xx	Indicates the maximum number of ACD agents for this queue.
ALOG	YES	ACD agents are automatically logged on when Meridian Mail is powered up.
NCFW	0	The DN to which calls are forwarded. Set to 0 for agent queues.

Step	Action
4	Do you want to add another ACD agent queue? • If yes, enter **NEW** in response to the REQ prompt and respond to the prompts as shown in step 3. • If no, enter **END** in response to the REQ prompt to exit overlay 23.

Adding agents to a queue

Introduction

Once you have created an ACD agent queue, you can add agents to it.

Before you begin

Gather together a list of the TNs of the agents you want to add to the queue.

If you have multiple agent queues because of a mixture of port types on your system (two or more of basic, full voice, and full multimedia ports), make sure you know the port type of each TN. You can add agents of one type only to a single queue.

See “Dedicating ports because of mixed port types” on page 23-24.

The terminal number

The terminal number (TN) is the hardware address of an ACD agent. Each voice port in Meridian Mail is associated with the TN of the Meridian 1 agent that will be servicing the port.

Format

TNs are in the format **lll s cc u**.

Parts description

These are the parts of TN.

Part	Name	Description	Range
lll	Loop	The network loop to which the agent is connected.	0 to 159 (any loop dedicated to Meridian Mail)
s	Shelf	The shelf (IPE module) on which the agent is located.	(0 to 3) 0 for EC
cc	Card	The card slot on which the agent is located.	1 to 10 2 and 3 for EC
u	Unit	The unit (port) on which the agent is located.	0 to 7

Example

20-0-2-0

The position ID

The position ID identifies a particular agent within a queue. It is used for ACD reporting/tracking purposes in addition to identification of agents. Each agent must, therefore, have a unique position ID.

The SCN DN

If a port is going to be used to originate calls, such as for outcalling, Fax on Demand, or networking, you must define a single-call non-ringing DN (SCN DN) as Key1. The SCN DN is a unique number (zzzz) that gives the appearance of a telephone number on a key.

Determine a numbering scheme

For ease of maintenance, assign sequentially numbered position IDs and SCN DNs.

Example

The ACD DN of the queue to which you are adding agents is 8100.

Position IDs are numbered 8101, 8102, and so on.

SCN DNs are numbered 8201, 8202, and so on.

Adding new ports to an installed system

If you are adding additional agents to an existing queue, you may have to modify the MAXP value for the queue to which you are adding agents. The MAXP value determines the maximum number of agents the queue can contain. If by adding new agents, you exceed this value, you will not be able to add the additional agents unless you change the MAXP value.

Instructions for adding new ports to an already installed Meridian Mail system are in the *System Installation and Modification Guide* (NTP 555-7001-215).

Modifying the MAXP value

To modify the MAXP value in the queue to which you are adding agents, follow these steps.

Step	Action
1	Log in.
2	Enter **LD 23** to load overlay 23.
3	Respond to prompts as shown in the following table.

Prompt	Response	Description
REQ	CHG	Indicates you are modifying a queue.
TYPE	ACD	Indicates you are modifying an ACD data block.
CUST	xx	Enter the SL-1 customer number (00 to 31).
ACDN	xxxxxxx	Enter the DN of the ACD queue to which you are adding or moving agents.
MAXP	xx	Modify this number so that it is equal to or greater than the new total number of agents for this queue.

4	Enter **END** in response to the REQ prompt to exit overlay 23.
5	Go to the procedure on page 23-58 to add agents to the queue.

Adding agents

To add an agent to a queue, follow these steps.

Step	Action
1	Log in.
2	Enter **LD 11** to load overlay 11.
3	Respond to prompts as shown in this table.

Prompt	Response	Description
REQ	NEW	
TYPE	SL1	
TN	lll s cc u	Enter the TN of the agent. lll is the loop number. s is the shelf number. cc is the card slot number. u is the unit (port) number.
CLS	VMA	Indicates Voice Messaging is allowed.
Key0	ACD xxxx yyyy	Enter the DN (xxxx) of the queue and the agent's position (yyyy).
Key1	SCN zzzzzzz	Enter a single-call, non-ringing DN if this port will be used to place outcalls by Meridian Mail features such as Outcalling, Fax on Demand, and networking.
Key2	MSB	Make Set Busy key
Key3	NRD	Not Ready key
Key6	TRN	Transfer key
Key7	AO3	Conference key
Key9	RLS	Release key

4 Do you want to add another agent?

- If yes, enter **NEW** in response to the REQ prompt and respond to prompts as shown in step 3.
- If no, enter **END** in response to the REQ prompt.

Creating a dummy queue

Introduction

A dummy queue does not have agents. Instead, it forwards to an agent queue.

When to use

Add a dummy queue for each Meridian Mail service that you want to make directly dialable by users and callers.

Examples

You want to provide users with Express Messaging capability. You, therefore, create a dummy queue for Express Messaging so that it has a unique DN that can be dialed.

You want to create six Voice Menus that you need to make available to callers. You, therefore, create six dummy queues so that each Voice Menu has a unique number that can be dialed.

Systems with mixed port types

If you have more than one port type on your system, be sure to forward the dummy queue to the right agent queue. The agent queue to which you forward the dummy queue must be serviced by ports of the appropriate type.

To determine the port requirements, see "Port requirements for Meridian Mail services" on page 23-18.

Example

All three port types are installed on your system. You have, therefore, created three ACD agent queues as follows.

ACD agent queue DN	Contains
7400	Full-service voice ports
7440	Basic service ports
7480	Full-service multimedia ports

You need to create a dummy queue for the Fax Item Maintenance service, which requires full-service multimedia ports. You, therefore, enter 7480 as the NCFW DN. This forwards the dummy queue to the agent queue that contains full-service multimedia ports.

Procedure

To create a dummy queue that forwards to an agent queue, follow these steps.

Step	Action
1	Log in.
2	Enter **LD 23** to load overlay 23.
3	Respond to prompts as shown in the following table.

Prompt	Response	Description
REQ	NEW	Indicates you are creating a new queue.
TYPE	ACD	Indicates you are creating an ACD data block.
CUST	xx	Enter the SL-1 customer number (00 to 31).
ACDN	xxxxxxx	Enter the DN of the ACD queue. This is the number you enter in the VSDN table.
MWC	NO	Indicates this is not a message center with agents.
MAXP	1	Even though this queue has no agents, MAXP must be set to 1.
NCFW	xxxxxxx	Enter the DN of the agent queue to which you are forwarding this queue.

4 Do you want to add another dummy queue?
- If yes, enter **NEW** in response to the REQ prompt and respond to the prompts as shown in step 3.
- If no, enter **END** in response to the REQ prompt to exit overlay 23.

Meridian Mail configuration

Once you have added all the necessary agent and dummy queues, you are ready to add the ACD DNs to the VSDN table. For instructions, see Chapter 24, “The VSDN table”.

Moving agents from one queue to another

Introduction

You must follow this procedure to move agents. You cannot simply change the ACD DN of an existing agent.

> **CAUTION**
>
> **Risk of data corruption**
>
> Do not move ACD agents by changing the ACD DN (on Key0) of an existing agent. Doing this can cause severe data corruption.

When to use

Use this procedure if you want to move existing agents from one queue to another queue.

Examples

You might need to do this if you have dedicated ports to a particular service and you find through analyzing traffic studies that you need more ports.

Or, you might find that the efficiency of the system has gone down, and you want to reduce the number of ports that are dedicated to a service and move them to a queue where they can be shared among more services.

Modifying MAXP

The MAXP value determines the maximum number of agents that can be in a queue. By moving agents to a queue, you may exceed the current MAXP value for that queue. If this happens, you must modify MAXP so that it is equal to or greater than the new total number of agents.

Procedure

To move an agent, you must first remove the agent from the queue it currently belongs to and then rebuild it under the other queue.

This is a high-level procedure for moving agents. Step-by-step procedures are on the corresponding pages.

Step	Action	See page
	Meridian 1 configuration	
1	Will rebuilding agents under the other queue cause the MAXP value of that queue to be exceeded?	
	• If yes, modify the MAXP value for the queue to which you are moving agents.	23-57
	• If no, go to step 2.	
2	Remove the agents from their current ACD queue.	23-63
3	Rebuild (add) the agents under the queue to which you are moving them.	23-55
	Meridian Mail configuration	
4	Modify the Channel Allocation Table.	23-63

Removing agents from a queue

When to use

Use this procedure if you need to move agents from one queue to another. Moving agents involves removing them from the queue they currently belong to and rebuilding them under the new queue.

Procedure

To remove an agent from a queue, follow these steps.

Step	Action
1	Log in.
2	Enter **LD 11** to enter overlay 11.
3	Respond to prompts as shown in the following table.

Prompt	Response	Description
REQ	OUT	Indicates you want to out (remove) an agent.
TYPE	SL1	
TN	lll s cc u	Enter the TN of the agent you want to remove. lll is the loop number. s is the shelf number. cc is the card slot number. u is the unit (port) number.

4 Do you want to remove another agent?
- If yes, enter **OUT** in response to the REQ prompt and respond to the prompts as shown in step 3.
- If no, enter **END** in response to the REQ prompt to exit overlay 11.

Modifying the Channel Allocation Table after moving agents

When to use

You need to modify the Channel Allocation Table only if you have moved agents from one queue to another.

When you move an agent from one queue to another, the ACD DN of the agent changes. This change must be reflected in the Channel Allocation Table (CAT).

Procedure

To modify the ACD DN of moved agents in the Channel Allocation table, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance.
2	Disable the ports that correspond to the moved agents. **Note:** See “Disabling ports” on page 23-44.
3	Select Channel Allocation Table from the System Status and Maintenance menu. **Result:** The Channel Allocation Table is displayed.
4	Move the cursor to the agent (port) that was moved.
5	Go to the ACD DN column and enter the DN of the ACD queue to which it was moved.

```
                        System Status and Maintenance                MORE ABOVE
Channel Allocation Table for Node 1 (C=Card D=DSP P=Port)
Choice of Services:
ALL All Services          AN  AMIS Networking       AS  Announcement Service
EN  Enterprise Networking EM  Express Messaging     FOC Fax Outcalling
ACC Meridian ACCESS       NW  Meridian Networking   PM  Prompt Maintenance
RA  Remote Activation     OC  RN/DNU Outcalling     TS  Thru-Dial Service
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging       VS  Voice Softkey

Limit; MaxVoice MinMulti; MaxFull;            ---------Allocated---------
  48      40        4        40               M/F:  4   V/F: 36   V/B:  4

 #  C-D-P    TN         ACD DN     SCN      Type  Capability Outbound
 5  4-1-1 032-0-02-08 3650      2808      Voice Full Basic ALL
 6  4-1-2 032-0-02-09 3650      2809      Voice Full Basic ALL
 7  4-2-1 032-0-02-10 3650      2810      Voice Full Basic ALL
 8  4-2-2 032-0-02-11 3650      2811      Voice Full Basic ALL
 9  4-3-1 032-0-02-12 3659      2812      Voice Full Basic ALL
                                                                  MORE BELOW
Select a softkey >

   Save        Cancel                                   Hide Choice of
                                                          Services
```

Step	Action
6	Did you move any other agents (ports)? • If yes, repeat steps 4 to 5 until you have modified the ACD DNs of all agents that were moved. • If no, go to step 8.
7	Press [Save] to save the changes.
8	Reenable the port(s). **Note:** See “Reenabling the ports” on page 23-46.

Chapter 24

The VSDN table

In this chapter

Section A: Introduction	24-3
Section B: Adding messaging VSDNs	24-11
Section C: Adding networking and ACCESS VSDNs	24-27
Section D: Adding voice service and fax service DNs	24-39
Section E: Session profiles	24-67
Section F: Viewing, modifying, and deleting VSDNs	24-115

Section A: Introduction

In this section

Overview 24-4
When to create a VSDN 24-5
Network Message Service requirements 24-6
Network Message Service requirements 24-6
The VSDN table 24-9

Overview

Introduction

Voice service directory numbers (VSDNs) are defined for every service that you want to make directly accessible to internal users or external callers, or both. These directory numbers (DNs) are entered in the Voice Services-DN (VSDN) table which maps DNs to services.

Access DNs

Part of defining a VSDN is specifying the access DN. This is the number that users and callers dial to access the service.

> **ATTENTION**
>
> Ensure that access DNs in your VSDN definitions do not duplicate mailbox numbers or Meridian 1 trunk route access codes.

Nightly audits

Every day at 3:30 a.m., Meridian Mail performs an audit. This audit can take anywhere from 10 minutes (if the system has not been modified since the last audit) to 2 hours (if many changes have been made, such as users or services being added or modified).

> **ATTENTION**
>
> Do not add, modify, or delete VSDNs during the nightly audit.

When to create a VSDN

Requirement

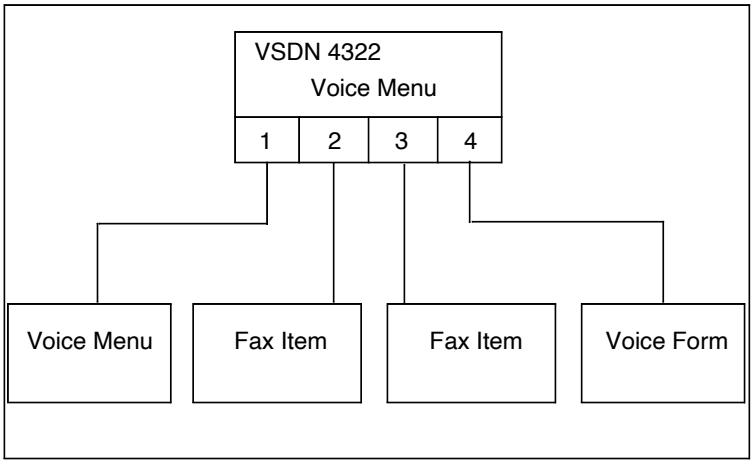
You need a VSDN for any service that you want to be directly accessible. This means that a caller dials a number to access a particular service such as a Voice Menu or Express Messaging.

You do not have to create VSDNs for services that are accessed indirectly through other services.

Example

You want to create a voice menu that starts up the following services:

- another Voice Menu
- two Fax Items
- a Voice Form



Only the first Voice Menu (that starts the other services) requires a VSDN since it is the service that you want callers to dial in to directly.

The other services that it invokes do not need VSDNs since they are not dialed in to directly. They are accessible only through the Voice Menu.

However, if you want to make the same service (like the voice form) also directly dialable, you need to create a VSDN for it.

Network Message Service requirements

NMS networks

If the Network Message Service (NMS) feature is installed, you must create a VSDN for each location at which you need a particular service.

Example

There are three NMS locations in your network: the prime location (the switch connected to Meridian Mail) and two satellite locations. You want to provide express messaging to all three locations. You, therefore, need to add three express messaging VSDNs, one for each NMS location.

DN format for the prime location

When adding VSDNs for services at the prime location, enter them in the local format.

Example

You create a VSDN for express messaging at the prime location with an access DN of 8365.

DN format for satellite locations

When adding a VSDN for a service at a satellite location, the access DN must be in a format which is dialable from the prime location, since this is what the switch passes to Meridian Mail. Consequently, it must include the ESN prefix or CDP steering code for the satellite location.

Example

You have an ESN dialing plan:

- The ESN prefix for satellite location 1 is 6444.
- The ESN prefix for satellite location 2 is 6555.
- The local extension for express messaging at satellite location 1 is 3544.
- The local extension for express messaging at satellite location 2 is 3652.

The access DN for express messaging at satellite location 1 is 64443544.

The access DN for express messaging at satellite location 2 is 65553652.

Accessing the VSDN table

Introduction

All of the procedures in this chapter are performed in the VSDN table. This procedure describes how to access the VSDN table.

Procedure

To access the VSDN table, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Voice Administration. **Result:** The Voice Administration menu is displayed.

```
Voice Administration

    1  Voice Messaging Options
    2  Voice Security Options
    3  Restriction/Permission Lists
    4  Voice Services Administration
    5  Outcalling Administration
    6  Voice Form Definitions

Select an item >

Exit
```

2	Select Voice Services Administration. **Result:** The Voice Services Administration menu is displayed.

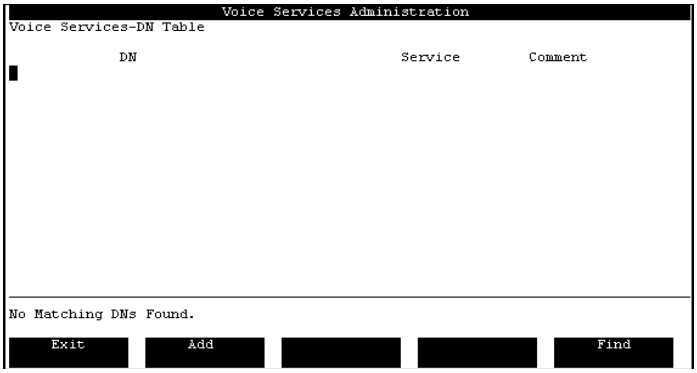
```
Voice Services Administration

    1  Voice Services-DN Table
    2  Voice Services Profile
    3  Announcement Definitions
    4  Thru-Dial Definitions
    5  Time-of-Day Control Definitions
    6  Voice Menu Definitions
    7  Fax Item Definitions

Select an item >

Exit    Set Display Options    Find Subset of VSDNs/Services
```

Step	Action
3	Select Voice Services-DN Table. **Result:** The Voice Services-DN Table is displayed.



4 What action do you want to perform?

IF you want to	THEN	AND see
add a VSDN	press [Add]	Section B: to Section D:.
view or modify a VSDN	select the VSDN and press [View/Modify]	page 24-116.
delete a VSDN	select the VSDN and press [Delete]	page 24-119.
find a VSDN or subset of VSDNs	press [Find]	Chapter 22.

The VSDN table

The screen

This is the VSDN table for an operational system in which a number of VSDNs have already been defined.

```
                    Voice Services Administration
Voice Services-DN Table

            DN                              Service        Comment
            3650                            VM             Voice Messaging
            3651                            EM             Express Messaging
            3652                            RA             Remote Activation
            3653                            PM             Prompt Maintenance
            3654                            MS  101        Main Menu
            3655                            AN             AMIS Networking
            3656                            NW             Meridian Mail Netwk
            3659                            FIM            Fax Item Maint.
            3690                            TR  1901       Transcription Serv.

Move the cursor to the item and press the space bar to select.

   Exit        Add        View/Modify      Delete        Find
```

Field descriptions

This table describes the fields in the VSDN table.

DN	
Description	This is the directory number of the service. It is the number that is dialed to access the service.
Service	
Description	This is the service that is accessed when the DN is dialed. Only the service acronym is displayed.
ID	For certain services, such as Announcements and Voice Menus, an ID is displayed next to the acronym. This is the specific service that is accessed.
Comment	
Description	This is a description or title that has been assigned to the VSDN.

Section B: Adding messaging VSDNs

In this section

Overview 24-12
Adding a VSDN for Voice Messaging 24-13
Adding a VSDN for Express Messaging 24-15
Adding a VSDN for Call Answering 24-17
Adding a VSDN for hospitality voice messaging 24-19
Adding a VSDN for the Post-Checkout Mailbox service 24-22
Adding a VSDN for the Greetings Service 24-24

Overview

Introduction

This section describes how to add VSDNs for Voice Messaging services.

Deciding which VSDNs you need

Use this table to decide which VSDNs you need to add to your system.

IF	THEN	AND see
MMUI or VMUIF Voice Messaging is installed	create a VSDN for VM	page 24-13.
you want express messaging	create a VSDN for EM	page 24-15.
you want express messaging to a particular mailbox with voice messaging-style prompts	create a VSDN for CA	page 24-17.
Hospitality voice messaging is installed	create a VSDN for HM (instead of VM) and CO	pages 24-19 and 24-22.
VMUIF voice messaging is installed	create a VSDN for GS	page 24-24.

Adding a VSDN for Voice Messaging

Description

Voice Messaging is the basic voice mail service that records voice messages when a phone is not answered (Call Answering) and allows users to compose and send voice messages.

When to use

Add a VSDN for the Voice Messaging service during initial Meridian Mail setup.

Hospitality systems

If Hospitality Voice Messaging is installed on your system, see "Adding a VSDN for hospitality voice messaging" on page 24-19 instead.

If installed, you can also add a DN for the Post-Checkout Mailbox service, as described on page 24-22.

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Procedure

To add the Voice Messaging VSDN, follow these steps.

Starting Point: The VSDN table

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN. **Note:** This is the DN of the primary ACD agent queue.

Step	Action
3	Enter VM in the Service field.

```
                    Voice Services Administration
Add DN Information

Choice of Services:
AS  Announcement Service  CA  Call Answering        EM  Express Messaging
FI  Fax Info Service      FIM Fax Item Maintenance  PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Access DN:        3650

Service:          VM

Comment:          Voice Messaging

Select a softkey >

   Save        Cancel
```

4	Enter an optional comment in the Comment field.
5	Do you want to add the VSDN with the information you have entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Adding a VSDN for Express Messaging

Description

Express Messaging allows users to directly leave a message in another user's mailbox without ringing a phone.

When to use

Express Messaging is a basic feature that should be available to users once Meridian Mail is operational. The VSDN for Express Messaging should, therefore, be added during initial Meridian Mail setup.

Mailbox ID

If you define a Mailbox ID, callers to the Express Messaging service are automatically transferred to the specified mailbox.

Types of express messaging services

You can create a number of Express Messaging services, each with its own VSDN.

Application 1: general Express Messaging service
This is the typical Express Messaging application that allows users to activate the Express Messaging service, dial any mailbox without ringing the associated phone, and leave a message directly in the mailbox.

For this type of service, do not enter a mailbox ID.

Application 2: suggestion box
In this application, when the Express Messaging DN is dialed, the caller is forwarded to a specific mailbox (a suggestion box) to leave a message.

This application requires that you

- set up a special mailbox just for this purpose. (See "Adding a local voice user" on page 8-6.)
- enter the mailbox ID in the Add DN Information screen

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Procedure

To add the Express Messaging VSDN, follow these steps.

Starting Point: The VSDN table

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN.
3	Enter EM in the Service field. **Result:** The Mailbox ID field is displayed.

```
                    Voice Services Administration
Add DN Information

Choice of Services:
AS  Announcement Service  CA  Call Answering        EM  Express Messaging
FI  Fax Info Service      FIM Fax Item Maintenance  PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Access DN:        3651_________________________

Service:          EM_     Mailbox ID:          _________________________

Comment:          Express Messaging_

Select a softkey >

   Save        Cancel
```

Step	Action
4	Do you want callers to be forwarded to a particular mailbox when using this service? • If yes, enter the number of the mailbox to which you want to forward users in the Mailbox ID field. • If no, leave the Mailbox ID field blank.
5	Enter an optional comment in the Comment field.
6	Do you want to add the VSDN with the information you have entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Adding a VSDN for Call Answering

Description

Call Answering is a service that transfers all calls to its DN directly to Voice Messaging for a particular preset mailbox, without ringing that mailbox's DN. For details on what messages/prompts the caller will hear, see "How Call Answering uses personal greetings and personal verifications" on page 5-7.

When to use

Add a VSDN for the Call Answering service during initial Meridian Mail setup.

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Procedure

To add a DN for the Call Answering Service, follow these steps.

Starting Point: The VSDN table

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN.
3	Enter CA in the Service field. **Result:** The Mailbox ID field is displayed.

```
                    Voice Services Administration
Add DN Information

Choice of Services:
AS  Announcement Service  CA  Call Answering        CO  Post Checkout Mailbox
EM  Express Messaging     FI  Fax Info Service      FIM Fax Item Maintenance
HM  Hospitality Messaging MS  Voice Menu Service    PM  Prompt Maintenance
RA  Remote Activation     TD  Time-of-Day Control   TR  Transcription Service
TS  Thru-Dial Service     VF  Voice Forms Service

Access DN:        5667

Service:          CA      Mailbox ID: 4142

Comment:          Call Answering

Select a softkey >
   Save        Cancel
```

Step	Action
4	Enter the number of the user's mailbox in the Mailbox ID field. All calls to this Call Answering service will be transferred directly to that mailbox.
5	Enter an optional comment in the Comment field.
6	Do you want to add the VSDN with the information you have just entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Adding a VSDN for hospitality voice messaging

Description

Hospitality voice messaging is the basic voice mail service that is used when Hospitality is installed. This service records voice messages when a phone is not answered (call answering) and allows users to compose and send voice messages.

In addition to these regular voice messaging features, hospitality voice messaging has two additional telset interfaces: one for guests and one for staff.

When to use

If you have a Hospitality Meridian Mail system, follow this procedure for adding the hospitality voice messaging VSDN instead of the one on page 24-13. Add the VSDN for hospitality voice messaging during initial Meridian Mail setup.

Auto logon

When you add the DN for hospitality voice messaging, you must specify if auto logon is enabled or disabled.

This is how auto logon works.

WHEN auto logon is	THEN guests and staff
enabled	• can log on to their mailboxes without entering the mailbox number and password when calling in from their own phone. • must enter their mailbox number and password if calling from a phone that has a mailbox with auto logon disabled or does not have a mailbox associated with it.
disabled	must enter their mailbox number and password to log on regardless of which phone they use to log on (their own or someone else's phone).

Auto logon in the user profile

There is also an Auto logon field in the Add and View/Modify Local Voice User screen.

Both of these fields (in the Add DN Information screen and the Add Local Voice User screen) must be enabled for users to be able to auto logon.

This table shows how these two fields interact.

WHEN the VSDN setting is	AND the local voice user setting is	THEN the user
enabled	enabled	can auto logon.
enabled	disabled	cannot auto logon.
disabled	enabled	cannot auto logon.
disabled	disabled	cannot auto logon.

Multiple voice messaging services

You can create two hospitality voice messaging services: one in which auto logon is disabled and one in which it is enabled.

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Procedure

To add the hospitality voice messaging VSDN, follow these steps.

Starting Point: The VSDN table

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN. **Note:** This is the DN of the primary ACD agent queue.
3	Enter HM in the Service field.

```
                    Voice Services Administration
Add DN Information

Choice of Services:
AN  AMIS Networking       EM  Express Messaging     HM  Hospitality Messaging
CO  Post Checkout Mailbox

Access DN:        3699

Service:          HM     Auto Logon:   Disabled Enabled

Comment:          Hospitality VM

Select a softkey >

   Save        Cancel
```

4	Do you want to enable auto logon for this service? • If yes, select Enabled in the Auto Logon field. • If no, select Disabled in the Auto Logon field.
5	Enter an optional comment in the Comment field.
6	Do you want to add the VSDN with the information you have entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Adding a VSDN for the Post-Checkout Mailbox service

Description

Post-Checkout Mailbox is a hospitality feature that allows guests who have checked out to call in for messages that were unread at the time of checkout.

When to use

You need to create this DN only if Hospitality Voice Messaging is installed and if you want to implement the Post-Checkout Mailbox feature.

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Procedure

To add a DN for the Post-Checkout Mailbox service, follow these steps.

Starting Point: The VSDN table

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN.
3	Enter CO in the Service field.

```
                    Voice Services Administration
Add DN Information

Choice of Services:
AN  AMIS Networking       EM  Express Messaging     HM  Hospitality Messaging
CO  Post Checkout Mailbox

Access DN:        3680

Service:          CO

Comment:          PostCheckOut MBox

Select a softkey >

Save      Cancel
```

Step	Action
4	Enter an optional comment in the Comment field.
5	Do you want to add the VSDN with the information you have entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Adding a VSDN for the Greetings Service

Description

The Greetings Service allows VMUIF users who do not have DTMF (touch-tone) phones to update their greetings without having to provide any keypad input. This service can also be provided to subscribers with digitone phones if they want a simplified interface for changing greetings.

When to use

If VMUIF is installed on your system, you should create a VSDN for the Greetings Service.

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Procedure

To add a DN for the Greetings Service, follow these steps.

Starting Point: The VSDN table

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN.
3	Enter GS in the Service field.

```
                    Voice Services Administration
Add DN Information

Choice of Services:
AS  Announcement Service  FI  Fax Info Service      FIM Fax Item Maintenance
GS  Greetings Service     PM  Prompt Maintenance    RA  Remote Activation
TS  Thru-Dial Service     TD  Time-of-Day Control   TR  Transcription Service
VF  Voice Forms Service   MS  Voice Menu Service    VM  Voice Messaging
                 -  -

Access DN:        8605

Service:          GS

Comment:          Greetings Service

Select a softkey >

 Save      Cancel
```

4 Enter an optional comment in the Comment field.

Step	Action
5	Do you want to add the VSDN with the information you have entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Section C: Adding networking and ACCESS VSDNs

In this section

Overview 24-28
Adding a VSDN for AMIS Networking 24-29
Adding a VSDN for Meridian Networking 24-31
Adding a VSDN for Enterprise Networking 24-33
Adding a VSDN for a Meridian ACCESS application 24-36

Overview

Enterprise Networking

Meridian Mail offers three types of networking capabilities that include AMIS Networking, Meridian Networking, and Enterprise Networking.

A VSDN is required for Enterprise Networking if you are expanding to Enterprise Networking or if you are adding Enterprise Networking.

AMIS and Enterprise Networking

When both AMIS Networking and Enterprise Networking are installed, they can share the same VSDN. The drawback to this method is that you will not be able to see separate statistics in Operational Measurements for these two services as they will be combined.

If both AMIS and Enterprise Networking are installed, you can do any one of the following:

- Create two separate VSDNs, one for AMIS (AN) and one for Enterprise Networking (EN).
- Create only one VSDN for AN that is shared by both networking types.
- Create only one VSDN for EN that is shared by both networking types.

Adding a VSDN for AMIS Networking

Description

AMIS Networking allows Meridian Mail users to send voice messages to and receive voice messages from other voice messaging systems that use the AMIS protocol.

When to use

If you are adding AMIS Networking to your system, you must create a VSDN for it. This VSDN establishes a network connection for the AMIS format message transfer.

If Enterprise Networking is installed, it can share this DN.

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Procedure

To add a DN for AMIS Networking, follow these steps.

Starting Point: The VSDN table

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN.
3	Enter AN in the Service field.

```
                    Voice Services Administration
Add DN Information

Choice of Services:
AN  AMIS Networking       AS  Announcement Service  EN  Enterprise Networking
EM  Express Messaging     FI  Fax Info Service      FIM Fax Item Maintenance
ACC Meridian ACCESS       NW  Meridian Networking   PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Access DN:        3655

Service:          AN

Comment:          AMIS Networking

Select a softkey >

   Save        Cancel
```

Step	Action
4	Enter an optional comment in the Comment field.
5	Do you want to add the VSDN with the information you have entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Adding a VSDN for Meridian Networking

Description

Meridian Networking allows Meridian Mail users to send voice messages to and receive voice messages from users at other Meridian Mail sites that are defined in the network database. This type of networking uses the Meridian protocol to transfer messages.

When to use

If you are adding Meridian Networking to your system and you want to use it, you must create a VSDN for it. This VSDN establishes a network connection for the transfer of voice messages.

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Procedure

To add a DN for Meridian Networking, follow these steps.

Starting Point: The VSDN table

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN.
3	Enter NW in the Service field.

```
                    Voice Services Administration
Add DN Information

Choice of Services:
AN  AMIS Networking       AS  Announcement Service  EN  Enterprise Networking
EM  Express Messaging     FI  Fax Info Service      FIM Fax Item Maintenance
ACC Meridian ACCESS       NW  Meridian Networking   PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Access DN:        3656

Service:          NW

Comment:          Meridian Networking

Select a softkey >

   Save        Cancel
```

Step	Action
4	Enter an optional comment in the Comment field.
5	Do you want to add the VSDN with the information you have entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Adding a VSDN for Enterprise Networking

Description

Enterprise Networking provides most of the functionality of Meridian Networking, but uses DTMF signaling, based on the AMIS protocol, instead of modems to transmit messages.

The Remote Voice User Propagation feature is unique to Enterprise Networking. It allows you to automatically add temporary remote voice users to your system.

When to use

If you are adding Enterprise Networking to your system and you want to implement it, you must create a VSDN. This DN is used to establish a network connection for the transfer of voice messages using Enterprise Networking.

Dedicated versus shared DN

You can create a DN specifically for Enterprise Networking (EN). Alternatively, Enterprise Networking can share a DN with any of the following services:

- AMIS networking (AN)
- Voice Menu Service (MS)
- Thru-Dial Service (TS)
- Announcement Service (AS)
- Time-of-day Controller Service (TD)

If Enterprise Networking shares a DN with any of these other services, it means that there is one less VSDN to configure.

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Adding an EN DN for Enterprise Networking

To add an EN DN for Enterprise Networking, follow these steps.

Starting Point: The VSDN table

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN.
3	Enter EN in the Service field.

```
                    Voice Services Administration
Add DN Information

Choice of Services:
AN  AMIS Networking       AS  Announcement Service  EN  Enterprise Networking
EM  Express Messaging     FI  Fax Info Service      FIM Fax Item Maintenance
ACC Meridian ACCESS       NW  Meridian Networking   PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Access DN:        3691

Service:          EN

Comment:          Enterprise Network

Select a softkey >

   Save        Cancel
```

4	Enter an optional comment in the Comment field.
5	Do you want to add the VSDN with the information you have entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Sharing the AMIS DN

To have Enterprise Networking share a DN with AMIS, add a VSDN for AMIS if this has not already been done. If an AMIS DN already exists, no additional configuration is required. See "Adding a VSDN for AMIS Networking" on page 24-29.

Sharing a DN with a voice service

If you want Enterprise Networking to share a DN with one of MS, TS, AS, or TD, follow these steps. This procedure assumes that at least one VSDN exists for one of these four services.

Starting Point: The Voice Services Administration menu

Step	Action
1	Select Voice Services Profile. **Result:** The Voice Services Profile screen is displayed.

```
                    Voice Services Administration
Voice Services Profile

Voice Services Volume: 1

Timeouts
   Command Entry:      3.5 seconds     Short Disconnect: 10.0 seconds
   Record (mm:ss):   02:00

Maximum Prompt Sizes for Announcements (mm:ss):          00:30
                         other voice recordings (mm:ss): 02:00

Act on AMIS/Enterprise Initiator Tone:  No Yes

Enable Update Logging:                  No Yes

Business Hours Default:       08:30 to 17:00

Holidays   Start Date         End Date        Start Time    Comments
                                                                MORE BELOW
Select a softkey >

    Save        Cancel
```

2	Is the Act on AMIS/Enterprise Initiator Tone field set to Yes? • If yes, leave it as is. • If no, set it to Yes.
3	Press [Save]. **Result:** Whenever a call comes into any voice menu (MS), thru-dialer (TS), announcement (AS), or time-of-day controller (TD), Meridian Mail will be able to tell whether it is an Enterprise Networking call and process it accordingly.

Adding a VSDN for a Meridian ACCESS application

Description

ACCESS applications include IVR applications and VISIT Messenger.

When to use

Create a VSDN for each ACCESS application that you want to make directly accessible to callers.

The ACCESS class

Every ACCESS application has a unique identifier known as a class. This is similar to the concept of an ID. It indicates which ACCESS application you want to run when the VSDN is dialed.

The Revert DN

When adding a VSDN for an ACCESS application, you can specify a Revert DN in your VSDN definition. If an ACCESS application goes off-line, calls are transferred to this DN.

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Procedure

To add a DN for an ACCESS application, follow these steps.

Starting Point: The VSDN table

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN.

Step	Action
3	Enter ACC in the Service field. **Result:** The Class and Revert DN fields are displayed.

```
                        Voice Services Administration
Add DN Information

Choice of Services:
AN  AMIS Networking       AS  Announcement Service  EN  Enterprise Networking
EM  Express Messaging     FI  Fax Info Service      FIM Fax Item Maintenance
ACC Meridian ACCESS       NW  Meridian Networking   PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Access DN:        3682

Service:          ACC     Class:     1334

                          Revert DN: 3900

Comment:          IVR App 1

Select a softkey >

     Save        Cancel
```

Step	Action
4	Enter the ACCESS class.
5	Enter a Revert DN if necessary.
6	Enter an optional comment in the Comment field.
7	Do you want to add the VSDN with the information you have entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Section D: Adding voice service and fax service DNs

In this section

Overview	24-40
Adding a VSDN for an announcement	24-41
Adding a VSDN for a thru-dial service	24-43
Adding a VSDN for a voice menu	24-45
Adding a VSDN for a time-of-day controller	24-48
Adding a VSDN for Voice Prompt Maintenance	24-52
Adding a VSDN for Remote Activation	24-54
Adding a VSDN for a voice form	24-56
Adding a VSDN for the Transcription Service	24-58
Adding a VSDN for the Fax Information Service	24-61
Adding a VSDN for the Fax Item Maintenance Service	24-64

Overview

Introduction

When you add a VSDN for any of the following services, you must assign a session profile to it:

- voice menu
- time-of-day controller
- fax item
- fax item maintenance service

Session profiles

There are three predefined session profiles from which to choose. They are based on the channel capability that is required to run the service:

- Basic service
- Full-service voice
- Full-service multimedia

If none of these predefined session profiles meets your needs, you can create a custom session profile. Procedures in this section indicate when you need to select or customize a session profile.

For more information about session profiles, see the section "Session profiles" on page 24-67.

Adding a VSDN for an announcement

Description

An announcement is a voice service that is part of the Voice Menus feature. An announcement is simply a recording that is played to a caller.

When to use

Create a VSDN for an announcement if you want users or callers to be able to access the announcement directly by dialing a number.

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Procedure

To create a VSDN for an announcement, follow these steps.

Starting Point: The VSDN table

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN.
3	Enter AS in the Service field. **Result:** The Announcement ID field is displayed.

```
                    Voice Services Administration
Add DN Information

Choice of Services:
AS  Announcement Service  CA  Call Answering        EM  Express Messaging
FI  Fax Info Service      FIM Fax Item Maintenance  PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Access DN:        3630

Service:          AS     Announcement ID: 4104

Comment:          Directions

Select a softkey >

   Save        Cancel
```

Step	Action
4	Enter the Announcement ID. **Note:** If you have not created the announcement yet, you must enter an ID to save the VSDN. Enter an ID and use this ID when creating the announcement.
5	Enter an optional comment in the Comment field.
6	Do you want to add the VSDN with the information you have entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Adding a VSDN for a thru-dial service

Description

A thru-dialer is a voice service that is part of the voice menus feature. Its function is to provide call handling. When a caller accesses a thru-dialer, he or she is prompted for an extension number. The thru-dialer then places the phone call.

When to use

Create a VSDN for a thru-dialer if you want users or callers to be able to access the thru-dialer directly by dialing a number.

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Procedure

To create a VSDN for a thru-dialer, follow these steps.

Starting Point: The VSDN table

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN.
3	Enter TS in the Service field. **Result:** The Thru-Dial ID field is displayed.

```
                    Voice Services Administration
Add DN Information

Choice of Services:
AS  Announcement Service  CA  Call Answering        EM  Express Messaging
FI  Fax Info Service      FIM Fax Item Maintenance  PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Access DN:        3644

Service:          TS     Thru-Dial ID: 4234

Comment:          Lunchtime ThruDial

Select a softkey >

     Save        Cancel
```

Step	Action
4	Enter the Thru-Dial ID. **Note:** If you have not created the thru-dialer yet, you must enter an ID to save the VSDN. Enter an ID and use this ID when creating the thru-dialer.
5	Enter an optional comment in the Comment field.
6	Do you want to add the VSDN with the information you have entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Adding a VSDN for a voice menu

Description

Voice menus present callers with a list of options from which they can make a selection by pressing the appropriate key on their telephone keypad.

When to use

Create a VSDN for a voice menu if you want users or callers to be able to access the voice menu directly by dialing a number.

Choosing the session profile

You must assign a session profile to all voice menus for which you add a VSDN. Use this table to decide what kind of session profile you need for the voice menu.

IF the voice menu	THEN
invokes one or more of the following *only:* • ACCESS applications (such as IVR) • announcements • thru-dial services • voice prompt maintenance • remote activation • voice menu commands (such as play prompt, call revert DN, or repeat menu choices) • other voice menus or time-of-day controllers that invoke the above services only	• select the basic service session profile. or • create a custom session profile and set channel capability to Basic.
invokes any of the following: • voice messaging • express messaging • call answering • fax items using call back delivery mode • other voice menus or time-of-day controllers that invoke any of the above services	• select the full-service voice session profile. or • create a custom session profile and set channel capability to Full Voice.
invokes any of the following: • fax item maintenance • fax items using same call or caller choice delivery mode	• choose the full-service multimedia session profile. or • create a custom session profile and set channel capability to Full MultiMedia.

When to create a custom session profile

Review the default session profiles starting on page 24-81. If the default session profiles do not meet your needs, you must create a custom profile. See "Customizing the session profile for Voice Menus, Fax Items, and Time-of-Day Controllers" on page 24-90.

Determining how many VSDNs you need

If the voice menu invokes fax services that you want to be able to deliver to different caller markets (such as national and international), you may have to create multiple VSDNs. See "Determining how many VSDNs you need for a callback fax service" on page 24-78.

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Procedure

To create a VSDN for a voice menu, follow these steps.

Starting Point: The VSDN table

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN.
3	Enter MS in the Service field. **Result:** The Voice Menu ID and Session Profile fields are displayed. The [Session Profile Detail] softkey is also displayed.

```
                    Voice Services Administration
Add DN Information

Choice of Services:
AS  Announcement Service  CA  Call Answering        EM  Express Messaging
FI  Fax Info Service      FIM Fax Item Maintenance  PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Access DN:        3640

Service:          MS     Voice Menu ID: 4170

Session Profile:  Custom Full_MultiMedia Full_Voice Basic

Comment:          New Products

Select a softkey >

 Save    Cancel    Session
                   Profile Detail
```

Step	Action
4	Enter the Voice Menu ID. **Note:** If you have not created the voice menu yet, you must enter an ID to save the VSDN. Enter an ID and use this ID when creating the voice menu.
5	Do you need to create a custom session profile? • If yes, see the section "Session profiles" on page 24-67 and then go to step 9. • If no, go to step 6.
6	Select one of the predefined session profiles (Basic, Full Voice, or Full MultiMedia).
7	Do you want to view the session profile? • If yes, press the [Session Profile Detail] softkey. • If no, go to step 9.
8	Review the session profile and press [Return to Previous Form] when you are ready to return to the Add DN Information screen.
9	Enter an optional comment in the Comment field.
10	Do you want to add the VSDN with the information you have entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Adding a VSDN for a time-of-day controller

Description

Time-of-day controllers direct calls to different services based on the time of day that the call is received.

When to use

Create a VSDN for a time-of-day controller if you want users or callers to be able to access the time-of-day controller directly by dialing a number.

Selecting the session profile

Use this table to decide what kind of session profile you need for the time-of-day controller.

IF the time-of-day controller	THEN
invokes one or more of the following *only:* • ACCESS applications (such as IVR) • announcements • thru-dial services • voice prompt maintenance • remote activation • other voice menus or time-of-day controllers that invoke the above services only	• choose the basic service session profile. or • create a custom session profile and set channel capability to Basic.
invokes any of the following: • voice messaging • express messaging • fax items using callback delivery mode • other voice menus or time-of-day controllers that invoke any of the above services	• choose the full-service voice session profile. or • create a custom session profile and set channel capability to Full Voice.
invokes any of the following: • fax item maintenance • fax items using same call or caller choice delivery mode	• choose the full-service multimedia session profile. or • create a custom session profile and set channel capability to Full MultiMedia.

When to create a custom session profile

Review the default session profiles starting on page 24-81. If the default session profiles do not meet your needs, you must create a custom profile. See "Customizing the session profile for Voice Menus, Fax Items, and Time-of-Day Controllers" on page 24-90.

Determining how many VSDNs you need

If the time-of-day controller invokes fax services that you want to be able to deliver to different caller markets (such as national and international), you may have to create multiple VSDNs. See "Determining how many VSDNs you need for a callback fax service" on page 24-78.

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Procedure

To create a VSDN for a time-of-day controller, follow these steps.

Starting Point: The VSDN table

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN.
3	Enter TD in the Service field. **Result:** The Time-of-Day Control ID and Session Profile fields are displayed. The [Session Profile Detail] softkey is also displayed.

```
                    Voice Services Administration
Add DN Information

Choice of Services:
AS  Announcement Service  CA  Call Answering        EM  Express Messaging
FI  Fax Info Service      FIM Fax Item Maintenance  PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Access DN:        3693

Service:          TD     Time-of-Day Control ID: 4101

Session Profile:  Custom Full_MultiMedia Full_Voice Basic

Comment:          TimeOfDayController

Select a softkey >

   Save        Cancel      Session
                           Profile Detail
```

Step	Action
4	Enter the Time-of-Day Control ID. **Note:** If you have not created the time-of-day controller yet, you must enter an ID to save the VSDN. Enter an ID and use it when creating the time-of-day controller.
5	Do you need to create a custom session profile? • If yes, see the section "Session profiles" on page 24-67 and then go to step 9. • If no, go to step 6.
6	Select one of the predefined session profiles (Basic, Full Voice, or Full MultiMedia).
7	Do you want to view the session profile? • If yes, press the [Session Profile Detail] softkey. • If no, go to step 9.

Step	Action
8	Review the session profile and press [Return to Previous Form] when you are ready to return to the Add DN Information screen.
9	Enter an optional comment in the Comment field.
10	Do you want to add the VSDN with the information you have entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Adding a VSDN for Voice Prompt Maintenance

Description

Voice prompt maintenance is a service that allows you to update prompts in voice menus and related services from a remote phone.

When to use

Create a VSDN if you want to use this service and have it directly accessible.

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Procedure

To create a VSDN for the voice prompt maintenance service, follow these steps.

Starting Point: The VSDN table

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN.
3	Enter PM in the Service field. **Result:** When more than one language is installed, the Language of Service field is displayed.

```
                    Voice Services Administration
Add DN Information

Choice of Services:
AS  Announcement Service  CA  Call Answering        EM  Express Messaging
FI  Fax Info Service      FIM Fax Item Maintenance  PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Access DN:        3641

Service:          PM     Language of Service:   American_English
                                                 Canadian_French
Comment:          Prompt Maintenance

Select a softkey >

   Save        Cancel
```

Step	Action
4	If more than one language is installed, select the language in which you want prompt maintenance prompts to be played.
5	Do you want to add the VSDN with the information you have entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Adding a VSDN for Remote Activation

Description

Remote Activation allows you to call in to Meridian Mail from a remote phone and assign a different service to a VSDN.

When to use

Create a VSDN for the Remote Activation service if you want it to be directly accessible by dialing a number.

The remote activation password

You must define a password for Remote Activation. When a caller dials in to the service, this password must be entered to gain access. This is a security measure to ensure that unauthorized personnel do not use this feature.

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Procedure

To create a VSDN for Remote Activation, follow these steps.

Starting Point: The VSDN table

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN.
3	Enter RA in the Service field. **Result:** The Password field is displayed.

```
                    Voice Services Administration
Add DN Information

Choice of Services:
AS  Announcement Service  CA  Call Answering        EM  Express Messaging
FI  Fax Info Service      FIM Fax Item Maintenance  PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Access DN:        3642

Service:          RA      Password: 14987422

Comment:          Remote Activation

Select a softkey >

   Save        Cancel
```

Step	Action
4	Enter a password. **Note:** This password must be defined. If no password is entered, remote activation is not enabled.
5	Do you want to add the VSDN with the information you have entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Adding a VSDN for a voice form

Description

Voice forms present callers with a series of questions to which callers respond with spoken answers.

When to use

Create a VSDN for a voice form if you want it to be directly accessible by dialing a number.

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Procedure

To create a VSDN for a voice form, follow these steps.

Starting Point: The VSDN table

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN.
3	Enter VF in the Service field. **Result:** The Voice Form ID field is displayed.

```
                    Voice Services Administration
Add DN Information

Choice of Services:
AS  Announcement Service  CA  Call Answering        EM  Express Messaging
FI  Fax Info Service      FIM Fax Item Maintenance  PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Access DN:        3701

Service:          VF     Voice Form ID: 4304

Comment:          JAG Feedback

Select a softkey >

   Save        Cancel
```

Step	Action
4	Enter the voice form ID. **Note:** If you have not created the voice form yet, you must enter an ID to save the VSDN. Enter an ID and use this ID when creating the voice form.
5	Do you want to add the VSDN with the information you have entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Adding a VSDN for the Transcription Service

Description

The Transcription Service is part of the Voice Forms feature. It allows a transcriber to log in to a voice form, listen to the recorded responses, and transcribe them.

When to use

Create a VSDN for the Transcription Service if you want it to be directly accessible by dialing a number.

Types of transcription services

You can create two different types of Transcription Services:

- a service that retrieves any voice form as specified by the transcriber
- a service that retrieves a specific voice form as defined in the Add DN Information screen

Application 1: General transcription service

In this application, when the transcriber logs on to the service, he or she is prompted for the ID of the voice form to be transcribed. This allows the transcriber to access any existing voice form.

If you want to create only one Transcription Service, create this kind and leave it up to the transcriber to decide which voice form to retrieve.

For this application, do not enter a Voice Form ID when adding the VSDN.

Application 2: Voice-form specific

In this application, a particular voice form is associated with the VSDN. Whenever the VSDN is dialed, that voice form is automatically retrieved for transcription. You can have multiple transcription VSDNs so that a number of voice forms can be called up directly depending on the VSDN that was dialed.

You may want to do this if you have just implemented a voice form to which you expect a lot of responses, and you, therefore, want to have it transcribed frequently.

For this application, enter a Voice Form ID when adding the VSDN.

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Procedure

To create a VSDN for the Transcription Service, follow these steps.

Starting Point: The VSDN table.

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN.
3	Enter TR in the Service field. **Result:** The Voice Form ID field is displayed.

```
                    Voice Services Administration
Add DN Information

Choice of Services:
AS  Announcement Service  CA  Call Answering        EM  Express Messaging
FI  Fax Info Service      FIM Fax Item Maintenance  PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Access DN:        3710

Service:          TR     Voice Form ID: _______

Comment:          General Transcriber

Select a softkey >

   Save        Cancel
```

Step	Action
4	Do you want this transcription service to automatically retrieve a particular voice form? • If yes, enter the Voice Form ID. **Note:** If you have not created the voice form yet, you must enter an ID to save the VSDN. Enter an ID and use it when creating the voice form. • If no, leave the Voice Form ID field blank.

Step	Action
5	Do you want to add the VSDN with the information you have entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Adding a VSDN for the Fax Information Service

Description

The Fax Information Service is part of the Fax on Demand feature. It is used to create fax items that are sent to callers on request.

When to use

Create a VSDN for a fax item if you want users or callers to be able to access it directly by dialing a number.

Selecting the session profile

Use this table to decide which session profile you need for a fax item.

If the fax delivery mode	THEN
is callback	• choose the full-service voice session profile. or • create a custom session profile and set the channel capability to Full Voice.
is caller choice or same call	• choose the full-service multimedia session profile. or • create a custom session profile and set the channel capability to Full MultiMedia.

When to create a custom session profile

Review the configurations of the default full-service voice session profile on page 24-83 and the full-service multimedia session profile on page 24-86. If the default session profiles do not meet your needs, you must create a custom profile. See "Customizing the session profile for Voice Menus, Fax Items, and Time-of-Day Controllers" on page 24-90.

Determining how many VSDNs you need

If you want this fax item to be delivered to different caller markets (such as national and international), you may have to create multiple VSDNs. See "Determining how many VSDNs you need for a callback fax service" on page 24-78.

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Procedure

To create a VSDN for a fax item, follow these steps.

Starting Point: The VSDN table

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN.
3	Enter FI in the Service field. **Result:** The Fax Item ID and Session Profile fields are displayed. The [Session Profile Detail] softkey is also displayed.

```
                    Voice Services Administration
Add DN Information

Choice of Services:
AS  Announcement Service  CA  Call Answering        EM  Express Messaging
FI  Fax Info Service      FIM Fax Item Maintenance  PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Access DN:        3752

Service:          FI      Fax Item ID: 4450

Session Profile:  Custom Full_MultiMedia Full_Voice

Comment:          Directions Fax

Select a softkey >

Save    Cancel    Session Profile Detail
```

Step	Action
4	Enter the Fax Item ID. **Note:** If you have not created the fax item yet, you must enter an ID to save the VSDN. Enter an ID and use it when creating the fax item.
5	Do you need to create a custom session profile? • If yes, see the section "Session profiles" on page 24-67 and then go to step 9. • If no, go to step 6.
6	Select one of the predefined session profiles (Full Voice or Full MultiMedia).

Step	Action
7	Do you want to view the session profile? • If yes, press the [Session Profile Detail] softkey. • If no, go to step 9.
8	Review the session profile and press [Return to Previous Form] when you are ready to return to the Add DN Information screen.
9	Enter an optional comment in the Comment field.
10	Do you want to add the VSDN with the information you have entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Adding a VSDN for the Fax Item Maintenance Service

Description

The Fax Item Maintenance service is part of the Fax on Demand feature. It is used to remotely maintain the content and characteristics of fax items using a telephone set. This service also allows you to verify changed content by sending a verification fax to a specified fax number.

When to use

Create a VSDN for the Fax Item Maintenance service if you want to be able to access it directly by dialing a number.

Selecting the session profile

You must use the full-service multimedia session profile or create a custom profile with channel capability set to Full Multimedia.

Do you need a custom session profile?

Review the configuration for the default full-service multimedia session profile on page 24-86. If the default session profile does not meet your needs, you must create a custom profile. See "Customizing the session profile for the Fax Item Maintenance Service" on page 24-109.

Before you begin

Access the VSDN table if you are not already at the screen. See "Accessing the VSDN table" on page 24-7.

Procedure

To create a VSDN for the Fax Item Maintenance service, follow these steps.

Starting Point: The VSDN table

Step	Action
1	Press the [Add] softkey. **Result:** The Add DN Information screen is displayed.
2	Enter the Access DN.

Step	Action
3	Enter FIM in the Service field. **Result:** The Session Profile field and [Session Profile Detail] softkey are displayed. If more than one language is installed, the Language of Service field is displayed.

```
                        Voice Services Administration
Add DN Information

Choice of Services:
AS  Announcement Service  CA  Call Answering        EM  Express Messaging
FI  Fax Info Service      FIM Fax Item Maintenance  PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Access DN:        3759

Service:          FIM     Language of Service:   American_English
                                                 Canadian_French
Session Profile:  Custom Full_MultiMedia

Comment:          Fax Maintenance

Select a softkey >

   Save        Cancel      Session
                           Profile Detail
```

Step	Action
4	If more than one language is installed, select the language of service. **Note:** This is the language in which system prompts are played while using the fax item maintenance service.
5	Do you need to create a custom session profile? • If yes, see the section "Session profiles" on page 24-67 and then go to step 9. • If no, go to step 6.
6	Select the Full MultiMedia profile.
7	Do you want to view the session profile? • If yes, press the [Session Profile Detail] softkey. • If no, go to step 9.
8	Review the session profile and press [Return to Previous Form] when you are ready to return to the Add DN Information screen.

Step	Action
9	Enter an optional comment in the Comment field.
10	Do you want to add the VSDN with the information you have entered? • If yes, press the [Save] softkey. • If no, press [Cancel], or make any necessary corrections and then press [Save]. **Result:** You are returned to the VSDN table. If you pressed the [Save] softkey, there is now a new entry in the table for this DN.

Section E: Session profiles

In this section

What is a session profile?	24-68
How session profiles work when multiple services are invoked by one VSDN	24-70
How Meridian Mail 9/10 session profiles are converted to Meridian Mail 12 session profiles	24-72
Fax callback number formats	24-74
Determining how many VSDNs you need for a callback fax service	24-78
The basic service session profile	24-81
The full-service voice session profile	24-83
The full-service multimedia session profile	24-86
Customizing the session profile for Voice Menus, Fax Items, and Time-of-Day Controllers	24-90
Specifying the channel capability, session time limit, and maximum number of invalid selections	24-92
Specifying fax service options	24-96
Specifying callback delivery options	24-102
Creating a custom cover sheet	24-107
Customizing the session profile for the Fax Item Maintenance Service	24-109

What is a session profile?

Description

A session profile is a set of operational characteristics that determines how the following features work:

- Voice Menus
- Time-of-Day Controllers
- the Fax Information Service (Fax Items)
- the Fax Item Maintenance Service

A session profile is required when you add a VSDN for any of these services.

Example

A session profile for a Voice Menu that invokes Fax on Demand services controls the following aspects (among others) of Voice Menu operation:

- the maximum session length
- the maximum number of invalid menu selections
- the maximum number of faxes that a caller can select
- how fax transmission errors are handled

When session profiles are required

The session profile is selected or defined when you add the VSDN. You can either

- select a predefined session profile
- create a custom session profile

You cannot create a session profile for one of these services if it does not have a VSDN. Session profiles are necessary only if a VSDN is necessary.

Three predefined profiles

There are three predefined session profiles to choose from. The names of the profiles indicate the type of ports that will be used.

Profile	Described on page
Basic service session profile	24-81
Full-service voice session profile	24-83
Full-service multimedia session profile	24-86

Custom session profiles

The three predefined session profiles cannot be modified in any way. If none of the three preconfigured session profiles meets your requirements for a particular service, you must create a custom session profile.

A session profile is customized for only one service (the service for which you are adding a VSDN). You cannot share the same custom session profile among a number of services.

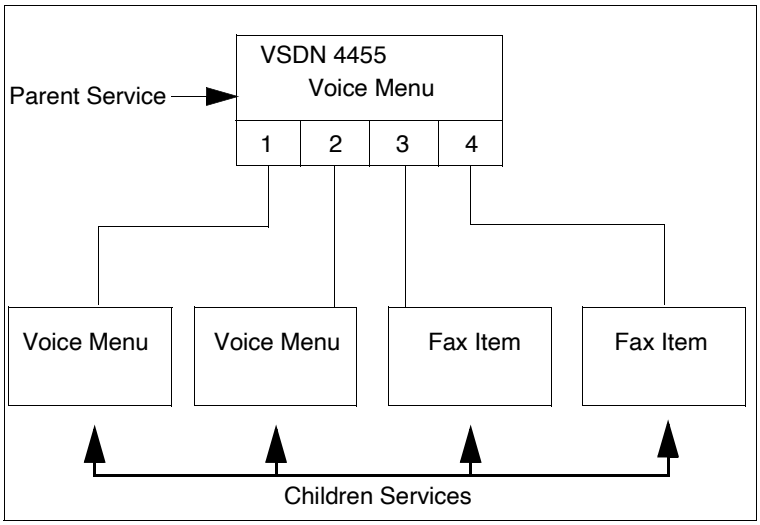
How session profiles work when multiple services are invoked by one VSDN

Introduction

Some services have the ability to invoke, or start up, other services. Two such services are Voice Menus and Time-of-Day Controllers.

Parent versus children services

When you create a Voice Menu or Time-of-Day Controller that invokes other services, it is considered the "parent" service. The services it invokes are the "children" services.



The parent service

The parent service must have a VSDN since this is the service through which users or callers gain access to the other services. The parent service will, therefore, also have a session profile associated with it.

Children services

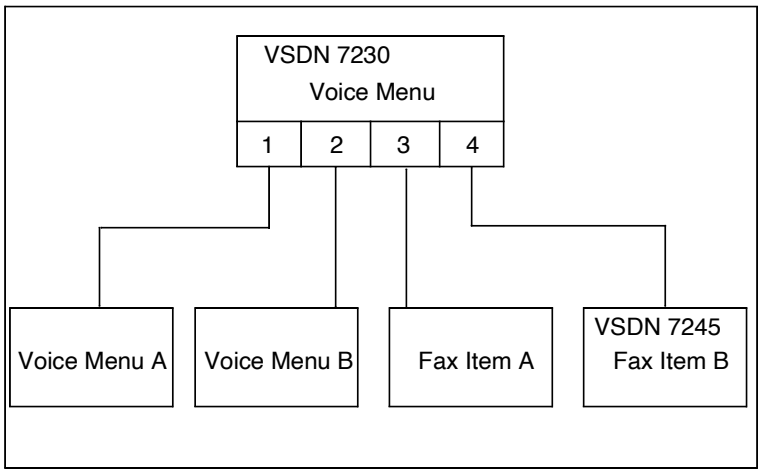
The session profile of the parent service is applied to all children services. If, however, you need a different session profile for one or more of the children services, you can add a VSDN for the child service and, therefore, give it a different session profile.

The VSDN of the child service does not need to be known to callers or users. It is not directly dialed.

Example

In this example, you have a Voice Menu that invokes four other services. The first three services, Voice Menu A, Voice Menu B, and Fax Item A do not have VSDNs. They use the session profile of the parent Voice Menu.

However, since a different session profile was needed for Fax Item B, a separate VSDN was created for this item and a unique session profile could, therefore, be created. The fourth option in this menu is set to call this VSDN.



How Meridian Mail 9/10 session profiles are converted to Meridian Mail 12 session profiles

Introduction

The following three fields that were in Meridian Mail 9 and Meridian Mail 10 session profiles have been replaced by one field, Treat Call Back Number As, in Meridian Mail 12:

- Call Back Number Area Code Translation
- Call Back International DDD
- IDDD Prefix

Description of changes

Call Back Number Area Code Translation

This field could be set to North American and None. This field no longer applies. Due to enhancements, dialing translations of numbers outside North America are now fully supported.

Call Back International DDD

This field was used to define whether international call back delivery was required, optional, or not allowed. This functionality is directly replaced by the new field.

IDDD Prefix

This field was used only if Call Back International DDD was set to optional. It allowed callers to indicate whether they wanted call back delivery to an international location or a national location relative to the Meridian Mail system. As of Meridian Mail 11, a service is set up either as National or International. There is, therefore, no longer a need for this field.

How profiles were converted

When you converted to Meridian Mail 12, any existing session profiles were automatically converted. The only field that was used in the conversion was the Call Back International DDD field.

This table shows how the old session profile field was mapped to the new field.

WHEN the Call Back International DDD field was	THEN the Treat Call Back Number As field was set to
Required	International.
Optional	International.
Not Allowed	National.

Optional Call Back International DDD

If you had any session profiles in which the Call Back International DDD field was set to Optional, callers who dial that VSDN are now prompted to enter call back numbers in the international format (country code + area/city code + fax number). They do not have the option of entering a number in the national format (area/city code + fax number).

Options

You can leave these services as is. However, if you want to give callers the opportunity to enter either a national number or an international number, you can do one of the following.

- Set up a “National” VSDN for the same service and publish this number.
- Create a Voice Menu as a front end to the service that allows callers to select national or international.

  This solution means that you do not have to publish another number. See “Determining how many VSDNs you need for a callback fax service” on page 24-78.

Fax callback number formats

Introduction

Session profiles for fax services or services that invoke fax services must specify the fax delivery method. When the fax delivery method is call back, the fax is delivered on a separate call. Callers are prompted to enter a call back number during the session. When the session is terminated, Meridian Mail phones the callback number in order to deliver the fax.

When the delivery method is call back or caller choice (in which case the caller might choose call back), the callback number format must be specified.

Description: callback number formats

When a caller enters a callback number, it must be translated into a number that Meridian Mail can dial so that the fax can be delivered.

This means that callers must enter callback numbers in certain formats depending on where they are located relative to the Meridian Mail system.

Example

Your Meridian Mail system is located in California.

Caller is located in Washington
Since the caller's country code is the same as yours, the caller needs to enter the callback number in the following format:

area/city code + fax phone number

Caller is located in France
Since the caller's country code is different from yours, the caller must enter the callback number in the following format:

country code + area/city code + fax phone number

Caller is an employee on your ESN network
An employee that is on your ESN network should specify the ESN number of the receiving fax machine in the format:

ESN prefix + fax phone extension

Callback number treatment

The format in which callers must enter their callback number is specified in the Treat Call Back Number As field in the Session Profile. There are four callback number treatment options:

- National
- International
- Dial as Entered
- ESN2

National

Purpose

This option is for services aimed at callers within your country code.

Both local and long distance callers need to enter the area/city code.

The prompt

Callers hear the following prompt when this option is chosen.

"Please enter the fax number, including area or city code, followed by number sign."

International

Purpose

This option is for services aimed at international callers that have country codes different from yours.

Local and long distance callers within your country code can use this type of service. However, they need to know their country code. The number cannot be processed without the country code.

The prompt

Callers hear the following prompt when this option is chosen.

"*Please enter the fax number, including country code and area or city code, followed by number sign."*

Dial as Entered

Purpose

This option is for services aimed at callers that

- are on the same switch
- are within the same Coordinated Dialing Plan (CDP) as the Meridian Mail system
- want to be able to enter a call back in any format (perhaps because they travel a lot), and know how to enter a call back number so that it is dialable from the Meridian Mail system

The prompt

Callers hear the following prompt.

"Please enter the fax number, followed by number sign."

Publish required formats

For callers who will be using this type of service, such as a sales force that travels extensively, provide written instructions for the required formats based on situation.

For example:

Within the head office:	*Enter the four-digit extension of the fax machine. Example: 7100*
For an ESN site:	*Enter 6 followed by your ESN fax number. Example: 6 333-7100*
For a local external call:	*Enter 9 followed by your fax number. Example: 9 555-7100*
For a long-distance call:	*Enter 91 followed by your area code and fax number. Example: 91 519 555-7100*

ESN

Purpose

This option is for callers (employees) who are on your ESN network.

The prompt

Callers hear the following prompt when this option is chosen.

"Please enter the ESN number of the fax machine followed by number sign."

Translation of callback numbers

Once a callback number is entered, Meridian Mail translates it into a dialable number. All callback formats, except Dial As Entered, require translation.

The way in which Meridian Mail should translate each callback format is defined in translation tables. This is described in Chapter 17, "Dialing translations".

Determining how many VSDNs you need for a callback fax service

Limitation

When the Fax Delivery Option field is set to Call Back or Caller Choice, you can choose only one of the four types of call back treatments (national, international, dial as entered, or ESN).

Consequence

This means that if you want to be able to deliver the same Fax Item to more than one of the following — national numbers, international numbers, ESN numbers, or any number — you must choose one of the following strategies:

- Create separate VSDNs for each required call back format.
- Create a Voice Menu as a front end.
- Create only one VSDN.

Option 1: separate VSDNs

Set up separate VSDNs for each caller market, with corresponding marketing materials that instruct callers to use the number that is appropriate for them (depending on their location).

Option 2: Voice Menu

Create a Voice Menu as a front end that allows callers to specify where their fax machine is located and how they need to enter the call back number.

You still need to create multiple VSDNs as described in the example on page 24-79. However, only the VSDN of the Voice Menu needs to be published to callers.

Option 3: a single VSDN

Create a single VSDN for all callers; that is, set up for international call back. Callers are always prompted to include their country code as part of the fax number, even if they are within the same country code.

This is the least effective solution since many people who are unfamiliar with international dialing may not know their own country code.

Example: creating a Voice Menu as a front end

Your company is located in Boston. You have a new product bulletin that you want to make available to your North American customers. However, you also have a strong European customer base, so you also want to make this fax bulletin available to your European customers. You want to create only one set of marketing materials and publish one number for both caller markets.

Setup

To set up this service, you must do the following.

1. Create a Fax Item.

   For example, Fax 1.

2. Add a VSDN (4110) for Fax 1.

   In the session profile, set the Treat Call Back Number As field to International.

   Callers do not have to know this VSDN.

3. Create the Voice Menu.

   - Make menu choice 1 invoke Fax Item 1.
   - Make menu choice 2 call (CL) the VSDN 4110.
   - Record a menu choices prompt that instructs callers on what to do.
     "If your fax machine is in North America, press 1. If your fax machine is in any other country, press 2."

4. Add a VSDN for the Voice Menu (4009).

   In the session profile, set the Treat Call Back Number As field to National.

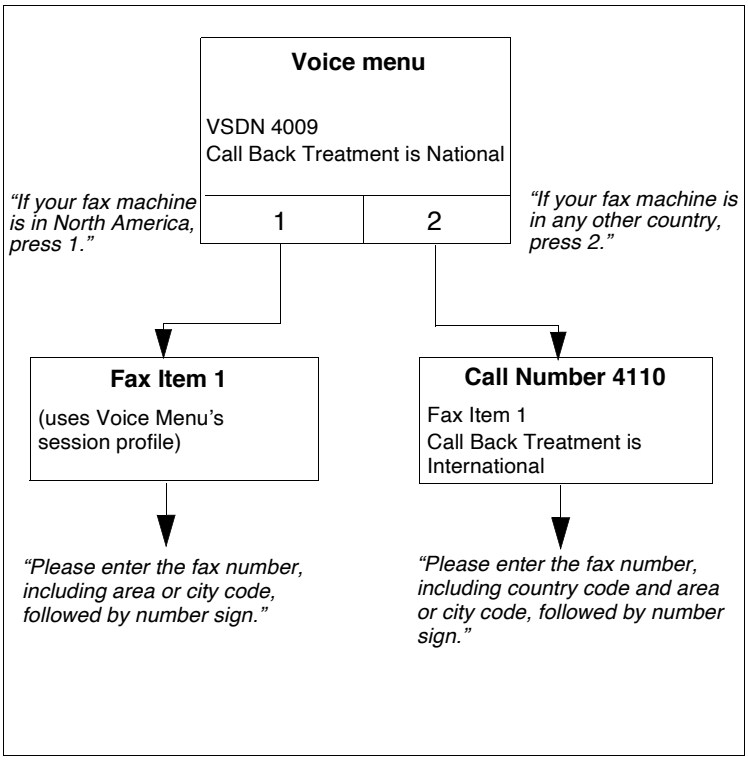
   The VSDN of this Voice Menu is the number you publish to callers.

Result

When a caller presses 1, the session profile for the Voice Menu is used. The caller is prompted to enter an area/city code and the fax number.

When a caller presses 2, VSDN 4110 is called. The session profile for this VSDN, therefore, is used. The caller is prompted to enter a country code, area/city code, and the fax number

.



The basic service session profile

When to use

You can use the Basic Service Session Profile for Voice Menus and Time-of-Day Controllers that run services that require basic service voice ports only. These services are

- Meridian ACCESS or IVR applications
- Announcements
- Thru-Dial Services
- Voice Prompt Maintenance
- Remote Activation
- Voice Menu commands (such as Call, Play Prompt, and Repeat Menu Choices)
- Time-of-Day Controllers and Voice Menus that invoke only the above services

The profile

This is the Basic Service Session Profile. It is a read-only screen. This screen is used when adding VSDNs and is accessible from the Add DN Information screen for Voice Menus and Time-of-Day Controllers.

```
                    Voice Services Administration
Session Profile

Channel Capability Required:          Full_MultiMedia Full_Voice Basic

Session Time Limit(minutes):          10

Maximum Number of Invalid Selections: 10

Select a softkey >

 Return to
Previous Form
```

Profile configuration

When you choose the Basic Service Session Profile, the following characteristics and controls are placed on the service:

- Basic service channels are used.
- The Voice Menu or Time-of-Day Controller session is limited to a maximum of 10 minutes.
- The maximum number of invalid selections that a caller can make in a Voice Menu is 10.

The full-service voice session profile

When to use

The following services require channels with a minimum channel capability of full-service voice:

- Fax Items that use the callback delivery option
- Voice Menus and Time-of-Day Controllers that invoke any service except
  - Fax Items that use same call or caller choice as the delivery mode
  - the Fax Item Maintenance Service

The profile

This is the full-service voice session profile. It is a read-only screen. This screen is used when adding VSDNs and is accessible from the Add DN Information screen for Voice Menus, Time-of-Day Controllers, and Fax Items.

Part 1

```
                    Voice Services Administration
Session Profile

Channel Capability Required:          Full_MultiMedia Full_Voice Basic

Session Time Limit(minutes):          10

Maximum Number of Invalid Selections: 10

Maximum Number of Fax Selections:     5

Page Limit for Fax Selections:        40

Fax Activity Revert DN:

Sender Fax Number:

Sponsor Fax Item ID:

                                                                MORE BELOW
Select a softkey >

 Return to
Previous Form
```

Note: If Fax on Demand is not installed, only the first three fields are displayed.

Part 2

```
                    Voice Services Administration                MORE ABOVE
Session Profile

Billing DN:

Page Transmission Error Handling:     Quit Continue

Fax Delivery Option:                  Call_Back Same_Call Caller_Choice

Call Back Extension Prompt:           No Yes

Treat Call Back Number As:            National International Dial_as_Entered ESN

Automatic Cover Sheet:                No Yes

Sender Name Display:

Call Back Dialing Restrictions:       2    List Name:  Local
Select a softkey >

 Return to
Previous Form
```

Profile configuration

When you choose the full-service voice session profile, the following characteristics and controls are placed on the service.

General characteristics and limitations

These limitations are applied to all Voice Menus, Fax Items, and Time-of-Day Controllers to which you assign the full-service voice session profile:

- Full-service voice channels are used.
- The length of the session is limited to 10 minutes.
- The maximum number of invalid selections a caller can make in a Voice Menu is 10.

Fax on Demand

These limitations and controls do not apply if Fax on Demand is not installed or if you are adding a VSDN for a service that does not invoke any fax services:

- For Voice Menus that invoke Fax Items, the maximum number of faxes a caller can select during one call session is 5. For Fax Items, the maximum is 1.
- The maximum number of pages that can be transmitted during a session is 40.
- If an error occurs during transmission of a fax page, the error is ignored and the next page is transmitted.

- The fax delivery option is call back. This means that callers do not have to make the call on a fax phone since they are prompted for a callback number. After the session is terminated, the fax is delivered to the specified number as long as it is not restricted.
- Callers are prompted for an extension number in addition to the callback number. This number is printed on the automatic cover sheet so that the fax can be delivered to the right person.
- The callback number is treated as a national number. This means that the callback number entered by callers must be within the same country code as your system.
- A system-generated cover sheet is attached to the fax.
- Restriction/Permission List 2 (named Local by default) is applied to call back delivery.

The full-service multimedia session profile

Introduction

This session profile is available only if you have multimedia ports installed on your Meridian Mail system.

When to use

You must use the full-service multimedia session profile or create a custom session profile with multimedia channel capability for the following types of services:

- Fax Items that you want delivered on the same call
- Fax Items for which you want the caller to choose the delivery mode (callback or same call)
- the Fax Item Maintenance Service
- Voice Menus and Time-of-Day Controllers that invoke any of the above fax services

The profile: for MS, TD, FI

When you select the default MultiMedia session profile in the Add DN Information screen for a Voice Menu (MS), Time-of-Day Controller (TD), or Fax Item (FI), this version of the screen is displayed. It is a read-only screen.

Part 1

```
                    Voice Services Administration
Session Profile

Channel Capability Required:          Full_MultiMedia Full_Voice Basic

Session Time Limit(minutes):          10

Maximum Number of Invalid Selections: 10

Maximum Number of Fax Selections:     5

Page Limit for Fax Selections:        40

Fax Activity Revert DN:

Sender Fax Number:

Sponsor Fax Item ID:

                                                                MORE BELOW
Select a softkey >

 Return to
Previous Form
```

Note: If the service is FI, Basic is not displayed in the Channel Capability Required field.

Part 2

```
                    Voice Services Administration                MORE ABOVE
Session Profile


Billing DN:

Page Transmission Error Handling:     Quit Continue

Fax Delivery Option:                  Call_Back Same_Call Caller_Choice

Call Back Extension Prompt:           No Yes

Treat Call Back Number As:            National International Dial_as_Entered ESN

Automatic Cover Sheet:                No Yes

Sender Name Display:

Call Back Dialing Restrictions:       2     List Name:  Local          ▌
------------------------------------------------------------------------
Select a softkey >

 Return to
Previous Form
```

Profile configuration

When you choose the full-service multimedia session profile, the following characteristics and controls are placed on the service.

General characteristics and limitations

These limitations are applied to all Voice Menus, Fax Items, and Time-of-Day Controllers to which you assign the full-service multimedia session profile:

- Full-service multimedia channels are used.
- The length of the session is limited to 10 minutes.
- The maximum number of invalid selections a caller can make in a Voice Menu is 10.

Fax on Demand

These following limitations and controls do not apply if Fax on Demand is not installed or if you are adding a VSDN for a service that does not invoke any fax services:

- For Voice Menus that invoke Fax Items, the maximum number of faxes a caller can select during one call session is 5. For Fax Items, the maximum is 1.
- The maximum number of pages that can be transmitted during a session is 40.
- If an error occurs during transmission of a fax page, the error is ignored and the next page is transmitted.
- Fax delivery is set to caller choice. This means the caller can request to have the fax delivered on the same call (to the fax phone on which the caller placed the call) or can specify the callback number of the fax phone to which he or she wants the fax delivered.
- If the caller chooses callback delivery, the caller is prompted for an extension number in addition to the callback number. This number is printed on the automatic cover sheet so that the fax can be delivered to the right person.
- The callback number is treated as a national number. This means that if a caller chooses callback delivery, the callback number entered by callers must be within the same country code as your system.
- A system-generated cover sheet is attached to the fax.
- Restriction/Permission List 2 (named Local by default) is applied to callback delivery.

The screen: FIM

This is the full-service multimedia session profile. This version of the screen is displayed when you are adding a VSDN for the Fax Item Maintenance Service. It is a read-only screen.

```
                    Voice Services Administration
Session Profile

Channel Capability Required:          Full_MultiMedia

Sender Fax Number:                    [redacted]

Billing DN:

Page Transmission Error Handling:     Quit Continue

Treat Call Back Number As:            National International Dial_as_Entered ESN

Call Back Dialing Restrictions:       2     List Name:  Local

Select a softkey >

 Return to
Previous Form
```

Profile configuration

When you choose the full-service multimedia session profile, the following characteristics and controls are placed on the Fax Item Maintenance Service:

- Full-service multimedia channels are used.
- If an error occurs during transmission of a verification fax page, the error is ignored and the next page is transmitted.
- The callback number is treated as a national number. This means that if a caller chooses callback delivery, the callback number entered by callers must be within the same country code as your system.
- The fax verification number is checked against Restriction/ Permission List 2 (named Local by default).

Customizing the session profile for Voice Menus, Fax Items, and Time-of-Day Controllers

Introduction

If the default session profiles do not meet your requirements for a particular service, create a custom session profile.

The custom Session Profile screen

This is the custom Session Profile screen for Voice Menus, Fax Items, and Time-of-Day Controllers.

Part 1

```
                    Voice Services Administration
Session Profile

Channel Capability Required:          Full_MultiMedia Full_Voice Basic

Session Time Limit(minutes):          10

Maximum Number of Invalid Selections: 10

Maximum Number of Fax Selections:     5

Page Limit for Fax Selections:        40

Fax Activity Revert DN:               ____________________________

Sender Fax Number:                    ___________________

Sponsor Fax Item ID:                  _______
                                                                MORE BELOW
The Session Profile will be saved only if the Previous Form is saved.

 Return to
Previous Form
```

Note: If Fax on Demand is not installed on your system, only the first three fields in this screen are displayed.

Part 2

```
                    Voice Services Administration          MORE ABOVE
Session Profile

Billing DN:                           ____________________________

Page Transmission Error Handling:     Quit Continue

Fax Delivery Option:                  Call_Back Same_Call Caller_Choice

Call Back Extension Prompt:           No Yes

Treat Call Back Number As:            National International Dial_as_Entered ESN

Automatic Cover Sheet:                No Yes

Sender Name Display:                  ___________________

Call Back Dialing Restrictions:       2_    List Name:  Local
The Session Profile will be saved only if the Previous Form is saved.

 Return to
Previous Form
```

Procedure

Following is a high-level procedure for creating a custom session profile. Detailed procedures are provided on the corresponding pages.

Step	Action	See page
1	Specify the channel capability, session time limit, and maximum number of invalid selections. **Requirement:** This step is necessary for all Voice Menus, Fax Items, and Time-of-Day Controllers.	24-92
2	Specify fax service options. **Requirement:** This step is necessary if the service you are defining is a Fax Item or a Voice Menu or Time-of-Day Controller that invokes a fax service.	24-96
3	Specify call back delivery options. **Requirement:** This step is necessary if step 2 was necessary and if the fax delivery option for the service is Call Back or Caller Choice.	24-102

Specifying the channel capability, session time limit, and maximum number of invalid selections

When to use

For all Voice Menus, Fax Items, and Time-of-Day Controllers, you must

- select the channel capability that is appropriate to the service for which you are adding a VSDN
- specify the session time limit
- specify the maximum number of invalid selections

If Fax on Demand is not installed, or if you are defining a VSDN for a Voice Menu or Time-of-Day Controller that does not invoke fax services, this is all you have to do to customize the session profile.

Fields in the Session Profile screen

Relevant fields are highlighted by the dotted box.

```
                    Voice Services Administration
Session Profile
Channel Capability Required:          Full_MultiMedia Full_Voice Basic

Session Time Limit(minutes):          10

Maximum Number of Invalid Selections: 10

Maximum Number of Fax Selections:     5

Page Limit for Fax Selections:        40

Fax Activity Revert DN:               ____________________________

Sender Fax Number:                    ___________________

Sponsor Fax Item ID:                  _______
                                                                MORE BELOW
The Session Profile will be saved only if the Previous Form is saved.

 Return to
Previous Form
```

Field descriptions

These fields are used by all services (Voice Menus, Fax Items, and Time-of-Day Controllers).

Channel Capability Required	
Description	The type of port that the service will use.
Valid Options	Full MultiMedia, Full Voice, Basic
See Also	Certain kinds of services require certain kinds of ports. See "Choosing the channel capability" on page 24-94.

Session Time Limit (minutes)	
Description	This is the maximum amount of time that a call session can last.
Default	10 minutes
Valid Range	0 to 99 (minutes)

Maximum Number of Invalid Selections	
Description	This field applies to Voice Menus and Fax Items. Each time a caller makes an invalid selection, an error counter is incremented by one.
Action taken	If this limit is reached, one of the following happens. • When the menu does not contain Fax Items, the session is terminated. • When the menu contains Fax Items or when a Fax Item is accessed directly, the following message is played. *"You have reached the maximum number of selections that may be made in one call. If you would like to make additional selections, please call in again."*
Security	To make it difficult for hackers to abuse your system via a voice menu, this field should be set to a relatively low number (for example, the default of 10).
Default	10
Valid Range	1 to 99

Choosing the channel capability

Use the following table to choose the channel capability that is required for a particular service.

IF the service is	AND	THEN select
a Voice Menu or a Time-of-Day Controller	it invokes one or more of the following services *only:* • ACCESS applications (such as IVR) • Announcements • Thru-Dial services • Voice Prompt Maintenance • Remote Activation • Voice Menu commands (such as Call, Play Prompt, or Repeat Menu Choices) • other Voice Menus or Time-of-Day Controllers that invoke the above services only	Basic.
	it invokes any of the following: • Voice Messaging • Express Messaging • Call Answering • Fax Items using callback delivery mode • other Voice Menus or Time-of-Day Controllers that invoke any of the above services	Full Voice.
	it invokes any of the following: • Fax Item maintenance • Fax Items using same call or caller choice delivery mode	Full MultiMedia.
a Fax Item	the fax delivery mode is call back	Full Voice.
	the fax delivery mode is same call or caller choice	Full MultiMedia.

Customizing the session profile

To begin customizing the session profile for a Fax Item, Voice Menu, or Time-of-Day Controller, follow these steps.

Starting Point: The Add DN Information screen

Step	Action
1	Select Custom in the Session Profile field.
2	Press the [Session Profile Detail] softkey. **Result:** The Session Profile screen is displayed.
3	Select the channel capability that is required for the service. **Note:** See “Choosing the channel capability” on page 24-94.
4	Change the current session time limit if necessary.
5	Change the maximum number of invalid selections if necessary.
6	Are you adding this VSDN for a Fax Item or for a Voice Menu or Time-of-Day Controller that invokes fax services? • If yes, go to “Specifying fax service options” on page 24-96. • If no, set the Maximum Number of Fax Selections to 0 and press [Return to Previous Form]. You are done customizing the session profile. The session profile will be saved when you save the VSDN.

Specifying fax service options

When to use

You must specify fax service options if you are defining a VSDN for

- a Fax Item
- a Voice Menu or Time-of-Day Controller that invokes fax services

Fields in the Session Profile screen

These are the fields in which you specify fax service options.

```
                    Voice Services Administration                MORE ABOVE
Session Profile

Maximum Number of Fax Selections:     5

Page Limit for Fax Selections:        40

Fax Activity Revert DN:               3600

Sender Fax Number:                    4165553500

Sponsor Fax Item ID:                  4455

Billing DN:

Page Transmission Error Handling:     Quit Continue

Fax Delivery Option:                  Call_Back Same_Call Caller_Choice
                                                                MORE BELOW
The Session Profile will be saved only if the Previous Form is saved.

 Return to
Previous Form
```

Field descriptions

This table describes the fields you use to define fax service options.

Maximum Number of Fax Selections	
Description	This is the maximum number of faxes that a caller can select during one call session.
Action taken	If this limit is reached, the following message is played. "*You have reached the maximum number of selections that may be made in one call. If you would like to make additional selections, please call in again.*"
Default	1 if you are creating a profile for a Fax Item (FI). The field cannot be modified for FI 5 if you are creating a profile for a Voice Menu (MS) or Time-of-Day Controller (TD)
Valid range	0 to 25 When this field is set to 0 (because no Fax Items are invoked by the service), the remaining fields in the screen are not displayed.

Page Limit for Fax Selections	
Description	This is the maximum number of pages that a caller can request for transmission.
Action taken	As a caller makes selections, Meridian Mail counts the total number of pages. If this maximum is reached, the caller is prohibited from making any more selections. The currently selected faxes are delivered.
Default	40
Valid range	1 to 99

Fax Activity Revert DN	
Description	This is the DN to which a caller is transferred if he or she encounters difficulties while engaged in fax-related activities.
Default	Blank
Other revert DNs	When this field is left blank, the Attendant DN defined in General Options is used. When the caller is in a Voice Menu with Fax Items, but outside the fax selections when difficulty is experienced, the caller is reverted to the revert DN that is defined for the Voice Menu.
Maximum length	30 digits

Sender Fax Number	
Description	This is the number of your sending fax machine. It identifies your system to the caller so that the caller can contact you if there was a transmission problem. It is displayed in the trim tab on the fax along with other information such as the start time of transmission and the page number.
Default	Blank

Sponsor Fax Item ID	
Description	Use this field if you want to create a custom cover sheet. This field specifies the ID of the Fax Item (the cover sheet).
How it works	The Fax Item associated with the ID entered in this field is transmitted after the automatic cover sheet (if turned on) or in place of it, and before the first caller-selected Fax Item(s).
Default	Blank
See also	For more information about customizing cover sheets, see “Creating a custom cover sheet” on page 24-107.

Billing DN	
Description	When fax delivery is callback, Meridian Mail places the call to deliver the fax. This is the number used by the owners of the system (you) for billing each fax callback delivery, if so desired.
Default	Blank When this field is left blank, the VSDN that the caller dialed is reported as the billing DN.

Page Transmission Error Handling	
Description	This field determines how Meridian Mail responds to page transmission errors.
Default	Continue
Valid Options	Continue, Quit • ***Continue*** The error is ignored and the next page is transmitted. • ***Quit*** The current delivery attempt is aborted.

Fax Delivery Option	
Description	This field determines how the selected faxes are delivered.
Default	Call Back
Channel capability	When the channel capability is Full Voice, this field is set to Call Back and cannot be modified. When the channel capability is Full MultiMedia, you can select any of the delivery options.
Valid options	Call Back, Same Call, Caller Choice • ***Call Back*** Selected faxes are delivered on a separate call. The caller is prompted to enter a call back phone number. This is the number to which the selected faxes are delivered. • ***Same Call*** The selected faxes are delivered on the same call. This means that the caller must phone from a fax phone. The faxes are delivered after the caller presses Receive on the receiving fax machine. • ***Caller Choice*** The caller chooses the fax delivery option. The caller hears the following prompt. *"To enter a fax number for later delivery, press 1. If you would like delivery during this call and are calling from a faxphone, press 2."*

Procedure

To specify fax service options, follow these steps.

Starting Point: The Session Profile

Step	Action
1	Change the maximum number of fax selections if necessary.
2	Change the page limit for fax selections if necessary.
3	If you want callers to be reverted to a specific DN if they encounter difficulties while engaged in fax-related activities, enter a Fax Activity Revert DN.
4	If you want the number of your sending fax phone to appear in the trim tab, enter this number in the Sender Fax Number field.

Step	Action
5	If you have created a custom cover sheet, enter its ID in the Sponsor Fax Item ID field.
6	If you want calls to this VSDN to be reported as a specific number (as the billing DN), enter it in the Billing DN field.
7	If an error is encountered during transmission, do you want Meridian Mail to ignore it and continue with the next page? • If yes, select Continue. • If no, select Quit.
8	If the Channel Capability is Full MultiMedia, select the fax delivery option.

IF you want	THEN select
faxes to be delivered on the same call on which the caller dialed into Meridian Mail	Same Call.
faxes to be delivered on a separate call, placed by Meridian Mail, to a call back number specified by the caller	Call Back.
callers to choose how they want their fax selections delivered (same call or call back)	Caller Choice.

9	Is the Fax Delivery Option field set to Call Back or Caller Choice? • If yes, go to “Specifying callback delivery options” on page 24-102. • If no, press [Return to Previous Form]. You are done customizing the session profile. The session profile will be saved when you save the VSDN.

Specifying callback delivery options

When to use

You must specify callback options if the Fax Delivery Option is set to Call Back or Caller Choice. In the case of caller choice, callers may choose to have faxes delivered to a callback number. It is, therefore, necessary to define callback options when the fax delivery method is up to the caller.

Fields in the Session Profile screen

The dotted box highlights the fields in which you specify call back options.

```
                    Voice Services Administration                MORE ABOVE
Session Profile

Billing DN:                                  ____________________________

Page Transmission Error Handling:            Quit Continue

Fax Delivery Option:                         Call_Back Same_Call Caller_Choice

Call Back Extension Prompt:                  No Yes

Treat Call Back Number As:                   National International Dial_as_Entered ESN

Automatic Cover Sheet:                       No Yes

Sender Name Display:                         Ex Machina_________

Call Back Dialing Restrictions:              2_   List Name: Local

The Session Profile will be saved only if the Previous Form is saved.

 Return to
Previous Form
```

Field descriptions

This table describes the fields in which you define callback options.

Call Back Extension Prompt	
Description	This field determines whether the caller is prompted for an extension number when arranging call back delivery. This extension is printed on the automatic cover sheet to ensure that the appropriate person receives the fax.
Default	Yes (the caller is prompted for an extension)
Valid Options	Yes, No

Treat Call Back Number As	
Description	This field determines the format of numbers that callers can enter for callback purposes and how the user is prompted to enter a callback number.
Default	National
Valid Options	National, International, Dial as Entered, ESN • ***National*** Only callers with callback numbers within the same country code as your system can use the service. • ***International*** Callers from other countries can use the service. • ***Dial as Entered*** Callers can enter a callback number in any format. Callers must, however, know what format is necessary depending on where they are located relative to your system. • ***ESN*** Only callers that are on your ESN network can use the service.
See also	See “Fax callback number formats” on page 24-74.

Automatic Cover Sheet	
Description	This is a system-generated cover sheet that you can choose to transmit along with selected Fax Items. In the case of caller choice delivery, this cover sheet is sent only if callback delivery is chosen.
Default	Yes
Valid Options	Yes, No
See also	If you want to create and use a custom cover sheet instead of using the automatic one, see “Creating a custom cover sheet” on page 24-107.

Sender Name Display	
Description	The sender name is displayed on the automatic cover sheet in the From field. This is typically the name of your organization or department.
Conditions of display	This field is displayed if the Automatic Cover Sheet field is set to Yes.
Default	Blank
Maximum length	20 characters

Call Back Dialing Restrictions	
Description	These are the dialing restrictions that are placed on the callback numbers that callers enter. It is important to restrict this number since you will be charged for all callback fax deliveries.
Default	Restriction/Permission List 2
Valid Options	Any of the available restriction/permission lists (1–80), or 0 to create a custom list for the service.

Procedure

To specify callback options, follow these steps.

Starting Point: The Session Profile

Step	Action
1	Do you want callers to be prompted for an extension number so that it can appear on the automatic cover sheet? • If yes, select Yes in the Call Back Extension Prompt field. • If no, select No.
2	Select the format of callback numbers to which you want to allow fax delivery in the Treat Call Back Number As field.

IF you want faxes to be delivered	THEN select
to callback numbers within your country code only	National.
to international numbers	International.
to on-switch extensions, to numbers in a CDP network, or to numbers as they are entered	Dial as Entered.
to numbers that are on your ESN network only	ESN.

3	Do you want the system-generated automatic cover sheet to be transmitted with the selected Fax Items? • If yes, select Yes in the Automatic Cover Sheet field. • If no, select No.
4	If the automatic cover sheet is enabled, do you want to identify your organization or department, or both, as the source of the fax on the cover sheet? • If yes, enter your organization's or department's name, or both, in the Sender Name Display field. • If no, leave the field blank.
5	Do you want to create a custom restriction/permission list for this service? • If yes, go to step 6. • If no, enter the number of the predefined restriction/ permission list that you want to assign to this service and go to step 8.

Step	Action
6	Enter 0. **Result:** The restriction/permission codes fields are displayed.

```
                    Voice Services Administration                MORE ABOVE
Session Profile

Call Back Dialing Restrictions:       0    List Name:  Custom

Restriction Codes:
_________________  _________________  _________________
_________________  _________________  _________________
_________________  _________________  _________________
_________________  _________________  _________________
_________________  _________________  _________________
_________________  _________________  _________________
_________________  _________________  _________________
_________________  _________________  _________________
_________________  _________________  _________________
_________________  _________________  _________________

Permission Codes:
_________________  _________________  _________________
                                                        MORE BELOW
The Session Profile will be saved only if the Previous Form is saved.

 Return to
Previous Form
```

7	Enter the restriction codes and permission codes for this service.
8	Press the [Return to Previous Form] softkey to return to the Add DN Information screen. **Note:** You are done customizing the session profile. The session profile will be saved when you save the VSDN.

Creating a custom cover sheet

Introduction

If you set the Automatic Cover Sheet field to Yes in the session profile, an automatic system-generated cover sheet will be transmitted.

The automatic cover sheet

This is the automatic cover sheet that is generated by the system.

```
<trim tab>
_____________________________________________

FACSIMILE TRANSMISSION

TO:      THE PERSON AT EXTENSION xxxx
FAX #:   nnnnnnnnnn
FROM:    sendername................
         (AUTOMATED FACSIMILE SERVICE)
PAGES:   nn (INCLUDING THIS COVER PAGE

_____________________________________________
IF THIS FACSIMILE IS NOT COMPLETELY READABLE OR IS
MISSING PAGES, PLEASE INFORM THE PERSON AT THE
EXTENSION xxxx; THEY WILL HAVE TO RE-REQUEST THE
INFORMATION FROM THIS SERVICE.
_____________________________________________
```

When to use

You might, however, want to create a custom cover sheet to replace the system-generated cover sheet, or to transmit in addition to the system-generated cover sheet.

Example

You have created a Voice Menu with Fax Items for your German customers. The system-generated cover sheet is in English. You decide to replace it with a custom cover sheet that is in German.

Creating a custom cover sheet

To create a custom cover sheet, you must do the following.

1. Create a Fax Item which will serve as the cover sheet for your service.

   For more information, refer to the *Fax on Demand Application Guide*.

2. Create a VSDN for the service (the stand-alone Fax Item or the service that invokes it).

3. Customize the session profile for the service.

   - Enter the ID of the Fax Item (that is the cover sheet) in the Sponsor Fax Item ID field.
   - If you want to suppress the system-generated cover sheet, set the Automatic Cover Sheet field to No.

Customizing the session profile for the Fax Item Maintenance Service

When to use

If the full-service multimedia session profile does not meet your requirements for the Fax Item Maintenance Service, you must create a custom session profile.

Fax delivery option

You do not have the option of choosing the fax delivery option for the Fax Item Maintenance Service. This service uses callback delivery only.

The custom Session Profile screen

This is the custom session profile for the Fax Item Maintenance Service.

```
                    Voice Services Administration
Session Profile

Channel Capability Required:          Full_MultiMedia

Sender Fax Number:                    416555500

Billing DN:                           5101

Page Transmission Error Handling:     Quit Continue

Treat Call Back Number As:            National International Dial_as_Entered ESN

Call Back Dialing Restrictions:       2    List Name:  Local


The Session Profile will be saved only if the Previous Form is saved.

 Return to
Previous Form
```

Field descriptions

This table describes the fields in the custom session profile for the Fax Item Maintenance Service.

Channel Capability Required	
Description	This is the type of port that the service will use. This field is read-only.
Default	Full_MultiMedia

Sender Fax Number	
Description	This is the number of your sending fax phone. It identifies your system to the caller so that the caller can contact you if there is a transmission problem. It is displayed in the trim tab on the fax along with other information such as the start time of transmission and the page number.
Default	Blank

Billing DN	
Description	Whenever a verification fax is sent, this is the number used by the owners of the system (you) for billing each fax callback delivery, if so desired.
Default	Blank When this field is left blank, the VSDN the caller dialed is reported as the billing DN.

Page Transmission Error Handling	
Description	This field determines how Meridian Mail responds to page transmission errors.
Default	Continue
Valid Options	Continue, Quit • ***Continue*** The error is ignored and the next page is transmitted. • ***Quit*** The current delivery attempt is aborted.

Treat Call Back Number As	
Description	This field determines the format of numbers that callers can enter for call back purposes and how the user is prompted to enter a call back number.
Default	National
Valid Options	National, International, Dial as Entered, ESN • ***National*** Only callers with callback numbers within the same country code as your system can use the service. • ***International*** Callers from other countries can use the service. • ***Dial as Entered*** Callers can enter a callback number in any format. Callers must, however, know what format is necessary depending on where they are located relative to your system. • ***ESN*** Only callers that are on your ESN network can use the service.
See also	See "Fax callback number formats" on page 24-74.

Call Back Dialing Restrictions	
Description	These are the dialing restrictions that are placed on the callback number to which the verification fax is sent. It is important to restrict this number, since you will be charged for all callback fax deliveries.
Default	Restriction/Permission List 2
Valid Options	Any of the available restriction/permission lists (1–80), or 0 to create a custom list.

Procedure

To customize the session profile for Fax Item Maintenance, follow these steps.

Starting Point: The Add DN Information screen

Step	Action
1	Select Custom in the Session Profile field.
2	Press the [Session Profile Detail] softkey. **Result:** The Session Profile screen is displayed.
3	Do you want the number of the sending fax machine to show up in the fax trim tab? • If yes, enter the number of the sending fax machine in the Sender Fax Number field. • If no, go to step 4.
4	Do you want calls to this VSDN to be reported as a specific number (as the billing DN) other than this VSDN? • If yes, enter this number in the Billing DN field. • If no, leave this field blank.
5	Do you want fax delivery to continue if an error is encountered during transmission? • If yes, select Continue in the Error Transmission Handling field. • If no, select Quit.
6	Select the kind of call back numbers to which you want to allow verification fax delivery in the Treat Call Back Number As field.

IF you want faxes to be delivered	THEN select
to call back numbers within your country code only	National.
to international numbers	International.
to on-switch extensions, to numbers in a CDP network, or to numbers as they are entered	Dial as Entered.
to numbers that are on your ESN network only	ESN.

Step	Action
7	Do you want to create a custom restriction/permission list for this service? • If yes, go to step 8. • If no, enter the number of the predefined restriction/ permission list that you want to assign to this service and go to step 10.
8	Enter 0. **Result:** The Restriction Codes and Permission Codes fields are displayed.

```
                    Voice Services Administration                MORE ABOVE
Session Profile

Call Back Dialing Restrictions:       0    List Name:  Custom

Restriction Codes:
_________________  _________________  _________________
_________________  _________________  _________________
_________________  _________________  _________________
_________________  _________________  _________________
_________________  _________________  _________________
_________________  _________________  _________________
_________________  _________________  _________________
_________________  _________________  _________________
_________________  _________________  _________________
_________________  _________________  _________________

Permission Codes:
_________________  _________________  _________________
                                                        MORE BELOW
The Session Profile will be saved only if the Previous Form is saved.

 Return to
Previous Form
```

9	Enter the restriction codes and permission codes that are appropriate for the service.
10	Press the [Return to Previous Form] softkey to return to the Add DN Information screen.

Section F: Viewing, modifying, and deleting VSDNs

In this section

Viewing and modifying a VSDN or session profile, or both 24-116
Deleting a VSDN 24-119

Viewing and modifying a VSDN or session profile, or both

The View/Modify DN Information screen

Existing VSDNs are modified in the View/Modify DN Information screen.

```
                    Voice Services Administration
View/Modify DN Information

Choice of Services:
AS  Announcement Service  CA  Call Answering        EM  Express Messaging
FI  Fax Info Service      FIM Fax Item Maintenance  PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Access DN:        3640_____________________

Service:          MS     Voice Menu ID: 4170

Session Profile:  Custom Full_MultiMedia Full_Voice Basic

Comment:          New Products

Select a softkey >

   Save      Cancel    Session
                       Profile Detail
```

See also

Fields in the View/Modify DN Information screen vary depending on the service for which you are modifying a VSDN. The fields are, however, identical to the ones in the Add DN Information screens.

For more information about DN information for a particular service, see the following sections:

- Section B: Adding messaging VSDNs on page 24-11.
- Section C: Adding networking and ACCESS VSDNs on page 24-27.
- Section D: Adding voice service and fax service DNs on page 24-39.

Using the find function

If many VSDNs have been defined on your system, you can use the Find function to retrieve a subset of VSDNs first, and then choose from this smaller list of VSDNs.

See Chapter 22, “Finding and printing VSDNs and service definitions”.

Procedure To view or modify a VSDN, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Voice Administration. **Result:** The Voice Administration menu is displayed.

```
Voice Administration

1  Voice Messaging Options
2  Voice Security Options
3  Restriction/Permission Lists
4  Voice Services Administration
5  Outcalling Administration
6  Voice Form Definitions

Select an item >

Exit
```

Step	Action
2	Select Voice Services Administration. **Result:** The Voice Services Administration menu is displayed.

```
Voice Services Administration

1  Voice Services-DN Table
2  Voice Services Profile
3  Announcement Definitions
4  Thru-Dial Definitions
5  Time-of-Day Control Definitions
6  Voice Menu Definitions
7  Fax Item Definitions

Select an item >

Exit    Set Display Options    Find Subset of VSDNs/Services
```

Step	Action
3	Select Voice Services-DN Table. **Result:** The Voice Services-DN Table is displayed.

```
Voice Services Administration
Voice Services-DN Table

            DN                              Service        Comment
            3650                            VM             Voice Messaging
            3651                            EM             Express Messaging
            3652                            RA             Remote Activation
            3653                            PM             Prompt Maintenance
            3654                            MS  101        Main Menu
            3655                            AN             AMIS Networking
            3656                            NW             Meridian Mail Netwk
            3659                            FIM            Fax Item Maint.
            3690                            TR  1901       Transcription Serv.

Move the cursor to the item and press the space bar to select.

Exit    Add    View/Modify    Delete    Find
```

4	Move the cursor to the VSDN you want to modify, and press the spacebar to select it.
5	Press the [View/Modify] softkey. **Result:** The View/Modify DN Information screen is displayed.
6	Make the necessary modifications in the DN information screen.
7	Do you need to modify a custom session profile? • If yes, press the [Session Profile Detail] softkey. • If no, press the [Save] softkey. You are done modifying the VSDN.
8	Make the necessary changes to the session profile. **Note:** For more information, see the section "Session profiles" on page 24-67.
9	Press the [Return to Previous Form] softkey when you are done modifying the session profile.
10	Press the [Save] softkey. **Result:** The VSDN and session profile are saved.

Deleting a VSDN

The Delete DN Information screen

Existing VSDNs are deleted from the Delete DN Information screen.

```
                    Voice Services Administration
Delete DN Information

Choice of Services:
AS  Announcement Service  CA  Call Answering        EM  Express Messaging
FI  Fax Info Service      FIM Fax Item Maintenance  PM  Prompt Maintenance
RA  Remote Activation     TS  Thru-Dial Service     TD  Time-of-Day Control
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging

Access DN:        3630

Service:          AS      Announcement ID: 4104

Comment:          Directions

Select a softkey >

OK to Delete   Cancel
```

Using the find function

If many VSDNs have been defined on your system, you can use the Find function to retrieve a subset of VSDNs first, and then choose from this smaller list of VSDNs.

See Chapter 22, “Finding and printing VSDNs and service definitions”.

Procedure To delete a VSDN, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Voice Administration. **Result:** The Voice Administration menu is displayed.

```
                    Voice Administration

          1  Voice Messaging Options
          2  Voice Security Options
          3  Restriction/Permission Lists
          4  Voice Services Administration
          5  Outcalling Administration
          6  Voice Form Definitions

Select an item >

    Exit
```

2	Select Voice Services Administration. **Result:** The Voice Services Administration menu is displayed.

```
                    Voice Services Administration

          1  Voice Services-DN Table
          2  Voice Services Profile
          3  Announcement Definitions
          4  Thru-Dial Definitions
          5  Time-of-Day Control Definitions
          6  Voice Menu Definitions
          7  Fax Item Definitions

Select an item >

    Exit                Set Display      Find Subset of
                         Options         VSDNs/Services
```

Step	Action
3	Select Voice Services-DN Table. **Result:** The Voice Services-DN Table is displayed.

```
                    Voice Services Administration
Voice Services-DN Table

          DN                          Service        Comment
          3650                        VM             Voice Messaging
          3651                        EM             Express Messaging
          3652                        RA             Remote Activation
          3653                        PM             Prompt Maintenance
          3654                        MS  101        Main Menu
          3655                        AN             AMIS Networking
          3656                        NW             Meridian Mail Netwk
          3659                        FIM            Fax Item Maint.
          3690                        TR  1901       Transcription Serv.

Move the cursor to the item and press the space bar to select.

 Exit      Add      View/Modify      Delete      Find
```

4	Move the cursor to the VSDN you want to delete, and press the spacebar to select it.
5	Press the [Delete] softkey. **Result:** The Delete DN Information screen is displayed. **Note:** If the service has a session profile, you can view it before deleting by pressing the [Session Profile Detail] softkey. The profile is read-only.
6	Do you want to delete the VSDN? • If yes, press the [OK to Delete] softkey. • If no, press the [Cancel] softkey.

Chapter 25

Voice services profile

In this chapter

Overview	25-2
Timeouts	25-3
How timeouts work	25-4
Modifying the voice services profile	25-6

Overview

Introduction

This chapter provides an overview of the use of timeouts, and explanations of all the parameters of the Voice Services Profile screen.

The Voice Services Profile screen

The Voice Services Profile screen displays all the general parameters that apply to all voice services, including timeouts. Default values are assigned when the system is installed. You can modify these values by following the procedure on page 25-6.

Timeouts

Definition

Timeout values determine how long the system will wait under certain conditions before the system takes action (such as disconnecting or playing a prompt). Timeouts are important because they aid callers by playing appropriate prompts when the system has not received correct input.

Types of timeouts

There are three types of timeouts to define:

- command entry
- short disconnect
- record

Examples

The command entry timeout is used when the system does not receive an anticipated response from the caller, such as entering an extension number or making a selection from a voice menu. This allows for the system to respond with a prompt to aid the caller, transfer the call to the revert DN, or disconnect the call.

The short disconnect timeout is used for disconnecting from a Thru-Dial service or from a voice menu, because the caller has not input an extension number or selected a voice menu option, after entering the service.

The record disconnect timeout is used during recording prompts to prevent recording unnecessary silences.

How timeouts work

Description

Timeout values are used to determine how long the system waits before taking some sort of action when an expected response is not received. The three types of timeouts are explained below.

Command entry timeout

The command entry timeout is used when the system is waiting for a response from the caller. It allows you to set time parameters which, when exceeded, prompt the system for a response. The default value for command entry timeout is 3.5 seconds. The accepted values are between 1.0 and 5.0 seconds.

Command entry timeout may be used for any of the following situations.

Announcements

When announcements are accessed directly, the system will wait this amount of time before disconnecting the call. This timeout is intended to put a limit on how long a caller will remain connected if the caller stays on the line and does nothing after the announcement is played.

In the case where an announcement is played multiple times, this amount of silence will be heard between each play.

Voice menu

This timeout is used for initial no response and delayed response. You can define the action to be taken for an initial no response and delayed response in the voice menu definition.

Note: If you are using a voice menu to accept AMIS or Enterprise Networking calls, or both, set this timeout to the maximum allowed value of five seconds. If this field is set to less than five seconds, an AMIS or Enterprise Networking call, or both, may be prematurely disconnected. The initial no response action in the voice menu definition should be set to repeat menu choices.

Thru-Dial service

Command entry timeout is used if the system is waiting for an initial response (such as an extension number or name), or if the caller has provided keypad input at some point but is now delaying in providing further input.

Fax information service

With a fax information service, a caller may be prompted for an action (such as entering a callback number or extension). When the caller does not respond and the command entry timeout is exceeded, a help prompt is played. If the caller still does not enter the required information, the prompt is played a second time. If the system times out again, the caller is transferred to the revert DN defined in the session profile.

Short disconnect timeout

The short disconnect timeout is used to disconnect a call, such as when the command entry timeout has been exceeded. Callers are usually given several opportunities to provide responses before the short disconnect timeout is used.

The default value is 10.0 seconds. Valid values are from 1.0 to 30.0 seconds.

This timeout value is used in the following situations:

- disconnecting from a thru-dial service
- disconnection from a voice menu

Record timeout

This timeout value is used with the recording of prompts for voice menus, announcements, and Thru-Dial services. If during recording this amount of silence is recorded, the system will disconnect the session.

The default is 02:00 (mm:ss). Valid values are from 00:06 to 05:00. This affects all voice services other than Fax on Demand, and Voice Messaging and its associated features (login, call answering, express messaging).

Modifying the voice services profile

Introduction

The Voice Services Profile screen shows the general parameters configured for all voice services (with the exception of voice messaging services).

Procedure

To make changes to the parameters in the Voice Services Profile, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Voice Administration. **Result:** The Voice Administration screen appears.
2	Select Voice Services Administration. **Result:** The Voice Services Administration screen appears.
3	Select Voice Services Profile. **Result:** The Voice Services Profile screen appears.
4	Enter all changes you want to make to the parameters in this screen.
5	When you have made all the necessary changes, press [Save] and then [Exit] to return to the previous screen. Press [Cancel] to return to the previous screen without saving changes.

The Voice Services Profile screen

This is the Voice Services Profile screen.

```
                    Voice Services Administration
Voice Services Profile

Voice Services Volume: 1

Timeouts
   Command Entry:      3.5 seconds     Short Disconnect: 10.0 seconds
   Record (mm:ss):   02:00

Maximum Prompt Sizes for Announcements (mm:ss):          00:30
                         other voice recordings (mm:ss): 02:00

Act on AMIS/Enterprise Initiator Tone:  No Yes

Enable Update Logging:                  No Yes

Business Hours Default:       08:30 to 17:00

Holidays   Start Date         End Date        Start Time    Comments
                                                                    MORE BELOW
Select a softkey >

     Save        Cancel
```

Field descriptions

The following fields appear on the Voice Services Profile screen.

Voice Services Volume	
Description	This is a read-only field that indicates which volume contains voice services files and voice forms (if any).

Timeouts	
Description	The values you enter in the timeout fields determine how long the system will wait under certain conditions before the system takes action.
Options	The timeouts to be defined are command entry, short disconnect, and record.
See also	See “How timeouts work” on page 25-4.

Maximum Prompt Sizes for Announcements (mm:ss)	
Description	This field controls the recording length for prompts for announcement definitions. If 80% of the maximum prompt size has been recorded, a tone is played to warn that the maximum prompt size has nearly been reached. If you are recording using the [Voice] softkey, when the time limit is exceeded the recording is stopped, and the system displays “Recording stopped. The time limit was exceeded”. If you are recording using Prompt Maintenance, and exceed the time limit, the system plays “Recording has stopped. You have reached the recording limit.”
Default	00:30
Valid range	00:30 to 10:00

Maximum Prompt Sizes for other voice recordings (mm:ss)	
Description	This field controls the maximum recording length for voice menu and thru-dial service prompts that are recorded using either the administration terminal or the Voice Prompt Maintenance service. If 80 percent of the maximum prompt size has been recorded, a tone is played to warn that the maximum prompt size has nearly been reached. If you are recording using the [Voice] softkey, when the time limit is exceeded the recording is stopped, and the system displays “Recording stopped. The time limit was exceeded”. If you are recording using Prompt Maintenance, and exceed the time limit, the system plays “Recording has stopped. You have reached the recording limit.”
Default	02:00
Valid range	00:30 to 10:00

Act on AMIS/Enterprise Initiator Tone	
Description	If an AMIS call comes in through a voice service DN, the voice service will either ignore (No) or react to the AMIS tone and transfer the call to the appropriate AMIS agent (Yes).
Default	No
Valid options	Yes, No • ***No*** When selected, you have to configure a DN specifically for the AMIS service in the VSDN table. • ***Yes*** When selected, allows AMIS to share a DN with a voice menu, thru-dial service, announcement service, time-of-day controller or fax information service.

Enable Update Logging	
Description	This field determines whether a SEER is generated whenever a VSDN entry, announcement, thru-dial service, time-of-day controller, voice menu, or fax item is added, modified, or deleted.
Default	No
Valid options	Yes, No • ***Yes*** A SEER is generated. This allows you to see which operation has been performed and on which DN or service ID. • ***No*** No SEER is generated.

Business Hours Default	
Description	These are the hours that your organization is typically open from Monday to Friday. Hours that fall outside of the range defined here are considered off-hours. The hours you enter here are used as defaults in the Add a Time of Day Control Definition screen. You can however, override these defaults if necessary when defining a time-of-day controller.
Default	08:30 to 17:00

Holidays	
Description	Identify the holidays that are observed by your organization (that is, the holidays for which your organization closes). Up to 20 holidays can be defined. The holidays you specify here are used when defining time-of-day controllers.
Parameters	For each holiday, you must specify the start date, end date, and start time.
Start Date	
Description	This field is mandatory. Specify the date on which the holiday begins. The date format follows that defined under the General Administration menu, in the General options screen.
End Date	
Description	This field is optional. The date entered here determines the day on which the holiday ends. If you enter a date, it must be later than or the same as the start date. If no end date is specified, the holiday will end on the start date. If the holiday ends on a regular business day, the holiday will end at the end of the business day (5:00 p.m., for example). However, if it is a nonbusiness day, the holiday will end at the end of the day (midnight).
Start Time	
Description	This field is mandatory. Enter the time at which the holiday starts on the start date. This is usually the normal start of the business day (specified using the 24-hour clock).
Comments	
Description	This field is optional. You may enter a comment to describe the holiday you are defining.

Chapter 26

Class of Service administration

In this chapter

Overview	26-2
Section A: Introduction to Class of Service	26-3
Section B: Adding, changing, printing, and deleting System Classes of Service	26-9
Section C: Assigning Classes of Service to users	26-63

Overview

Introduction

Class of Service (COS) administration includes

- defining the system's Classes of Service (COSs) (Up to 15 COSs are permitted plus personal COSs.)
- assigning a COS for each individual user

Section A

This section is the Introduction to Class of Service. It includes concepts and types of COS.

Section B

This section gives details and procedures on creating (adding), changing, printing, and deleting System COSs.

Section C

This section discusses various factors involved with assigning users to COSs.

Section A: Introduction to Class of Service

In this section

What is a Class of Service? 26-4
System Class of Service versus Personal Class of Service 26-6
How Class of Service is administered 26-7

What is a Class of Service?

Description

A Class of Service (COS) is a template that contains information about the capabilities that a user has and the values that are assigned to specific parameters. It is essentially a method of classifying users according to their needs. When you add a user to the system, you must specify the Class of Service to which he or she belongs.

The Meridian Mail COS applies dialing restrictions to Meridian Mail features, controls Meridian Mail resources, and determines which features are available to the owner of the mailbox.

Meridian 1 classes of service

The Meridian Mail Class of Service feature should not be confused with Class of Service on the Meridian 1/SL-1 switch. Meridian 1 Class of Service applies certain dialing restrictions to lines or sets, or trunks, not to Meridian Mail features. (See "Access restrictions" in the *X11 Software Features Guide* [NTP 553-3001-305].)

Example

Before adding users, you should carefully consider the user types that you need to represent with COSs. The following scenario provides an example of the kinds of COSs you can create (add).

For instance, you might only need to add three COSs: one for secretaries, one for executives, and a standard one for all other employees. If employees in certain departments are found to have different needs, you could add one for Accounting, one for Engineering, and so on. The COSs that you end up creating will depend entirely on the types of users that you will be adding to the system.

Once you have created your COSs and added users, you may realize that a particular group of users requires some additional capabilities. You don't have to change each individual user. You only need to change the settings in the COS, and all the users assigned to that COS will automatically pick up the changes.

If an individual user requests additional functionality (or even reduced functionality) or greater mailbox storage capacity, you can do one of two things: reassign the user to another COS that meets his or her needs, or create a personal COS for that user (only if no existing COSs are adequate). Personal COSs are described in more detail in the following section.

System Class of Service versus Personal Class of Service

System COS

Up to 15 COSs can be defined. When adding a user, you will assign him or her to one of these COSs or to a Personal COS, if necessary.

Personal COS

In addition to the 15 system COSs, the personal COS will always be available when adding a user. The personal COS is a special class. It allows you to deal with those users who require capabilities that do not fit any existing COS. A mailbox with a personal COS remains independent of changes made to other COSs.

Keep in mind, however, that as the number of personal COSs increases, the task of maintaining your classes of service and users will become more difficult since they all will have to be managed.

How Class of Service is administered

Planning, adding, and assigning Classes of Service (COSs)

These are the steps involved in planning, adding, and assigning COSs.

Stage	Description
1	Plan the COSs for the system based on the known needs of the local users.
2	Add the COSs that have been planned.
3	Assign the COSs to the system.
4	Assign users to the COSs according to their needs.

Changing COS for one or several users

These are the steps involved in changing users from one COS to another.

Stage	Description
1	Analyze the users' current needs.
2	Assign the users to COSs that meet their current requirements.

Multiple Administration Terminals

If you have the Multiple Administration Terminal feature installed in your system and you are logged in at a Multiple Administration Terminal (MAT), you can only view existing Classes of Service. You cannot add, modify, or delete Classes of Service from this terminal.

Section B: Adding, changing, printing, and deleting System Classes of Service

In this section

Adding a Class of Service	26-10
The Add Class of Service screen (MMUI)	26-13
The Add Class of Service screen (VMUIF)	26-30
Assigning Classes of Service to the system	26-49
The Find Class of Service screen	26-50
Finding, listing, or printing a Class of Service	26-51
Modifying a Class of Service	26-54
Deleting a Class of Service	26-59

Adding a Class of Service

Introduction

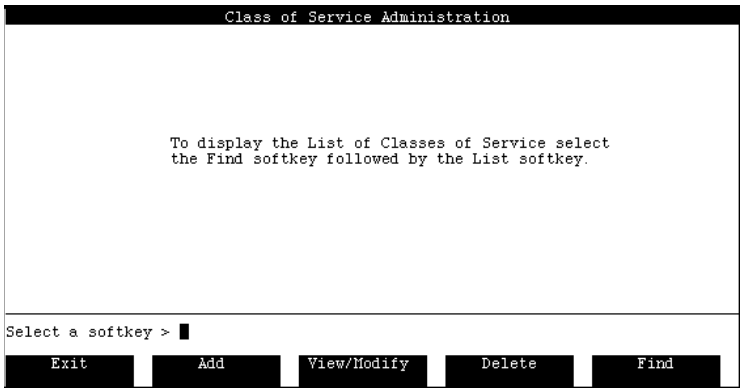
This section describes how to add a Class of Service (COS) to the system.

Procedure

To add a new class of service, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Class of Service Administration. **Result:** The following screen appears.



2	Press the [Add] softkey. **Result:** You are prompted for the class of service number.

Step	Action
3	Enter a number between 1 and 15. **Result:** The Add Class of Service screen is displayed.

```
Class of Service Administration
Add Class of Service

Class of Service Number:                1

Class of Service Name:                  _____________________

Select a softkey >

Save        Cancel        Change Defaults
```

4	Give the class of service a name. **Note:** The Voice Messaging Interface Type field is read-only and appears only if you have VMUIF installed. It cannot be modified.
5	At this point, you may save the new COS with default values, or discard the COS, or change the defaults, as follows. a. To save the COS with default values, press [Save]. b. To discard the COS, press [Cancel]. c. To change the default values for this COS, press the [Change Defaults] softkey. **Result:** Additional screens are displayed showing the default values. These fields can be modified as required to customize the COS you have added. For field descriptions, see “The Add Class of Service screen (MMUI)” on page 26-13 or “The Add Class of Service screen (VMUIF)” on page 26-30.

Adding a class of service for users with dial pulse sets

If the system was installed with the VMUIF interface and there is a possibility that some users will have dial pulse phone sets, then at least one of the VMUIF classes of service that you add should support users who have dial pulse phone sets. The following fields in the Add Class of Service screen must be configured as indicated in order to support dial pulse:

- *Dial Pulse support:* Yes
- *Auto Logon:* Yes
- *Skip to First New Message:* Yes
- *Read Message Retention:* This must be a value other than zero so that read messages are automatically deleted on a regular basis (such as every seven days).

A dial pulse user can also record a personal greeting by calling a greeting change service. If a personal greeting is not recorded, the default system greeting is played.

If a dial pulse user logs in from a phone other than his or her home phone, a mailbox and password are required. (The user must, therefore, call in from a phone with touch-tone support.) However, once logged on, the mailbox operates as if it was accessed from a household phone (no further commands are required). However, if the user does enter a DTMF command, the call reverts to the standard DTMF interface.

The Add Class of Service screen (MMUI)

Introduction

New classes of service are added to the system through the Add Class of Service screen.

MATs

Class of Service screens are read-only from Multiple Administration Terminals (MATs).

The Add Class of Service screen

The screens that follow appear when you press the [Change Defaults] softkey on the Add Class of Service screen. This is the first part of the Add Class of Service/Change Defaults screen.

```
                    Class of Service Administration
Add Class of Service
Class of Service Number:                    1
Class of Service Name:                      _____________________
Personal Verification Changeable by User:   No Yes
Voice Storage Limit (minutes):              3__
Maximum Message Length (mm:ss):             03:00
Delayed Prompts:                            No Yes
Dual Language Prompting:                    No Yes
Auto Logon:                                 No Yes
                                                                MORE BELOW
Select a softkey >
Save        Cancel
```

Field descriptions

This table gives descriptions of the fields highlighted by the broken line in the preceding screen.

Class of Service Number	
Description	This is a read-only field. This field is prefilled with the number you entered to access this screen. The COS number is used to identify the Class of Service.
Valid range	1 to 15

Class of Service Name	
Description	This is the name of the class of service. This field is mandatory. The COS definition cannot be saved if this field is blank.
Maximum length	The COS name can be up to 30 characters in length.
Valid characters	All characters are valid with the exception of “+”, “_”, or “?”, which are invalid.

Personal Verification Changeable by User	
Description	(MMUI only) If this field is set to No, only the administrator is allowed to record personal verifications for users belonging to the COS. If the field is set to Yes, users can record their own personal verifications from their telephone sets. The latter option is generally desirable since callers prefer to hear the voice of the person they are calling.
Default	The default value is No.

Voice Storage Limit	
Description	This field defines the maximum amount of storage available to the user.
How this limit is used	If messages exceed this limit, a message is played to the mailbox owner indicating that the mailbox is full and that the mailbox owner will be restricted in what he or she can do while logged in to Meridian Mail. The following restrictions are imposed: • The mailbox owner can only listen to and delete messages. • The mailbox owner cannot record a personal greeting, or compose, send, or forward messages. • After messages are deleted to reduce the storage used to below the limit, the mailbox owner must still log off and then log back in before the various mailbox functions are restored. The following conditions also exist when the mailbox is full: • Callers using Express Messaging are still allowed to leave a message. • Callers who access the Call Answering service for the user's mailbox are able to leave a message.
Affected fields	The Maximum Message Length and Maximum Call Answering Message Length cannot be greater than the Voice Storage Limit.
Default	The default value is 3 (minutes).
Valid range	You may enter a value from 1 to 360 (minutes).

Maximum Message Length	
Description	This value determines the longest possible composed message or personal greeting that a user belonging to this COS is allowed to record.
Default	The default value is 03:00.
Valid range	You may enter a value between 00:30 and 99:00 in 10-second increments.
Restrictions	This value cannot be greater than the Voice Storage Limit. If you set this field to a number that exceeds the idle login timer, message lengths will be restricted to the login timer value. The default idle login timer value is 03:00. To change this value, contact your support organization.

Delayed Prompts	
Description	When this field is set to Yes, the system will prompt users for an action if the user does not initiate any action for 3.5 seconds. It is recommended that this field be set to Yes (especially for new users). Once the users belonging to the COS are familiar with the interface, you may get requests to turn delayed prompting off. You can inform experienced users that they do not need to wait for the prompts to finish before entering a command. This field should remain set to Yes for the benefit of new users.
Default	The default is Yes.

Dual Language Prompting	
Description	(MMUI only) This field is displayed on multilingual systems only. The selection made here affects the prompts played to callers during Call Answering and Express Messaging sessions. (It does not apply to the prompts played to users while logged into their own mailboxes. The language in which prompts are played to users while logged in to Meridian Mail is determined by the field Preferred Language, in the Add or View/ Modify Local Voice User screen.)
Default Language Overrides User's Preferred Language	The "Default Language Overrides User's Preferred Language" field, which is defined in the Voice Messaging Options screen, affects which language is heard first during a call answering session, as follows: • If the Default Language Overrides User's Preferred Language field is set to No, and the user's language is different from the primary default language, callers will hear prompts in the user's preferred language followed by the primary default language. • If the Default Language Overrides User's Preferred Language field is set to No, and the user's language is the same as the primary default language, callers will hear prompts in the primary default language followed by the secondary default language. • If the Default Language Overrides User's Preferred Language field is set to Yes, callers will hear prompts in the primary default language followed by the secondary default language. Users continue to hear prompts in their preferred language during login sessions.
Default	The default is Yes.
See also	For more information about dual language prompting works, see "Setting up languages on systems with dual language prompting" on page 20-19.

Auto Logon	
Description	When this field is set to Yes, the user does not need to enter a mailbox number or password to gain access to Meridian Mail. When set to No, the user must enter a mailbox number and password. For reasons of mailbox security, this field should be set to No, unless the mailboxes of the users that will be added to this COS are in a secure location and desire this feature.
Default	The default is No.
Exceptions	Set this field to Yes if the users that will be added to this COS have requested auto logon and their phones are in a secure location. To create completely hands-free message retrieval for MMUI users, use auto logon in conjunction with auto play.
HVS users	The Hospitality Voice Messaging DN can have auto logon enabled or disabled (this is done in the VSDN table). If auto logon is enabled for the user but disabled for the DN, the setting in the VSDN table will override the setting in the user profile.

The Add Class of Service screen (cont'd)

This is the second part of the Add Class of Service/Change Defaults screen.

```
                    Class of Service Administration                MORE ABOVE
View/Modify Class of Service

Administrator Capability:                  No Yes

Broadcast Capability:                      No Yes

Network Broadcast Capability:              No Yes

Auto Play:                                 No Yes

Auto Deletion of Invalid PDL Addresses:    No Yes

Callers Notified of Busy Line:             No Yes

Prompt Played during Call Answering:       Name Number

Maximum Call Answering
Message Length (mm:ss):                    01:00
                                                                MORE BELOW
Select a softkey >

   Save        Cancel
```

Field descriptions

This table gives descriptions of the fields highlighted by the broken line in the preceding screen.

Administrator Capability	
Description	(MMUI only) If this field is set to Yes, users belonging to this COS will be allowed to record a custom call answering greeting for the system and personal verifications for all other users. For instructions on how to record a customized call answering greeting for the system, see "Recording a customized call answering greeting" on page 20-29.)
Special COS	You can set this field to Yes to add a special COS if there are any administrative assistants at the customer site who need to be able to perform these limited administrative tasks. For all other types of users, this field should be set to No.
Default	The default is No.

Broadcast Capability	
Description	Set this field to Yes if you want users to be able to compose and send broadcast messages. Broadcast messages are sent to all users at this Meridian Mail site. ***Note:*** This field cannot be set to No if the Network Broadcast Capability field is set to Yes.
Default	The default is No.

Network Broadcast Capability	
Description	(MMUI only) Set this field to Yes if you want users to be able to send network messages to all users at a specific remote site, or to any combination of sites. This field only appears if the system has Meridian Mail Networking installed. This field can only be set to Yes if the Broadcast Capability field is also set to Yes.
Default	The default is No.

Auto Play	
Description	(MMUI only) When this field is set to Yes, the messages in the user's mailbox are automatically played when the user logs on. Playback begins with the first new message. Once all new messages are played, any existing old (read) messages are then played back, starting with the oldest. However, the pound sign (#) can be pressed at any time to end playback. When this field is set to No, the user must explicitly request that each message be played by pressing <2> on the telephone keypad. Auto Play can be used in combination with Auto Logon to allow totally hands-free message retrieval.
Default	The default is No.

Auto Deletion of Invalid PDL Addresses	
Description	When this field is set to Yes, invalid addresses in categories A to D will be removed from a user's PDL in the following circumstances: • The user selects the PDL while addressing a message for Compose. • The user presses Play <2> while editing the PDL. ***Note:*** If Auto Delete is set to No, the user will be notified of the existence of bad addresses but no action will be taken to remove them.
Categories	Category A: local mailbox has been deleted Category B: network site has been deleted or COS capabilities/feature disabled. Category C: capabilities or features have been disabled (for example, delivery to non-user or AMIS) Category D: delivery to non-user or AMIS number has become restricted
Default	The default is Yes.

Callers Notified of Busy Line	
Description	When this field is set to Yes, a special prompt is played when the called line is busy, informing the caller that the user is on the phone. After the prompt is played, the caller is connected to Meridian Mail to leave a message. If the field is set to No, the normal Call Answering system greeting or personal greeting is played. ***Note:*** If the user's mailbox is associated with two (or more) DNs, they must all be busy for this prompt to be played.
Default	The default is Yes.

Prompt played During Call Answering	
Description	This field controls what type of call answering prompt will be heard by a caller if the user is on the line when another caller phones, or if the call is not answered, or if it is directed to the mailbox by a Call Answering DN. The origin of the caller (internal or external) and the types of personal greetings recorded (internal, external, temporary) are also factors in deciding which prompts will be played. For details on the interaction of these factors, see "How Call Answering uses personal greetings and personal verifications" on page 5-7.
Valid Options	Name, Number • *Name* plays the personal verification, unless it has not been recorded. • *Number* plays the phone number. In both cases, the prompt is incorporated into a system-provided message explaining that the caller has been routed to the user's mailbox.
Default	The default is Name.

Maximum Call Answering Message Length	
Description	This value determines the longest possible call answering message or Express Messaging message that a caller can record and leave in a user's mailbox.
Format	The value must be entered in the format mm:ss.
Default	The default is 01:00.
Valid range	You may enter a value between 00:30 and 99:00 in ten-second increments.
Restriction	This value cannot be greater than the Voice Storage Limit.

The Add Class of Service screen (cont'd)

This is the third part of the Add Class of Service/Change Defaults screen.

```
                    Class of Service Administration                MORE ABOV
Add Class of Service

Receive Composed Messages:                  No Yes

Message Waiting Indication Options:         None Any Urgent

External Call-Sender
Restriction/Permission List:                2   List Name:  Local

Read Message Retention (days):              0
("0" implies that read messages
are retained until the user
deletes them manually.)

Send Messages to External Users:            No Yes

Retain Copy of Sent Messages:               No Yes
                                                                   MORE BELO
Select a softkey >

   Save        Cancel
```

Field descriptions

This table gives descriptions of the fields highlighted by the broken line in the preceding screen.

Receive Composed Messages	
Description	If this field is set to No, users' mailboxes will not accept composed messages. If AMIS networking is installed, setting this field to No automatically sets the field Receive AMIS Open Network Messages to No.
Default	The default is Yes.

Message Waiting Indication Options	
Description	The chosen setting determines the type of messages that will cause a message waiting indication (a flashing light or an interrupted dial tone) on the user's telephone set. Set this field to Any to notify users of all new messages, Urgent to notify users of only those messages tagged as urgent, or None if users are not to be notified at all. This field should be set to None for users who don't have a physical telephone set, but do have a mailbox. For example, a salesperson may only rarely be at the office and does not have a phone as a result, but still requires a number for callers to leave messages.
Default	The default is Any.

External Call Sender Restriction/Permission List	
Description	This field specifies the number and name of the Restriction/Permission list that will be applied when the Call Sender feature is used to call back external callers. The lists are defined in the Restriction/Permission List screen, accessible from Voice Administration.
Requirement	To allow users to use call sender to place calls to external users, the External Call Sender Allowed field must be enabled in the Voice Messaging Options screen.
Default	The default is 2 (Local).
Valid range	This number can range from 0 to 80. The value 0 = unrestricted.

Read Message Retention (days)

Description

This field specifies the number of days that messages are kept in users' mailboxes after they have been read. The value in this field is limited by the system-wide value set in the Maximum Read Message Retention field in the Voice Messaging Options screen. For details, see "The Voice Messaging Options screen" on page 20-6.

Once the lesser of these two values is reached, read messages are automatically deleted. If 0 is entered in both fields, read messages are not automatically deleted by the system, but can be deleted only by the user.

Valid range

You can enter a value from 0 to 99.

Default

The default is 0.

Read message retention

The following table shows which value is used to determine how long the user's read messages are kept.

System retention limit	User retention limit	Amount of time read messages are kept
0 (zero)	0 (zero)	Messages are kept until the user deletes them. The system will not automatically delete read messages.
0 (zero)	A value other than zero	The user retention limit determines how long messages are kept.
A value other than zero	0 (zero)	The system retention limit determines how long messages are kept.
A value other than zero	A value other than zero	The lesser value is used to determine how long messages are kept.

Send Messages to External Users

Description

This field is not applicable to single-customer systems (that is, systems that do not have the Meridian Mail Multi-Customer feature installed).

Default

The default is No.

Retain Copy of Sent Messages	
Description	(MMUI only) When this field is set to Yes, copies of sent messages are not deleted from the user's mailbox. When it is set to No, messages are deleted as soon as they are sent. Carefully consider how many users you can allow to have this capability, since the more users who have this ability, the faster your available storage space will be used up.
Default	The default is No.

The Add Class of Service screen (cont'd)

This is the last part of the Add Class of Service/Change Defaults screen.

```
                    Class of Service Administration                MORE ABOVE
Add Class of Service

are retained until the user
deletes them manually.)

Send Messages to External Users:          No Yes

Retain Copy of Sent Messages:             No Yes

Delivery to Non-User Capability:          No Yes

Remote Notification Capability:           No Yes

Extension Dialing
Restriction/Permission List:              2   List Name:  Local

Custom Revert
Restriction/Permission List:              2   List Name:  Local

Select a softkey >

   Save        Cancel
```

Field descriptions

This table gives descriptions of the fields highlighted by the broken line in the preceding screen.

Delivery to Non-User Capability	
Description	This enables the user to direct a message to an external DN. ***Note:*** This field is displayed only if Outcalling is installed. There are more fields displayed if Yes is selected. Refer to the *Outcalling Application Guide* (NTP 555-7001-320) for details about configuring the class of service fields for remote notification and delivery to non-users.
Default	The default is No.

Remote Notification Capability	
Description	This field permits the user to receive notification of messages, automatically, to an external DN or a paging device. ***Note:*** This field is displayed only if Outcalling is installed. There are more fields displayed if Yes is selected. Refer to the *Outcalling Application Guide* (NTP 555-7001-320) for details about configuring the class of service fields for remote notification and delivery to non-users.
Default	The default is No.

Receive AMIS Open Network Messages	
Description	This field permits the users to receive messages from users at the AMIS Open Network sites. ***Note:*** This field is displayed only if the AMIS Networking feature Network is installed.
Default	The default value is No.

Compose/Send AMIS Open Network Messages	
Description	This field determines whether users are allowed to compose and send messages to AMIS Open Network users. If this field is set to Yes, the AMIS Open Network Restriction/Permission List is displayed. ***Note:*** This field is displayed only if the AMIS Networking feature is installed.
Valid options	Yes, No No indicates that users cannot compose and send AMIS open network messages. However, users can still compose and send AMIS messages to remote users that are located at virtual nodes within a Meridian Network.
Default	The default value is No.

AMIS Open Network Restriction/Permission List	
Description	This field gives the number and name of the Restriction/Permission list that applies when a user sends an AMIS Open Network message. The lists are defined in the Restriction/Permission List screen, accessible from Voice Administration.
Valid range	This number can range from 0 to 80. The value 0 = unrestricted.
Default	The default is 2 (Local).

Extension Dialing Restriction/Permission List	
Description	(MMUI only) This field gives the number and name of the Restriction/Permission list that applies when a user dials a phone number while logged in to his or her mailbox (known as Thru-dialing). The lists are defined in the Restriction/Permission List screen, accessible from Voice Administration.
Valid range	This number can range from 0 to 80. The value 0 = unrestricted.
Default	The default is 2 (Local).

Custom Revert Restriction/Permission List	
Description	The custom revert DN is the extension to which a caller is passed when the caller presses 0 during a Meridian Mail session. Since users can customize this DN from their telephone sets you must determine which dialing codes you want to restrict (or explicitly permit). For example, you may want to ensure that users cannot revert callers to long distance numbers. This field gives the number and name of the Restriction/Permission list that is applied to the custom revert DN. The lists are defined in the Restriction/Permission List screen, accessible from Voice Administration.
Valid range	This number can range from 0 to 80. The value 0 = unrestricted.
Default	The default is 2 (Local).

The Add Class of Service screen (VMUIF)

Introduction

New classes of service are added to the system through the Add Class of Service screen. The following screens are available to VMUIF systems.

MATs

Class of Service screens are read-only from Multiple Administration Terminals (MATs).

The Add Class of Service screen—VMUIF

The screens that follow appear when you press the [Change Defaults] softkey on the Add Class of Service screen. This is the first part of the Add Class of Service/Change Defaults screen.

```
                    Class of Service Administration
Add Class of Service

Class of Service Number:                  1

Class of Service Name:                    _

Voice Messaging Interface Type:           MMUI VMUIF

Maximum Number of SubMailboxes:           0

Voice Storage Limit (minutes):            3

Maximum Message Length (mm:ss):           03:00

Maximum Personal Greeting Length (mm:ss): 01:00

Delayed Prompts:                          No Yes

                                                          MORE BELOW
Select a softkey >

 Save      Cancel
```

Field descriptions

This table gives descriptions of the fields highlighted by the broken line in the preceding screen.

Class of Service Number	
Description	This is a read-only field. This field is prefilled with the number you entered to access this screen. The COS number is used to identify the Class of Service.
Default	This field is prefilled with the number you entered to access the screen
Valid range	1 to 15

Class of Service Name	
Description	This field defaults to the name entered in the first Add Class of Service screen and is mandatory. The COS definition cannot be saved if this field is blank.
Default	Blank
Maximum length	The COS name can be up to 30 characters in length.
Valid characters	All characters are valid with the exception of “+”, “_”, or “?”, which are invalid.

Voice Messaging Interface Type	
Description	This is a read-only field and is displayed only if VMUIF is installed. This field indicates what the voice messaging interface type is on your system.

Maximum Number of SubMailboxes	
Description	(VMUIF only) A value other than zero in this field means that submailbox capability is enabled for this COS. Submailboxes allow each member of a household to have his or her own personal mailbox, all of which are accessible from a single DN. A value of 0 implies that submailbox capability is disabled. If enabled, between 1 and 8 submailboxes are permitted. The value entered here is the maximum number of mailboxes permitted on a single DN. If a user requests additional submailboxes (and the total exceeds the maximum number configured here), you will have to reassign the user to another COS that has a sufficient number of submailboxes. ***Note:*** Once you have entered a value in this field and assigned users to this COS, this field becomes read-only and you cannot change this value. This is because submailboxes are chargeable by Northern Telecom. When you have used up all of your allotted submailboxes, contact your sales representative.
Valid range	Values from 1 to 8 are permitted.
Default	The default is 0.

Voice Storage Limit	
Description	This field defines the maximum amount of storage available to the user. If submailboxes are enabled for this COS, all submailboxes contend for the same storage space.
How this limit is used	If messages exceed this limit, a message is played to the mailbox owner indicating that the mailbox is full and that the mailbox owner will be restricted in what he or she can do while logged in to Meridian Mail. The following restrictions are imposed: • The mailbox owner can only listen to and delete messages. • The mailbox owner cannot record a personal greeting, or compose, send, or forward messages. • After messages are deleted to reduce the storage used to below the limit, the mailbox owner must still log off and then log back in before the various mailbox functions are restored. The following conditions also exist when the mailbox is full: • Callers who access the Call Answering for the user's mailbox cannot leave a message.
Affected fields	The Maximum Message Length, Maximum Personal Greeting Length, and Maximum Call Answering Message Length cannot be greater than the Voice Storage Limit.
Default	The default value is 3 (minutes).
Valid range	You may enter a value from 1 to 360 (minutes).

Maximum Message Length	
Description	This value determines the longest possible composed message or personal greeting that a user belonging to this COS is allowed to record.
Default	The default value is 03:00.
Valid range	You may enter a value between 00:30 and 99:00 in ten-second increments. The default is 03:00.
Restriction	This value cannot be greater than the Voice Storage Limit. If you set this field to a number that exceeds the idle login timer, message lengths will be restricted to the login timer value. The default idle login timer value is 03:00. To change this value, contact your support organization.

Maximum Personal Greeting Length	
Description	(VMUIF only) This value determines the longest possible personal greeting that a user belonging to this COS is allowed to record.
Default	The default is 01:00.
Valid range	You may enter a value between 00:30 and 05:00.
Restriction	This value cannot be greater than the Voice Storage Limit.

Delayed Prompts	
Description	When this field is set to Yes, the system will prompt users for an action if the user does not initiate any action for 3.5 seconds. It is recommended that this field be set to Yes (especially for new users). Once the users belonging to the COS are familiar with the interface, you may get requests to turn delayed prompting off. You can inform experienced users that they do not need to wait for the prompts to finish before entering a command. This field should remain set to Yes for the benefit of new users.
Default	The default is Yes.

The Add Class of Service screen—VMUIF (cont'd)

This is the second part of the Add Class of Service/Change Defaults screen.

```
                    Class of Service Administration                MORE ABOVE
Add Class of Service

Dial Pulse Support:                          No Yes

Auto Logon:                                  No Yes

Login from Call Answering:                   No Owner Group

Lockout Duration (hh:mm):                    00:00
(00:00 implies no mailbox reset)

Broadcast Capability:                        No Yes

Callers Notified of Busy Line:               No Yes

Receive Messages for Call Answering:         No Yes

Maximum Call Answering
                                                                MORE BELOW
Select a softkey >

   Save        Cancel
```

Field descriptions

This table gives descriptions of the fields highlighted by the broken line in the preceding screen.

Dial Pulse Support	
Description	(VMUIF only) Set this field to Yes to add a class of service that supports users with rotary or dial pulse phone sets. This option allows the user to log in to his or her mailbox without having to enter a mailbox number, password or any other key presses. ***Note:*** If this field is set to Yes, Auto Logon (the next field) must also be set to Yes.
Default	The default is No.

Auto Logon	
Description	When this field is set to Yes, the user does not need to enter a mailbox number or password to gain access to Meridian Mail, when calling from his or her home phone. When set to No, the user must enter a mailbox number and password. For reasons of mailbox security, this field should be set to No.
Exceptions	Set this field to Yes if • Dial Pulse Support is enabled (in which case, auto logon must be enabled). • The users that will be added to this COS have requested auto logon and their phones are in a secure location.
Default	The default is No.

Login from Call Answering	
Description	(VMUIF only) This field determines whether users can log in to their mailboxes during or after a call answering session. When this feature is enabled, users have an alternative method of logging in which does not require that they dial a special access DN. Users can access their mailbox from a phone other than their home phone by dialing their telephone number and then pressing *.
Default	The default is Owner.
Valid options	No, Owner • ***No*** prohibits the user from logging in from call answering. • ***Owner*** allows users to log in to their mailboxes only if the destination mailbox is their own. After pressing *, the user is prompted to enter his or her password.

Lockout Duration	
Description	(VMUIF only) When a user's mailbox is disabled (as shown by the Logon Status field in the Add or View/Modify Local Voice User screen) due to password violation, this field determines how long the user is locked out before he or she can log in again. You may enter a value from 00:00 to 23:59. If you enter a value of 00:00, this means that the user will be locked out until you decide to reenable the mailbox.
Valid range	The range of values that may be entered in this field is from 00:00 to 23:59.
Default	The default is 00:00.

Broadcast Capability	
Description	Set this field to Yes if you want users to be able to compose and send broadcast messages. A broadcast message is one that is sent to all users in the same customer group.
Default	The default is No.

Callers Notified of Busy Line	
Description	When this field is set to Yes, a special prompt is played when the called line is busy, informing the caller that the user is on the phone. After the prompt is played, the caller is connected to Meridian Mail to leave a message. If the field is set to No, the normal Call Answering system greeting or personal greeting is played. ***Note:*** If the user's mailbox is associated with two (or more) DNs, they must all be busy for this prompt to be played.
Default	The default is Yes.

Receive Messages for Call Answering	
Description	(VMUIF only) If this field is set to No, users' mailboxes will not take call answering messages but can still be used to send messages. This feature is useful for users who do not have their own phone (and therefore are not expected to receive calls), but who need a mailbox so that they can compose and send messages.
Default	The default is Yes.

The Add Class of Service screen—VMUIF (cont'd)

This is the third part of the Add Class of Service/Change Defaults screen.

```
Class of Service Administration                    MORE ABOVE
Add Class of Service

Maximum Call Answering
Message Length (mm:ss):                    01:00

Receive Composed Messages:                 No Yes

Message Waiting Indication Options:        None Any Urgent

Skip to First New Message:                 No Yes

Announce Caller:                           No Yes

Replay Header with Message:                No Yes

Call Sender:                               No Yes
                                                   MORE BELOW
Select a softkey >

Save      Cancel
```

Field descriptions

This table gives descriptions of the fields highlighted by the broken line in the preceding screen.

Maximum Call Answering Message Length	
Description	This value determines the longest possible call answering message that a caller can record and leave in a user's mailbox. You may enter a value between 00:30 and 99:00 in 10 second increments.
Default	The default is 01:00.
Valid range	The permitted values are from 00:30 to 99:00.
Restriction	This value cannot be greater than the Voice Storage Limit.

Receive Composed Messages	
Description	If this field is set to No, users' mailboxes will not accept composed messages. If AMIS networking is installed, setting this field to No automatically sets the Receive AMIS Open Network Messages field to No.
Default	The default is Yes.

Message Waiting Indication Options	
Description	The chosen setting determines the type of messages that will cause a message waiting indication (a flashing light or an interrupted dial tone) on the user's telephone set.
Default	The default is Any.
Valid options	None, Any Urgent • ***None*** should be selected for users who do not have physical telephone sets, but do have mailboxes. • ***Any*** notifies users of all new messages. • ***Urgen***t notifies users of only those messages tagged as urgent.

Skip to First New Message	
Description	(VMUIF only) This field determines what happens when users log in to listen to new messages.
Default	The default is No.
Valid Options	Yes, No • ***Yes*** causes the first new message to be automatically played when a user successfully logs on. • ***No*** means that users must use the Play command to listen to new messages.

Announce Caller	
Description	(VMUIF only) If this field is set to Yes, the prompt "From <caller>" will be announced in the header/envelope for messages.
Default	The default is No.

Replay Header with Message	
Description	(VMUIF only) If Yes is selected, the header will be played whenever a user selects the Play command to listen to messages that have been left in the mailbox. The header includes information such as the time at which the message was sent, the caller's name, and so on.
Default	The default is Yes.

Call Sender	
Description	Call Sender allows users to place a call to the (internal) originator of a call answering message or a voice message automatically. After listening to a message, the user presses 9 to dial the caller's number. ***Note:*** This feature is blocked if the user has logged in through remote notification.
Dial pulse	Do not enable this field if Dial Pulse Support is enabled.
Default	The default is No.
Valid Options	Yes, No • No disables Call Sender so that users cannot use the feature to call back internal or external callers who have left messages. • Yes enables Call Sender to internal callers only.
External call sender	To allow users to use Call Sender to place calls to external callers, the following fields must be set to Yes: • Call Sender • External Call Sender Allowed in the Voice Messaging Options screen Restrictions must also be applied in the External Call Sender Restriction/Permission List field in the class of service.

The Add Class of Service screen—VMUIF (cont'd)

This is the fourth part of the Add Class of Service/Change Defaults screen.

```
                    Class of Service Administration                MORE ABOVE
Add Class of Service

External Call-Sender
Restriction/Permission List:                2_  List Name:  Local

Read Message Retention (days):              0_
("0" implies that read messages
are retained until the user
deletes them manually.)

Compose Capability:                         No Yes

Send Messages to External Users:            No Yes

Delivery to Non-User Capability:            No Yes

Remote Notification Capability:             No Yes
                                                                MORE BELOW
Select a softkey >

   Save        Cancel
```

Field descriptions

This table gives descriptions of the fields highlighted by the broken line in the preceding screen.

External Call-Sender Restriction/Permission List	
Description	This field specifies the number and the list name of the Restriction/Permission list that will be applied when the Call Sender feature is used to call back external callers. The lists are defined in the Restriction/Permission List screen, accessible from Voice Administration.
Valid range	This number can range from 0 to 80. The value 0 = unrestricted.
Default	The default is 2 (Local).

Read Message Retention (days)

Description	This field specifies the number of days that messages are kept in users' mailboxes after they have been read. The value in this field is limited by the value set in the Maximum Read Message Retention field in the Voice Messaging Options screen. For details, see "The Voice Messaging Options screen" on page 20-6.
Valid range	You can enter a value from 0 to 99.
Default	The default is 0.
Which value is used	The following table shows which value is used to determine how long the user's read messages are kept.

System retention limit	User retention limit	Amount of time read messages are kept
0 (zero)	0 (zero)	Messages are kept until the user deletes them. The system will not automatically delete read messages.
0 (zero)	A value other than zero	The user retention limit determines how long messages are kept.
A value other than zero	0 (zero)	The system retention limit determines how long messages are kept.
A value other than zero	A value other than zero	The lesser value is used to determine how long messages are kept.

Compose Capability	
Description	(VMUIF only) Set this field to Yes to give users the ability to compose and send voice messages to other users. If this value is set to No, then the user only has call answering capability. If this field is set to Yes, the "Treatment for Unsent Messages if the User Disconnects During Compose" field is displayed. ***Note:*** Once you have assigned users to the COS and put it to use, you cannot modify this field. This feature is chargeable by Nortel. If you need to revoke compose capability from a particular user, you will have to reassign the user to another COS. Conversely, if a user does not have this capability and later requests it, you will have to reassign the user to a COS that has compose capability enabled.
Default	The default is No.

Send Messages to External Users	
Description	This field is not applicable to single-customer systems (that is, systems that do not have the Meridian Mail Multi-Customer feature installed).
Default	The default is No.

Treatment for Unsent Messages if the User Disconnects During Compose	
Description	(VMUIF only) This field is displayed only if the Compose Capability field is set to Yes. The selection you make in this field determines what happens to an unsent message if the user disconnects while composing the message.
Valid options	Delete—delete the unsent message Send—send the possibly incomplete message
Default	The default is Delete.

Delivery to Non-User Capability	
Description	This enables the user to direct a message to an external DN. ***Note:*** This field is displayed only if Outcalling is installed. There are more fields displayed if Yes is selected. Refer to the *Outcalling Application Guide* (NTP 555-7001-320) for details about configuring the class of service fields for remote notification and delivery to non-users.
Default	The default is No.

Remote Notification Capability	
Description	This field permits the user to receive notification of messages, automatically, to an external DN or a paging device. ***Note:*** This field is displayed only if Outcalling is installed. There are more fields displayed if Yes is selected. Refer to the *Outcalling Application Guide* (NTP 555-7001-320) for details about configuring the class of service fields for remote notification and delivery to non-users.
Default	The default is No.

The Add Class of Service screen—VMUIF (cont'd)

This is the fifth part of the Add Class of Service/Change Defaults screen.

```
                    Class of Service Administration                MORE ABOVE
Add Class of Service

Compose Capability:                          No Yes

Send Messages to External Users:             No Yes

Delivery to Non-User Capability:             No Yes

Remote Notification Capability:              No Yes

Receive AMIS Open Network Messages:          No Yes

Compose/Send AMIS Open Network Messages:     No Yes

Custom Revert
Restriction/Permission List:                 2  List Name:  Local

Select a softkey >

   Save        Cancel
```

Field descriptions

This table gives descriptions of the fields highlighted by the broken line in the preceding screen.

Receive AMIS Open Network Messages	
Description	This field permits the users to receive messages from users at the AMIS Open Network sites. ***Note:*** This field is displayed only if the AMIS Networking feature is installed.
Default	The default value is No.

Compose/Send AMIS Open Network Messages	
Description	This field determines whether users are allowed to compose and send messages to AMIS Open Network users. If this field is set to Yes, the AMIS Open Network Restriction/Permission List is displayed. ***Note:*** This field is displayed only if the AMIS Networking feature is installed.
Valid options	Yes, No No indicates users cannot compose and send AMIS Open Network messages. However, users can still compose and send AMIS messages to remote users that are located at virtual nodes within a Meridian Network.
Restriction	If the interface is VMUIF, this field cannot be set to Yes if the Compose Capability field is set to No.
Default	The default value is No.

AMIS Open Network Restriction/Permission List	
Description	This field gives the number and name of the Restriction/Permission list that applies when a user sends an AMIS Open Network message. The lists are defined in the Restriction/Permission List screen, accessible from Voice Administration.
Valid range	This number can range from 0 to 80. The value 0 = unrestricted.
Default	The default is 2 (Local).

Custom Revert Restriction/Permission List	
Description	The custom revert DN is the extension to which a caller is passed when the caller presses 0 during a Meridian Mail session. This field gives the number and name of the Restriction/Permission list that is applied to the custom revert DN. These lists are defined in the Restriction/Permission List screen, accessible from Voice Administration.
Valid range	This number can range from 0 to 80. The value 0 = unrestricted.
Default	The default is 2 (Local).

Assigning Classes of Service to the system

Introduction

After creating (adding) a new Class of Service (COS), it must be made available for use. This is done in the General Options screen. See Chapter 13, “General options. ”

The Find Class of Service screen

Introduction

The Find Class of Service screen is used to locate a specific Class of Service (COS).

The screen

The following is the Find Class of Service screen.

```
                    Class of Service Administration
Find Class of Service

Class of Service Number:    ___

Class of Service Name:      ________________________

Voice Messaging Interface:  Any MMUI VMUIF

Select a softkey >

 Exit        List        Print List    Print Details
```

Field descriptions

This table gives descriptions of the fields in the Find Class of Service screen.

Class of Service Number	
Description	This is the number of an existing COS.
Class of Service Name	
Description	This field is used for the name of a specific COS or a subset of COSs.
Voice Messaging Interface	
Description	This field appears only if VMUIF is installed on your system. Leave this field set to Any or VMUIF.
Valid options	Any, VMUIF

Finding, listing, or printing a Class of Service

Introduction

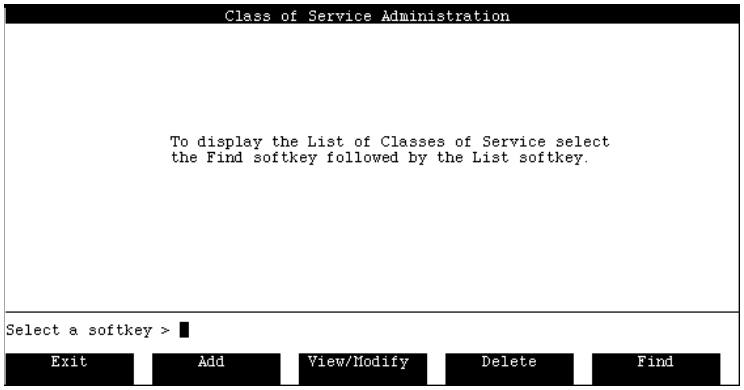
This section details the steps for finding, listing, or printing a Class of Service (COS) or COSs.

Procedure

To list or print COSs, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Class of Service Administration. **Result:** The following screen appears.



Step	Action
2	Press the [Find] softkey. **Result:** The Find Class of Service screen is displayed. The Find Class of Service screen is where you may specify the search criteria for retrieving a particular class of service or a subset of classes.

```
                    Class of Service Administration
Find Class of Service

Class of Service Number:     ___

Class of Service Name:       ______________________________

Voice Messaging Interface:   Any MMUI VMUIF

Select a softkey >

Exit        |           | List        | Print List | Print Details
```

Step	Action
3	To view a list of all Classes of Service on your system, press [List]. **Result:** The List of Classes of Service screen is displayed.

```
                    Class of Service Administration
List of Classes of Service

COS COS         VceMsg  Storage   Retain  Compose   DNU     AMIS       DualLang
Num Name        I/F     (Mins.)   ReadMsg   Msgs    /RN  Receive/Send  Prompt
 1 regular lo MMUI       3         0               N/N     No   No       No
 2 reg w. dnu MMUI       3         0               Y/N     No   No       No
 3 manager    MMUI       10       14               Y/Y     Yes  Yes      No
 4 executive  MMUI       30        0               Y/Y     Yes  Yes      Yes
 5 foreign    MMUI       3         0               N/N     No   No       No
 6 directory  MMUI       3         0               N/N     No   No       No

Select a softkey >

Exit        |           | View/Modify | Delete |
```

Note: For MMUI COSs, the Compose Msgs column remains blank. For VMUIF COSs, the Dual Lang Prompt column remains blank.

Step	Action
4	To print a list of all Classes of Service on your system, press [Print List]. **Result:** The List of Classes of Service is printed.
5	To view or print a particular Class of Service or a specific group of Classes of Service, specify search criteria on the Find screen as follows.

IF	THEN
you want a specific COS and know its number	enter the number in the Class of Service Number field.
you want a specific COS and know its name	enter the name in the Class of Service Name field.
you want a group of COSs with similar names	enter the appropriate search pattern in the Class of Service Name field. (This pattern will consist of letters and wildcard characters.)
you want to find those COSs for a particular interface	specify either MMUI or VMUIF.

6 To view or print the selected Classes of Service, press the appropriate softkey as follows.

IF	THEN
you want a list of the COSs according to the search criteria	press the [List] softkey.
you want to print the list of COSs	press the [Print List] softkey.
you want to print the details of a single COS	enter the COS number or name in the appropriate field and press the [Print Details] softkey.

Modifying a Class of Service

Introduction

This section deals with changing the values in any of the fields for a specific Class of Service (COS).

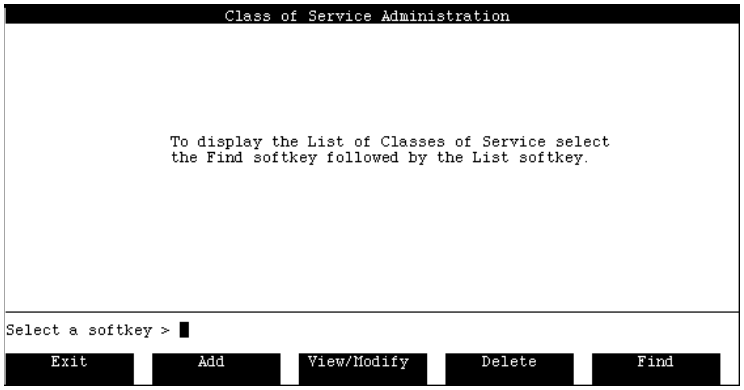
To modify an existing COS, you must be logged on at the main administration terminal (not a multiple-administration terminal).

Procedure

A COS is changed by modifying its values. To change the values, follow these steps.

Starting Point: The Main Menu.

Step	Action
1	Select Class of Service Administration. **Result:** The Class of Service Administration screen is displayed.



Step	Action
2	Press the [Find] softkey. **Result:** The Find Class of Service screen is displayed.

```
                    Class of Service Administration
Find Class of Service

Class of Service Number:     ___

Class of Service Name:       ____________________________

Voice Messaging Interface:   Any MMUI VMUIF

Select a softkey >

Exit        List        Print List        Print Details
```

3 Specify the search criteria.

IF	THEN
you want to find a particular COS	enter the COS number in the Class of Service Number field.
you want to find a subset of COSs according to name	enter the appropriate search pattern in the Class of Service Name field. (This pattern will consist of letters and wildcard characters.)
you want to find those COSs for a particular interface	specify either MMUI or VMUIF.

Step	Action
4	Press the [List] softkey. **Result:** The List of Classes of Service screen is displayed.

```
                        Class of Service Administration
List of Classes of Service

COS COS        VceMsg  Storage   Retain  Compose   DNU     AMIS       DualLang
Num Name       I/F     (Mins.)   ReadMsg   Msgs    /RN  Receive/Send  Prompt
 1 regular lo MMUI       3         0              N/N     No   No       No
 2 reg w. dnu MMUI       3         0              Y/N     No   No       No
 3 manager    MMUI       10       14              Y/Y     Yes  Yes      No
 4 executive  MMUI       30        0              Y/Y     Yes  Yes      Yes
 5 foreign    MMUI       3         0              N/N     No   No       No
 6 directory  MMUI       3         0              N/N     No   No       No

Select a softkey >

     Exit                 View/Modify     Delete
```

Note: For MMUI COSs, the Compose Msgs column remains blank. For VMUIF COSs, the Dual Lang Prompt column remains blank.

5	Move the cursor to the definition you want to modify.
6	Press the spacebar to select it.

Step	Action
7	Press the [View/Modify] softkey. **Result:** The View/Modify Class of Service screen is displayed.

```
                    Class of Service Administration
View/Modify Class of Service

Class of Service Number:                    1

Class of Service Name:                      regular local voice user

Voice Messaging Interface Type:             MMUI VMUIF

Personal Verification Changeable by User:   No Yes

Voice Storage Limit (minutes):              3

Maximum Message Length (mm:ss):             03:00

Delayed Prompts:                            No Yes

Dual Language Prompting:                    No Yes
                                                                MORE BELOW
Select a softkey >

Save        Cancel
```

Note: The fields that appear in the View/Modify Class of Service screen depend on what features are installed on your system. For detailed field descriptions, see “The Add Class of Service screen (MMUI)” on page 26-13 or “The Add Class of Service screen (VMUIF)” on page 26-30.

8 Make the necessary changes to the COS.

9 Save or cancel the changes.

IF	THEN
you want to save the changes	press the [Save] softkey. **Result:** The changes to the COS are saved. All users belonging to the COS will use the updated values in the COS. The List of Classes of Service screen is displayed.
you want to exit the screen without saving the changes	press the [Cancel] softkey. **Result:** Any changes that you have made are not saved and the List of Classes of Service screen is displayed.

Field descriptions

The View/Modify Class of Service screen contains the same fields as the Add Class of Service screen. For field descriptions, see "The Add Class of Service screen (MMUI)" on page 26-13 or "The Add Class of Service screen (VMUIF)" on page 26-30.

Deleting a Class of Service

Introduction

This section deals with deleting a Class of Service (COS) from the system.

Procedure

Starting Point: Main Menu

Step	Action
1	Select Class of Service Administration. **Result:** The Class of Service Administration is displayed.

```
Class of Service Administration

To display the List of Classes of Service select
the Find softkey followed by the List softkey.

Select a softkey >
Exit | Add | View/Modify | Delete | Find
```

Step	Action
2	Press the [Find] softkey. **Result:** The Find Class of Service screen is displayed.

```
Class of Service Administration
Find Class of Service

Class of Service Number:
Class of Service Name:
Voice Messaging Interface:  Any MMUI VMUIF

Select a softkey >
Exit | | List | Print List | Print Details
```

Step	Action
3	Specify the search criteria.

IF	THEN
you want to find a particular COS	enter the COS number in the Class of Service Number field.
you want to find a subset of COSs according to name	enter the appropriate search pattern in the Class of Service Name field. (This pattern will consist of the letters and wildcard characters to indicate the pattern that the found COSs must match.)
you want to find those COSs for a particular interface	specify either MMUI or VMUIF.

4 Press the [List] softkey.

Result: The List of Classes of Service screen is displayed.

```
                    Class of Service Administration
List of Classes of Service

COS COS        VceMsg  Storage   Retain  Compose   DNU     AMIS       DualLang
Num Name       I/F     (Mins.)   ReadMsg   Msgs    /RN  Receive/Send  Prompt
 1 regular lo MMUI       3         0              N/N     No   No       No
 2 reg w. dnu MMUI       3         0              Y/N     No   No       No
 3 manager    MMUI       10       14              Y/Y     Yes  Yes      No
 4 executive  MMUI       30        0              Y/Y     Yes  Yes      Yes
 5 foreign    MMUI       3         0              N/N     No   No       No
 6 directory  MMUI       3         0              N/N     No   No       No

Select a softkey >

   Exit          View/Modify     Delete
```

Note: For MMUI COSs, the Compose Msgs column remains blank. For VMUIF COSs, the Dual Lang Prompt column remains blank.

5 Move the cursor to the definition you want to delete.

6 Press the spacebar to select it.

Step	Action
7	Press the [Delete] softkey. **Result:** The Delete Class of Service screen is displayed.

```
                    Class of Service Administration
Delete Class of Service

Class of Service Number:                    1

Class of Service Name:                      regular local voice user

Voice Messaging Interface Type:             MMUI VMUIF

Personal Verification Changeable by User:   No Yes

Voice Storage Limit (minutes):              3

Maximum Message Length (mm:ss):             03:00

Delayed Prompts:                            No Yes

Dual Language Prompting:                    No Yes
                                                                MORE BELOW
Select a softkey >

OK To Delete    Cancel
```

Note: The fields that appear in the Delete Class of Service screen depend on what features are installed on your system. For detailed field descriptions, see “The Add Class of Service screen (MMUI)” on page 26-13 or “The Add Class of Service screen (VMUIF)” on page 26-30.

8 Delete the COS or exit the screen without deleting.

IF	THEN
you want to delete the COS	press the [OK to Delete] softkey.
you want to exit the screen without deleting the COS	press the [Cancel] softkey.

Section C: Assigning Classes of Service to users

In this section

Assigning a Class of Service to a user 26-64
Creating and Assigning a Personal Class of Service to a user 26-65
The Class of Service conversion utility for converted systems 26-66

Assigning a Class of Service to a user

Description

To assign a user to a particular COS, select the COS number in the Class of Service field in the Add Local Voice User screen. For a complete description of this screen, see Chapter 8, “Local voice users”.

See also

Please see Chapter 8, “Local voice users” for the procedures.

Creating and Assigning a Personal Class of Service to a user

Description

If a user has special requirements that are not met by any of the existing COSs, you can create a personal COS for that user. All personal COSs must be maintained individually, since any changes made to a system COS will not affect the personal COSs that exist on the system. If, for example, it is decided that all users will be given access to a particular feature, you would have to modify all personal COSs as well as the system COSs.

See also

To create a personal COS, see "Assigning a user to a class of service" on page 8-20.

The Class of Service conversion utility for converted systems

Description

If you have converted your system from Release 8 or earlier, all existing users will each have a personal class of service. This means that all users still have their Meridian Mail Release 8 personal settings and are not connected to or related to any system COSs. Therefore, after a conversion you must ensure that all existing users are reassigned to system COSs. This is done by adding the necessary COSs, then using the COS Conversion utility.

Process

This utility checks each user's personal COS. If it matches an existing system COS, the user is assigned to that COS. User mailboxes that do not match a system COS remain with personal COSs. You can use this utility to view these unassigned mailboxes and then use the utility to either add a system COS based on the personal COSs or assign the unassigned mailbox to a defined COS.

See also

The COS Conversion utility is available from the tools level and allows you to reassign users to COSs. See the *System Administration Tools Guide* (NTP 555-7001-305) for details.

Chapter 27

Hardware administration

In this chapter

Overview	27-2
The Hardware Administration menu	27-3
Section A: Viewing the node configuration	27-5
Section B: Viewing the data port configuration	27-17
Section C: Printing node and data port information	27-45

Overview

Introduction

The Hardware Administration screens allow you to view the contents of the hardware database in your Meridian Mail system.The hardware database is a system utility that maintains a current listing and description of all nodes, cards, and ports in your system.

CAUTION
Risk of audit failure

Do not leave any Hardware Administration menu on the administrative console overnight, as important system audits may fail due to lack of available memory, and there will be a security risk.

Available configurations

The MMP40 processor card is required for all Meridian Mail platforms, with the exception of Card Option. The Card Option platform uses the 68K processor card.

Modifying the hardware database

The Hardware Administration function allows you to view aspects of the Hardware database. If you or a representative from your support organization need to modify the hardware database, you must use the “Modify hardware” tool. Refer to *System Administration Tools* (NTP 555-7001-305).

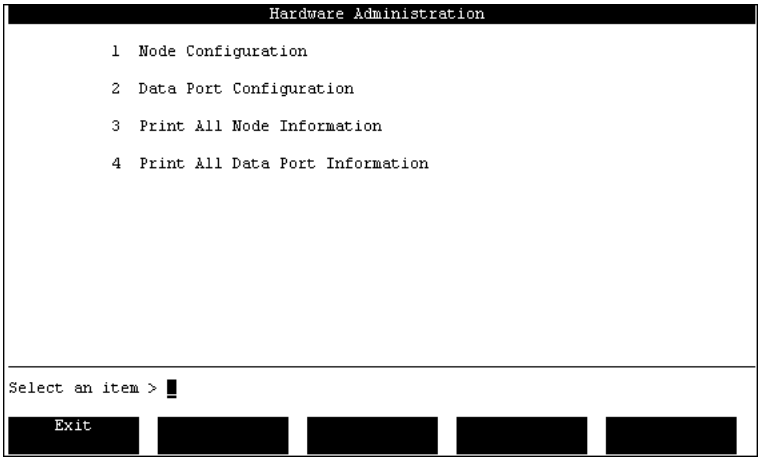
The Hardware Administration menu

Introduction

The Hardware Administration menu is accessed directly from the main System Administration menu.

Hardware Administration menu

The Hardware Administration menu is displayed in the following illustration.



Procedure

To access the Hardware Administration facilities, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Hardware Administration. **Result:** The Hardware Administration menu appears.
2	Choose the number of the action you wish to perform and press <Return>. **Result:** The screen corresponding to your selection appears. See the following sections for details: See “The Node Configuration screen” on page 27-7. See “The Data Port Configuration screen” on page 27-23. See “Printing node and data port information” on page 27-47.
3	Press [Exit] to return to the Main Menu.

Section A: Viewing the node configuration

In this section

Overview	27-6
The Node Configuration screen	27-7
The View Node screen	27-10

Overview

Introduction

The Node Configuration screen provides a summary listing of the cards found in all nodes in your system (see “The Node Configuration screen” on page 27-7).

The View Node screens provide a more detailed view of individual nodes (see “The View Node screen” on page 27-10).

The Node Configuration screen

Introduction

The Node Configuration screen is used to view a summary listing of the cards in all nodes on your system.

Accessing the Node Configuration screen

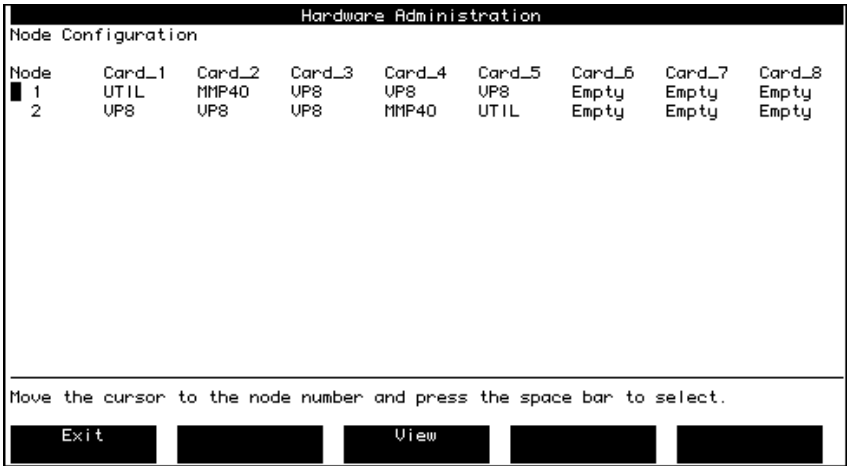
To view the Node Configuration screen, follow these steps.

Step	Action
1	Select Hardware Administration from the Main Menu. **Result:** The Hardware Administration menu appears.
2	Select Node Configuration from the Hardware Administration menu. **Result:** The Node Configuration screen appears.

The screen

The following illustration shows a Node Configuration screen for a two-node MMP40 system.

Note: The illustrations in this section do not necessarily represent the hardware configuration on your system. They are examples only.



Field descriptions

The following fields appear on the Node Configuration screen.

Node	
Description	Refers to the number of the node within the configuration.
Default	None.

Card_x	
Description	Identifies the card slot in the defined node, where "x" represents the position of the card slot. The card slots are numbered from left to right.
Valid entries	The possible card types are listed here. Depending on your system type, you will not see all of these cards on your system. **MMP40** This is the Meridian Mail processor (CPU) card which includes a 24 MHz 68040 processor, 16 Mbytes of memory, up to two RS-232 serial ports, and a SCSI interface processor. It is displayed for MMP40 systems. **RSM** This is an RS-232 service module (for non-EC systems). **Bus** This is the high-speed bus (also called HABC for High Availability Bus Controller). **MSP** This is the multi-purpose signal processor. **NVP** This is the 16 kbyte network voice processor. **NVP32** This is the 32 kbyte network voice processor.

UTIL
This card, on EC systems only, contains a high speed bus. It also includes four auxiliary RS-232 ports. (1- to 4-node systems require one of these cards; 5-node systems with 60 or more ports require two of these cards.)

VP4/VP8 cards
These cards are voice processor cards that provide four and eight channels respectively.

Empty
The card slot is empty.

The View Node screen

Introduction

The View Node screen provides a detailed view of the cards and ports that make up a node, including card types and locations, port types, and port attributes.

MSP nodes and SPN nodes

Two types of nodes are described in this section: an MSP node and an SPN node.

The MSP node is always node 1 on your system. It contains system-related cards such as the MMP40 card. Depending on the system size, it may also contain voice cards.

An SPN node is a voice node and contains mostly voice cards. All other nodes besides node 1 are SPN nodes.

Viewing node configurations

To view the node configurations for your system, follow these steps.

Step	Action
1	Select Hardware Administration from the Main Menu. **Result:** The Hardware Administration menu appears.
2	Select Node Configuration from the Hardware Administration menu. **Result:** The Node Configuration screen appears.
3	Move the cursor to the node you want to view and press <Spacebar>. **Result:** Your selection is highlighted.
4	Select [View] to view the configuration information for the highlighted node. **Result:** The View Node screen appears. See “View Node screen (MSP node)” on page 27-11. and “View Node screen (SPN node)” on page 27-12 for examples.
5	Select [Exit] to return to the Node Configuration screen when you have finished viewing the node configuration. Select [Exit] again to return to the Hardware Administration main menu.

View Node screen (MSP node)

The following diagram illustrates a View Node screen for an EC MMP40 system when the node is an MSP node.

```
                          Hardware Administration                MORE ABOVE
View Node 1  (C=Card D=DSP P=Port)

C-D-P     Card_Type  Port_Type  Attributes

6         UTIL                  J4: 9   J5: 10
6   1               Data:       Terminal Printer NWModem MMLink AML/CSL SMDI PMS
                                AdminPlus MSLink Modem
6   2               Data:       Terminal Printer NWModem MMLink AML/CSL SMDI PMS
                                AdminPlus MSLink Modem
6   3               Data:       Terminal Printer NWModem MMLink AML/CSL SMDI PMS
                                AdminPlus MSLink Modem
6   4               Data:       Terminal Printer NWModem MMLink AML/CSL SMDI PMS
                                AdminPlus MSLink Modem

7         MMP40
7   1               Data:       Terminal Printer NWModem MMLink AML/CSL SMDI PMS
                                AdminPlus MSLink Modem
7   2               Data:       Terminal Printer NWModem MMLink AML/CSL SMDI PMS
                                                                      MORE BELOW
Select a softkey >

     Exit
```

Note: If the MMP40 node you are viewing is an MSP node, the following types of cards may be installed:

- MMP40, Bus, RSM, and VP on non-EC systems
- MMP40, UTIL, and VP on EC systems

View Node screen (SPN node)

The following diagram illustrates the View Node screen for an EC MMP40 system when the node is an SPN node.

```
                          Hardware Administration
View Node 2  (C=Card D=DSP P=Port)

C-D-P     Card_Type  Port_Type  Attributes

1         VP8
1-1-1                Voice:    TN: Octal   36 -0-2 -8  AgtPosId: 9999
1-1-2                Voice:    TN: Octal   36 -0-2 -9  AgtPosId: 9999
1-2-1                Voice:    TN: Octal   36 -0-2 -10 AgtPosId: 9999
1-2-2                Voice:    TN: Octal   36 -0-2 -11 AgtPosId: 9999
1-3-1                Voice:    TN: Octal   36 -0-2 -12 AgtPosId: 9999
1-3-2                Voice:    TN: Octal   36 -0-2 -13 AgtPosId: 9999
1-4-1                Voice:    TN: Octal   36 -0-2 -14 AgtPosId: 9999
1-4-2                Voice:    TN: Octal   36 -0-2 -15 AgtPosId: 9999

2         VP8
2-1-1                Voice:    TN: Octal   40 -0-2 -0  AgtPosId: 9999
2-1-2                Voice:    TN: Octal   40 -0-2 -1  AgtPosId: 9999
2-2-1                Voice:    TN: Octal   40 -0-2 -2  AgtPosId: 9999
                                                                MORE BELOW
Select a softkey >
   Exit
```

Note: An SPN node might have the following types of cards installed:

- MMP40, NVP32, or NVP16 on non-EC systems
- MMP40, VP4, or VP8 on EC systems

Field descriptions

The View Node screens display the following read-only information about each card on the node.

C-D-P	
Description	This is the physical location of the port in the Meridian Mail system, where • C is the card • D is the DSP number (which is displayed for voice processor cards only) • P is the port number

Card_Type	
Description	This indicates the function of the card.
Valid entries	The possible card types are listed here. Depending on your system type, you will not see all of these cards on your system. **MMP40** This is the Meridian Mail processor (CPU) card which includes a 24 MHz 68040 processor, 16 Mbytes of memory, up to two RS-232 serial ports, and a SCSI interface processor. It is displayed for MMP40 systems. **RSM** This is an RS-232 service module (for non-EC systems). **Bus** This is the high-speed bus (also called HABC for High Availability Bus Controller). **MSP** This is the multi-purpose signal processor. **NVP** This is the 16 kbyte network voice processor. **NVP32** This is the 32 kbyte network voice processor.

UTIL
This card, on EC systems only, contains a high speed bus. It also includes four auxiliary RS-232 ports. (1- to 4-node systems require one of these cards; 5-node systems with 60 or more ports require two of these cards.)

VP4/VP8 cards
These cards are voice processor cards that provide four and eight channels respectively.

Empty
The card slot is empty.

Port_Type	
Description	This field describes the type of port, where • **Data** indicates a serial data communications port • **Device** indicates a mass storage device or tape drive • **Voice** indicates a voice processor port • **Multi** indicates a multimedia port

J4 (UTIL card only)	
Description	This indicates the Meridian 1 network loop number connected to J4 on the utility card. This field is read-only, and is configured at the Tools level. See the *System Administration Tools Guide* (NTP 555-7001-305).

J5 (UTIL card only)	
Description	This indicates the Meridian 1 network loop number connected to J5 on the utility card. This field is read-only, and is configured at the Tools level. See the *System Administration Tools Guide* (NTP 555-7001-305).

Attributes (for ports with type = Data)	
Description	• **Terminal** indicates a connection to an administration terminal. • **Printer** indicates a printer serial connection. • **NWModem** indicates a connection to a modem used for networking calls. ***Note:*** Ports on the MMP40 and the SBC card do not support networking. The RSM card (on non-EC systems) or UTIL card (on EC systems) do support networking. • **MMLink** indicates the Meridian ACCESS Link, which is the communications channel for Meridian ACCESS. • **AML/CSL** (Meridian Link) indicates there is a communications channel between Meridian Mail and a Meridian 1. • **SMDI** (not applicable) indicates a communications channel between Meridian Mail and a DMS-100, DMS-10, SL-100, AT&T, ROLM, or NEC switch. • **PMS** (for Hospitality systems) is the serial link between Meridian Mail, the PMS system, and the Meridian 1 for PMS data. • **AdminPlus** indicates a connection to a PC equipped with Meridian Mail Reporter. • **Modem** indicates a connection to a modem used for remote access. • **MSLink** indicates a connection to a PC running Meridian Mail AutoAdmin.

Attributes (for ports with type = Device)	
Description	• **Disk** indicates a mass storage subsystem (hard disk) is present. • **Tape** indicates a cartridge tape subsystem is present.

Attributes (for ports with type = Voice or Multi)	
Description	• **TN** (Meridian 1) This stands for Terminal Number <Density + Address> where Density is either Single, Double, or Quadruple. (This is Octal on Card Option systems.) The Address consists of the set of numbers lll-ss-c-uu, where: lll = loop (0–255) ss = shelf (0–3 for single density, 0–1 for double, 0 for quadruple) c = card (0–15) uu = unit (0–3 for single density, 0–7 for double, 0–15 for quadruple) • **AgtPosId** indicates the Agent Position ID for the voice port. This is equivalent to the Position ID for the virtual agent. It is unique across the entire Meridian 1 customer and is associated with a particular (agent) telephone set. It is not necessary to fill in this field, but you may want to use this field to further label and track your ports. The default value is 9999.

Section B: Viewing the data port configuration

In this section

Overview	27-18
The Data Port Configuration screen	27-23
Viewing data ports	27-25
View Terminal data ports	27-27
View Printer data port	27-30
View MMLink data port	27-32
View/Modify NWModem data port	27-34
View PMS data port	27-36
View AdminPlus data port	27-38
View Modem data port	27-40
View MSLink data port	27-42

Overview

Introduction

The Data Port Configuration screen summarizes the data ports on all nodes in your system. From this screen, you can select and view data port configurations for devices that are part of your system.

For Networking systems, the modem port settings can be modified through these screens. To modify any other data port (except AML/CSL), use “Modify hardware” at the Tools level. See *System Administration Tools* (NTP 555-7001-305).

Cumulative baud rate

The cumulative baud rate of ACCESS links and AdminPlus and MSLink data ports on a node cannot exceed 19 200 on node 1, 38 400 on other nodes, and 9600 on Card Option.

Recommended data port uses for Card Option

The following table describes the recommended port uses for a Card Option system.

Port	Allowable Uses
DP1	Network Modem, GAC, Printer, ACCESS/AdminPlus/AutoAdmin
DP2	Network Modem, GAC, Printer, ACCESS/AdminPlus/AutoAdmin
DP3	Network Modem, Printer, PMSI to PMS System, ACCESS/AdminPlus/AutoAdmin
DP4	Network Modem, Printer, PMSI to SL–1, ACCESS/AdminPlus/AutoAdmin

Recommended data port uses for EC systems

The following table describes the recommended data port uses for EC systems.

Port	Allowable uses
Node 1, MMP40 port 1	System console
Node 1, MMP40 port 2	AML
Node 1, Utility Card port 1	Network Modem, GAC, MAT, Printer, ACCESS/AdminPlus/AutoAdmin
Node 1, Utility Card port 2	Network Modem, GAC, MAT, Printer, ACCESS/AdminPlus/AutoAdmin
Node 1, Utility Card port 3	Network Modem, PMSI Link to PMS, GAC, MAT, Printer, ACCESS/ AdminPlus/AutoAdmin
Node 1, Utility Card port 4	Network Modem, PMSI Link to SL-1, GAC, MAT, Printer, ACCESS/AdminPlus/ AutoAdmin
Node 2, MMP40 port 1	GAC, MAT, Printer, ACCESS/AdminPlus/ AutoAdmin
Node 2, MMP40 port 2	GAC, MAT, Printer, ACCESS/AdminPlus/ AutoAdmin
Node 3, MMP40 port 1	GAC, MAT, Printer, ACCESS/AdminPlus/ AutoAdmin
Node 3, MMP40 port 2	GAC, MAT, Printer, ACCESS/AdminPlus/ AutoAdmin
Node 4, MMP40 port 1	GAC, MAT, Printer, ACCESS/AdminPlus/ AutoAdmin
Node 4, MMP40 port 2	GAC, MAT, Printer, ACCESS/AdminPlus/ AutoAdmin
Node 5, MMP40 port 1	GAC, MAT, Printer, ACCESS/AdminPlus/ AutoAdmin
Node 5, MMP40 port 2	GAC, MAT, Printer, ACCESS/AdminPlus/ AutoAdmin
Second Utility card port 1	Network Modem, GAC, MAT, Printer
Second Utility card port 2	Network Modem, GAC, MAT, Printer

Port	Allowable uses
Second Utility card port 3	Network Modem, GAC, MAT, Printer
Second Utility card port 4	Network Modem, GAC, MAT, Printer

Recommended data port uses for Modular Option systems

The following table describes the recommended data port uses for Modular Option systems.

Port	Allowable uses
Node 1, MMP40 port 1: DP1	System console
Node 1, MMP40 port 2: DP2	AML
Node 1, RSM port 1: DP3	Network Modem, SMDI, GAC, MAT, Printer, ACCESS/AdminPlus/ AutoAdmin
Node 1, RSM port 2: DP4	Network Modem, SMDI, GAC, MAT, Printer, ACCESS/AdminPlus/ AutoAdmin
Node 1, RSM port 3: DP5	Network Modem, SMDI, PMSI Link to PMS, GAC, MAT, Printer, ACCESS/ AdminPlus/AutoAdmin
Node 1 RSM port 4: DP6	Network Modem, SMDI, PMSI Link to SL-1, GAC, MAT, Printer, ACCESS/ AdminPlus/AutoAdmin
Node 2, MMP40 port 1: DP7	SMDI, GAC, MAT, Printer, ACCESS/ AdminPlus/AutoAdmin
Node 2, MMP40 port 2: DP8	ACCESS/AdminPlus/AutoAdmin, Maintenance
Node 2, RSM port 1: DP9	Network Modem, SMDI, GAC, MAT, Printer
Node 2, RSM port 2: DP10	Network Modem, SMDI, GAC, MAT, Printer
Node 2, RSM port 3: DP11	Network Modem, SMDI, GAC, MAT, Printer
Node 2, RSM port 4: DP12	Network Modem, SMDI, GAC, MAT, Printer
Node 3, MMP40 port 1: DP13	SMDI, GAC, MAT, Printer, ACCESS/ AdminPlus/AutoAdmin
Node 3, MMP40 port 2: DP 14	ACCESS/ AdminPlus/AutoAdmin, Maintenance

Port	Allowable uses
Node 3, RSM port 1: DP 15	Network Modem, SMDI, GAC, MAT, Printer
Node 3, RSM port 2: DP16	Network Modem, SMDI, GAC, MAT, Printer
Node 3, RSM port 3: DP 17	Network Modem, SMDI, GAC, MAT, Printer
Node 3, RSM port 4: DP 18	Network Modem, SMDI, GAC, MAT, Printer
Node 4, MMP40 port 1: DP 19	SMDI, GAC, MAT, Printer, ACCESS/ AdminPlus/AutoAdmin
Node 4, MMP40 port 2: DP 20	ACCESS/AdminPlus/AutoAdmin, Maintenance
Node 4, RSM port 1: DP21	Network Modem, SMDI, GAC, MAT, Printer
Node 4, RSM port 2: DP 22	Network Modem, SMDI, GAC, MAT, Printer
Node 4, RSM port 3: DP 23	Network Modem, SMDI, GAC, MAT, Printer
Node 4, RSM port 4: DP 24	Network Modem, SMDI, GAC, MAT, Printer
Node 5, MMP40 port 1: DP 25	SMDI, GAC, MAT, Printer, ACCESS/ AdminPlus/AutoAdmin
Node 5, MMP40 port 2: DP26	ACCESS/AdminPlus/AutoAdmin, Maintenance
Node 5, RSM port 1: DP 27	Network Modem, SMDI, GAC, MAT, Printer
Node 5, RSM port 2: DP 28	Network Modem, SMDI, GAC, MAT, Printer
Node 5, RSM port 3: DP 29	Network Modem, SMDI, GAC, MAT, Printer
Node 5, RSM port 4: DP 30	Network Modem, SMDI, GAC, MAT, Printer

The Data Port Configuration screen

Introduction

The Data Port Configuration screen summarizes the data ports on all nodes in your system. You can select and view the data port configurations for only those devices that are part of your system.

Accessing the Data Port Configuration screen

To view the Data Port Configuration screen, follow these steps.

Step	Action
1	Select Hardware Administration from the Main Menu. **Result:** The Hardware Administration menu appears.
2	Select Data Port Configuration from the Hardware Administration menu. **Result:** The Data Port Configuration screen appears.

The screen

The following illustration shows the Data Port Configuration screen for a 2-node MMP40 EC system.

```
                          Hardware Administration
Data Port Configuration

Port Location    Description            Device Type   Status
1-3-1            Node 1 MMP40 Port 1    Terminal        InService
 1-3-2           Node 1 MMP40 Port 2    AML/CSL         InService
 1-8-1           Node 1 RSM Port 1      AdminPlus       InService
 1-8-2           Node 1 RSM Port 2      Terminal        InService
 1-8-3           Node 1 RSM Port 3      PMS             InService
 1-8-4           Node 1 RSM Port 4      Modem           InService

Move the cursor to the data port location and press the space bar to select.

     Exit                          View/Modify
```

Field descriptions

The Data Port Configuration screen displays the following information.

Port Location	
Description	This is the physical location of the port in the Meridian Mail system (node-card-port).
Description	
Description	This field identifies the node, card type, and port.
Device Type	
Description	This field identifies the function of the port.
Valid values	See the data port tables in the "Overview" on page 27-18.
Status	
Description	This field identifies the current operational state of the port.
Valid values	The status will be one of the following: **InService** The data port is operational. **OutOfService** The data port is no longer operational because the node has been disabled. **Faulty** The system has detected an error in the data port. **Unequipped** The data port has not been defined in the hardware database.

Viewing data ports

Introduction

This section describes the different data port screens that can be displayed. Depending on the device type that has been selected when you press View/Modify, the appropriate version of the View Data Port screen appears as follows:

- Terminal data ports (console or MAT/GAC)
- Printer data ports
- MMLink data ports
- NWModem data ports
- PMS data ports
- AdminPlus data ports
- Modem data ports
- MSLink data ports

Procedure

To view data ports, follow these steps.

Step	Action
1	Select “Hardware Administration” from the Main Menu. **Result:** The Hardware Administration menu appears.
2	Select Data Port Configuration from the Hardware Administration menu. **Result:** The Data Port Configuration screen appears.

Step	Action
3	Move the cursor to the port you want to view (or modify, if NWModem) and press <Space Bar>. **Result:** Your selection is highlighted.
4	Select [View/Modify] to view the configuration information for the highlighted port. **Result:** The View Node screen appears for the selected device. (If NWModem was selected, the Modify Data Port screen is displayed.) For further information, see the appropriate section for the selected device, as follows: “View Terminal data ports” on page 27-27 “View Data Port screen—MAT or GAC” on page 27-28 “View Printer data port” on page 27-30 “View MMLink data port” on page 27-32 “View/Modify NWModem data port” on page 27-34 “View PMS data port” on page 27-36 “View Modem data port” on page 27-40 “View MSLink data port” on page 27-42
5	Select [Exit] to return to the Data Port Configuration screen when you have finished viewing the data port configuration. Select [Exit] again to return to the Hardware Administration screen. **Result:** The “Hardware Administration” screen is redisplayed.

View Terminal data ports

View Data Port screen—Console

The View Data Port screen for terminals (Console) allows you to view information about the terminal connected to the selected port.

```
                    Hardware Administration
  View Data Port
  Data Port Location:    1-1-1
  Device Type:           Terminal
  Device Name:           MODEMCON
  Baud Rate:             1200 2400 4800 9600
  Parity:                Even Odd None
  Number of Windows:     6
  Window Width:          80
  Window Height:         24

Select a softkey >
   Exit
```

View Data Port screen—MAT or GAC

The View Data Port screen for terminals (MAT or GAC) allows you to view information about the terminal connected to the selected port.

```
Hardware Administration
View Data Port

Data Port Location:    1-2-1

Device Type:           Terminal

Device Name:           CONSOLE

Baud Rate:             Autobaud

Parity:                Even Odd None

Number of Windows:     6

Window Width:          80

Window Height:         24

Select a softkey >

Exit
```

Field descriptions

The View Data Port (Terminal — Console or MAT/GAC) screens display the following read-only information about the terminals connected to the device type.

Data Port Location	
Description	This is the physical location of the port (node-card-port).
Valid entries	A terminal must be located on port 1 of node 1.
Device Type	
Description	This field describes the device type.
Valid entries	“Terminal” is displayed.
Device Name	
Description	This is the name that identifies the terminal. This name is assigned by the system when Meridian Mail is installed, or when the port is reconfigured using the Install/data tape. The Device Name for a terminal data port can also be modified later using the “Modify hardware” tool.

Baud Rate	
Description	The selected baud rate is highlighted.
Valid entries	The baud rate must be set to 2400 for all system types except Card Option. For Card Option systems, 2400 is recommended, but it must match the baud rate set on the Option 11 switch.
Parity	
Description	This is the method by which data is communicated.
Valid entries	This can be set to Even, Odd, or None, depending on the current setup of the terminal connected to the port. It is usually set to None.
Number of Windows	
Description	This field specifies the number of windows that can be used simultaneously.
Valid entries	Set this field to 6 for the system administration terminal.
Window Width	
Description	This field specifies the window width used.
Valid entries	Set this field to 80 for the terminal.
Window Height	
Description	This field specifies the window height used.
Valid entries	Set this field to 24 for the terminal.

View Printer data port

Introduction

The View Data Port screen for printers allows you to view the baud rate and parity of the printer that is connected to the selected port.

A printer can be attached directly to the administration terminal. It does not require a separate data port.

SEERs and Operational Measurement reports can be directed to a particular printer. If you choose to do this, define the printer port using the "Modify hardware" tool. See *System Administration Tools* (NTP 555-7001-305). Once this has been done, specify the printer in the General Options screen. See Chapter 13, "General options. "

View Data Port screen

This is the View Data Port screen for printer ports.

```
                    Hardware Administration
  View Data Port
  Data Port Location:    1-1-2
  Device Type:           Printer
  Device Name:           PRT0112
  Baud Rate:             1200 2400 4800 9600
  Parity:                Even Odd None

Select a softkey >
   Exit
```

Field descriptions

The View Data Port (Printer) screen displays the following read-only information about the terminals connected to the device type.

Data Port Location	
Description	This is the physical location of the port (node-card-port).
Device Type	
Description	This field describes the device type.
Valid entries	"Printer" is displayed.
Device Name	
Description	This is the name that identifies the printer data port. This name is assigned by the system when Meridian Mail is installed, or when the port is reconfigured using Install/data tape or the "Modify hardware" tool.
Baud Rate	
Description	The selected baud rate is highlighted.
Valid entries	The setting will depend on the current setup of the printer connected to the port.
Parity	
Description	This is the method by which data is communicated.
Valid entries	The setting will depend on the current setup of the printer connected to the port.

View MMLink data port

View Data Port screen

The View Data Port screen for Meridian ACCESS Link allows you to view the link characteristics.

```
Hardware Administration
View Data Port

Data Port Location:    1-1-3

Device Type:           MMLink

Device Name:           ACCO113

Baud Rate:             4800 9600

Parity:                Even Odd None

Select a softkey >

Exit
```

Field descriptions

The following read-only information is displayed on the screen.

Data Port Location	
Description	This is the physical location of the port (node-card-port).
Valid entries	On node 1, this must be an RSM port (on non-EC systems) or the Utility port (on an EC system).
Device Type	
Description	This field describes the type of port.
Valid entries	This field is set to “MMLink.”
Device Name	
Description	This is the name of the device. This name is assigned by the system when Meridian Mail is installed, or when the port is reconfigured using the Install/data tape, or the “Modify hardware” tool.

Baud Rate	
Description	This field can be set to any rate for MMLink, subject to the cumulative baud rates specified for the system.
Valid entries	4800 and 9600 are the only available baud rates.

Parity	
Description	This is the method by which data is communicated.
Valid entries	This field is not used for MMLink.

View/Modify NWModem data port

Modify Data Port screen

The Modify Data Port screen for Networking modems allows you to view the NWModem data port information, and to specify the directory number (DN) of the modem connected to the selected port.

```
Hardware Administration
Modify Data Port

Data Port Location:    1-1-4

Device Type:           NWModem

Device Name:           MODO114

Network Modem DN:      _______

Select a softkey >

Save    Cancel
```

Field descriptions

The following fields are displayed on this screen. Only the Network Modem DN field is modifiable.

Data Port Location	
Description	This is the physical location of the port in the Meridian Mail system (node-card-port).
Valid entries	Do not configure networking on an SBC or MMP40 port. For EC Systems, use one of the ports on the Utility card. For non-EC systems, use one of the ports on the RSM card.

Device Type	
Description	This field describes the type of port.
Valid entries	This field is set to “NWModem.”

Device Name	
Description	This is the name of the device. This name is assigned by the system when Meridian Mail is installed, or when the port is reconfigured using the Install/data tape, or the “Modify hardware” tool.

Network Modem DN	
Description	This is the directory number (up to eight digits) used to identify the modem connected to the port.

View PMS data port

Introduction

PMS data ports are applicable only to Hospitality systems. You do not need to configure this port if your Meridian Mail hospitality system is not connected to a Property Management System (PMS).

View Data Port screen

The View Data Port screen for PMS allows you to view the baud rate and parity of the serial connection to the Meridian 1.

```
                    Hardware Administration
  View Data Port
  Data Port Location:   1-8-3
  Device Type:          PMS
  Device Name:          PMS0 183
  Baud Rate:            1200 2400 4800 9600
  Parity:               Even Odd None

Select a softkey >
  Exit
```

Field descriptions

The following read-only fields are displayed on this screen.

Data Port Location	
Description	This is the physical location of the port in the Meridian Mail system (node-card-port).

Device Type	
Description	This field describes the type of port.
Valid entries	This field is set to “PMS.”

Device Name	
Description	This is the name of the device. This name is assigned by the system when Meridian Mail is installed, or when the port is reconfigured using the Install/data tape, or the “Modify hardware” tool.
Baud Rate	
Description	The selected baud rate is highlighted.
Valid entries	The baud rate must be set to 1200.
Parity	
Description	This is the method by which data is communicated.
Valid entries	This field must be set to None.

View AdminPlus data port

Introduction

This screen is available only if AdminPlus is installed.

View Data Port screen

The View Data Port for AdminPlus screen allows you to view the baud rate and parity of the serial connection to the Meridian Mail Reporter PC.

```
                    Hardware Administration
  View Data Port
  Data Port Location:    1-8-1
  Device Type:           AdminPlus
  Device Name:           ADMN0 18 1
  Baud Rate:             2400 4800 9600
  Parity:                Even Odd None

Select a softkey >
   Exit
```

Field descriptions

The following read-only fields are displayed on this screen.

Data Port Location	
Description	This is the physical location of the port in the system (node-card-port).
Device Type	
Description	This field describes the type of port.
Valid entries	This field is set to “AdminPlus.”
Device Name	
Description	This is the name of the device. This name is assigned by the system when Meridian Mail is installed, or when the port is reconfigured using the Install/data tape.

Baud Rate	
Description	The selected baud rate is highlighted.
Valid entries	The baud rate should be set to 2400, 4800, or 9600, subject to the cumulative baud rate restrictions for MMLink, MSLink, and AdminPlus data ports on a node. See “Cumulative baud rate” on page 27-18.
Parity	
Description	This is the method by which data is communicated.
Valid entries	This field must be set to None.

View Modem data port

View Data Port screen The View Data Port for Modems screen allows you to view the modem characteristics.

```
                    Hardware Administration
  View Data Port

  Data Port Location:    1-8-4

  Device Type:           Modem

  Device Name:           CON0 184

  Baud Rate:             1200 2400 4800 9600

  Parity:                Even Odd None


Select a softkey >

   Exit
```

Field descriptions The following read-only fields are displayed on this screen.

Data Port Location	
Description	This is the physical location of the port in the system (node-card-port).
Device Type	
Description	This field describes the type of port.
Valid entries	This field is set to Modem.
Device Name	
Description	This is the name of the device. This name is assigned by the system when Meridian Mail is installed, or when the port is reconfigured using the Install/data tape.

Baud Rate	
Description	The selected baud rate is highlighted.
Valid entries	The setting depends on the current setup of the modem connected to the port.

Parity	
Description	This is the method by which data is communicated.
Valid entries	The setting depends on the current setup of the modem connected to the port.

View MSLink data port

View Data Port screen

The View Data Port screen for MSLink allows you to view the link characteristics of the link to the PC running Meridian Mail AutoAdmin.

```
                    Hardware Administration
  View Data Port

  Data Port Location:   2-3-1

  Device Type:          MSLink

  Device Name:          MSL0231

  Baud Rate:            2400 4800 9600 19200 38400

  Parity:               Even Odd None


Select a softkey >

    Exit
```

Field Descriptions

The following read-only information is displayed on the screen.

Data Port Location	
Description	This is the physical location of the port (node-card-port).
Device Type	
Description	This field describes the type of port.
Valid entries	This field is set to “MSLink.”
Device Name	
Description	This is the name of the device. This name is assigned by the system when Meridian Mail is installed, or when the port is reconfigured using the Install/data tape.

Baud Rate	
Description	This field can be set to any rate for MSLink, subject to the cumulative baud rates specified for the system.
Valid entries	2400, 4800, 9600, 19 200, and 38 400 are the available baud rates.

Parity	
Description	This is the method by which data is communicated.
Valid entries	This field must be set to None. It cannot be modified.

Section C: Printing node and data port information

In this section

Overview 27-46
Printing node and data port information 27-47

Overview

Introduction

The Hardware Administration menu can be used to print the following information for your system:

- node configuration
- data port configuration

Printing node and data port information

Introduction

Node and data port information can be printed through the Hardware Administration menu.

Procedure

To print node and data port information, follow these steps.

Step	Action
1	Select “Hardware Administration” from the Main Menu. **Result:** The Hardware Administration menu appears.
2	Choose either “Print All Node Information” or “Print All Data Port Information” and press <Return>. **Result:** The following softkeys appear: [Continue Printing] and [Cancel Printing].You are prompted to check that the printer is ready and online.
3	Press [Continue Printing] to print the information. **Result:** The node or data port information begins printing. Once printing is complete, the Hardware Administration menu is redisplayed. You may stop printing at any time by selecting [Cancel Printing].
4	Use [Cancel Printing] to cancel printing and return to the Hardware Administration menu. **Result:** Printing stops and the Hardware Administration menu is displayed. There may be some delay before control is returned to the screen while the system waits for the printer to stop printing.

Chapter 28

System status and maintenance

In this chapter

Overview	28-2
What is system status and maintenance?	28-3
Section A: System Status	28-5
Section B: Card Status	28-19
Section C: DSP Port Status	28-29
Section D: Channel Allocation Table	28-45
Section E: Disk Maintenance	28-61
Section F: Diagnostic Schedules	28-75

Overview

Introduction

The System Status and Maintenance function provides monitoring and control screens through which you can obtain views of the operational state of the system at four levels:

- system
- card
- DSP port
- disk

The System Status and Maintenance functions are used in the course of routine maintenance, and allow you to take any component of the system out of service for maintenance. It also allows you to perform diagnostics on selected components and schedule regular diagnostic activities.

A component can be taken out of service by disabling it (forcing it out of its operational state), or by performing a courtesy disable, which progressively disables active DSP ports as they become idle. The Courtesy Disable function available within System Status and Maintenance avoids any disruption of calls in progress.

See also

For help in developing a regular maintenance routine that includes System Status and Maintenance functions, see Chapter 18, “Routine maintenance”.

What is system status and maintenance?

System Status and Maintenance menu

When you select System Status and Maintenance from the Main Menu, this menu is displayed.

```
                    System Status and Maintenance

          1  System Status

          2  Card Status

          3  DSP Port Status

          4  Channel Allocation Table

          5  Disk Maintenance

          6  Diagnostic Schedules

          7  System Event and Error Reports


Select an item >

     Exit                                Silence Alarm
```

Types of tasks

A variety of tasks can be performed from this menu. The types of tasks are as follows.

System courtesy down
Take this action for broad maintenance activities, such as reconfiguring the Meridian 1, which requires powering down Meridian Mail.

Courtesy disable ports or (forced) disable nodes
Take this action to disable all ports on a node. This is necessary to put certain cards out of service (such as the MMP40 card) if they need to be replaced or if diagnostics need to be run.

Card disable
Take this action before performing diagnostics on an in-service card.

Courtesy disable or (forced) disable of DSP ports
Take this action before performing tests on a DSP port.

Channel Allocation Table modification

When you move agents from one queue to another (in order to dedicate them to a particular service), you must also modify the Channel Allocation Table to show this change.

Disk maintenance

On systems with Disk Shadowing installed, this selection allows you to disable or reenable Disk Shadowing. On both shadowed and unshadowed systems, this selection allows you to view the state of disks and run disk diagnostics.

Schedule diagnostic activities

This action provides a means of scheduling voice path diagnostics for a Meridian Mail system.

System Events and Error Reports

This allows you to set various System Error and Event Reporting options. For details, see Chapter 29, “SEERs and Meridian Mail Alarms”.

Section A: System Status

In this section

Overview	28-6
The System Status screen	28-8
Disabling/activating the system (“Courtesy Down”)	28-15
Disabling/enabling nodes	28-17
Courtesy disabling/enabling ports	28-18

Overview

Introduction

The System Status screen allows you to view the operational status of the system, change the status of nodes, courtesy disable the system, or courtesy disable ports on individual nodes.

This screen is identical to the System Status screen displayed from the Logon screen, except that this screen has more softkeys available which allow you to perform specific maintenance tasks.

When to use this feature

The System Status functions can be used to

- check the status of your system if you suspect that your system is not performing properly
- disable the system, a node, or DSP ports to perform routine maintenance or diagnostics
- disable a node to put a faulty card out of service so that it can be replaced (it is good practice to courtesy disable ports on the node that you want to disable)

System not performing properly

You may suspect a problem in your system if

- callers are unable to get through to users' mailboxes to leave a message
- users are unable to access Meridian Mail (phone rings, but Meridian Mail never picks up)
- the call must ring several times before the call is transferred to Meridian Mail

The above scenarios suggest that one of the following may be true:

- not enough channels are idle to handle the current demand
- parts of the system are faulty (the AML link, a node, or DSP port, for example)

Checking system status

Check the System Status screen to determine if callers or users are unable to get through to Meridian Mail because all channels are busy (active), or because parts of the system are faulty or disabled.

The System Status screen

Introduction

This section describes the System Status screen.

The System Status screen that you access from the System Status and Maintenance menu provides the following functions:

- Enable Node (see “Disabling/enabling nodes” on page 28-17)
- Disable Node (see “Disabling/enabling nodes” on page 28-17)
- Courtesy Disable Ports (see “Courtesy disabling/enabling ports” on page 28-18)
- Courtesy Down System/Activate System (see “Disabling/activating the system (“Courtesy Down”)” on page 28-15)

Note: Enable Node, Disable Node, and Courtesy Disable Ports softkeys do not appear on single node systems.

Reaching the screen—two ways

There are two ways to reach two different versions of the System Status screen: from the Main Menu and from the Logon/Status screen.

From the Main Menu

To reach the System Status screen from the Main Menu, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance. **Result:** The System Status and Maintenance menu is displayed.
2	Select System Status. **Result:** The System Status screen is displayed.

```
                          System Status and Maintenance
System Status: InService          Alarm Status: Critical=Off Major=On  Minor=On

Last Event:   66-11 Disk 0 is still down                              6/10 12:08

Link Status:   1-7-2: InService

                                   DSP Port Status                 Storage Used
Node  Type Status        Active Idle OutSv Faulty Pending Others    Voice Text
 1    MSP  InService
 2    SPN  InService       0     24    0     0      0      0          0%   1%
 3    SPN  InService       0     24    0     0      0      0          0%   1%
 4    SPN  InService       0     24    0     0      0      0          0%   1%

Select a softkey >

 Exit    Enable Node    Disable Node    Courtesy Disable Ports    Courtesy Down System
```

From the Logon/Status screen

To reach an abbreviated version of the System Status Screen from the Logon/Status screen, follow these steps.

Starting Point: The Logon/Status screen

Step	Action
1	Press the [System Status] softkey. **Result:** The System Status screen is displayed.

```
                                  System Status
System Status: InService          Alarm Status: Critical=Off Major=On  Minor=On

Last Event:   66-11 Disk 0 is still down                                6/10 12:08

Link Status:   1-7-2: InService

                                     DSP Port Status                 Storage Used
Node  Type Status        Active Idle OutSv Faulty Pending Others    Voice Text
 1    MSP  InService
 2    SPN  InService        0    24     0     0      0        0        0%   1%
 3    SPN  InService        0    24     0     0      0        0        0%   1%
 4    SPN  InService        0    24     0     0      0        0        0%   1%

Select a softkey >

    Exit
```

Note: You will not be able to access the maintenance softkeys from this version of the screen.

Field descriptions

The following fields appear on the System Status screen.

System Status	
Description	This field displays the current system status.
Possible status types	There are four possible status types. ***InService*** This indicates the system is running. ***CourtesyPending*** This indicates that the system is in the process of shutting down. This appears after using the [Courtesy Down System] softkey. Incoming calls are directed to an attendant. Calls in progress are not interrupted. Each DSP port is courtesy disabled as it becomes idle. The software remains loaded. ***CourtesyDown*** This indicates that the system has shut down and is no longer operational or accepting calls, but the software remains loaded. When the system is down, the [Courtesy Down System] softkey becomes [Activate System]. When the [Activate System] softkey is used, the system restarts. ***Loading*** This indicates the system is loading software during bootup.

Alarm Status	
Description	This indicates the state of each of the types of alarms described below.
Alarm types	There are three possible alarm types. ***Critical*** These alarms indicate a service-affecting problem that requires immediate attention. ***Major*** These alarms indicate a service-threatening problem that may be allowed to persist for up to 24 hours. If not attended to, the alarm could become critical. ***Minor*** These alarms indicate a problem that has no impact on the system or users. For more details, see Chapter 29, "SEERs and Meridian Mail Alarms".
Alarm states	Each alarm type can be in one of the following states. ***Off*** This state indicates that there are no new alarms. This does not necessarily mean that there are no error conditions. ***On*** This status indicates that one or more alarm situations were detected. ***Unk*** This indicates that the status is unknown.
Last Event	
Description	This is the most recent system event or error report (SEER) logged.
Link Status	
Description	This is the state of the AML link to the Meridian 1.
Link states	The link can be in one of the following states: ***InService*** This indicates that the link is operational. ***Faulty*** This state indicates that a hardware problem exists but that the data port remains operational.

Node	
Description	This is the node number.
Type	
Description	This is the type of node.
Status	
Description	This is the status of the nodes in your system. ***Note:*** The status at this level does not indicate the status of a given card on the node. For information on cards, see "The Card Status screen" on page 28-21.
Node states	***InService*** This state indicates that the node is operational. ***Unequipped*** This indicates that the node has not been defined in the hardware database. Refer to *System Administration Tools* (NTP 555-7001-305) for instructions on modifying the hardware database. ***Faulty*** This indicates that a hardware problem was detected or a critical program on the node is not operational. ***OutOfService*** This indicates that the node is no longer operational as a result of a forced disable. ***Loading*** This state indicates that the node is currently starting up and loading software into memory. ***ShuttingDown*** This state indicates that the node is being put out of service. ***Booting*** This indicates that the operating system is being loaded on the node.

DSP Port Status	
Description	These fields reflect the state of each DSP port on the associated node. For each DSP port that is in a particular state, an entry is made in the appropriate column.
DSP States	A DSP port may be in one of the following states. ***Active*** This indicates that the DSP port is operational and is currently in use. ***Idle*** This indicates that the DSP port is operational but not in use at the moment. The DSP port is ready to accept calls. ***OutSv*** This state indicates that the associated DSP port is not operational, as a result of a courtesy disable or forced disable. ***Faulty*** This state indicates that an error has been detected in the DSP port. ***Pending*** This state indicates that there has been a request to either shut down or restart the DSP port. The port is in the process of either shutting down or restarting. ***Others*** This state indicates that the DSP port is temporarily unavailable. This usually occurs while the system is booting up. The status remains as "Others" while the software is loading. Once fully loaded, the status becomes "Active" or "Idle." The status may also appear as "Others" when you reenable a port (for as long as the necessary software is loading). The status returns to "Idle" once the port has been enabled.

Storage Used	
Description	These fields indicate the amount of voice and text storage used as a percentage of available storage on the user volume of this node. (If the disk on a node is bad, percentages are not displayed.)

Disabling/activating the system (“Courtesy Down”)

Introduction

Use Courtesy Down for broad maintenance activities, such as reconfiguring the Meridian 1, which requires powering down Meridian Mail.

During a Courtesy Down, incoming calls are directed to an attendant. Calls in progress are not interrupted. Each DSP port is courtesy disabled as it becomes idle. The software remains loaded. This prevents Meridian Mail users from being suddenly disconnected from their voicemail session.

Procedure

These steps describe how to Courtesy Down the Meridian Mail system, and reenable the system after a Courtesy Down.

Starting Point: The System Status screen

Step	Action
1	Press [Courtesy Down System]. **Result:** You are prompted as to whether you want to Courtesy Down the system.
2	Press the up arrow until Yes appears as the response and press return. **Result:** The [Activate System] softkey replaces the [Courtesy Down System] softkey. It may take some time to disable the system since all active DSP ports on all nodes must first become idle.
3	After the system reaches CourtesyDown state, are all DSP ports now in the “OutSv” or “Others” columns? • If yes, go to step 4. • If no, disable the DSP ports manually according to the steps in “Disabling/enabling DSP ports in single mode” on page 28-40 or “Disabling/enabling DSP ports in range mode” on page 28-42, then go to step 4.

Step	Action
4	Perform the required maintenance activities.
5	Reenable the system by pressing [Activate System]. **Note:** The system can be reenabled at any time during the Courtesy Down process.
6	After the system returns to “InService” status, are all DSP ports either Idle or Active? • If all DSP ports are Idle or Active, press [Exit]. • If some DSP ports are in the OutSv or Others columns, reenable the DSP ports manually according to the steps in “Disabling/enabling DSP ports in single mode” on page 28-40 or “Disabling/enabling DSP ports in range mode” on page 28-42, then press [Exit].

Disabling/enabling nodes

Introduction

Take this action to disable all ports on a node. This is necessary in order to put certain cards out of service (such as the MMP40 card) if they need to be replaced or if diagnostics need to be run.

Note 1: You cannot disable an MSP node.

Note 2: This function is not available on single node systems.

Tip

Once the node is disabled, you can reactivate the system while the node is disabled. This will allow Meridian Mail to remain operational for users on the other nodes while you are working on the disabled node.

Procedure

To disable, then re-enable a node, use the following steps.

Starting Point: The System Status screen

Step	Action
1	Is the node currently disabled? • If no, go to step 2. • If yes, go to step 5.
2	Courtesy Down the system. See “Disabling/activating the system (“Courtesy Down”)” on page 28-15.
3	Press the [Disable Node] softkey. **Result:** You are prompted for the node number.
4	Enter the node number followed by <Return>. **Result:** The node status changes to “OutOfService.”
5	Perform any required maintenance activities.
6	Press [Enable Node]. **Result:** You are prompted for the node number.
7	Enter the node number followed by <Return>. **Result:** The node status changes to “InService.”

Courtesy disabling/enabling ports

Introduction

When you courtesy disable ports, incoming calls on a particular node are directed to an attendant. Calls in progress are not interrupted. Each DSP port is courtesy disabled as it becomes idle. The software remains loaded. This prevents Meridian Mail users from being suddenly disconnected from their voicemail session.

Take this action to courtesy disable all ports on a node. This is necessary in order to put certain cards out of service if they need to be replaced or if diagnostics need to be run.

Note: This function is not available on single node systems.

Procedure

To courtesy disable ports, then re-enable them, use the following steps.

Starting Point: The System Status screen

Step	Action
1	Is the node currently disabled? • If no, go to step 2. • If yes, go to step 4.
2	Press [Courtesy Disable Ports]. **Result:** You are prompted for the number of an in-service node.
3	Enter the node number followed by <Return>. **Result:** As the DSP ports for the node become free, the System Status screen will show the DSP ports for that node as being in “Pending” then in “OutSv” state.
4	Perform any required maintenance activities.
5	Press [Enable Node]. **Result:** You are prompted for the number of an out-of-service node.
6	Enter the node number followed by <Return>. **Result:** The status of the DSP ports for the node changes to “Others” and then to “Idle.”

Section B: Card Status

In this section

Overview 28-20
The Card Status screen 28-21
Enabling/disabling cards 28-27
Running out-of-service diagnostics 28-28

Overview

Introduction

The Card Status option on the System Status and Maintenance menu allows you to check the status of the cards on your system, enable or disable voice processor cards as required, and run out-of-service diagnostics on a disabled or faulty card.

To disable cards that are not voice processor cards (for example, an MMP40 card), you must use the disable-node function (see "Disabling/enabling nodes" on page 28-17).

When to use this feature

The Card Status screen can be used to

- check the status of the cards in your system if you suspect that your system is not performing properly (see "The Card Status screen" on page 28-21)

  The Card Status screen will show you if any of the cards are faulty or disabled. If a card is faulty or disabled, perform a diagnostic check on the card (see "Running out-of-service diagnostics" on page 28-28).
- disable a voice processor card to perform a diagnostic check, or to replace the card (see "Enabling/disabling cards" on page 28-27)

Note: Only voice processor cards can be disabled through the Card Status screen. To disable other cards, you must use the disable-node function (see "Disabling/enabling nodes" on page 28-17).

- perform a diagnostic check on a card that you suspect is not working properly, or on a new card that has just been installed in your system (see "Running out-of-service diagnostics" on page 28-28)

The Card Status screen

Introduction

The Card Status screen displays the operational status of the cards in your system. The enable/disable softkeys displayed on this screen are used to enable and disable voice processor cards only.

If you suspect a problem with your system hardware, you can use this screen to check that all the cards on a node are functioning properly. You can also run diagnostics on a card from the Card Status screen.

Before running diagnostics on a card, you must first disable it. See "Enabling/disabling cards" on page 28-27.

Reaching the screen

To check card status, use the following steps.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance. **Result:** The System Status and Maintenance menu is displayed.
2	Select Card Status
3	Do you have a multinode system? • If yes, you are prompted for the node number. Enter the node number followed by <Return>. **Result:** The Card Status screen for the node you requested is displayed. • If no, you are immediately taken to the Card Status screen.

Card status screen

The screen has the same appearance for all Meridian Mail platforms, but the types of cards listed under the Description field will vary. The types of cards available are described in the section “Field descriptions” on page 28-23.

```
                    System Status and Maintenance
Card Status for Node 2

System Status: InService          Alarm Status: Critical=Off Major=On  Minor=On

Card#    Location   Description                              Status

  1       2-1-0     16 Megabyte Meridian Mail Processor      InService
  2       2-2-0     Voice Processor                          InService
  3       2-3-0     Voice Processor                          InService
  4       2-4-0     Voice Processor                          InService

Select a softkey >

     Exit        Enable Card    Disable Card                OutOfService
                                                            Diagnostics
```

Field descriptions

The following fields appear on the Card Status screen.

System Status	
Description	This field displays the current system status.
Possible status types	There are four possible status types. ***InService*** This indicates the system is running. ***CourtesyPending*** This indicates that the system is in the process of shutting down. ***CourtesyDown*** This indicates that the system has shut down and is no longer operational or accepting calls. ***Loading*** This indicates the system is loading software during bootup.

Alarm Status	
Description	This indicates the state of each of the types of alarms described below.
Alarm types	There are three possible alarm types. ***Critical*** These alarms indicate a service-affecting problem that requires immediate attention. ***Major*** These alarms indicate a service-threatening problem that may be allowed to persist for up to 24 hours. If not attended to, the alarm could become critical. ***Minor*** These alarms indicate a problem that has no impact on the system or users. For more details, see Chapter 29, "SEERs and Meridian Mail Alarms".
Alarm states	Each alarm type can be in one of the following states. ***Off*** This state indicates that there are no new alarms. This does not necessary mean that there are no error conditions. ***On*** This status indicates that one or more alarm situations were detected. ***Unk*** This indicates that the status is unknown.
Card #	
Description	This is the number of each card in the selected node.
Location	
Description	This is the physical location (Node-Card-Port) of each card in the selected node.
Description	
Description	This is the type of card at that location.
Valid entries	The possible card types are listed here. Depending on your system type, you will not see all of these cards on your system.

16 Megabyte Meridian Mail processor (MMP40)
This is the Meridian Mail processor (CPU) card which includes a 24 MHz 68040 processor, 16 Mbytes of memory, up to two RS-232 serial ports, and a SCSI interface processor. It is displayed for MMP40 systems.

RS232 Service Module (RSM)
This is an RS-232 card (for non-EC systems).

High Speed Bus
This is the high-speed bus (also called HABC for High Availability Bus Controller).

Network Voice Processor (NVP)
This is the 16 kbyte network voice processor.

32K Network Voice Processor (NVP32)
This is the 32 kbyte network voice processor.

Utility (UTIL)
This card, on EC systems only, contains a high speed bus. It also includes four auxiliary RS-232 ports. (1- to 4-node systems require one of these cards; 5-node systems with 60 or more ports require two of these cards.)

Voice Processor (VP4/VP8)
These cards are voice processor cards that provide four and eight channels respectively.

Empty
The card slot is empty.

Status	
Description	This is the current state of each card on the selected node.
Card states	***InService*** This state indicates that the card is operational. ***Faulty*** This state indicates that a hardware problem has been detected for the card. ***Unequipped*** This state may indicate one of two conditions: (a) the card slot is empty but a card is defined as being in that location in the hardware database or (b) the card is in the slot but is not defined in the hardware database. ***OutOfService*** This state indicates that the card has been disabled.

Enabling/disabling cards

Introduction

Only voice processor cards can be disabled from the Card Status screen. To disable other cards (such as the MMP40 card), you must use the disable-node function (see "Disabling/enabling nodes" on page 28-17).

Procedure

Starting Point: The Card Status screen

Step	Action
1	Press [Disable Card]. **Result:** You are prompted for the number of the card you wish to disable. **Note:** You can only disable voice processor cards from this screen.
2	Enter the number of the card followed by <Return>. **Result:** The system may take some time disabling the card. The message "WORKING..." will be displayed during this interval. The card is disabled when its status changes to "OutOfService".
3	Perform diagnostics on the card as described in "Running out-of-service diagnostics" on page 28-28.
4	Press [Enable Card]. **Result:** You are prompted for the number of an out-of-service card.
5	Enter the number of an out-of-service card followed by <Return>. **Result:** The system may take some time enabling the card. The message "WORKING..." will be displayed during this interval. The card is enabled when its status changes to "InService".

Running out-of-service diagnostics

Introduction

If you suspect a card is faulty, run out-of-service diagnostics on the card. If the test shows the card is faulty, it is assigned a "Faulty" status which can be observed on the Card Status screen.

Procedure

Starting Point: The Card Status screen

Step	Action
1	Are you running out-of-service diagnostics on a voice processor card? • If yes, disable the voice processor card according to the instructions in "Enabling/disabling cards" on page 28-27. • If no, disable the node according to the instructions in "Disabling/enabling nodes" on page 28-17.
2	Press [OutOfService Diagnostics]. **Result:** You are prompted for the number of an out-of-service card.
3	Enter the card number followed by <Return>. **Result:** The message "WORKING..." will be displayed while diagnostics are running. When diagnostics are completed, the result is displayed in a screen message.

IF diagnostics	THEN
fail	the card status will be "Faulty." There is a hardware problem with the card and it should be replaced. Refer to the *Installation and Maintenance Guide* for your platform.
pass	the card can be reenabled.
pass on a card that was already in a "Faulty" state	the card is put in "OutOfService" state.

Section C: DSP Port Status

In this section

Overview	28-30
The DSP Port Status screen	28-31
Detailed view of the DSP Port Status screen	28-38
Single mode and range mode	28-39
Disabling/enabling DSP ports in single mode	28-40
Disabling/enabling DSP ports in range mode	28-42

Overview

Introduction

The DSP Port Status screen allows you to view the operational status of the DSP ports in the system and enable or disable individual ports when necessary.

Definition: DSP

A DSP is a Digital Signal Processor which is located on a voice processor card. Each DSP supports two physical port locations. As a result, each DSP can support two voice processing ports or one multimedia port (for multimedia services, both physical ports of a DSP are used to configure one multimedia port). The configured port (voice or multimedia) is referred to as a DSP port or just as a port.

When to use this feature

You would use this feature to

- check the status of DSP ports (are any ports Faulty or OutOfService?)
- disable a port prior to modifying information relating to the port on the Channel Allocation Table

  If you are dedicating a port, or assigning a specific outbound service to a port, you must show this on the Channel Allocation Table. A port must be disabled before any information relating to it can be modified on the Channel Allocation Table.
- reenable a port that was taken out of service

The DSP Port Status screen

Introduction

This section describes the DSP Port Status screen.

The DSP Port Status screen that you access from the System Status and Maintenance menu provides the following functions:

- Enable Port (see pages 28-40 to 28-42)
- Disable Port (see pages 28-40 to 28-42)
- Courtesy Disable Port (see pages 28-40 to 28-42)
- Change to Range Mode/Change to Single Mode (see "Single mode and range mode" on page 28-39)

Reaching the screen—two ways

There are two ways to reach two different versions of the System Status screen.

From the Main Menu

To reach the DSP Port Status screen from the Main Menu, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance. **Result:** The System Status and Maintenance menu is displayed.
2	Select DSP Port Status.

Step	Action
3	Do you have a multinode system? • If yes, you are prompted for the node number. Enter the number followed by <Return>. • If no, the DSP Port Status screen is displayed immediately. **Result:** The DSP Port Status screen is displayed.

```
                          System Status and Maintenance
DSP Port Status for Node 2 (C=Card D=DSP P=Port)

System Status: InService          Alarm Status: Critical=Off Major=On  Minor=On

C-D-P        DSP Port Status
2-1-*         1-Idle
2-2-*         2-Idle
2-3-*         3-Idle          4-Idle
2-4-*         5-Idle          6-Idle
3-1-*         7-Idle          8-Idle
3-2-*         9-Idle         10-Idle
3-3-*        11-Idle         12-Idle
3-4-*        13-Idle         14-Idle
4-1-*        15-Idle         16-Idle
4-2-*        17-Idle         18-Idle
4-3-*        19-Idle         20-Idle
4-4-*        21-Idle         22-Idle

Select a softkey >

   Exit      Enable Port   Disable Port   Courtesy      Change to
                                          Disable Port   Range Mode
```

From the Logon screen

To reach an abbreviated version of the DSP Port Status Screen from the Logon screen, follow these steps.

Starting Point: The Logon/Status screen

Step	Action
1	Press the [DSP Port Status] softkey. **Result:** The DSP Port Status screen is displayed.

```
                                DSP Port Status
DSP Port Status

      Ports
Node  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

  2   .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  3   .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
  4   .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .




a = Active/In Use    . = Idle              O = Out of Service     ? = Unknown
F = Faulty           P = Pending           U = Unequipped         R = NoResource
L = Loading          C = CourtesyDown

Select a softkey >

     Exit                                   Detailed
```

Note: You will not be able to access the maintenance softkeys from this version of the menu.

See also

For a description of the Detailed view of this screen, see “Detailed view of the DSP Port Status screen” on page 28-38.

DSP port status screen

The following is an example of the DSP Port Status screen displayed when you select DSP Port Status from the System Status and Maintenance menu.

```
                    System Status and Maintenance
DSP Port Status for Node 2 (C=Card D=DSP P=Port)

System Status: InService          Alarm Status: Critical=Off Major=On  Minor=On

C-D-P        DSP Port Status
2-1-*         1-Idle
2-2-*         2-Idle
2-3-*         3-Idle          4-Idle
2-4-*         5-Idle          6-Idle
3-1-*         7-Idle          8-Idle
3-2-*         9-Idle         10-Idle
3-3-*        11-Idle         12-Idle
3-4-*        13-Idle         14-Idle
4-1-*        15-Idle         16-Idle
4-2-*        17-Idle         18-Idle
4-3-*        19-Idle         20-Idle
4-4-*        21-Idle         22-Idle

Select a softkey >

Exit | Enable Port | Disable Port | Courtesy Disable Port | Change to Range Mode
```

When the status for a port is not displayed, this means that both ports from the DSP were used to configure one multimedia port, so only one configured port is present instead of two.

In the screen example, the first two ports on card 2 have been configured into one multimedia port (port 1). And the next two ports on card 2 have also been configured into one multimedia port (port 2).

The port numbering on this screen is also adjusted so that no number is skipped, even if a port is blocked for a multimedia port. As a result, the port numbers reflect the total number of configured ports on the node. The port numbers shown here match the port numbers shown in the DSP Port Status screen accessed from the Logon screen.

Field descriptions

The following fields appear on the DSP Port Status screen.

System Status	
Description	This field displays the current system status.
Possible status types	There are four possible status types. ***InService*** This indicates the system is running. ***CourtesyPending*** This indicates that the system is in the process of shutting down. ***CourtesyDown*** This indicates that the system has shut down and is no longer operational or accepting calls. ***Loading*** This indicates the system is loading software during bootup.

Alarm Status	
Description	This indicates the state of each of the types of alarms described below.
Alarm types	There are three possible alarm types. ***Critical*** These alarms indicate a service-affecting problem that requires immediate attention. ***Major*** These alarms indicate a service-threatening problem that may be allowed to persist for up to 24 hours. If not attended to, the alarm could become critical. ***Minor*** These alarms indicate a problem that has no impact on the system or users. For more details, see Chapter 29, “SEERs and Meridian Mail Alarms”.
Alarm states	Each alarm type can be in one of the following states. ***Off*** This state indicates that there are no new alarms. This does not necessarily mean that there are no error conditions. ***On*** This status indicates that one or more alarm situations were detected. ***Unk*** This indicates that the status is unknown.

C-D-P (location)	
Description	This is the physical location of each DSP port on the selected node (card number-DSP-port).

DSP Port Status	
Description	This is the current state of each DSP port. The status can be one of the following.
DSP states	***Active*** This status indicates that the DSP port is operational and in use. ***Idle*** This status indicates that the DSP port is operational but not currently in use. ***Faulty*** This status indicates that the system has detected an error in the DSP port. ***UnEquipped*** This status indicates that the DSP port is not defined in the hardware database. For more information about modifying the hardware database, refer to *System Administration Tools* (NTP 555-7001-305). ***POutService*** This status indicates that the DSP port is in the process of shutting down. If [Courtesy Disable Port] was used, the DSP port is still active while in this state. Once the active call is disconnected, the port status will be OutOfService. ***OutOfService*** This status indicates that the DSP port is no longer operational as a result of a courtesy disable or forced disable. ***NoResources*** This status indicates a transition state that occurs during the initial stages of software loading (after a request to enable a port). When software begins to load, the port is initially in this state, followed by Loading and then Idle, once the software has finished loading.

DSP states (continued)	***Loading*** This status indicates that the DSP port is currently starting up after a request to enable and that the necessary software is loading. ***CtsyDown*** This status indicates that the DSP port is down as a result of a Courtesy Down System. ***PCtsyDown*** This status indicates that the DSP port is in the process of shutting down as a result of a Courtesy Down System, pending the disconnection of any active calls. The DSP port is still active while in this state. Once the active call is disconnected, the port status will be CtsyDown.

Detailed view of the DSP Port Status screen

Introduction

When you access the DSP Port Status screen from the Logon screen, you can get a detailed view by pressing the [Detailed] softkey.

For each port, you are told the port type (basic-voice, full-voice, or multimedia) and the port status (for example, Idle, Active, or OutOfService).

When to use this feature

If you have a mixture of port types (basic-voice, full-voice, multimedia), the detailed view presents a clear picture of what types of ports are installed in your system, how many, and where.

The screen

The following is an example of the DSP Port Status screen—Detailed view.

```
                                DSP Port Status
DSP Port Status

      Ports
Node  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24

  2  M. M. M. M. BO BO BO BO VO VO VO VO VO VO VO VO VO VO VO VO
  3  VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO
  4  VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO VO




V = Full Voice       B = Basic Voice       M = Multimedia
a = Active/In Use    . = Idle              O = Out of Service     ? = Unknown
F = Faulty           P = Pending           U = Unequipped         R = NoResource
L = Loading          C = CourtesyDown
------------------------------------------------------------------------------
Select a softkey >

     Exit                                   Brief
```

In this example, node 2 has four idle multimedia ports (M.). Node 2 also has four basic-voice ports that are out of service (BO). All other ports are full-voice ports that are out of service (VO).

Single mode and range mode

Description

Single mode allows you to enable, disable, or courtesy disable individual DSP ports one at a time.

Range mode allows you to enable, disable, or courtesy disable a contiguous range of DSP ports at once. For example, it will work if you need to disable ports 3 to 7, but not if you need to disable ports 1, 3, and 7.

Disabling/enabling DSP ports in single mode

Introduction

This section describes how to disable ports in single mode (one port at a time).

Note: If a port is faulty and you attempt to disable it, the screen message will be the same as if you are disabling an idle port. However, the port will not be disabled. A faulty port cannot be disabled or enabled.

Disable Port versus Courtesy Disable Port

The procedure in this section asks you to check if a port is idle or active before disabling it. If a port is idle, you can use the Disable Port softkey. If a port is active (it is processing a call to Meridian Mail), you can use the Courtesy Disable Port softkey.

The courtesy disable method waits until the call is disconnected before disabling the port. This prevents users from being disconnected suddenly from Meridian Mail.

If you use the Disable Port softkey to disable an active port, the caller is abruptly disconnected.

Procedure

Starting Point: The System Status and Maintenance menu

Step	Action
1	Select DSP Port Status. • If you have a single node system, the DSP Port Status screen is displayed. Go to step 3. • If you have a multinode system, go to step 2.
2	For multinode systems, enter the number of the node on which the DSP port resides, followed by <Return>. **Result:** The DSP Port Status screen is displayed.
3	Is the DSP port active? • If yes, press [Courtesy Disable Port]. • If no, press [Disable Port]. **Result:** You are prompted for the number of a DSP port.
4	Enter the DSP port number followed by <Return>. **Result:** The system may take some time to disable the port. In the case of a courtesy disable, the system waits until the active call has been disconnected. The system displays a message informing you that the port is being disabled. The message “WORKING...” may also be displayed. While the port is being disabled, its status will change to POutService and then to OutOfService.
5	Perform any required maintenance activities.
6	Press [Enable Port]. **Result:** You are prompted for the number of a DSP port.
7	Enter the DSP port number followed by <Return>. **Result:** The system may take some time to enable the port. The system displays a message informing you that the port is being enabled. The message “WORKING...” may also be displayed. While the port is being enabled, its status will change to “Loading” and then to “Idle.”
8	Press [Exit] to return to the System Status and Maintenance menu.

Disabling/enabling DSP ports in range mode

Introduction

Range mode allows you to disable or enable a contiguous range of DSP ports at once. This saves time over disabling or enabling ports one at a time.

Note: If a port is faulty and you attempt to disable it, the screen message will be the same as if you are disabling an idle port. However, the port will not be disabled. A faulty port cannot be disabled or enabled.

Disable Port versus Courtesy Disable Port

The procedure in this section asks you to check if the ports are idle or active before disabling them. If the ports are idle, you can use the Disable Port softkey. If some of the ports are active (they are processing calls to Meridian Mail), you can use the Courtesy Disable Port softkey.

The courtesy disable method waits until the call is disconnected before disabling the port. This prevents users from being disconnected suddenly from Meridian Mail.

If you use the Disable Port softkey to disable an active port, the caller is abruptly disconnected.

Procedure

Starting Point: The System Status and Maintenance menu

Step	Action
1	Select DSP Port Status. • If you have a single node system, the DSP Port Status screen is displayed. Go to step 3. • If you have a multinode system, go to step 2.
2	For multinode systems, enter the number of the node on which the DSP port resides, followed by <Return>. **Result:** The DSP Port Status screen is displayed.
3	Press [Change to Range Mode]. **Result:** The softkey now shows [Change to Single Mode].
4	Are DSP ports active? • If yes, press [Courtesy Disable Port]. • If no, press [Disable Port]. **Result:** You are prompted for the number of the first DSP port in the range you want to force disable or courtesy disable.
5	Enter the number of the first DSP port in the range followed by <Return>. **Result:** You are prompted for the number of the last DSP port in the range.
6	Enter the number of the last DSP port in the range followed by <Return>. **Result:** The system will begin to disable the DSP ports. This may take some time. If you are courtesy disabling the ports, the system will wait for each port to become idle before it disables them. While the ports are being disabled, their status will change to “POutService” and then to “OutOfService.” The message “WORKING...” may also be displayed at this time. After the disabling is completed, the system displays a message indicating the number of ports that were successfully disabled, and the number of ports that could not be disabled.
7	Perform any required maintenance activities.
8	Press [Enable Port]. **Result:** You are prompted for the number of the first DSP port in the range of ports you wish to enable.

Step	Action
9	Enter the number of the first DSP port followed by <Return>. **Result:** You are prompted for the number of the last DSP port in the range.
10	Enter the number of the last DSP port followed by <Return>. **Result:** The system may take some time enabling the ports. The system displays a message to inform you that the DSP ports are being enabled. While the ports are being enabled, their status will change to “Loading” and then to “Idle.” After the enabling is completed, the system displays a message indicating the number of ports that were successfully enabled, and the number of ports that could not be enabled.
11	Press [Exit] to return to the System Status and Maintenance menu.

Section D: Channel Allocation Table

In this section

Overview 28-46
The Channel Allocation Table 28-47
Modifying the Channel Allocation Table 28-59

Overview

Introduction

The Channel Allocation Table (CAT) allows you to

- view how channels are currently allocated across different queues and services
- see what the distribution of port types is (the number of basic, full-voice, and multimedia ports)
- move agents from one queue to another as part of the procedure to dedicate a port

When to use this feature

Normally, you will not have to configure this table. When the Meridian Mail software is installed, the installation technician configures the switch to match the Channel Allocation Table.

This is also true when you perform a channel expansion (to add new agents). You generally do not have to modify the CAT because it is updated with the information that was provided during the expansion.

However, when you move agents from one queue to another (in order to dedicate them to a particular service), you will have to modify the CAT to show that the agent is now associated with a different queue and that the agent is dedicated to a particular service.

When to dedicate ports

Dedicating ports to a particular service reduces the overall efficiency of your port usage, so you should consider whether it is necessary to dedicate ports. Note that even when you have separate queues set up for basic, full-voice, and multimedia ports, these ports can be shared for outbound services (such as Remote Notification and Fax Outcalling).

For more information about port types and dedicating ports, see the section "Planning your configuration" on page 23-13.

The Channel Allocation Table

Introduction

The Channel Allocation Table (CAT) determines how agents on the switch are associated with DSP ports on Meridian Mail.

Agents are identified by a terminal number (TN), an ACD directory number (DN), and a single call non-ringing (SCN) DN. Each DSP port must be associated with an existing ACD agent in the Meridian 1 database. This is to handle the queuing of calls coming in to Meridian Mail, and to handle dial-out features such as Remote Notification and Delivery to Non-Users.

> **ATTENTION**
>
> The Channel Allocation Table (CAT) should only be configured by those who know how to program the switch.

When to use

When you move agents from one queue to another (in order to dedicate them to a particular service), you will have to modify the CAT to indicate the ACD DN with which the agent is now associated, as well as the service to which it is dedicated.

Note that even when you have separate queues set up for basic, full-voice, and multimedia ports, these ports can be shared for outbound services (such as Remote Notification and Fax Outcalling).

For a complete explanation of how to dedicate ports, and how to decide if you need to dedicate ports, see the section "Planning your configuration" on page 23-13.

Reaching the screen

To reach the Channel Allocation Table screen, use the following procedure.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance. **Result:** The System Status and Maintenance menu is displayed.
2	Select Channel Allocation Table.
3	Do you have a multinode system? • If yes, you are prompted for the node number. Enter the node number followed by <Return>. **Result:** The Channel Allocation Table for the node you requested is displayed. • If no, you are immediately taken to the Channel Allocation Table.

The CAT screen

The Channel Allocation Table also lists the maximum number of voice ports and minimum number of multimedia ports that you can configure, and how the different port types are currently allocated. The Choice of Services list at the top of the screen lists all the services that can be dedicated to a port. To hide this list, press the [Hide Choice of Services] softkey.

```
                          System Status and Maintenance
Channel Allocation Table for Node 2 (C=Card D=DSP P=Port)
Choice of Services:
ALL All Services          AN  AMIS Networking       AS  Announcement Service
EN  Enterprise Networking EM  Express Messaging     FOC Fax Outcalling
ACC Meridian ACCESS       NW  Meridian Networking   PM  Prompt Maintenance
RA  Remote Activation     OC  RN/DNU Outcalling     TS  Thru-Dial Service
TR  Transcription Service VF  Voice Forms Service   MS  Voice Menu Service
VM  Voice Messaging       VS  Voice Softkey

Limit; MaxVoice MinMulti; MaxFull;            ---------Allocated---------
  72      68        2        68               M/F:  2   V/F: 66   V/B:  2

 #  C-D-P    TN        ACD DN     SCN     Type  Capability Outbound
 1  2-1-1 009-0-02-00 3651      2800      Multi Full       ALL
          009-0-02-01 blocked for Multimedia port 2-1-1.
 2  2-2-1 009-0-02-02 3651      2802      Multi Full       ALL
          009-0-02-03 blocked for Multimedia port 2-2-1.
 3  2-3-1 009-0-02-04 3659      2804      Voice Full Basic ALL
                                                                  MORE BELOW
Select a softkey >

     Save        Cancel                                  Hide Choice of
                                                            Services
```

How port information is presented

Ports that are configured to support multimedia services (multimedia ports) require the use of both DSP ports supported by a DSP. The location of the first port supported by the DSP is considered the location of the multimedia port. The second physical port location supported by the DSP is considered to be blocked for the multimedia port. This is reflected in the CAT by a row following the multimedia port with the message “blocked for Multimedia port C-D-P,” where C-D-P is the “Card-DSP-Port” number of the multimedia port.

The number of DSP ports on a system may be very large. Therefore, when you choose to view the CAT on a multinode system, you are prompted for a node number to limit the scope to one node at a time. The CAT screen then displays information for that node.

Field descriptions

The following items appear on the Channel Allocation Table screen.

Choice of Services	
Description	This is a list of voice or fax services and their associated acronyms.
Service restrictions	The following services are available only if voice menus are installed: • AS (Announcement Service) • PM (Prompt Maintenance) • RA (Remote Activation) • TS (Thru-Dial Service) • MS (Voice Menu Service) Greeting Change Service (GS) is available only if Voice Messaging (VMUIF) is installed. Express Messaging (EM) and Call Answering (CA) are available only if Voice Messaging (MMUI) or Hospitality is installed. Transcription Service (TR) and Voice Forms Service (VF) are available only if the Voice Forms feature is installed. Meridian Networking (NW), Meridian ACCESS (ACC), AMIS Networking (AN), RN/DNU Outcalling (OC), and Fax Outcalling (FOC) appear only if the feature is installed.

Limit	
Description	This is the number of physical port locations on the system from which voice and multimedia ports are derived.

MaxVoice	
Description	This is the maximum number of voice ports (basic and full) allowed on the system according to your system's keycode. This number plus the MinMulti number is the maximum number of ports allowed on the system.

MinMulti	
Description	This is the minimum number of multimedia ports required on the system according to your system's keycode. The system will not allow you to reduce the number of multimedia ports on the system to below the MinMulti value.

MaxFull	
Description	This is the maximum number of full service ports (full service voice or multimedia) allowed on the system according to your system's keycode.

Allocated	
Description	This field shows how the ports are currently allocated between full service multimedia, full service voice, and basic service voice.
Allocations	• ***M/F*** The number of full service multimedia ports on the system. • ***V/F*** The number of full service voice ports on the system. • ***V/B*** The number of basic service voice ports on the system. Basic service ports must also be voice ports. ***Note:*** Multimedia ports require full service capability, so basic service multimedia ports are not available.

C-D-P	
Description	This is the physical location of the DSP port in the Meridian Mail system.
Numbering scheme	This number represents the card-DSP-port number. The node number is shown in the title at the top of the screen for multinode systems. This is a read-only field. The number to the left of the C-D-P field counts the ports and corresponds to the port numbers shown in the DSP Port Status screen.
TN	
Description	This is the terminal number or routing address. This is a read-only field specifying the physical location of the corresponding agent in the switch. The elements in the address represent the network loop, shelf, card slot, and unit (port) on the switch.
ACD DN	
Description	This is the primary DN. This is the directory number assigned to the ACD agent queue that contains this port. ***Note:*** Before changing the Primary DN, the DSP port must be disabled (use the DSP Port Status screen). If the port is not disabled, this is a read-only field.
Multiple queues	If you have more than one agent queue in your configuration (to service different types of ports or dedicated services), ensure that you enter the ACD DN of the queue that contains this port. This ACD DN is configured in Overlay 23 on the Meridian 1.

SCN	
Description	This is the Single Call Non-ringing DN. This DN corresponds to the secondary DN of the agent that corresponds to this port. This DN is the Key 1 Single Call Non-ringing DN (SCN-DN) assigned to the corresponding agent (not the agent ID associated with Key 0 on the agent set). ***Note:*** Before changing the SCN DN, the DSP port must be disabled (use the DSP Port Status screen). If the port is not disabled, this is a read-only field.
Considerations	This DN is taken from Overlay 11 on the Meridian 1. If the DN is not the same as the SCN DN taken from Overlay 11 on the Meridian 1, then features that require Meridian Mail to generate a call (such as Call Sender and Thru-Dial) will not function. For more information about this DN, refer to "Programming the Meridian 1" in the *Installation and Maintenance Guide* (NTP 555-70x1-250).
For Card Option Users	Do not change the SCN DNs. They have been configured by Meridian Mail technicians. Changing them could create a conflict.

Type	
Description	This field could show "Voice" or "Multi."
Values	***Voice*** This indicates a port that can provide voice services (such as Voice menus, Announcements, RN/DNU Outcalling, and so on). ***Multi*** This indicates a port that can provide multimedia-related services (such as Fax Outcalling), as well as voice services. A "Multi" port is configured from two port locations. As a result, the next port location is labeled as "blocked."

Capability	
Description	This field indicates the range of services supported on this port. The two ranges are “Basic” and “Full.” Note that all basic services can also run on full service ports.
Basic services	The following “Basic” services are available: • ACC—Meridian ACCESS • AS—Announcement Service • MS—Voice Menu Service • PM—Prompt Maintenance • RA—Remote Activation • TS—Thru-Dial Service • VS—Voice Softkey
Full services	“Full” services include all basic services plus the following: • VM—Voice Messaging • EM—Express Messaging • CA—Call Answering • AN—AMIS Networking Agent • OC—RN/DNU Outcalling • HM—Hospitality Messaging • CO—Post-Checkout Mailbox • VF—Voice Forms Service • TR—Transcription Service • NW—Meridian Networking • FOC—Fax Outcalling ***Note:*** RN/DNU Outcalling supports Remote Notification and Delivery to Non-User features. Fax Outcalling supports Fax-on-Demand same-call delivery and fax call-back delivery, Fax Information (FI), and Fax Item Maintenance (FIM).

Outbound	
Description	When Meridian Mail makes an outbound call, it checks this column to see what ports can be used. "ALL" indicates the port can be used for any outbound service (the port is shared for outbound calls). If you are dedicating the port to a particular service (outbound or inbound service), enter the service acronym in this column. This will prevent Meridian Mail from using that port for another outbound service.
Example	If you enter "OC" in this column for a particular port, the only outbound calls that can be made through this port are OC (RN/DNU) calls. At the same time, OC can use only this port to make outbound calls. ***Note:*** You must disable the DSP port (see the DSP Port Status screen) before changing the service associated with it.
Defaults	The default is "ALL," which indicates a shared DSP port.
Fax Outcalling considerations	A multimedia port can be shared for outbound services (enter "ALL" in the Outbound column). You can achieve optimum traffic capacity for fax calls on a multimedia port by dedicating the port to Fax Outcalling and then using only the Fax Call Back method of delivery. For details, refer to the *Site and Installation Planning Guide* (NTP 555-70x1-200).
Meridian ACCESS considerations	If you enter ACC (Meridian ACCESS) in the Outbound column, a second field, Class, is displayed. For information and examples on how to configure ACCESS applications (for example, Meridian IVR), refer to the "Configuration examples" chapter in the *Meridian ACCESS Configuration Guide* (NTP 555-7001-315).

Should you dedicate ports?

Introduction

When you dedicate a port to a particular service (for example, Fax on Demand, Outcalling [RN/DNU]), that port cannot be used for any other service, including voice messaging (call answering, logging in to Meridian Mail). That port is reserved for the service that you have assigned to it.

When ports are shared, they can be used for any service, including voice messaging.

Sharing your ports usually produces the most efficient system. When a port is dedicated, you can have a situation where callers are unable to log in to Meridian Mail because all shared ports are busy, while the dedicated port remains unused because it is reserved for the particular service assigned to it.

Ports are dedicated for incoming calls through the use of ACD queues and the VSDN table.

Ports are dedicated for outgoing calls through the “Outbound” column on the CAT table. Ports that are assigned to different queues can be shared for outgoing calls (for example, Remote Notification and Fax Outcalling).

See also

For a complete explanation of dedicated ports, see the section "Planning your configuration" on page 23-13.

When would you dedicate a port to a particular service

If you need to ensure that you always have a certain number of ports free for a particular service (for example, an important voice menu, FOC, or OC), then you may decide you need to dedicate ports to that service.

Dedicating ports for basic, full-voice, and multimedia services

If you have a mixture of port types (basic service, full service voice, and multimedia ports), then you need to set up a separate ACD queue for each port type. In effect, the ports become dedicated to a specific level of service, for incoming calls. The separate queues ensure that a call made to Meridian Mail is connected to a port that is capable of providing the service

requested (for example, a call to a fax menu is directed to a multimedia port).

For outgoing calls made by Meridian Mail (for example, Remote Notification, Delivery to Non-User, and Fax Outcalling), the ports can be shared.

How outbound calls are processed

These are calls made by Meridian Mail (for example, to deliver a remote notification, a delivery-to-non-user message, or a fax). When Meridian Mail makes an outbound call, it seeks a port that has the service capability to make the call (a basic port for basic services, a full-voice port for full services, a multimedia port for fax deliveries).

Meridian Mail begins by seeking the lowest-grade port required. If those are busy, Meridian Mail searches the next higher port type.

Example
For example, RN requires the use of a full-voice port. Meridian Mail seeks an idle full-voice port to make the call. If all full-voice ports are busy, Meridian Mail will seek an idle multimedia port (if the multimedia ports are set up to be shared).

Port type/service required	Action taken
Basic-service (ACCESS)	Meridian Mail seeks an idle basic service port to complete the call. If all basic ports are busy (active), Meridian Mail seeks an idle full-voice port. If all full-voice ports are busy, Meridian Mail seeks an idle multimedia port.
Full-voice (RN, DNU)	Meridian Mail seeks an idle full-voice port. If all full-voice ports are busy, Meridian Mail seeks an idle multimedia port.
Multimedia (Fax delivery)	Meridian Mail seeks an idle multimedia port. If all multimedia ports are busy, Meridian Mail waits for one of the multimedia ports to become idle.

When ports are shared for outbound calls

All idle ports can be used for any outbound service. The only restriction is that a full-voice service must use a full-voice port or a multimedia port, and a multimedia service must use a multimedia port.

When ports are dedicated for outbound calls

When you assign a specific outbound service to a port (for example, OC or FOC), then no other outbound service can use that port. The port can still be used for any inbound service (incoming calls), unless you have also set up a separate queue for that port.

If you want the port to be completely reserved for a particular service, make it fully dedicated by setting up a separate queue as well as assigning the particular service to the port in the "Outbound" column in the CAT table.

For more information, see "Fully dedicating ports – blocking inbound and outbound calls" on page 23-49.

Modifying the Channel Allocation Table

Channel allocation and dedication

Consider whether it is beneficial or necessary to dedicate ports (channels). See “Should you dedicate ports?” on page 23-23. See the section “Planning your configuration” on page 23-13.

> **ATTENTION**
>
> - Update the Channel Allocation Table only when the system is idle or during low traffic periods.
> - The Channel Allocation Table should only be configured by those who are knowledgeable about programming the switch.

Procedure

To modify the Channel Allocation Table, use the following steps.

Starting Point: The System Status and Maintenance menu

Step	Action
1	Disable the DSP port(s) you wish to reconfigure. • To disable a single port, see “Disabling/enabling DSP ports in single mode” on page 28-40. • To disable a range of ports, see “Disabling/enabling DSP ports in range mode” on page 28-42.
2	Select Channel Allocation Table from the System Status and Maintenance menu. • If you have a single node system, the Channel Allocation Table is displayed. Go to step 4. • If you have a multinode system, go to step 3.
3	Enter the number of the node on which the port resides, followed by <Return>.
4	Modify the ports.For each disabled port, you can change the values in the following fields: • ACD DN • SCN DN • Capability (for voice ports) • Outbound (Service)

Step Action

Note: Ports that are not disabled can only be viewed. For disabled ports, the port capability (Full or Basic) is highlighted and the ACD DN, SCN, and Outbound fields are underlined.

```
                          System Status and Maintenance
Channel Allocation Table for Node 2 (C=Card D=DSP P=Port)

Limit; MaxVoice MinMulti; MaxFull;            ---------Allocated---------
  72      68        2        68               M/F:  2   V/F: 66   V/B:  2

 #  C-D-P    TN        ACD DN     SCN     Type  Capability Outbound
 1  2-1-1 009-0-02-00 3651       2800      Multi Full       ALL
          009-0-02-01 blocked for Multimedia port 2-1-1.
 2  2-2-1 009-0-02-02 3651       2802      Multi Full       ALL
          009-0-02-03 blocked for Multimedia port 2-2-1.
 3  2-3-1 009-0-02-04 3659       2804      Voice Full Basic ALL
 4  2-3-2 009-0-02-05 3659       2805      Voice Full Basic ALL
 5  2-4-1 009-0-02-06 3650       2806      Voice Full Basic ALL
 6  2-4-2 009-0-02-07 3650       2807      Voice Full Basic ALL
 7  3-1-1 009-0-03-00 3650       2808      Voice Full Basic ALL
 8  3-1-2 009-0-03-01 3650       2809      Voice Full Basic ALL
 9  3-2-1 009-0-03-02 3650       2810      Voice Full Basic ALL
10  3-2-2 009-0-03-03 3650       2811      Voice Full Basic ALL
                                                                MORE BELOW
Select a softkey >

    Save        Cancel                                   Display Choice
                                                          of Services
```

5 Are you satisfied with the changes?

- If yes, press [Save].
- If no, press [Cancel].

Result: On a single node system, you are returned to the System Status and Maintenance menu.

On a multinode system, you are prompted for another node. If you have to reallocate ports on another node, return to step 3. Otherwise, press [Cancel] to return to the System Status and Maintenance menu.

6 Reenable any DSP ports you have put out of service.

- To enable a single port see “Disabling/enabling DSP ports in single mode” on page 28-40.
- To enable a range of ports see “Disabling/enabling DSP ports in range mode” on page 28-42.

Section E: Disk Maintenance

In this section

Overview	28-62
Checking disk status	28-63
Disabling disk shadowing (unsynching)	28-68
Replacing a failed disk	28-69
Reenabling disk shadowing (synching a disk pair)	28-70
Running diagnostics on a disk or a disk pair	28-72

Overview

Introduction

The Disk Maintenance screen allows you to view the operational state of the disks on your system. If your system is a shadowed system, you can also synch or unsynch a disk pair using the functions available through this screen.

When to use this feature

Shadowed or Unshadowed system

If you suspect that your disks are not functioning properly, use the Disk Maintenance screen to check the status of the disks on your system. See “Checking disk status” on page 28-63.

If you suspect a particular disk or disk pair is not functioning properly, you can run a diagnostic check using the [Diagnostics] softkey on the Disk Maintenance screen. See “Running diagnostics on a disk or a disk pair” on page 28-72.

Shadowed system

If you need to replace or repair one of the disks in a disk pair, you must first disable disk shadowing for the disk pair (unsynch the disk pair). The Disk Maintenance screen provides a softkey for unsynching a disk pair. See “Disabling disk shadowing (unsynching)” on page 28-68.

After a disk has been replaced or repaired, you need to synchronize the disk pair. The Disk Maintenance screen provides a softkey for synching a disk pair. See “Reenabling disk shadowing (synching a disk pair)” on page 28-70.

Checking disk status

Introduction

The Disk Maintenance screen lists the disks on your system and displays their current states.

Disk status

A disk can be in one of the following states:

- ***ReadWrite*** The disk is in service (functioning properly according to Meridian Mail).
- ***NoAccess*** The disk is disabled. Check your SEERs for more information.
- ***Faulty*** The disk has failed a diagnostics check that was performed using the [Diagnostics] softkey from the Disk Maintenance screen.

Shadowed systems only

- ***Write*** The disk is being written to. A disk may have this status during a disk synchronization.

Procedure

To check disk status, use the following steps.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance. **Result:** The System Status and Maintenance menu is displayed.
2	Select Disk Maintenance. **Result:** The Disk Maintenance screen is displayed.

Disk Maintenance screen: Unshadowed system

The following is an example of the Disk Maintenance screen on an unshadowed system.

```
                    System Status and Maintenance
Disk Maintenance

System Status: InService          Alarm Status: Critical=Off Major=On  Minor=On

Disk Node  HWLOC   Prime
     Type (N-C-ID) Status
1    MSP   1-7-0   ReadWrite
2    SPN   2-1-0   ReadWrite
3    SPN   3-7-0   NoAccess
4    SPN   4-1-0   ReadWrite

Select a softkey >

     Exit                                                   Diagnostics
```

Disk Maintenance screen: Shadowed system

The following is an example of the Disk Maintenance screen on a shadowed system.

```
                    System Status and Maintenance
Disk Maintenance

System Status: InService          Alarm Status: Critical=Off Major=On  Minor=On

Disk Node  HWLOC   Prime        HWLOC   Shadow      Pair
Pair Type (N-C-ID) Status      (N-C-ID) Status      Status
1    MSP   1-7-0   ReadWrite    1-7-2   ReadWrite   InSynch
2    SPN   2-1-0   ReadWrite    2-1-2   NoAccess    OutofSynch
3    SPN   3-7-0   NoAccess     3-7-2   ReadWrite   OutofSynch
4    SPN   4-1-0   ReadWrite    4-1-2   ReadWrite   InSynch

Select a softkey >

     Exit        Synch Disk    UnSynch Disk                    Diagnostics
                   Pair          Pair
```

Field descriptions

The following fields appear on the Disk Maintenance screen.

System Status	
Description	This field displays the current system status.
Possible status types	The possible status types are as follows. ***InService*** This indicates the system is running. ***CourtesyPending*** This indicates that the system is in the process of shutting down. ***CourtesyDown*** This indicates that the system has shut down and is no longer operational or accepting calls. ***Loading*** This indicates the system is loading software during bootup.

Alarm Status	
Description	This indicates the state of each of the types of alarms described below.
Alarm types	There are three possible alarm types. ***Critical*** These alarms indicate a service-affecting problem that requires immediate attention. ***Major*** These alarms indicate a service-threatening problem that may be allowed to persist for up to 24 hours. If not attended to, the alarm could become critical. ***Minor*** These alarms indicate a problem that has no impact on the system or users. For more details, see Chapter 29, “SEERs and Meridian Mail Alarms”.
Alarm states	Each alarm type can be in one of the following states. ***Off*** This state indicates that there are no new alarms. This does not necessary mean that there are no error conditions. ***On*** This status indicates that one or more alarm situations were detected. ***Unk*** This indicates that the status is unknown.

Disk Pair (appears only on Shadowed systems)	
Description	This is the number assigned to the disk pair.
When used	You are prompted for the disk pair number when performing the Synch Disk Pair, Unsynch Disk Pair, or Diagnostics functions.

Disk (appears only on Unshadowed systems)	
Description	This is the number assigned to the disk.

Node Type	
Description	This is the type of node (for example, an MSP node or SPN node).

HWLOC	
Description	The hardware location of the disk (node number–card number–disk ID).
Example	The numbers 1–7–0 refer to: Node number (1) Card number (7) Disk id (0)

Prime Status	
Description	This is the status of the disk on the node in an unshadowed system, or the status of the prime disk of a disk pair in a shadowed system.
Possible states	A disk can be in one of the following states: ***ReadWrite*** The disk is operating properly. ***NoAccess*** The disk is disabled. ***Write*** The disk is being written to (during a disk synchronization in a shadowed system). ***Faulty*** The disk failed a diagnostic check that was performed using the [Diagnostics] softkey on the Disk Maintenance screen.

Shadow Status	
Description	This is the status of the shadow disk of a disk pair in a shadowed system.
Possible states	A disk can be in one of the following states: ***ReadWrite*** The disk is operating properly. ***NoAccess*** The disk is disabled. ***Write*** The disk is being written to (during a disk synchronization). ***Faulty*** The disk failed a diagnostic check that was performed using the [Diagnostics] softkey on the Disk Maintenance screen.

Pair Status	
Description	This is the status of the disk pair. This field appears only on a shadowed system.
Possible states	A disk pair can be in one of the following states: ***InSynch*** Both disks are functioning properly and the disk pair is in synch. ***OutofSynch*** One of the disks has been disabled, so the disk pair is out of synch. ***Synching*** The disk pair is currently being synchronized. When this is happening, the screen also displays the progress of the synchronization in terms of percentage completed. ***NoAccess*** Both disks in the disk pair are in NoAccess state.

Disabling disk shadowing (unsynching)

Introduction

Disk shadowing is disabled for a disk pair by unsynching the disk pair. It is necessary to disable disk shadowing if you need to repair or replace one of the disks in a disk pair.

Procedure

To disable disk shadowing, use the following steps.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance. **Result:** The System Status and Maintenance menu is displayed.
2	Select Disk Maintenance. **Result:** The Disk Maintenance screen is displayed.
3	Press the [Unsynch Disk Pair] softkey. **Result:** You are prompted to enter a disk pair number.
4	Enter the disk pair number for the disk pair that you need to disable. **Result:** The system asks you which disk should be disabled (the Primary Disk or the Shadow Disk).
5	Select the disk that you plan to repair or replace (Primary disk or Shadow Disk). **Result:** The disk is placed in NoAccess state (it is disabled). **Note:** If the other disk is in NoAccess state, the request to disable the disk is denied. One of the disks in a disk pair must be in ReadWrite state to keep the node operational.

Replacing a failed disk

Where to find information

The procedures for replacing a failed disk are provided in the *Installation and Maintenance Guide* (NTP 555-70x1-250).

Reenabling disk shadowing (synching a disk pair)

Introduction

After a disk has been replaced or repaired, you need to synchronize the disk pair to reenable disk shadowing. The Disk Maintenance screen provides a softkey for synching a disk pair.

Tip

If you need to synch more than one disk pair, you can begin synching subsequent disk pairs as soon as the first disk pair has started synching. You do not have to wait for one disk pair to finish synching before synching another disk pair.

Timing

This procedure takes at least thirty minutes. The actual time depends on the size of the source disk.

Procedure

To re-enable disk shadowing, use the following steps.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance. **Result:** The System Status and Maintenance menu is displayed.
2	Select Disk Maintenance. **Result:** The Disk Maintenance screen is displayed.
3	Press the [Synch Disk Pair] softkey. **Result:** You are prompted to enter a disk pair number.
4	Enter the number of the disk pair that you need to synch (to re-enable disk shadowing for the disk pair) and press <Return>. **Result:** The synching begins.

What happens during synchronization

The screen displays the progress of the synchronization. It displays the percentage of synchronization that is complete.

The status of the disk that is being written to changes to “Write” until the synching is complete. When complete, the status of both disks is set to ReadWrite if both disks are functioning properly. If one of the disks in the disk pair is faulty, the synching will fail and you are notified by a screen message.

Screen showing disk synchronization

The following is an example of a Disk Maintenance screen with a disk synchronization in progress.

```
                          System Status and Maintenance
Disk Maintenance

System Status: InService          Alarm Status: Critical=Off Major=On  Minor=On

Disk Node  HWLOC   Prime        HWLOC   Shadow      Pair
Pair Type (N-C-ID) Status      (N-C-ID) Status      Status
1    MSP   1-7-0   ReadWrite    1-7-2   ReadWrite   InSynch
2    SPN   2-1-0   ReadWrite    2-1-2   Write       Synching on Node  2   3%done
3    SPN   3-7-0   NoAccess     3-7-2   ReadWrite   OutofSynch
4    SPN   4-1-0   ReadWrite    4-1-2   ReadWrite   InSynch

Select a softkey >
Disk Pair 2 disk synchronization started.
     Exit        Synch Disk      UnSynch Disk                    Diagnostics
                   Pair            Pair                                        ]
```

Running diagnostics on a disk or a disk pair

Introduction

If you suspect a problem with a disk, run the diagnostic function on the disk. The system responds with a message indicating if the disk is ok (passed) or faulty (failed).

Procedure

To run the diagnostic function on a disk or disk pair, use the following steps.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance. **Result:** The System Status and Maintenance menu is displayed.
2	Select Disk Maintenance. **Result:** The Disk Maintenance screen is displayed.
3	Press the [Diagnostics] softkey. **Result:** You are prompted to enter a disk number (or a disk pair number on a shadowed system).
4	Enter the number of the disk or disk pair you want to check. **Result (on a shadowed system):** The system asks you which disk you want to check (the Primary Disk or the Shadow Disk). Select one of the disks. After a few moments, the system responds with the results of the diagnostic check. **Result (on an unshadowed system):** After a few moments, the system responds with the results of the diagnostic check.

Possible results

The system will respond with one of the following messages.

Message	Meaning
Disk diagnostics passed.	The disk is functioning normally.
Disk diagnostics failed. xxxx (where “xxxx” is the error code)	The disk is not functioning properly. A SEER is generated which will provide more details on what the problem is and what action you should take.
Invalid component state to do disk diagnostics.	If the disk is not in a valid state (InService, OutOfService, Faulty, or Unconfigured), then the diagnostics routine will not run. Contact your regional support centre.
Cannot perform diagnostics. Disk Synchronization in progress.	The disk pair you have selected is currently being synched. You must wait for the synching to complete before you can run diagnostics on one of the disks in the disk pair.
Invalid node state to run diagnostics on this disk.	The node must be InService, OutOfService, or in Standby state for the diagnostics routine to run.

Section F: Diagnostic Schedules

In this section

Overview 28-76
What are Voice Path Diagnostics? 28-77
Changing the parameters and schedule for diagnostics 28-78
Analyzing the results of the diagnostics 28-82

Overview

Introduction

The Diagnostics Schedules screen allows you to schedule a diagnostic check on the voice channels in your system. You can control what time the diagnostics take place (to avoid peak traffic periods), and whether a faulty channel is taken off-line.

When to use this feature

If you have not enabled voice path diagnostics yet, you would use this feature to

- schedule when you want voice path diagnostics to take place

If the voice path diagnostic tests are causing a traffic problem, you can use this feature to

- change the voice path diagnostics schedule to a less-busy time
- disable voice path diagnostic testing
- change what happens when voice path diagnostics fail (whether channels taken offline or left InService)
- change the duration of the voice path diagnostics
- change the minimum number of channels that must be idle before voice path diagnostics will run

What are Voice Path Diagnostics?

Definition: Voice Path Diagnostics

Voice Path Diagnostics is a feature that tests the operational state of the voice channels.

How the test is done

The system sets up calls which go from Meridian Mail to the switch and back. Two channels are tested at a time (one to make the call to the switch, one to receive the call from the switch). Only InService channels are tested.

The test continues until either

- all InService channels are tested
  or
- the maximum duration allowed for the tests runs out

Definition: Originator and Destination

The Originator is the port used to make the call from Meridian Mail to the switch. The Destination is the port used to receive the call back from the switch to Meridian Mail.

Possible test results

A channel can pass, fail, or be left untested. For more details, see “Analyzing the results of the diagnostics” on page 28-82.

Changing the parameters and schedule for diagnostics

Introduction

The parameters and schedule for diagnostics are defined on the Diagnostic Schedules screen.

On this screen you can

- enable or disable diagnostics
- change the time or days that diagnostics are run
- change the maximum duration for voice path diagnostics
- determine if a faulty channel is automatically taken out of service
- determine the minimum number of idle channels that must be present before voice path diagnostics are run

Note: Changes to the schedule or parameters while diagnostics are running will not take effect until the current diagnostics session is completed.

The Diagnostic Schedules screen

The following is an example of the Diagnostic Schedules screen.

```
                    System Status and Maintenance
Diagnostic Schedules

Start Time (hh:mm):          02:00

Schedule Diagnostics on the Following Days:
            Monday           No Yes
            Tuesday          No Yes
            Wednesday        No Yes
            Thursday         No Yes
            Friday           No Yes
            Saturday         No Yes
            Sunday           No Yes

Bus Controller Diagnostics: Disabled Enabled

Voice Path Diagnostics:     Disabled Enabled

Mark Channel Faulty if Voice Path Diagnostics Fail:         No Yes
                                                            MORE BELOW
Select a softkey >

   Save        Cancel
```

All the fields do not fit on the first screen. When you scroll to the next screen, one additional field is displayed: “Minimum Number of Idle Channels for Voice Path Diagnostics.”

Field descriptions

The following fields appear on the Diagnostic Schedules screen.

Start Time (hh:mm)	
Description	This is the time that voice path diagnostics begin.
Tip	Set the start time to a low-traffic part of the day.
Default	3:00 am (03:00)

Schedule Diagnostics on the Following Days	
Description	For each day listed, select Yes to allow diagnostics to run on that day, or select No to disable diagnostics for that day.
Default	For each day, the default is Yes.

Voice Path Diagnostics	
Description	This field determines if voice path diagnostics are enabled or disabled.
Default	Enabled

Mark Channel Faulty if Voice Path Diagnostics Fail	
Description	Set this field to Yes if you want a faulty channel to be taken out of service. If you set this field to No, the channel remains InService. In either case, a SEER is issued indicating the channel is faulty.
Considerations	If channels are taken out of service by the diagnostics routine, system performance may be affected as the number of channels InService decreases. Keep in mind that even if faulty channels are left InService, you still need to investigate why the channel is being tagged as faulty by the diagnostics routine.
Default	No

Maximum Duration of Voice Path Diagnostics (hh:mm)	
Description	This is the maximum length of time voice path diagnostics are allowed to run during one session.
Considerations	While diagnostics are running, two channels are unavailable for use. This may impact system performance if the diagnostics continue into a high-traffic time period.
Default	2 hours (02:00)

Minimum Number of Idle Channels for Voice Path Diagnostics	
Description	This is the number of channels that must be idle in addition to the two channels required for the diagnostic tests. If this field is set to 2, then 4 channels must be idle before voice path diagnostics will begin. After voice path diagnostics finishes testing a pair of channels, it checks again to make sure there are enough idle channels in addition to the two channels required for testing, as specified in this field, before continuing.
Considerations	If the diagnostics are causing a traffic problem, you may wish to increase the number of idle channels that must be present.
Example	If this field is set to 2, then 4 channels must be idle before each diagnostic test. After voice path diagnostics finishes testing a pair of channels, it checks that at least 4 channels are idle before acquiring 2 of those idle channels for the next test. In this manner, voice path diagnostics continues until all channels have been tested, or until the Maximum Duration value is exceeded.
Default	2

Procedure

To change the parameter or schedule settings for the diagnostic routines, use the following steps.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance. **Result:** The System Status and Maintenance menu is displayed.
2	Select Diagnostic Schedules. **Result:** The Diagnostic Schedules screen is displayed.
3	Fill in the fields as required. See “Field descriptions” on page 28-79.
4	Are you satisfied with the changes? • If yes, press [Save]. **Result:** The changes are saved and you are returned to the System Status and Maintenance menu. • If no, press [Cancel]. **Result:** The changes are not saved and you are returned to the System Status and Maintenance menu.

Analyzing the results of the diagnostics

Introduction The results of the diagnostics are provided through SEERs.

Possible test results The following possible results are presented in the SEERs.

Test result	Originator's state	Destination's state	Meaning/Action taken
Passed	n/a	n/a	Both the originator and destination ports are tagged as passed.
Failed (after testing)	Untested	Passed	The originator port is faulty. A major alarm SEER is generated to inform you of the failure. If the Mark Channel Faulty if Voice Path Diagnostics Fail field on the Diagnostic Schedules screen is set to Yes, the originator port's status is changed to OutOfService.
Failed (after testing)	Passed	Untested	The destination port is faulty. A major alarm SEER is generated to inform you of the failure. If the Mark Channel Faulty if Voice Path Diagnostics Fail field on the Diagnostic Schedules screen is set to Yes, the destination port's status is changed to OutOfService.
Failed (due to inability to test)	Untested	Untested	The status of the ports remain unchanged because the ports were not tested. The maximum duration for diagnostics ran out before these ports were tested.

Summary SEER (number 7400)

When a diagnostics session is completed (all InService channels are tested, or the maximum duration allowed expires), a summary SEER is generated.

The SEER number is 7400, with severity level “Info,” and type “Admin.”

This SEER provides the following information:

- the total number of InService channels found on the system
- the total number of channels tested
- the total number of channels failed
- the total number of channels untested
- a list of failed channels

Other SEERs (class 74)

Scan the SEERs generated during the diagnostic session for class 74 SEERs. Class 74 SEERs include SEERs related to failed or untested channels.

Impact on Operational Measurement reports

On the Services Summary report, the count for the Voice Path Diagnostics service will be greater than or equal to the number of channels tested.

The count for the default voice service (usually Voice Menus) will also show some additional calls in the time period in which voice path diagnostics was running. This is because the default voice service is used to assist in establishing the call loop between Meridian Mail and the switch.

Chapter 29

SEERs and Meridian Mail Alarms

In this chapter

Overview	29-2
Section A: SEERs and Alarms	29-3
Section B: Customizing SEER processing	29-15
Section C: Notification options for SEERs and alarms	29-27

Overview

Introduction

This chapter describes System Event and Error Reports (SEERs) and Meridian Mail alarms in the following sections.

Section A: SEERs and Alarms provides conceptual information about SEERs and Alarms. Procedures for SEER retrieval and alarm silencing are described in this section.

Section B: Customizing SEER processing provides information regarding SEER remapping, SEER throttling, and SEER escalation.

Section C: Notification options for SEERs and alarms describes the SEER and alarm processing path in the Meridian Mail system. Also, the procedures for setting up SEERs printing, filtering, and triggering are described.

Section A: SEERs and Alarms

In this section

What is a SEER?	29-4
Retrieving SEERs	29-6
What is an alarm?	29-9
How to check alarm status	29-10
Silencing an alarm	29-12

What is a SEER?

Concept

System Event and Error Reports (SEERs), which are generated by the Meridian Mail system software components, identify every significant system event and error that occurs.

An event is a minor glitch or an announcement of normal system activities (for example, the start of an automatic tape backup). Events documented in a SEER do not usually indicate a problem with the Meridian Mail functionality.

An error is a hardware or software fault that may prevent Meridian Mail from functioning properly (for example, a hardware component that failed diagnostics, or a failure to find a system file). An error creates one or more SEERs.

You must be able to read, interpret, and assess the severity of events and errors to determine if they are regular system events (such as a system audit) or system errors. An understanding of SEERs is also essential for diagnosing problems. Before asking for help in dealing with a major system problem, the system administrator must be ready to provide a collection of SEER reports from which the Northern Telecom support staff can determine the history of the problem. From these reports, maintenance personnel will be able to diagnose the problem effectively.

SEER components

Each SEER is identified by a number consisting of two parts:

- SEER class, which classifies a particular software component
- SEER number, which identifies a particular report for a class

Example

SEER 6603 is SEER number 03 from class 66.

Note: Due to ongoing improvements in the software, there may be instances where the information on the SEER itself is different from the information presented in the *Maintenance Messages (SEERs) Reference Manual* (NTP 555-7001-510). Should this occur, the information in the SEER printed out by your system should take precedence.

How SEERs are accessed

SEERs can be displayed on a terminal or printed out on a printer. The reports provide information about the SEER class, SEER number, the severity level of errors, the date and time the SEER was generated, and a description of the event or error that occurred at that time. This information is used primarily by system administrators and maintenance personnel to confirm that a system is running correctly, to isolate a system fault, to diagnose a hardware or software problem, or to solve a problem.

SEERs are printed and stored in the SEER file on the system disk at the time of the error or event. The SEERs stored on disk can be viewed or printed at a later time. The SEER file holds up to 4000 records.

Retrieving SEERs

Introduction

This topic provides information required for retrieving SEERs from the SEER history file that resides on the system disk. SEERs are retrieved by class only.

The SEER Retrieval screen

This is an example of the SEER Retrieval screen.

```
                    System Event and Error Reports
SEER Retrieval

SEER Class:        11

Severity Level:    Critical Major Minor All

SEER Type:         Error Admin System All




Report Start (mm/dd/yy hh:mm):   05/31/96 12:00        (or blank for oldest)
Report End   (mm/dd/yy hh:mm):   05/31/96 16:00        (or blank for newest)

Select a softkey>

   Exit                          View Reports   Print Reports
```

Field descriptions

This table describes the fields in the SEER Retrieval screen.

SEER Class	
Description	The class of SEERs that you want to retrieve. If you leave the field blank, all classes will be retrieved.
Classes	For a list of supported SEERs classes, refer to the *Maintenance Messages (SEERs) Reference Manual* (NTP 555-7001-510).
Default	The field is blank.
Severity Level	
Description	The severity level of the SEERs class.
Options	Critical, Major, Minor, All
Default	All
SEER Type	
Description	The SEER type required.
Options	Error, Admin, System, All
Default	All
Report Start/End	
Description	This field allows the administrator to specify the start and end date and time for the SEER retrieval. If left blank, the search provides all SEERs meeting the search criteria that are in the history file.
Default	The field is blank.

Procedure

To retrieve SEERs from the history file, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance. **Result:** The System Status and Maintenance screen is displayed.
2	Select System Event and Error Reports from the menu. **Result:** The System Event and Error Reports screen is displayed.
3	Select SEER Retrieval. **Result:** The SEER Retrieval screen is displayed.
4	Complete the SEER Class, Severity Level, and SEER Type fields for the SEERs that you want to retrieve. **Note:** If the SEER Class field is left blank, all classes of SEERs are retrieved.
5	Enter the Report Start and Report End criteria to narrow the search to a specific date and time interval. Otherwise, leave these fields blank.
6	Use this table to determine the next step. **IF you want to** — **THEN press the** view the SEERs retrieved by the search — [View Reports] softkey. print the SEERs retrieved by the search — [Print Reports] softkey. **Result:** For View Reports, the reports are displayed. For Print Reports, press the [Continue Printing] softkey to print the report. Press the [Cancel Printing] softkey to cancel printing and return to the SEER Retrieval screen.
7	Press the [Exit] softkey to return to the System Event and Error Reports menu.

What is an alarm?

Introduction

An alarm is an audible notification that something is not right with the Meridian Mail system. Alarms are sounded if a corresponding severity level SEER is issued to indicate a system problem.

Alarm types

There are three types of alarms: critical, major, and minor.

Critical alarm
These alarms indicate a service-affecting problem that requires immediate attention.

Major alarm
This type of alarm indicates a service-threatening problem that may be allowed to persist (for up to 24 hours). If not attended to, the alarm could become critical.

Minor alarm
This type of alarm indicates a problem that has no impact on the system or users.

How to check alarm status

Introduction

This procedure explains how to check for the status of alarms.

Checking alarm status from outside Meridian Mail

To check which alarms are on (or off) if you are not currently logged in to Meridian Mail, follow these steps.

Starting Point: Meridian Mail Logon/Status screen

Step	Action
1	Press the [System Status] softkey. **Result:** The System Status screen is displayed.

```
                                 System Status
System Status: InService          Alarm Status: Critical=On  Major=On  Minor=On

Last Event:   41-67 A VSS terminated on Node 2, Cause=UnexpectedUnLoad1/02 20:47

Link Status:   1-3-2: InService

                                     DSP Port Status                 Storage Used
Node  Type Status        Active Idle OutSv Faulty Pending Others    Voice Text
 1    MSP  InService        0     1     5     0      0       0       19%   6%
 2    SPN  InService        0    16     0     0      0       0        1%   3%_

Select a softkey >

    Exit
```

Step	Action
2	View the Alarm Status field in the upper right-hand corner for the alarms status.

Checking alarm status from within Meridian Mail

To check which alarms are on (or off) if you are logged in to Meridian Mail, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance. **Result:** The System Status and Maintenance screen is displayed.
2	Select System Status from the menu. **Result:** The System Status screen is displayed.

```
                          System Status and Maintenance
System Status: InService          Alarm Status: Critical=Off Major=Off Minor=On

Last Event:   91-5  MWIAUDIT VS202: The Audit is Finished.           12/20 11:46

Link Status:   1-2-2: InService

                                   DSP Port Status                 Storage Used
Node  Type Status        Active Idle OutSv Faulty Pending Others    Voice Text
 1    MSP  InService        0    19     1     0      0        0        4%   1%
 2    SPN  InService        0    23     1     0      0        0        0%   1%_

Select a softkey >

     Exit        Enable Node     Disable Node     Courtesy        Courtesy Down
                                                 Disable Ports       System
```

Step	Action
3	View the Alarm Status field in the upper right-hand corner for the alarms status.

Silencing an alarm

Introduction

The Meridian Mail system will sound an alarm if the corresponding severity level SEER is issued indicating that a problem exists. Alarms are silenced from the Logon/Status or the System Status and Maintenance screen.

Alarms persist until you silence them. (There is no timeout period after which they are turned off by the system.)

System Status and Maintenance screen

This is an example of the [Silence Alarm] softkey on the System Status and Maintenance screen.

```
System Status and Maintenance

        1  System Status
        2  Card Status
        3  DSP Port Status
        4  Channel Allocation Table
        5  Disk Maintenance
        6  Diagnostic Schedules
        7  System Event and Error Reports

Select an item > _

[Exit]  [      ]  [      ]  [Silence Alarm]  [      ]
```

When the [Silence Alarm] softkey is pressed, the softkeys change to include [Silence Critical Alarm], [Silence Major Alarm], and [Silence Minor Alarm] as shown below.

```
Select a softkey > _

[      ]  [Cancel]  [Silence Critical Alarm]  [Silence Major Alarm]  [Silence Minor Alarm]
```

Silencing an alarm when logged in to Meridian Mail

To silence an alarm when logged in to Meridian Mail, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance. **Result:** The System Status and Maintenance screen is displayed.
2	Press the [Silence Alarms] softkey. **Result:** The [Silence Critical], [Silence Major], and [Silence Minor Alarm] softkeys are displayed.
3	Press the appropriate softkey to cancel the type of alarm that is sounding. **Result:** The alarm is silenced. Press [Cancel] to return to the System Status and Maintenance screen.

Silencing an alarm from the Logon/ Status screen

To silence an alarm from the Meridian Mail Logon/Status screen, follow these steps.

Starting Point: The Meridian Mail Logon/Status screen

Step	Action
1	Press the [Silence Alarms] softkey. **Result:** The [Silence Critical], [Silence Major], and [Silence Minor Alarm] softkeys are displayed.
2	Press the appropriate softkey to cancel the type of alarm that is sounding. **Result:** The alarm is silenced. Press [Cancel] to return to the Meridian Mail Logon/Status screen.

Section B: Customizing SEER processing

In this section

Overview	29-16
Using SEER remapping	29-17
Using SEER throttling	29-20
Using SEER escalation	29-23

Overview

Introduction

This section includes descriptions of three SEERs features: remapping, throttling, and escalation, as well as procedures for setting up these features on the Meridian Mail system.

Using SEER remapping

Description

SEERs remapping allows the system administrator to remap or reassign the severity level of up to 60 SEERs to a higher or lower severity level. The remapping can be applied to individual SEERs only, and the revised configuration is stored in the System Profile on disk. This means that the parameters do not have to be reentered after a system reboot.

Note: SEER remapping is not the same as memory remapping. Memory remapping is done using the special utility, SE_UTIL function, with the aid of your distributor. For information on memory remapping, refer to the *Maintenance Messages (SEERs) Reference Manual* (NTP 555-7001-510).

The SEER remapping changes are made using the SEER Remap Table. Changes are effective immediately upon saving the table. No validation is performed on the revised SEERs to determine if the entered SEER actually exists, if the severity level is different from the existing severity level, or if the SEER has already been remapped using memory remapping.

If the altered severity level is no longer required, delete the entry from the SEER Remap Table instead of resetting the severity level back to the original.

The SEER Remap Table

This is an example of the SEER Remap Table.

```
                    System Event and Error Reports
SEER Remap Table

SEER   Severity  Message   SEER   Severity  Message   SEER   Severity  Message
                 Trigger                     Trigger                     Trigger
_____  ________  ___     _____  ________  ___     _____  ________  ___
_____  ________  ___     _____  ________  ___     _____  ________  ___
_____  ________  ___     _____  ________  ___     _____  ________  ___
_____  ________  ___     _____  ________  ___     _____  ________  ___
_____  ________  ___     _____  ________  ___     _____  ________  ___
_____  ________  ___     _____  ________  ___     _____  ________  ___
_____  ________  ___     _____  ________  ___     _____  ________  ___
_____  ________  ___     _____  ________  ___     _____  ________  ___
_____  ________  ___     _____  ________  ___     _____  ________  ___
_____  ________  ___     _____  ________  ___     _____  ________  ___
_____  ________  ___     _____  ________  ___     _____  ________  ___
_____  ________  ___     _____  ________  ___     _____  ________  ___
_____  ________  ___     _____  ________  ___     _____  ________  ___
                                                                  MORE BELOW
Select a softkey>

   Save        Cancel
```

Field descriptions

The following table describes the fields in the SEER Remap Table.

SEER	
Description	The four- or five-digit number of the SEER to be remapped.
Default	None
Severity	
Description	The new severity for the SEER.
Options	Info, Minor, Major, or Critical (Only the first two letters of the option need to be entered into the field.)
Default	Blank
Message Trigger	
Description	This field is used to set the message trigger on.
Options	Enter Yes to set the message trigger; if you leave the field blank, the message trigger remains off.
Default	Blank

Procedure

To remap SEERs, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance. **Result:** The System Status and Maintenance menu is displayed.
2	Select System Event and Error Reports. **Result:** The System Event and Error Reports menu is displayed.
3	Select SEER Remap Table. **Result:** The SEER Remap Table is displayed.
4	Enter the SEER number in the SEER field.
5	Use the tab key to move the cursor to the Severity field. Enter the new severity.
6	Use the tab key to move the cursor to the Message Trigger field. To set the message trigger, enter Yes in this field.
7	Use this table to determine the next step. **IF** — **THEN** you have more SEERs to remap — repeat steps 4 through 6. you have entered all SEERs in the table that require remapping — go to step 8.
8	Press the [Save] softkey to save the remapping table. **Result:** The table is saved and the SEERs are remapped. Press the [Cancel] softkey to cancel changes to the remap table. **Result:** The changes are cancelled and you are returned to the System Event and Error Reports menu.

Using SEER throttling

Introduction

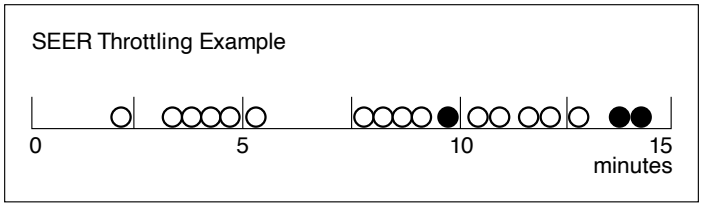
To reduce SEER proliferation, the customer administrator can control the flow of duplicate messages for a specified period of time. SEER throttling monitors SEERs and stops printing a specific SEER type if too many of that type are generated within a given interval.

If the parameters for throttling are exceeded, the throttled SEER will not be sent to the Message Trigger Mailbox or the SEER printer. The configuration for SEER throttling is stored in the System Profile; therefore, the throttling data does not have to be reentered after a system reboot.

When SEER throttling is invoked, a SEER is generated to alert users. SEER throttling will "timeout" after an interval and allow the system to continue to print the prohibited SEER type. If the original error condition still exists, another spurt of SEERs will be displayed until SEER throttling is triggered again. This provides you with ongoing monitoring of the error situation.

Example

In this example, the throttling threshold count is set to 5, and the throttling threshold interval is set to 5 minutes. The circles in the following diagram represent occurrences of the same SEER. Note that the sixth occurrence of the SEER is not throttled, even though it occurs within five minutes of the first occurrence of the SEER, because throttling of an individual SEER is reset at the end of the throttling threshold period (for example, 5 minutes, 10 minutes, and so on).



G100412

Example (cont'd)

The black circles indicate instances when the SEER has been throttled. The throttled SEER will not be sent either to the Message Trigger Mailbox or the SEER printer (if filtered printing was chosen).

SEER Configuration screen

This is an example of the SEER Configuration screen.

```
                    System Event and Error Reports
SEER Configuration

Message Trigger Mailboxes:
       Mailbox:   7555
       Mailbox:   7556

SEER Printer Output:                      None Filtered Unfiltered

SEER Throttle Threshold Count:   5        Throttle Interval (hh:mm):   00:05
SEER Escalation Threshold Count: 0        Escalation Interval (hh:mm): 00:05

SEER Filters:
       SEER Severity Threshold:           None Critical Major Minor
       SEER Type Threshold:               Error Admin

Select a softkey>

     Save        Cancel
```

Field descriptions

The following table describes the fields used for SEER throttling in the SEER Configuration screen.

SEER Throttle Threshold Count	
Description	This field is used to indicate the number of duplicate SEERs that must occur within the SEER Throttle Threshold Interval at which time the duplicate SEER will be throttled for the reminder of the SEER throttle threshold interval.
Range	0 to 100. The 0 indicates that SEER Throttling is not activated.
Default	5

SEER Throttle Interval	
Description	This field is used to specify the time period in hours and minutes (hh:mm) where the number of duplicate SEERs must exceed the SEER Throttle Threshold Count value at which time the SEER Throttling is to occur.
Range	00:01 to 24:00 (1 minute to 24 hours)
Default	00:05

Setting SEER throttling

To set throttling for SEERs, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance. **Result:** The System Status and Maintenance screen is displayed.
2	Select System Event and Error Reports from the menu. **Result:** The System Event and Error Reports screen is displayed.
3	Select SEER Configuration. **Result:** The SEER Configuration screen is displayed.
4	In the SEER Throttle Threshold Count field, enter the threshold count.
5	In the SEER Throttle Interval field, enter the interval that you want to use for throttling the SEERs.
6	Press the [Save] softkey to save your choices. **Result:** The changes are saved and you are returned to the System Event and Error Reports menu. Press the [Cancel] softkey to cancel changes to the SEER configuration. **Result:** The changes are cancelled and you are returned to the System Event and Error Reports menu.

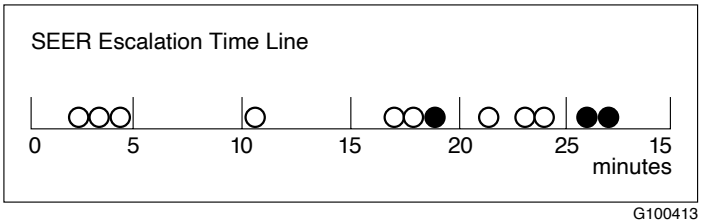
Using SEER escalation

Introduction

The administrator can escalate the severity level of frequently issued minor and major SEERs to the next level. If the same SEER is issued a specified number of times during a specified period of time, the severity level of the SEER is escalated to the next highest severity level. This applies to Minor and Major SEERs only. Info SEERS cannot be escalated.

Example

The escalation threshold count is set to 4, and the escalation threshold interval is set to 10 minutes for this example. The occurrence of a Major SEER is represented by a circle.



The black circles indicate occurrences of the major SEER that will be escalated to a critical severity level. The occurrence of the SEER at 11 minutes will not be escalated because the fourth occurrence of the SEER is outside the 10-minute interval; however, in the 10 to 20 minute range four SEERs occur, causing the fourth SEER to be escalated to the critical severity level.

SEER Configuration screen

This is an example of the SEER configuration screen.

```
                    System Event and Error Reports
SEER Configuration

Message Trigger Mailboxes:
       Mailbox:   7555
       Mailbox:   7556

SEER Printer Output:                      None Filtered Unfiltered

SEER Throttle Threshold Count:   5        Throttle Interval (hh:mm):   00:05
SEER Escalation Threshold Count: 0        Escalation Interval (hh:mm): 00:05

SEER Filters:
       SEER Severity Threshold:           None Critical Major Minor
       SEER Type Threshold:               Error Admin

Select a softkey>

    Save        Cancel
```

Field descriptions

The following table describes the fields used for SEER escalation in the SEER Configuration screen.

SEER Escalation Threshold Count	
Description	This field is used to indicate the number of duplicate SEERs that must occur within the SEER Escalation Threshold Interval before the SEER severity is raised to the next highest level.
Range	0 to 100. The 0 indicates that SEER Escalation is not activated.
Default	0

SEER Escalation Interval	
Description	This field is used to specify the time period in hours and minutes (hh:mm) where the number of duplicate SEERs must exceed the SEER Escalation Threshold Count value before the SEER severity is raised to the next highest level.
Range	00:01 to 24:00 (1 minute to 24 hours)
Default	00:05

Setting SEER escalation

To set SEERs escalation, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance. **Result:** The System Status and Maintenance screen is displayed.
2	Select System Event and Error Reports from the menu. **Result:** The System Event and Error Reports screen is displayed.
3	Select SEER Configuration. **Result:** The SEER Configuration screen is displayed.
4	In the SEER Escalation Threshold Count field, enter the threshold count.
5	In the Escalation Interval field, enter the interval that you want to use for SEERs escalation.
6	Press the [Save] softkey to save your choices. **Result:** The changes are saved and you are returned to the System Event and Error Reports Menu. Press the [Cancel] softkey to cancel changes to the SEER configuration. **Result:** The changes are cancelled and you are returned to the System Event and Error Reports menu.

Section C: Notification options for SEERs and alarms

In this section

Overview	29-28
Notification options for SEERs and alarms	29-29
Using SEER filtering	29-31
Using SEER triggering	29-35
SEERs printing	29-38
Setting the SEER printer port name	29-40

Overview

Introduction

This section describes

- the route that a SEER takes after it is issued by the Meridian Mail system
- using the SEER filtering and triggering features
- setting up printing for SEERs

Notification options for SEERs and alarms

Introduction

This section describes the route that a SEER follows after it has been issued by the Meridian Mail system.

How the Meridian Mail system processes a SEER

The following provides an overview of how the Meridian Mail system processes a SEER.

1. The SEER is issued by the Meridian Mail system. An audible alarm sounds if the severity level is critical, major, or minor and the alarm feature has been wired on your system.
2. The system scans the memory remap table for the SEER that has been issued. If the SEER matches an entry in the memory remap table, the SEER's severity and type is changed to that of the table entry.
3. If the SEER does not match an entry in the memory remap table, the system scans the SEER remap table. If the SEER matches an entry in the SEER remap table, the SEER's severity is changed to that of the table entry.
4. Next, the remapped SEER severity is escalated if the escalation thresholds are exceeded. The SEER is sent to the SEER history file.

5. The next step in the SEER path is determined by the following.

IF the SEER configuration is set to	THEN
Unfiltered	printer filtering and throttling is applied to the SEER and the output is sent to the printer. The processing ends.
Message Trigger is set to YES in the Remap Table	SEER filtering is bypassed and the SEER is sent to the Message Trigger mailbox after passing through SEER throttling. The processing continues with step 6.
Filtered and Message Trigger is not set to Yes	SEER filtering is applied to the SEER. If the SEER passes through the filter, processing continues with step 6.

6. SEER throttling checks the SEER to see if it is a duplicate that exceeds the throttling threshold.

7. If the SEER passes SEER Throttling and the Message Trigger is set to Yes, a trigger message is composed and deposited in the Message Trigger mailbox. Also, the SEER is printed on the console printer.

Using SEER filtering

Introduction

SEER filtering parameters allow the administrator to limit the number of SEERs sent to the Message Trigger Mailbox. Only the SEERs required for proper system operation, maintenance, or hacker monitoring activity should be sent to the Message Trigger Mailbox.

The administrator may choose to filter the SEERs based on the severity or type of SEER, or both. The filtering parameters can also be used to limit the SEERs that are sent to the SEER printer if the appropriate SEER Printer Output option is selected. You cannot filter individual SEERs or SEER classes.

Filtering by severity level

The following table describes the filtering possibilities if SEER filtering is set using the severity level only.

Minimum Severity Level	SEERs sent to Message Trigger Mailbox
None	Only those SEERs which have the Message Trigger Field set to YES in the SEER Remap Table.
Critical	Only critical SEERs. This is the default value.
Major	Only major and critical SEERs.
Minor	Minor, major, and critical SEERs. ***Note:*** An appropriate warning appears if Minor is selected, as there is a possibility of flooding the Message Trigger Mailbox at this level of SEER.

Filtering by SEER type

The following table describes the filtering possibilities if SEER filtering is set according to the SEER type only.

SEER type	SEERs sent to Message Trigger Mailbox
Error	Error SEERs only. Error level SEERs may indicate a system problem which can be corrected by the administrator, perhaps with the assistance of technical support.
Admin	Admin and Error SEERs only. The ADMIN level of filtering is designed to allow the administrator to concentrate on those SEERs which are important, and not overload the administrator with informational SEERs. This will eliminate the nightly audit SEERs, and others which do not require the attention of the typical system administrator.

Filtering by severity and SEER type

When multiple filtering parameters are set, only those SEERs which pass through both filters are sent to the Message Trigger Mailbox.

For example, if the severity level is set to Critical and the SEER type is set to Error only Critical Error type SEERs will be sent to the Message Trigger Mailbox.

SEER Configuration screen

This is an example of the SEER Configuration screen.

```
                    System Event and Error Reports
SEER Configuration

Message Trigger Mailboxes:
        Mailbox:   7555
        Mailbox:   7556

SEER Printer Output:                      None Filtered Unfiltered

SEER Throttle Threshold Count:   5        Throttle Interval (hh:mm):   00:05
SEER Escalation Threshold Count: 0        Escalation Interval (hh:mm): 00:05

SEER Filters:
        SEER Severity Threshold:          None Critical Major Minor
        SEER Type Threshold:              Error Admin

Select a softkey>

    Save        Cancel
```

Field descriptions

The following table describes the fields used for SEER filtering in the SEER Configuration screen.

SEER Filters	
Description	This read-only field indicates that the remaining fields in the screen are applicable to the filter which determines whether a SEER is sent to the Message Trigger Mailbox or to the printer, or both.

SEER Severity Threshold	
Description	This field is used to specify the minimum severity level a SEER must have to be sent to the Message Trigger Mailbox and/or the SEER printer. If None is selected, only SEERs that have the Message Trigger Field set to Yes in the SEER Remap Table are sent.
Options	None, Critical, Major, or Minor
Default	Critical

SEER Severity Threshold	
Description	This field is used to specify the SEER type a SEER must have to be sent to the Message Trigger Mailbox and/or the SEER printer.
Options	Error and Admin
Default	Admin

Setting SEER filtering

To set SEERs filtering, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance. **Result:** The System Status and Maintenance screen is displayed.
2	Select System Event and Error Reports from the menu. **Result:** The System Event and Error Reports screen is displayed.
3	Select SEER Configuration. **Result:** The SEER Configuration screen is displayed.
4	In the SEER Severity Threshold field, select the severity.
5	In the SEER Type Threshold field, select the type of SEER that you want filtered.
6	Press the [Save] softkey to save your choices. **Result:** The changes are saved and you are returned to the System Event and Error Reports menu. Press the [Cancel] softkey to cancel changes to the SEER configuration. **Result:** The changes are cancelled and you are returned to the System Event and Error Reports menu.

Using SEER triggering

Introduction

SEER triggering is used so that the system administrator can be paged when a SEER generated by Meridian Mail meets filtering and throttling criteria used for the Message Trigger Mailbox.

The administrator can specify up to two mailbox numbers that will receive a message if a SEER meets the requirements to be sent to the SEER printer when filtered output is selected. SEER filtering can be bypassed by specifying Yes for the Message Trigger field for the SEER in the SEER Remap Table. The message is tagged as urgent and includes the SEER number, severity, and type.

Remote Notification can be configured for the mailbox to allow a support person to be notified immediately of the occurrence of the SEER by page or phone.

SEER Configuration screen

This is an example of the SEER Configuration screen.

```
                    System Event and Error Reports
SEER Configuration

Message Trigger Mailboxes:
       Mailbox:   7555
       Mailbox:   7556

SEER Printer Output:                      None Filtered Unfiltered

SEER Throttle Threshold Count:   5        Throttle Interval (hh:mm):   00:05
SEER Escalation Threshold Count: 0        Escalation Interval (hh:mm): 00:05

SEER Filters:
       SEER Severity Threshold:           None Critical Major Minor
       SEER Type Threshold:               Error Admin

Select a softkey>

     Save        Cancel
```

Field descriptions

The following table describes the fields used for SEER triggering in the SEER Configuration screen.

Message Trigger Mailboxes	
Description	This read-only field indicates that the next pair of fields in the screen are applicable to the configuration of the Message Trigger Mailboxes. When a SEER occurs that meets the Trigger requirements (as set in the SEER Filters fields), a message containing the SEER number and severity is sent to the mailbox specified belonging to the corresponding customer group specified. (For SEERs related to the Meridian Mail Hacker Monitor, the CLID and mailbox/dialed number are included.) These mailboxes can be configured with Remote Notification to page or phone a person when the message arrives in the mailbox.
Customer Number	
Description	The customer number that contains the mailbox that you want to set as the Message Trigger mailbox.
Default	1
Mailbox	
Description	This is the mailbox number to which the SEER trigger message is sent when the SEER triggering criteria are met. Validation is performed on the mailbox number to ensure its existence. This mailbox can be either a local voice user mailbox or an NMS mailbox (local site mailbox).
Default	The field is blank.

Procedure

To set SEERs triggering, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance. **Result:** The System Status and Maintenance screen is displayed.
2	Select System Event and Error Reports from the menu. **Result:** The System Event and Error Reports screen is displayed.
3	Select SEER Configuration. **Result:** The SEER Configuration screen is displayed.
4	In the Message Trigger Mailboxes field, enter the mailbox or mailboxes where the message is to be sent.
5	Check that the correct SEERs Filters have been set. (See “Setting SEER filtering” on page 29-34.)
6	Press the [Save] softkey to save your choices. **Result:** The changes are saved and you are returned to the System Event and Error Reports Menu. Press the [Cancel] softkey to cancel changes to the SEER configuration. **Result:** The changes are cancelled and you are returned to the System Event and Error Reports menu.

SEERs printing

Introduction

This section describes setting up SEERs printing in the SEERs configuration screen.

SEER Configuration screen

This is an example of the SEER Configuration screen.

```
                    System Event and Error Reports
SEER Configuration

Message Trigger Mailboxes:
       Mailbox:   7555
       Mailbox:   7556

SEER Printer Output:                      None Filtered Unfiltered

SEER Throttle Threshold Count:   5        Throttle Interval (hh:mm):   00:05
SEER Escalation Threshold Count: 0        Escalation Interval (hh:mm): 00:05

SEER Filters:
       SEER Severity Threshold:           None Critical Major Minor
       SEER Type Threshold:               Error Admin

Select a softkey>

     Save        Cancel
```

Field descriptions

The following table describes the field used for setting up SEER printing in the SEER Configuration screen.

SEER Printer Output	
Description	This field is used to indicate whether SEER printing should be turned on or off and whether unfiltered SEERs are printed or not.
Options	Filtered, Unfiltered, None
Default	Unfiltered

Setting SEERs printing

To set up SEERs printing, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select System Status and Maintenance. **Result:** The System Status and Maintenance screen is displayed.
2	Select System Event and Error Reports from the menu. **Result:** The System Event and Error Reports screen is displayed.
3	Select SEER Configuration. **Result:** The SEER Configuration screen is displayed.
4	In the SEER Printer Output field, select None, Filtered, or Unfiltered.
5	Press the [Save] softkey to save your choice. **Result:** The changes are saved and you are returned to the System Event and Error Report screen. Press the [Cancel] softkey to cancel changes to the SEER configuration. **Result:** The changes are cancelled and you are returned to the System Event and Error Reports menu.

Setting the SEER printer port name

Introduction

Use the SEER printer port name field in the General Options screen to allow SEER printing on a printer other than the SEER console printer.

General Options screen

This is an example of the General Options screen.

```
                          General Administration                    MORE ABOVE
General Options

                                 Integrated Mailbox Administration
                                 Voice Messaging (MMUI)
                                 Voice Messaging (VMUIF)
                                 Voice Menus & Announcements
                                 Voice Forms
                                 Meridian Mail Networking

Date Format for Administration
and Maintenance Reports:         mm/dd/yy yy/mm/dd dd/mm/yy

Valid printer port/device names can be viewed by selecting View/Modify for
each printer from Data Port Configuration in the Hardware Administration menu.

SEER Printer Port Name:          PRT0232_____   (Blank implies the console port)

Reports Printer Port Name:       ____________   (Blank implies the console port)

Select a softkey >

     Save        Cancel
```

Field description

This table describes the SEER Printer Port Name field.

SEER Printer Port Name	
Description	This is the printer port to which the SEER printer is connected. It requires additional data ports on an RSM card. The data ports must be defined as printer ports in the hardware database.
Default	The default is blank. If this field is left blank, the SEERs will print to the console printer port.
Maximum length	The printer port name may consist of a maximum of 12 alphanumeric characters.

Procedure

To set or change the SEER printer port name values, follow these steps.

Note: Remember that not specifying a printer port name implies sending the SEERS printing to the console.

Starting Point: The Main Menu

Step	Action
1	Select General Administration from the Main Menu. **Result:** The General Administration screen is displayed.
2	Select General Options from the General Administration menu. **Result:** The General Options screen is displayed.
3	Use the cursor keys to move to the SEER printer name field.
4	Enter a port name in the SEER Printer Port Name field. **Note:** If this field is left blank, SEERs printing is done on the console.
5	Use the softkeys to save or cancel the changes. • Press [Save]. **Result:** The changes are saved, and you are returned to the General Administration screen. • Press [Cancel]. **Result:** The changes are not saved, and you are returned to the General Administration screen.

Chapter 30

Operational Measurements

In this chapter

Overview	30-2
Section A: Overview of Operational Measurements (OM)	30-3
Section B: Setting up Operational Measurements	30-11
Section C: Interpreting Operational Measurements	30-25

Overview

Introduction

This chapter describes Operational Measurement (OM) reports and the procedures required to gather, store, and analyze OM information.

Section A: Overview of Operational Measurements (OM), describes Operational Measurements and how they are useful.

Section B: Setting up Operational Measurements, provides information required to set up Meridian Mail so that the Operational Measurements data is gathered and stored.

Section C: Interpreting Operational Measurements, provides procedures and guidelines for interpreting Operational Measurement reports.

Section A: Overview of Operational Measurements (OM)

In this section

Overview	30-4
What are Operational Measurements?	30-5
How Operational Measurements are useful	30-7

Overview

Introduction

This section describes Operational Measurements and provides information about their use.

What are Operational Measurements?

Introduction

The Operational Measurement (OM) reports allow administrators and Nortel support staff to study how a Meridian Mail system is being used. These reports may be used to determine if a change in the system is required to improve the level of service provided by Meridian Mail. For example, if overall traffic on the system is higher than was originally anticipated, a channel expansion may be necessary.

OM reports also show which features are being used a lot, and which features are not being used at all. OM reports can also reveal potential technical problems with the system, such as low disk space (the amount of disk space affects Meridian Mail's ability to store messages and perform its functions).

Traffic reports

Traffic reports shows how much the system is being used. The reports identify the number of calls processed, and the number of times users log in to Meridian Mail or access particular features such as Voice Messaging, Voice Menu applications, and Outcalling. For detailed descriptions, examples, and analyses of available traffic reports, see Chapter 31, "Operational Measurements traffic reports".

User Usage reports

User Usage reports monitor how specific users employ voice messaging, Meridian Networking (if installed), and AMIS Networking (if installed). Information is broken down to show user activity on a daily basis. For detailed descriptions, examples, and analyses of User Usage reports, see Chapter 32, "User Usage reports".

Outcalling Audit Trail reports

Outcalling Audit Trail reports provide you with statistics that allow you to monitor the use of Remote Notification (RN) and Delivery to Non-User (DNU) features. Two different reports can be generated: a summary report and a detail report. Each report provides statistics for a certain period of time (as specified by you) by user's name and mailbox. The information in the summary report helps in problem determination. The detail report provides call detail records that allow you to

troubleshoot outcalling problems. For a detailed description of these reports, see Chapter 33, “Audit Trail reports”.

Fax Audit Trail reports

Fax Audit Trail reports provide you with statistics that allow you to monitor how users are using the Fax on Demand features. Two different reports can be generated: a summary report and a detail report. Each report provides statistics for a certain time period (as specified by you). The information in the summary report helps in problem determination. The detail report provides call detail records that allow you to trouble shoot fax problems. For a detailed description of these reports, see Chapter 33, “Audit Trail reports”.

How Operational Measurements are useful

Overview

The information that follows describes ways of using Operational Measurements (OM) report statistics.

Using OM to monitor system usage

You can use OM reports to monitor how the system is being used. For example, you can use these reports to determine which features are being used and which are not, and if the use of the system matches what the expectations were when the system size was being determined. If the system is busier than was anticipated, then you may need to expand the system.

Using OM to detect potential system problems

Similarly, OM reports can also be used to identify potential system problems, and possibly the cause of the problems. Although you should always use input from the users of the system to help determine if there is a problem, OM reports provide more definite data to work with.

Example

If callers or users complain that they cannot access the Meridian Mail system, channels may be tied up or disk space may be low. OM reports can help you determine if the problem is with system capacity or inefficient usage.

Potential problems that can be detected using OM

Some of the potential problems that can be detected through OM reports are discussed in the following examples.

Example 1: Disk space low

If the voice space used on a disk volume is consistently over your disk usage warning level, then disk space is getting low. Steps should be taken to reduce the voice space used. Check the Voice Space Used column of the Disk Usage Detail report, and see “Analyzing the Disk Usage Detail report” on page 31-54 in Chapter 31.

Potential problems (cont'd)

Example 2: Channels busy

The Channel Usage Detail report shows the number of calls and voice mail usage (in CCS) per channel. If the number of calls is high or the average message length is exceptionally long, the channels may be too busy to handle all incoming calls. As a result, users may not be able to access Meridian Mail. Several of the "Analyzing" sections that follow the sample reports refer to analyzing or dealing with high traffic problems.

Example 3: Inefficient usage

The Services Summary Traffic report provides an overview of how much your Meridian Mail features are being used. If you notice that some features are not being used at all, this may indicate that the users are not aware of the feature (or do not know how to use it), or that the feature is not required. The users may require more training. Use broadcast messages to give brief pointers or to inform users of available training courses or material.

Example 4: Unauthorized usage

If the Thru-Dial feature is being accessed more frequently during off-hours or if the average length of the Thru-Dial sessions is long, this may indicate that unauthorized users (hackers) are accessing your Meridian Mail system in order to use the Thru-Dial feature (for example, to make long distance calls). If you notice unusual use of the Thru-Dial feature, review the dialing restrictions for Thru-Dial (refer to the *Voice Services Application Guide* [NTP 555-7001-325] for details). Also, if you are using an access password for Thru-Dial, change the access password and continue to monitor the Thru-Dial usage. For more information, see "Services Summary report" in Chapter 31, "Operational Measurements traffic reports", for the number of Thru-Dial sessions and the average session lengths during specific time periods.

Using OM as a billing tool

As an accounting and billing tool, Operational Measurements are used to generate the daily user billing files (for local activity). Use the User Usage reports to compile data for billing. If you have the AdminPlus feature installed, use Meridian Mail Reporter (MMR) to compile data for billing.

If your organization does not bill users of Meridian Mail, you may not need to use the User Usage component of Operational Measurements. However, it can also be used for tracking problems or history or for security reasons (for example, who is logging on and receiving messages).

Using OM as a capacity planning tool

As a capacity planning tool, Operational Measurements are used to generate traffic reports that you subsequently analyze to determine whether your system requires an upgrade either in disk storage, channel capacity, or perhaps in the number of nodes (should the number of users on your system approach one of the limits discussed in the *Messaging Overview* [NTP 555-7001-100]). If your organization's use of Meridian Mail is fairly stable, you need only use the traffic measurement component of Operational Measurements on an infrequent basis to verify that the system's resources are adequate for your needs.

Section B: Setting up Operational Measurements

In this section

Overview	30-12
Using the Operational Measurements menu	30-13
Calculating disk space required for OM data storage	30-15
Operational Measurements Options screen	30-19
Fields in the Operational Measurement Options screen	30-21
Setting Meridian Mail to collect and receive data	30-24

Overview

Introduction

This section describes the procedures for setting up Meridian Mail Operational Measurements. These procedures include the following:

- using the Operational Measurements menu
- calculating disk space required for OM data storage
- setting Meridian Mail to collect and receive data

Using the Operational Measurements menu

Introduction

The Operational Measurements menu is used to access the screens necessary for

- viewing or changing the parameters related to the collection and storage of OM data
- viewing and printing the OM reports available on your system

Operational Measurements menu

The following is an example of the Operational Measurements menu.

```
                    Operational Measurements

          1  Operational Measurement Options

          2  Traffic Reports

          3  Outcalling Audit Trail Report

          4  Fax Audit Trail Report

Select an item > _

     Exit
```

Note: The Outcalling and Fax Audit Trail report options appear only if these features are installed on your system.

Procedure

To use the Operational Measurements menu, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Operational Measurements. **Result:** The Operational Measurements menu is displayed.
2	To choose an item from the menu, enter the number and press <Return>. **Result:** The appropriate screen is displayed. **Note:** To return to the Main Menu at any time, press the [Exit] softkey twice.

Calculating disk space required for OM data storage

Introduction

Use this section to calculate the disk space required for Operational Measurement data storage.

Understanding system disk capacity requirements

Planning for system disk capacity for OM data is very important. Because OM data must be stored in a fixed amount of disk space, it is periodically overwritten by new data. You must ensure that you view or print any vital information before it is overwritten (the Operational Measurement Options screen defines how long data is stored). You must also ensure that OM data does not exceed the available storage capacity.

ATTENTION

If total storage exceeds 100%, you will run out of disk space. You should attempt to keep your disk usage for OM data below 60% to allow sufficient space for the rest of the system.

Should your calculations yield a result greater than 100%, reduce the number of days for which traffic or user usage data, or both, are stored, and repeat your calculations. The values presented in the "Storage requirement estimates" on page 30-17 are based on typical parameters for various Meridian Mail configurations. Should your system deviate markedly in any of these assumed traffic patterns, you will need to experiment to determine what your system can accommodate.

Procedure

To calculate the total disk storage required for OM data, follow these steps. As you follow these steps, refer to the "Storage requirement estimates" on page 30-17.

Step	Action
1	Determine the number of days that you wish to store the OM traffic data and user usage data before it is overwritten. Make a note of the number of days you decide on so that you can enter these values in the Operation Measurement Options screen (see "Operational Measurements Options screen" on page 30-19).
2	Use the table "Storage requirement estimates" on page 30-17 to determine the billing data cost and the user usage data cost. The "data cost" refers to the percentage of disk volume VS1 text space required. For example, a single-node, 24-port, 26-hour system would have a billing data cost of 2.89% and a user usage data cost of 0.36%.
3	Multiply the billing data cost by three (two days plus the current day's data are stored). For example, 3 x 2.89%
4	Multiply the number of traffic days by 1 percent to the result of step 3. For example, 8 x 1%
5	Multiply the number of user usage days by the user usage data cost. For example, 31 x 0.36%
6	Add the results from step 3, step 4, and step 5.

Example

For a single-node, 24-port, 26-hour system, and 31 user usage days, and 8 days of traffic stored:

number of days traffic data is stored = 8
number of days user usage data is stored = 31
billing data cost = 2.89%
user usage data cost = 0.36%

Total storage = (3 x 2.89%) + (8 x 1%) + (31 x 0.36%) = 27.83%

Storage requirement estimates

Use this table to estimate the amount of storage required for each operational measurement. Billing data cost and user usage data cost refer to the percentage of VS1 text space used.

System type	Number of ports	Billing data cost	User usage data cost
Card Option			
5, 10 hr	12	1.77%	0.22%
24 hr	12	1.56%	0.20%
54 hr	12	0.74%	0.09%
100 hr	12	0.44%	0.06%
Single node			
5, 11 hr	24	3.25%	0.41%
24, 26, 54 hr	24	2.89%	0.36%
100 hr	24	2.38%	0.30%
200 hr	24	2.09%	0.26%
2 node			
26 hr	48	6.06%	0.76%
54, 84, 114 hr	48	5.48%	0.69%
200 hr	48	5.31%	0.67%
400 hr	48	4.68%	0.59%
3 node			
30, 60, 90, 120, 200 hr	48	4.40%	0.55%
400 hr	48	4.00%	0.50%
4 node			
45, 90, 120, 180, 300 hr	72	5.85%	0.74%
600 hr	72	5.20%	0.65%
5 node			
60, 120, 180, 240, 400 hr	96	6.22%	0.78%
800 hr	96	5.50%	0.69%

Traffic assumptions

The preceding table is based on a typical system with an eight-hour business day, and the following traffic:

- 25% of the time at busy hour traffic (2 hours)
- 5% of the time at greater than busy hour traffic (25 minutes)
- 70% of the time at less than 75% of busy hour traffic (5 hours and 35 minutes)
- average call holding time of 40 seconds

Operational Measurements Options screen

Introduction

The Operational Measurement Options screen is used by the system administrator to define how system and user statistics are collected. This includes the time at which traffic data collection begins and ends every day, how often collected traffic statistics are written to disk, and whether or not traffic data, user usage data, or audit trail data is collected. Also included are the number of days of data that are stored for traffic, user usage data, and audit trail reports, and the percentage at which audit trail data collection will automatically be disabled.

Note: If the AdminPlus/Meridian Mail Reporter option is installed, it is important that a minimum set of OMs are collected. Refer to the *Meridian Mail Reporter 2.0 User's Guide* (P0847870).

Operational Measurement Options screen

The following is an example of the Operational Measurement Options screen.

Part 1

```
                    Operational Measurements
Operational Measurement Options

Collect Traffic Data:                      Disabled Enabled

Traffic Period Start (hh:mm):              01:00

Traffic Period End (hh:mm):                01:00

Traffic Commit Interval (hh:mm):           01:00

Number of days of Traffic Data stored:     8

Collect User Usage/Session Trace Data:     Disabled Enabled

Number of days of User Usage Data stored:  31

Collect Audit Trail Data:                  Disabled Enabled
                                                              MORE BELOW

   Save        Cancel
```

Part 2

```
                    Operational Measurements                  MORE ABOVE
Operational Measurement Options

Traffic Period End (hh:mm):                01:00

Traffic Commit Interval (hh:mm):           01:00

Number of days of Traffic Data stored:     8

Collect User Usage/Session Trace Data:     Disabled Enabled

Number of days of User Usage Data stored:  31

Collect Audit Trail Data:                  Disabled Enabled

Number of days of Audit Data stored:       7

Shutdown Audit Trail at Volume Full (%):   85 %

   Save        Cancel
```

Fields in the Operational Measurement Options screen

Overview

The following section describes the fields on the Operational Measurement Options screen.

Collect Traffic Data

When this field is Enabled, a statistical record of voice messaging and other voice services, voice channel traffic, Meridian Networking and AMIS Networking message traffic, and disk space usage will be collected and stored on disk. The default is Enabled.

Traffic Period Start (hh:mm)

This is for the time at which data begins to be collected, based on the 24-hour clock. The valid range is from 00:00 to 23:30. You may enter values only in half-hour increments, for example, 01:00, 01:30; 02:00, 02:30, and so on. The default is 01:00.

Traffic Period End (hh:mm)

This is for the time at which data stops being collected, based on the 24-hour clock. To continuously collect traffic data, set the Period Start field equal to the Period End field (that is, Period Start = 01:00 and Period End = 01:00). In this manner, data will be collected 24 hours a day. The valid range is 00:00 to 23:30. You may enter values only in half-hour increments, for example, 01:00, 01:30; 02:00, and 02:30. The default is 01:00.

Traffic Commit Interval (hh:mm)

The value in this field determines how often the collected traffic statistics are written to the hard disk within the defined traffic period. The default is 01:00. The valid range is from 00:00 to 23:30.

Commit intervals should be entered in half-hour increments and be equally divisible into the period range. The smallest allowed interval is 30 minutes. However, a one-hour interval will provide similar granularity of data and will require only half as many writes to disk (resulting in less disk usage) as the 30-minute interval.

Example

If the Collect Traffic Data field is set to Enabled and

Traffic Period Start = 08:00,
Traffic Period Stop = 17:00,
Traffic Commit Interval = 1:30,

traffic data is collected between 8:00 a.m. and 5:00 p.m. daily, and traffic reports are written to the hard disk every 1 hour and 30 minutes during this period. The first report is written out at 9:30 a.m. and the last one is written out at 5:00 p.m.

Note: The traffic commit interval can be set to 24 hours. However, an interval greater than two hours is not recommended because the accumulated numbers may be too large to be accommodated by the fields in the report screens. If a number is too large, >999 is displayed in the field to indicate overflow. Furthermore, any data that is not written to disk is lost if a system reboot occurs.

Number of days of Traffic Data stored

This field determines the number of days that traffic data is maintained before being overwritten by new traffic data.

Example

If this field is set to 8, on the 9th day you will not be able to view traffic data collected on the first day as it will have been overwritten, but you will be able to view the data from the remaining eight days. The old traffic data is removed from the disk at 1:20 a.m. each day. The data for the current day is not included in the number of days of traffic data stored. The valid range is 1 to 8 days. The default is 8 days.

Collect User Usage/ Session Trace Data

This field controls the collection of both user usage data and session trace data. Session trace data includes detailed voice messaging session statistics. The session statistics are kept for two days, regardless of how long you define user usage data to be stored. (For example, on Monday you can view Saturday's data, but not Friday's data.) Session reports can be accessed using the Session Trace tool (refer to *System Administration Tools* [NTP 555-7001-305]). The default is Enabled.

Number of days of User Usage Data stored

This field controls the number of days of user usage summary statistics data that is kept on the hard disk before it is overwritten. The range is from 1 to 63. The default is 31.

Collect Audit Trail Data

This field appears only if Outcalling or Fax On Demand is installed. When this field is set to Enabled, Outcalling or Fax Audit Trail reports are generated by the system. These reports can be used to obtain information about a specific outcalling or fax callback session. The reports give you either summary or detailed information about the number of calls, the start time and duration of calls, the numbers called, and details of the call status. The default is Enabled. See Chapter 33, "Audit Trail reports," in this guide for more information.

Number of Days of Audit Data stored

This field appears only if either Outcalling or Fax On Demand is installed. This field is used if the Collect Audit Trail Data field is set to Enabled. This field indicates the number of days the audit trail data will be stored on disk before being overwritten. The number of days can range from 1 to 63, with a default of 7.

Shutdown Audit Trail at Volume Full (%)

This field appears only if either Outcalling or Fax On Demand is installed.This field is used if the Collect Audit Trail Data field is set to Enabled. When the volume on which audit trail data is stored meets this percentage, collection of audit trail data is disabled. (Note that this is a percentage of text space, not voice space.) The range for this field is from 1% to 100%. The default is 85%.

OM Collection ACCESS Class

This field indicates the class number of the ACCESS application for which Operational Measurements should be collected. The valid range for this number is 0 to 8999. It is primarily intended to be used to collect messenger desktop access of Meridian Mail ports.

Note: This field is available only if ACCESS is installed.

Setting Meridian Mail to collect and receive data

Introduction

Use the Operational Measurement Options screen to define the parameters for collecting the OM information from your Meridian Mail system.

Procedure

To set the Operational Measurement parameters, follow these steps.

Starting Point: The Operational Measurements menu

Step	Action
1	Select Operational Measurements. **Result:** The Operational Measurement Options screen appears.
2	Set the parameters as required. For information on setting these parameters, see “Fields in the Operational Measurement Options screen” on page 30-21.
3	Choose step 4 to save the changes or step 5 to cancel.
4	Press [Save]. **Result:** The changes are saved and the Operational Measurements menu is redisplayed. **Note:** Any saved changes force all traffic data to be committed at the time of the save, regardless of the interval and period specified. This action will also create an irregular time period (the time up to the save) that will appear on the traffic reports. Also, a SEER is issued to indicate that the changes have taken effect.
5	Press [Cancel]. **Result:** Any changes you have made are discarded; the Operational Measurements menu is redisplayed.

Section C: Interpreting Operational Measurements

In this section

Overview	30-26
Calculating centi-call seconds	30-27
Interpretation guidelines	30-28

Overview

Introduction

This section describes the calculation of centi-call seconds and provides guidelines that are useful when interpreting OM reports.

Calculating centi-call seconds

Introduction

Many of the OM reports provide usage time in centi-call seconds. Centi-call seconds (CCS), or hundreds of call seconds, can be calculated using the formula in this section.

Definition

CCS is a traffic measurement statistic. One CCS is equal to 100 seconds of call connection time per hour. The CCS is based on the total number of call seconds, not the average length, multiplied by the number of accesses.

Formula

To calculate the CCS value, use the following formula.

$$CCS = \frac{60\ minutes}{interval\ (in\ minutes)} \times \frac{total\ call\ seconds}{100\ seconds}$$

The first part of the formula compensates for intervals that are not one hour.

Examples

320 total call seconds during a half-hour interval produces the following CCS:

$$CCS = \frac{60\ minutes}{30\ minutes} \times \frac{320\ seconds}{100\ seconds} = 2 \times 3.2 = 6.4 \approx 6$$

If the interval is one hour, the first part of the formula can be ignored. For example, 320 total call seconds over a one-hour interval produces the following CCS:

$$CCS = \frac{60\ minutes}{60\ minutes} \times \frac{320\ seconds}{100\ seconds} = 1 \times 3.2 = 3.2 \approx 3$$

Interpretation guidelines

Introduction

When interpreting the OM reports, consider the following guidelines.

Service counts

Look not only at the counts for each service but also at the relationship between the counts for different services.

Example

Both Express Messaging and Call Answering features allow messages to be left in the system. Therefore, both counts should be taken into consideration when looking at the total number of incoming messages during a particular time period.

System size

Know the size of the system, both channels and disk capacity. Smaller systems will be much more sensitive to high traffic counts and durations than larger systems.

How your organization uses the system

Know how your organization uses the system.

Many of the counts and durations will have a direct relationship to how the organization uses the system as part of its overall operation (for example, voice messaging only, auto attendant, menus, and so on). If you do not know how the organization functions, find someone within the organization who does, and interpret the information together. That person will provide the necessary knowledge about how the organization works, and you can provide the information about the system.

If there is unusual system activity

Make sure you have taken any unusual operational activity into consideration.

For example, is it a national holiday? an election day? or was there a major news event recently? Such unusual activities may cause an abnormal usage of your system that will distort the figures.

Report relationships

Many reports relate to one another.

For instance, the Services Summary report provides a summary of the voice menus, fax, announcement traffic, and other services, but the Services Detail report provides much more detail about particular services. Know what reports a system can produce, and know which ones relate to others. Read through each report and move back and forth through the information, making sure you have optimized the interpretation and analysis process.

User consultation

Consult the users of the system to gain further insight into a report's findings.

Find out how the system is working for the users and if they have any problems to report. Some apparent system problems may be the result of improper usage of the system (perhaps due to lack of training or awareness of certain system features).

Impact of new features or services

Consider how long a feature or service has been in operation.

When something is new, it may generate more traffic than normal as a result of curiosity, or it may generate less traffic due to lack of familiarity with the new feature, so the initial figures may be distorted.

Working with multiple Meridian Mail systems

If you are working with numerous Meridian Mail systems, remember that each Meridian Mail system is unique.

Make sure you apply all the previously described guidelines separately to each system.

Chapter 31

Operational Measurements traffic reports

In this chapter

Overview	31-2
Section A: Generating traffic reports	31-3
Section B: Traffic reports	31-9

Overview

Introduction

This chapter is devoted to Operational Measurement (OM) traffic reports. These reports show how much the system is being used. The reports identify the number of calls processed, and the number of times a user logs in to Meridian Mail or accesses particular features such as Voice Messaging, Voice Menu applications, and Outcalling.

Section A: Generating traffic reports, describes how to generate, view, and print OM traffic reports. The section also describes the Traffic Reports screen, which lists the reports that can be generated.

Section B: Traffic reports, provides descriptions and analyses for all of these reports.

Section A: Generating traffic reports

In this section

Overview 31-4
Traffic Reports screen 31-5
Generating traffic reports 31-7

Overview

Introduction

This section describes the Traffic Reports screen and the procedure for generating, viewing, and printing traffic reports. All traffic reports that can be generated are listed on the Traffic Report screen. For descriptions and analyses for all of the traffic reports, see Section B: Traffic reports, on page 31-9.

Traffic Reports screen

Introduction

This section describes the Traffic Reports screen. Access the Traffic Reports screen by selecting Traffic Reports on the Operational Measurements screen.

The screen

The following is an example of the Traffic Reports screen.

```
                          Operational Measurements
 Traffic Reports

 Services Summary:                      No Yes
 Voice Messaging Detail:                No Yes
 Channel Usage Detail:                  No Yes
 Services Detail:                       No Yes
 Networking Detail:                     No Yes
 AMIS Networking Detail:                No Yes
 Outcalling Detail:                     No Yes
 Fax Delivery Detail:                   No Yes
 Disk Usage Detail:                     No Yes
 Hospitality Statistics:                No Yes
 Guest Console Statistics:              No Yes

 Report Start (mm/dd/yy hh:mm): 05/01/96 18:00 (or blank for oldest)
 Report End   (mm/dd/yy hh:mm): 05/02/96 18:00 (or blank for newest)

Select a softkey >

   Exit                          View Reports   Print Reports
```

Available traffic reports

Each line in the Traffic Reports screen represents a specific type of report. The following is a list of the available traffic reports. Some of the reports are available only if additional features are installed on your Meridian Mail system. For descriptions and analyses of these reports, see Section B: Traffic reports:

- Services Summary
- Voice Messaging Detail
- Channel Usage Detail
- Services Detail (if the Fax on Demand, Voice Forms, or Voice Menus feature is installed)
- Networking Detail (if Meridian Networking is installed)
- AMIS Networking Detail (if AMIS Networking is installed)
- Outcalling Detail (if Outcalling is installed)

- Fax Delivery Detail (if Fax on Demand is installed)
- Disk Usage Detail
- Hospitality Statistics (if the Hospitality feature is installed)
- Guest Console Statistics (if the Hospitality feature is installed)

Generating traffic reports

Introduction

This section describes the procedure for generating traffic reports. The Traffic Reports screen allows you to choose which reports you want to view and print. Also, you have the option of choosing a Report Start and Report End date and time.

Procedure

To generate traffic reports, follow these steps.

Starting Point: The Operational Measurements screen

Step	Action
1	Select Traffic Reports from the Operational Measurements screen. **Result:** The Traffic Reports screen displays.
2	Move the cursor to the report titles you wish to view or print. Use the arrow keys to toggle the field value to Yes.
3	(This step is optional.) Specify start and stop times for the report period by entering the values in the Report Start (mm/dd/yy hh:mm) and Report End (mm/dd/yy hh:mm) fields. (The format mm/dd/yy hh:mm is the default. The format can be changed in General Administration, General Options. For more information, see Chapter 13, “General options”. **Note:** The values you enter are based on the 24-hour clock. The valid range is from 00:00 to 23:59 (12:00 midnight to 11:59 p.m.). If the Report Start and Report End fields are left blank, the defaults of start of available data and end of available data are used respectively.
4	Go to step 5 to view the reports on the terminal, step 6 to print the reports, or step 7 to cancel.

Step	Action
5	Press [View Reports]. **Result:** The selected report screens are displayed one at a time. Follow the instructions in the table below to view the next report, exit the screen, or view the next page in the same report.

IF you want to	THEN press softkey
leave the current report and go to the next report	[Next Report].
exit all reports and return to the Traffic Reports screen	[Exit].
view subsequent pages of the current report (if available)	[Next Page].

For descriptive and analytical information on individual reports, see Section B: Traffic reports, on page 31-9.

6	Press [Print Reports]. **Result:** You are prompted to ensure the printer is ready and online. During printing, you have two options available.

IF you want to	THEN press softkey
print the reports	[Continue Printing].
cancel printing at any time	[Cancel Printing].

Note: There may be some delay before control is returned to the screen because it waits for the printer to stop printing.

7	Press [Exit]. **Result:** The Operational Measurements menu is displayed again.

Section B: Traffic reports

In this section

Overview	31-11
Services Summary report	31-12
Fields in the Services Summary report	31-13
Analyzing the Services Summary report	31-15
Voice Messaging Detail report	31-18
Fields in the Voice Messaging Detail report	31-19
Analyzing the Voice Messaging Detail report	31-21
Channel Usage Detail report	31-22
Fields in the Channel Usage Detail report	31-23
Analyzing the Channel Usage Detail report	31-25
Services Detail report	31-26
Fields in the Services Detail report	31-27
Analyzing the Services Detail report	31-29
Networking Detail report	31-31
Fields in the Networking Detail report	31-32
Analyzing the Networking Detail report	31-35
AMIS Networking Detail report	31-37
Fields in the AMIS Networking Detail report	31-38
Analyzing the AMIS Networking Detail report	31-40
Outcalling Detail report	31-41
Fields in the Outcalling Detail report	31-42
Analyzing the Outcalling Detail report	31-45
Fax Delivery Detail report	31-47
Fields in the Fax Delivery Detail report	31-48
Analyzing the Fax Delivery Detail report	31-50
Disk Usage Detail report	31-52
Fields in the Disk Usage Detail report	31-53

Analyzing the Disk Usage Detail report 31-54
Hospitality Statistics report 31-56
Fields in the Hospitality Statistics report 31-57
Analyzing the Hospitality Statistics report 31-58
Guest Console Statistics report 31-59
Fields in the Guest Console Statistics report 31-60
Analyzing the Guest Console Statistics report 31-61

Overview

Introduction

This section provides descriptions and analyses of each traffic report. Included are an example report screen and field descriptions.

Services Summary report

Overview

The Services Summary report provides statistics for each of the services installed in your system. The total number of times a user dialed a service (number of accesses), and the average length of each access are given.

The screen

The following is an example of the Services Summary report screen.

```
                          Operational Measurements
Services Summary

                                                   Average        Voice
                                        Number of  Length       Mail Usage
Interval Start-End Service Name         Accesses  (in seconds)    (in CCS)
5/01 18:00-19:00   Thru-Dial                53         7             4
                   Voice Menus             301        12            36
                   Voice Messaging        1022        65           664
                   Call Answering         1437        29           416
                   AMIS                      0         0             0
                   Express Messaging        86        49            42
                   Voice Announcements      31       111            34
                   Meridian Networking       0         0             0
                   Voice Administration      0         0             0
                   Voice Prompt Admin        0         0             0
                   Time of Day Control       0         0             0
                   Post Check Out            0         0             0
                   Delivery to Non-User      0         0             0

Select a softkey > _

   Exit        Next Report                 Next Page
```

Fields in the Services Summary report

Interval Start-End

Data are divided into intervals. The length of the interval depends on the entry made in the Traffic Commit Interval field in the Operational Measurement Options screen. The number of intervals displayed depends on the entries made in the Traffic Period Start and Traffic Period End fields in the Operational Measurement Options screen.

Example

If data is collected 24 hours a day (from 01:00 to 01:00), and the commit interval is one hour, the report will divide the data into 24 intervals for each day included in the report. The amount of data displayed in this report depends on the Report Start and Report End entries that were made in the Traffic Reports screen. If no report start and end dates and times were given, all data currently stored on disk are displayed.

Service Name

This field displays the name of the service that was accessed.

Number of Accesses

This field displays the number of calls (peg count) made to the corresponding service. The number of Thru-Dial accesses includes accesses to Voice Service Thru-Dial (automated attendants), Call Service Thru-Dial, and Logon Thru-Dial.

Note: If a call continues past the interval, the access is counted only in the second interval (when the call is completed), although the call length is properly divided between the two intervals.

Example 1

If a call starts ten minutes before the end of an interval, that ten minutes of call length is counted in that interval. If the same call continues for five minutes into the next interval, the five minutes is counted in the second interval. The number of accesses is increased by zero in the first interval and by one in the second interval. The call is pegged in this way to match the way calls are tracked by the switch.

Example 2

If a call that spans two intervals is the only call to that service in those intervals, the number of accesses in the first interval would be zero while the number of accesses in the second interval would be one.

Average Length (in seconds)

This field displays the average length of the corresponding voice service sessions during the specified interval.

Voice Mail Usage (in CCS)

This field displays the amount of time that a Meridian Mail service was active in the defined interval. The value is given in CCS (hundred call-seconds), a traffic measurement statistic. One CCS is equal to 100 seconds of call connection time per hour. The CCS is based on the total number of call seconds, not the average length multiplied by the number of accesses.

Analyzing the Services Summary report

Introduction

Use the summary report, including the CCS values, to get an overall sense of which services are generating the most traffic and which are generating little or no traffic. Consider the example and the information that follows when doing your analysis.

Example

The second line in the sample report on page 31-12 shows that 301 calls, with an average length of 12 seconds, were placed to the Voice Menu service for a total of 3612 seconds (301 x 12). This equates to 36 CCS in the one-hour interval. The CCS count is computed for the one-hour interval as follows:

$$CCS = \frac{3612\ seconds}{100\ seconds} = 36.12 \approx 36$$

A feature is not being used

This may mean that the feature is not working properly, or that the users are not aware of the feature and therefore do not use it.

Suggested action

After the administrator notices a low (or no) usage of a particular feature, it is up to the administrator to do additional research to determine if there is a technical problem with the feature, or if it simply is not being used, or if it is normal for the usage to be low for the observed time period.

If a particular feature is generating an unusually high amount of traffic

If a feature is generating an unusually high amount of traffic, you may encounter system performance problems such as no free channels.

Suggested actions

Run the report that goes with that service, if there is one, for more information. As the administrator, you may need to do more research beyond checking the OM reports to learn more about the nature of the problem to come up with a solution. For example, you need to determine if the high traffic level was due

to some unusual event that affected your organization (if so, the high traffic would not be expected to continue).

If the high traffic for a particular feature is expected to continue, one solution may be to dedicate a channel to the feature so that the feature does not tie up the whole system. For more details on dedicating channels, see Chapter 23, "Configuring Meridian Mail services". Another solution is to expand the system if overall traffic for the whole system is higher than what was originally anticipated for the system.

Check the average length for Voice Menu and Announcement accesses

Another area to check is the average length for Voice Menu and Announcement accesses (see "Services Summary report" on page 31-12).

Suggested action

If the average length is long, review your menus and announcements to see if they can be shortened or rearranged for more efficient use.

In menus, place the popular items first so that users do not need to stay on the line as long before the item they want is presented. If a menu has a long average length and it accesses an announcement, try to shorten the announcement.

High number of Call Answering accesses

Suggested action

If the number of Call Answering accesses is high, check the logon count versus the number of times Call Answering has been accessed (the Voice Messaging Detail report gives the logon count).

If the logon count is low compared to the number of Call Answering accesses, this means that users are accumulating several messages before logging on to listen to them. Too many accumulated messages lowers the amount of available disk space to the point where overall system performance may be affected.

Users are having trouble logging in at a certain time

Suggested action

If users are having trouble logging in to Meridian Mail at a certain time, check the level of traffic for that time period.

You may have found your heavy traffic period or busy hour. If there is no way to reduce the traffic during that time period, you may need to expand your system.

The number of Thru-Dial accesses is unusually high

If you have an unusually high number of Thru-Dial accesses, this may be a sign of hackers present on your system.

Suggested actions

If you suspect hackers are accessing the Thru-Dial feature, first check how the Thru-Dial service is set up to see if the OM data are unusual. If your research suggests the possible presence of hackers, review the dialing restrictions for Thru-Dial (refer to the *Voice Services Application Guide* [NTP 555-7001-325] for details). Also, if you are using an access password for Thru-Dial, change the access password and continue to monitor the Thru-Dial usage.

Voice Messaging Detail report

Introduction

The Voice Messaging Detail report provides information about logon sessions, Call Answering sessions, and messages composed during logon sessions. If data is unavailable for a given statistic, N/A (not available) is displayed instead of a value. For example, if the interval is one minute long, the system may interpret that interval as having zero length, so no data is available. A 1-minute interval may be created if you update and save the OM options, which forces all traffic data to be written to disk at that point and results in an irregular interval.

If a value is too large to fit in a field, >999 is displayed.

The screen

The following is an example of the Voice Messaging Detail report screen.

```
                              Operational Measurements
Voice Messaging Detail (VM Logon, Call Answering and Express Messaging)

                      Number     Number of  Session    Messages    Message
                      of Calls   Sessions   Length     Created     Length
Interval Start-End    Int  Ext   EM/Ans Log  Avg  Max  EM/Ans Log  Avg  Max
5/01 13:00-14:00      18   0     2     16    238  470   0     2    20   25
5/01 14:00-15:00      12   2     5      9    310  310   1    32    14   14
5/01 15:00-16:00      17   1     1     17    478  614   1    20    20   20

Select a softkey > _

     Exit        Next
                 Report
```

Fields in the Voice Messaging Detail report

Interval Start-End

Data are divided into intervals. The length of the interval depends on the entry made in the Traffic Commit Interval field in the Operational Measurement Options screen. The number of intervals displayed depends on the entries made in the Traffic Period Start and Traffic Period End fields in the Operational Measurement Options screen.

Example

If data are collected 24 hours a day (from 01:00 to 01:00), and the commit interval is one hour, the report will divide the data into 24 intervals for each day included in the report. The amount of data displayed in this report depends on the Report Start and Report End entries that were made in the Traffic Reports screen. If no report start and end dates and times were given, all data currently stored on disk are displayed.

Number of Calls (Int and Ext)

This field shows the number of Voice Messaging, Call Answering, or Express Messaging calls made. The data are displayed in the following subfields.

Int

This display indicates the number of calls made from inside the switch during the specified interval.

Ext

This display indicates the number of calls made from outside the switch during the specified interval.

Number of Sessions (EM/Ans and Log)

This is the number of sessions in the interval.

EM/Ans

This display indicates the number of sessions used for Express Messaging and Call Answering services.

Log

This display indicates the number of time users logged into their mailboxes during the interval.

Note: The sum of the values in these two columns should equal the sum of the two Number of Calls values. To determine the number of messages that were actually received or created during these sessions, check the Messages Created fields.

Session Length (Avg and Max)

This field indicates the average length and maximum length (in seconds) of Call Answering, Express Messaging, and logon sessions for the interval.

Messages Created (EM/Ans and Log)

This field indicates the number of messages created during the interval.

EM/Ans

This display indicates the number of messages left during Express Messaging and Call Answering services.

Log

This display indicates the number of messages that were created (using the compose, forward, or reply command) during the interval.

Message Length (Avg and Max)

This field indicates the average length and the maximum length (in seconds) of messages received and created during the interval. Since message length has an impact on disk storage, use this information to determine if enough disk space has been provisioned for voice messages.

Analyzing the Voice Messaging Detail report

Introduction

The first line in the sample report on page 31-18 shows that 18 calls were placed to Meridian Mail. Sixteen were logon sessions (for example, to compose, forward, or listen to messages). Two calls accessed the Express Messaging or Call Answering feature (an attempt to leave a message at another mailbox). If the number of sessions does not equal the number of calls, there is a problem with your system.

EM/Ans Sessions and Messages are similar in number

The number of EM/Ans sessions should match or be close to the number of EM/Ans messages created. When there are more EM/Ans sessions than EM/Ans messages created (as in the sample report), this means that during an Express Messaging session, or after reaching the Call Answering greeting, users are hanging up without leaving a message, or they are pressing 0 to transfer to an attendant. Either of these results in Express Messaging or Call Answering sessions but no messages created.

Suggested actions

If the disparity between the two numbers is high, the users may need some training on the use of Express Messaging and Call Answering. Also, users should review their greetings. If greetings are unfriendly or if instructions are too complex, this may be causing users to hang up without leaving a message.

There is a high number of calls and long messages

On this report, watch for high numbers of calls and long messages. Too many calls in a short period of time and users leaving long messages will tie up channels and prevent others from accessing Meridian Mail.

Suggested action

You may need to expand your system.

Channel Usage Detail report

Introduction

The Channel Usage Detail report provides details about channel activity for incoming and outgoing calls, including average session lengths and CCS statistics.

The screen

The following is an example of the Channel Usage Detail report screen.

```
                              Operational Measurements
Channel Usage Detail

                          Number of Number of  Incoming    Outgoing   Voice
                          Incoming  Outgoing  Avg Length  Avg Length Mail Usage
Interval Start-End Channel  Calls     Calls  (in seconds)(in seconds) (in CCS)
5/01 18:00-19:00        1     0         0          0           0        0.0
       09:00-10:00      2    44         0         42           0       18.5
                        3    43         0         47           0       20.2
                        4    40         0         49           0       19.6
                        5    46         0         40           0       18.4
                        6    48         1         35          30       17.1
                        7    47         1         39          31       18.6
                        8    45         1         38          30       17.4
                        9    47         2         36          33       17.6
                       10    43         0         47           0       20.2
                       11    46         0         40           0       18.4
                       12    44         0         42           0       18.5
                       13    49         0         40           0       19.6
_______________________ __
Select a softkey > _

   Exit        Next        |           Next        |
               Report      |           Page        |
```

Fields in the Channel Usage Detail report

Interval Start-End

Data are divided into intervals. The length of the interval depends on the entry made in the Traffic Commit Interval field in the Operational Measurement Options screen. The number of intervals displayed depends on the entries made in the Traffic Period Start and Traffic Period End fields in the Operational Measurement Options screen.

Example

If data are collected 24 hours a day (from 01:00 to 01:00), and the commit interval is one hour, the report will divide the data into 24 intervals for each day included in the report. The amount of data displayed in this report depends on the Report Start and Report End entries that were made in the Traffic Reports screen. If no report start and end dates and times were given, all data currently stored on disk are displayed.

Channel

This field indicates the channel being monitored.

Number of Incoming Calls

This field indicates the number of incoming calls during the interval.

Number of Outgoing Calls

This field indicates the number of outgoing calls during the interval.

Incoming Avg Length (in seconds)

This field indicates the average length of incoming calls during the interval.

Outgoing Avg Length (in seconds)

This field indicates the average length of outgoing calls during the interval.

Voice Mail Usage (in CCS)

This field represents the amount of time in terms of CCS that a Meridian Mail channel was active in the defined interval. CCS is a traffic measurement statistic. The value is displayed in the nearest one tenth of a CCS (for example, 11.0).

Note: There is a similar Voice Mail Usage field in the Services Summary Traffic report (see “Services Summary report” on

page 31-12). However, because the two fields measure usage differently (one in terms of channels and the other in terms of voice services), there may be small differences between the two fields if you calculate the totals for the displayed values.

Analyzing the Channel Usage Detail report

Introduction

The CCS for each channel gives an indication of how busy each channel is. With Automated Call Distribution (ACD), the traffic (measured in CCS) should be evenly distributed across all channels over a lengthy period (for example, 12 hours).

Equal distribution of channel traffic

Channels with short durations will have a higher number of calls than channels with long durations, but the average amount of traffic (for example, CCS) for each nondedicated channel should be similar.

Suggested action

If the traffic is not evenly distributed, check if all channels are working properly. If a channel has no traffic at all for the entire period of the report, this may indicate that the channel is out of service. If any channels are dedicated to a particular service, the number of calls for the dedicated channels may differ significantly from the number of calls on the other channels.

Users are having trouble accessing Meridian Mail

Users may have trouble accessing Meridian Mail (for example, callers are getting ringback or a busy signal) if the system is busy.

Suggested action

Check if the dedicated channel appears to have much fewer calls than other channels. If so, you may be better off removing the dedication and opening the channel to all services. A busy system cannot afford to have any channels that are not sharing the full load on the system.

Services Detail report

Introduction

This report is available only if Fax on Demand, Voice Forms, or Voice Menus is installed on your system. The Services Detail report records the number of accesses, direct or indirect, to voice menus, announcements, fax items, thru-dial service, time-of-day controllers, and voice forms. Direct accesses occur when a user dials the VSDN of the service. Indirect accesses occur when a service is accessed from another service through a menu selection.

The screen

The following is an example of the Services Detail report screen.

```
                          Operational Measurements
Services Detail

Interval Start-End
                  Service    For each menu item, the number of accesses are:
Cust#  ID         Accesses     1   2   3   4   5   6   7   8   9   0   *   #
     18:00-19:00  No Activity
5/01 09:00-10:00
      AS 1003       11        0   0   0   0   0   0   0   0   0   0   0   0
      MS 1011        2        0   0   0   0   0   0   0   0   0   0   0   0
      FI 3001        2        0   0   0   0   0   0   0   0   0   0   0   0
      MS 4022        2        1   0   0   1   0   0   0   0   0   0   0   0
      MS 4023        5        0   0   1   0   0   1   0   2   0   0   0   0
      MS 4033       42        6  21   0   0   0   0   0   0   0   0   0   0
      MS 4058      167       41 116   0   6   4   0   0   0   0   1   2   0
      VF 1013        1        -   -   -   -   -   -   -   -   -   0   -   -
      TD 1023        2        -   -   -   -   -   -   -   -   -   -   -   -
      TS 1033        1        -   -   -   -   -   -   -   -   -   0   -   -

Select a softkey > _

 Exit      Next Report      Next Page
```

Fields in the Services Detail report

Interval Start-End

Data are divided into intervals. The length of the interval depends on the entry made in the Traffic Commit Interval field in the Operational Measurement Options screen. The number of intervals displayed depends on the entries made in the Traffic Period Start and Traffic Period End fields in the Operational Measurement Options screen.

Example

If data are collected 24 hours a day, and the commit interval is one hour, the report will divide the data into 24 intervals for each day included in the report. The amount of data displayed in this report depends on the Report Start and Report End entries that were made in the Traffic Reports screen. If no report start and end dates and times were given, all data currently stored on disk are displayed.

ID

This is the service followed by the ID number. The services are as follows.

Acronym	Service	Acronym	Service
AS	Announcement	VF	Voice Forms
MS	Voice Menu	TD	Time of Day
FI	Fax Information	TS	Thru-Dial

Service Accesses

This is the number of times the service was accessed (either directly or indirectly) during the measurement period.

For each menu item, the number of accesses are

This is the total number of times that each menu option was used during the measurement period. For stand-alone announcements and fax items, all frequencies are 0. If announcements or fax items are accessed through a voice menu, then there is an access count if a caller presses 0 to revert to the attendant.

Note: The number of accesses for the individual menu items may not add up to the number of accesses for the menu itself (Service Accesses) because some callers will hang up after reaching the menu if they do not want to choose any of the menu options, or if they want to talk to a live person.

Similarly, calls from rotary dial phones that are able to directly access a menu will be counted in the Service Accesses column but not in the number of accesses for individual menu items, since the rotary dial phone does not have the touch-tone capability required to select a menu item.

For Thru-Dial and Voice Forms, the number of accesses for key "0" count the number of times callers press zero to revert to the attendant. The "-" (dashes) emphasize no other count keys are being counted. For Time of Day, all menu item accesses are shown as dashes.

Analyzing the Services Detail report

Introduction

This report provides a detailed breakdown of which menu items, announcements, or fax items are actually being accessed, and a sense of the traffic that each service is generating.

Note: For a proper analysis of this report, have a printed copy of the service in front of you for reference.

While reviewing the report, consider the following.

If the menu requires reorganization

Menu items that are at the end of the menu (for example, item 8 or 9) are being accessed more frequently than earlier items.

Suggested action

You may wish to reorganize the menu so that the popular items are presented first.

This structure prevents users from having to wait through all the earlier options before hearing the one they want, thus reducing the call length.

A service is generating a high volume of traffic

A particular service is generating a high volume of traffic.

Suggested action

Find out if there is any call blockage (that is, users are unable to access the system).

If announcements or menus are causing call blockage, see if the information can be provided in some other way than through Meridian Mail (for example, through hard-copy memos or bulletin boards). If the service is a definite requirement and its usage cannot be decreased, then your system may require a channel expansion.

There are menu items with few or no accesses

If a menu item has few or no accesses, the reason may be either that there is a lack of training or awareness regarding those items, or that those items are simply not required.

Suggested action

If you find that certain services are not required, either remove them or replace them with more useful services. Check with the application owners to ensure the correct telephone number has been provided to the target audience. Be sure to rerecord the greetings and menu choices to reflect the changes.

The traffic pattern is unusual

Is the traffic high or low for a particular service?

Suggested action

Consult the users to determine if there was some unusual reason for the change in traffic.

If the high or low traffic is expected to return to acceptable levels, no adjustment may be necessary to the system.

Networking Detail report

Introduction

This report is available only on systems with Meridian Mail Networking installed. The Networking Detail report displays traffic totals for each active site within the Meridian Mail network for traffic generated by Meridian Mail, Enterprise, and AMIS Virtual Node Networking. Statistics are shown for the number of messages received at each site from other network sites and the messages delivered to network sites. Statistics are also displayed for network usage and failures.

The screen

The following is an example of the Networking Detail report screen.

```
                              Operational Measurements
Networking Detail

Interval Start-End
       Messages      Messages Delivered        Network Usage      Failures
       Received   Eco Std Urg NDN Ack Failed   Att Suc  Time   No   Not  Prot
Site  (from Site) (-----to site-----) to Send           (min)  Res Reach Error
05/01 10:00-11:00
 111   100          10 10  5  0  0      0       2  1   2:32   6   12     0
 112   100           0  0  2  0  0      0       4  2   4:04   0    0     0
05/01 11:00-12:00
 111    25          15 11  8  0  0      0       3  1   3:02   4    9     0
 112    50           0  0  4  0  0      0       6  4   5:09   2    3     0

Select a softkey > _

     Exit        Next
                 Report
```

Fields in the Networking Detail report

Interval Start-End

Data are divided into intervals. The length of the interval depends on the entry made in the Traffic Commit Interval field in the Operational Measurement Options screen. The number of intervals displayed depends on the entries made in the Traffic Period Start and Traffic Period End fields in the Operational Measurement Options screen.

Example

If data is collected 24 hours a day and the commit interval is one hour, the report will divide the data into 24 intervals for each day included in the report. The amount of data displayed in this report depends on the Report Start and Report End entries that were made in the Traffic Reports screen. If no report start and end dates and times were given, all data currently stored on disk are displayed.

Site

This is the remote site ID to which the row of data applies.

Messages Received

This field indicates the number of messages received successfully by the local site from the specified remote site.

Messages Delivered

This is the number of messages delivered from the local site to the identified remote site during the specified interval. This statistic is further subdivided into the following categories based on the type of message.

Eco

These are messages that have been classed as economy.

Std

These are messages that have been classed as standard.

Urg

These are messages that have been classed as urgent.

NDN

These are non-delivery notification messages sent by the system to users whose messages could not be delivered to some of the intended recipients due to incorrect addressing.

Ack

These are acknowledgments sent to the remote site to indicate that a message (that was tagged for acknowledgment) was read by the Meridian Mail user at the local site.

Failed to send

This indicates messages for which each delivery attempt failed and the messages could not be delivered to the remote site within the stale time threshold (refer to the *Meridian Networking Installation and Administration Guide* [NTP 555-7001-244] for information about stale-dating). Failed to Send messages are returned to the user with a Non-Delivery Notification (NDN). The user then may forward the message to the remote user again.

Network Usage

This statistic indicates the number of networking calls placed by the local site to the specified remote site during the specified interval. It is further broken down into the following categories.

Att

This indicates the number of attempted calls. For outgoing sessions, this field is incremented each time a channel is acquired to make a call to this remote site (for Meridian Networking, a modem is also successfully allocated). For incoming sessions, it is incremented when the call is answered, and the network passwords and site IDs are confirmed.

Note: Virtual Node AMIS does not use network passwords.

Suc

This indicates the number of successful calls. For Meridian Networking outgoing connections, it is incremented when the call is placed to this remote site and the network passwords and site IDs are confirmed. For incoming sessions, it is incremented provided the maximum number of ports is not exceeded. For Virtual Node AMIS or Enterprise sessions, it is incremented

once for each session in which at least one message is successfully sent or received.

Time (min)
This indicates the total amount of time (in minutes) used by networking calls to and from the specified remote site.

Failures

A failure refers to a single unsuccessful attempt to send a networking message. Networking will attempt to send these messages the next time it is scheduled to send messages to the remote site. If a message experiences many failures and is not delivered within a certain period of time, it will be reported in the Failed to Send field and the message is returned to the sender.

No Res
The No Resources failure means that one of the following occurred:

- no channels available
- maximum number of outgoing connections is reached
- if Meridian Networking, there were no modems available

Not Reach
This field is incremented each time a network connection is dropped or a problem is encountered while sending or receiving message information.

Prot Error
This field is incremented if a protocol violation is detected.

Analyzing the Networking Detail report

Introduction

This report provides a detailed breakdown of the networking usage on the system. While viewing the reports, consider the following information.

Note: For a proper analysis of this report, have a diagram of the network in front of you to refer to.

High number of "Failed to Send" messages

If the number of "Failed to Send" messages is high, there may be a problem with your networking setup.

Suggested action

Check to make sure that the remote site is not down. If the remote site is up and running, check the networking schedule parameters to see if they are correct. For details on changing networking parameters, refer to one of the following documents:

- *Meridian Networking Installation and Administration Guide* (NTP 555-7001-244)
- *Virtual Node AMIS Networking Installation and Administration Guide* (NTP 555-7001-245)
- *Enterprise Networking Installation and Administration Guide* (NTP 555-7001-246)

The number of NDNs delivered is high

If the number of NDNs delivered is high, this indicates that messages couldn't be delivered to local users. This may be due to one of the following:

The local users do not exist, the address in the message is incorrect, or the user cannot receive composed messages (Class of Service field):

- The local systems disk is full.
- The network setup is incorrect.
  - Site numbers and location IDs are defined differently from remote sites.
  - Mailbox number/dial plan is configured incorrectly.

Suggested action

Check that the disk is not full. If that is not the problem, confirm that the network setup is the same as the remote site's network database. If this is not the problem, confirm the existence of the remote site which the mailboxes cannot be delivered to and confirm that the site can receive composed messages.

The ratio of urgent networking messages to others sent is high

If the number of urgent networking messages sent is high compared to the number of standard messages, the system may not have enough channels or modems (Meridian Mail Networking only) to support the actual traffic.

Suggested action

If this is a problem, you may want to change the networking configuration. For details on changing networking parameters, refer to one of the following documents:

- *Meridian Networking Installation and Administration Guide* (NTP 555-7001-244)
- *Virtual Node AMIS Networking Installation and Administration Guide* (NTP 555-7001-245)
- *Enterprise Networking Installation and Administration Guide* (NTP 555-7001-246)

AMIS Networking Detail report

Introduction

This report is available only on systems with AMIS Networking capability. The AMIS Networking Detail report displays open AMIS traffic totals for AMIS Networking for your site. (Virtual Node AMIS traffic is displayed by site on the Networking Detail Report.) AMIS Virtual Node traffic is not included in this report. Statistics are shown for the number of AMIS messages received at your site and delivered to other voice messaging systems, the connect time, and the number of failures for each time interval displayed in the report.

The screen

The following is an example of the AMIS Networking Detail report screen.

```
                              Operational Measurements
AMIS Networking Detail

                                                          Connect    Failures
                     Messages  Messages Delivered          Time    No   Not  Prot
Interval Start-End  Received  Eco Std Urg NDN Failed      (mm:ss)  Res Reach Error
 5/0  10:00-11:00    12       0   5   2   0    0         4:00     0    1    1
 5/0  11:00-12:00     0       0   2   0   0    0         2:00     0    1    0
 5/0  12:00-13:00    24       0   5   1   0    0         8:00     0    0    1
 5/0  13:00-14:00     6       0   2   1   0    0         3:00     0    1    1

Select a softkey > _

     Exit          Next
                   Report
```

Fields in the AMIS Networking Detail report

Interval Start-End

Data are divided into intervals. The length of the interval depends on the entry made in the Traffic Commit Interval field in the Operational Measurement Options screen. The number of intervals displayed depends on the entries made in the Traffic Period Start and Traffic Period End fields in the Operational Measurement Options screen.

Example

If data are collected 24 hours a day (from 01:00 to 01:00), and the commit interval is one hour, the report will divide the data into 24 intervals for each day included in the report. The amount of data displayed in this report depends on the Report Start and Report End entries that were made in the Traffic Reports screen. If no report start and end dates and times were given, all data currently stored on disk are displayed.

Messages Received

This field indicates the number of AMIS messages that were received at the local site during the time interval indicated.

Messages Delivered

This field indicates the number of AMIS messages (originating from the local site) that were delivered to other voice messaging systems during the interval indicated. This statistic is further subdivided according to the type of message.

Eco

This indicates the number of messages, tagged as economy, that were delivered to other AMIS voice messaging systems during the specified interval.

Std

This indicates the number of messages, tagged as standard, that were delivered to other AMIS voice messaging systems during the specified interval.

Urg

This indicates the number of messages, tagged as urgent, that were delivered to other AMIS voice messaging systems during the specified interval.

NDN

These are nondelivery notification messages sent by the local system to users at other messaging systems whose messages could not be delivered to the intended recipient at the local site. Messages may not be delivered for the following reasons:

- The address is incorrect (for example, the mailbox does not exist).
- The user does not have the ability to receive AMIS messages (Class of Service field).
- The disk is full.
- A system error occurred.

Failed

This indicates the number of unsent messages. These messages experienced a series of failures and could not be sent before the stale period.

Connect Time (mm:ss)

This number indicates the total amount of time (in minutes and seconds) used by AMIS Networking calls during the time interval indicated.

Failures

This indicates the number of AMIS messages that were not successfully delivered to other AMIS messaging systems due to specific problems. This statistic is further subdivided into the types of problems that may prevent messages from being delivered.

No Res

The No Resources failure means that a voice port could not be accessed to send these messages to another AMIS site.

Not Reach

This field is incremented each time a network connection is dropped or a problem is encountered while sending or receiving message information.

Prot Error

The Protocol Error failure means that the connection was made to the remote AMIS site, but message delivery was prevented by a protocol error.

Analyzing the AMIS Networking Detail report

Introduction

This report provides a detailed breakdown of the AMIS Networking usage on the system. While viewing the reports, consider the following information.

The number of NDNs delivered or the number of "Failed to Send" messages is high

If the number of NDNs delivered or the number of "Failed to Send" messages is high, there may be a problem with your networking setup or the switch/telephone network. Since Open AMIS requires the user to enter the DN to dial at the destination messaging system, it may be that users are addressing messages incorrectly.

Also, if the failed to send is high, check the "Number Of Messages To Transmit Per Session" field. Try setting it to a higher number, for example, nine. (Also, make sure a billing DN is defined.)

Suggested action

Refer to the *AMIS Networking Installation and Administration Guide* (NTP 555-7001-242) for details on the proper setup of the networking feature.

The ratio of urgent networking messages to others sent is high

If the number of urgent networking messages sent is high compared to the number of standard messages, the system may not have enough channels to support the actual traffic.

Suggested action

If this is a problem, you may want to change the networking configuration in the Networking Call Maximum field. Refer to the *AMIS Networking Installation and Administration Guide* (NTP 555-7001-242) for details on changing networking parameters.

Outcalling Detail report

Introduction

This report is available only if Outcalling is installed on your system. The Outcalling Detail report details outcalling activity for the Remote Notification (RN) and Delivery to Non-Users (DNU) services.

The screen

The following is an example of the Outcalling Detail report screen.

```
                              Operational Measurements
Outcalling Detail (Remote Notification and Delivery to Non-User)

                     Number of     Number of Attempts   Number of   Wait Time
                   New Requests  New Request  Retries  Successes   Avg   Max
Interval Start-End   RN   DNU      RN   DNU   RN   DNU   RN   DNU  (sec) (sec)
5/01  13:00-14:00    3     1       3     1     2     0     0     1    15   54

Select a softkey > _

   Exit        Next
               Report
```

Fields in the Outcalling Detail report

Interval Start-End

Data are divided into intervals. The length of the interval depends on the entry made in the Traffic Commit Interval field in the Operational Measurement Options screen. The number of intervals displayed depends on the entries made in the Traffic Period Start and Traffic Period End fields in the Operational Measurement Options screen.

Example

If data are collected 24 hours a day (from 01:00 to 01:00), and the commit interval is one hour, the report will divide the data into 24 intervals for each day included in the report. The amount of data displayed in this report depends on the Report Start and Report End entries that were made in the Traffic Reports screen. If no report start and end dates and times were given, all data currently stored on disk are displayed.

Number of New Requests

This field indicates the total number of new requests that were made for outcalling services during the interval.

RN

This indicates the number of new requests for the Remote Notification service.

DNU

This indicates the number of new requests for the Delivery to Non-User service.

Number of Attempts

This indicates the total number of Remote Notification and Delivery to Non-User attempts made during the interval.

New Request

This number represents the number of attempts that have been made to answer the new requests for RN and DNU. If the Number of Attempts does not equal the Number of New Requests (see the previous field), the system is not keeping up with outcalling requests and more channels may need to be allocated to outcalling.

Retries

This number represents the number of times that the Remote Notification and Delivery to Non-Users services have retried calls because one of the following occurred at the destination number.

Event at Destination Number	Service Affected
the number was busy	RN and DNU
there was no answer	RN and DNU
the phone or pager service answered but no logon occurred	RN
the required DTMF confirmation was not given	DNU

Number of Successes

This indicates the number of successful remote notifications and messages successfully delivered to non-users that occurred during the interval.

RN

RN successes are measured in terms of user login. In other words, an RN call is considered successful if the user logs in to his or her mailbox when the notification is received (on the same call as the notification). If the user receives the notification, hangs up, and then logs in to his or her mailbox, this is not counted as a success since the user terminated the notification call without logging in.

Note: For remote notification to a pager, RN calls are never counted as successful in reports because the paging service cannot log in to the mailbox. A better measure of the effectiveness of RN calls to pagers is to compare the number of RN retries to RN attempts. However, bear in mind that an RN retry does not necessarily mean the RN attempt to the paging service failed; it only signifies that the user did not log on within the retry interval.

DNU

A DNU call is considered successful if the called party answers the call (and DTMF confirmation is given if required).

Wait Time

These values are an indication of how long it takes for the outcalling agent to acquire a channel to outcall to the specified directory number (DN).

Avg (sec)

This is the average amount of time, based on all outcalling attempts made during the interval, that it took the outcalling agent to acquire the resources necessary to make the outcall.

Max (sec)

This number represents the outcalling attempt that took the longest amount of time to acquire the resources necessary to make the outcall.

Analyzing the Outcalling Detail report

Low usage of Outcalling features

The sample report may indicate minimal use of the Outcalling features. The following reasons may help explain why.

Users do not know how to use the service
If so, train all outcalling users on how to use the service.

Users are unaware that the service exists
If so, inform the users of the service and provide training if necessary.

Users do not need to use the service
Consult the users to determine if they really do not need the service. Delete the service from the mailbox of those users who confirm that they do not need the outcalling service.

Technical problem with the service
Have the problem investigated and fixed.

The number of retries is high

If the number of retries is high, the reason may be one of the following:

- The destination number was busy.
- There was no answer at the destination.
- The user at the destination answered the call but did not log in.

Users are not retrieving messages

If users are consistently not retrieving messages, they may not be aware of how to properly use the outcalling service; or there could be a technical problem preventing users from retrieving the messages.

Suggested action
Consult the users to find out if the problem is with the system or with the users.

New attempts and new requests are unequal

The number of new attempts should roughly equal the number of new requests. If the number of new requests is somewhat greater than the number of new attempts, then the system is not keeping up with the demand for outcalling RN or DNU.

Suggested action

The system may need more channels. Increase the limit set by "Maximum Number of Outcalling Channels" on the Outcalling Administration screen to allow more channels to be used for outcalls.

The wait time is high

The wait time indicates how long the outcalling agent has to wait for a free channel. If the wait time is high, this also indicates a need for more channels. Increase the limit set by "Maximum Number of Outcalling Channels" on the Outcalling Administration screen to allow more channels to be used for outcalls.

The number of attempts and successes are not equal

The number of successes should equal the number of attempts. If the numbers are not equal, then the reason may be one of the following:

- There may be a problem with the destination phone/pager.
- Although Meridian Mail may not have any outcalling restrictions, the switch might. For example, long distance dialing may be restricted.
- The Outcalling feature may have been set up incorrectly by either the administrator or the user.
- If the channels were tied up for a long time, the retry time outs may have expired. If the wait times are high, then this is probably what happened.

Suggested action

You may need to dedicate channels to outcalling or increase the number of channels dedicated to outcalling.

Fax Delivery Detail report

Introduction

This report is available only if Fax on Demand is installed on your system. The Fax Delivery Detail report details activity for the fax services.

The screen

The following is an example of the Fax Delivery Detail report screen.

```
                          Operational Measurements
Fax Delivery Detail

                     Number of     Number of     Number of  Number of  Wait Time
Interval Start-End  New Requests  New Attempts  Retries    Successes   Avg   Max
5/01  13:00-14:00        5            5           2          5         60    90
5/01  14:00-15:00       12           12           5         11         66   112
5/01  15:00-16:00        7            7           3          7         62   100
5/01  16:00-17:00       10           10           5          9         65   105

Select a softkey > _

   Exit        Next
               Report
```

Fields in the Fax Delivery Detail report

Interval Start-End

Data are divided into intervals. The length of the interval depends on the entry made in the Traffic Commit Interval field in the Operational Measurement Options screen. The number of intervals displayed depends on the entries made in the Traffic Period Start and Traffic Period End fields in the Operational Measurement Options screen.

Example

If data are collected 24 hours a day (from 01:00 to 01:00), and the commit interval is one hour, the report will divide the data into 24 intervals for each day included in the report. The amount of data displayed in this report depends on the Report Start and Report End entries that were made in the Traffic Reports screen. If no report start and end dates and times were given, all data currently stored on disk are displayed.

Number of New Requests

This indicates the total number of new requests that were made for the fax callback services during the interval.

Number of New Attempts

This indicates the number of attempts made to process new requests for fax callback services during the interval.

Number of Retries

This indicates the number of attempts made to process old requests for fax callback services during the interval because one of the following occurred during the call:

- No carrier was received from the destination fax machine.
- Transmission errors occurred.

Number of Successes

This indicates the number of successful fax callbacks during the interval.

Wait Time

Avg

This indicates the average amount of time, based on all fax callback attempts made during the interval, that the fax outcalling agent needed to acquire the resources necessary to make the call.

Max

This number represents the fax callback attempt that took the longest amount of time during the interval to acquire the resources necessary to make the call.

Analyzing the Fax Delivery Detail report

There is minimal use of fax outcalling

There could be several reasons for minimal use of the Fax Outcalling features.

Users do not know how to use the service

If so, train all fax callback users on how to use the service.

Users are unaware that the service exists

If so, inform the users of the service and provide training if necessary.

Technical problem with the service

Have the problem investigated and fixed.

The number of retries is high

If the number of retries is high, the reason may be one of the following:

- The destination number was busy or the machine was out of paper.
- There was no answer at the destination.
- A transmit error prevented the fax from being received.

The number of new attempts should equal the number of new requests. If the number of new requests is greater than the number of new attempts, then the system is not keeping up with the demand for fax outcalling. The system may need more multimedia channels.

If the wait time is high, this also indicates a need for more channels. The wait time indicates how long the fax outcalling agent has to wait for a free channel.

The number of successes do not equal the number of attempts

The number of successes should equal the number of attempts. If the numbers are not equal, then the reason may be one of the following:

- There may be a problem with the destination fax device.
- Although Meridian Mail may not have any outcalling restrictions, the switch might. For example, long distance dialing may be restricted.

- The fax outcalling feature may have been set up incorrectly by either the administrator or the user.
- If the channels were tied up for a long time, the retry time-outs may have expired. If the wait times are high, then this is probably what happened. You may need to dedicate channels to fax outcalling or increase the number of channels dedicated to fax outcalling.

The wait time is high

If the wait times are too long for the desired service levels, increase the Maximum Number of Fax Delivery Channels on the Fax Administration screen and add multimedia ports to the system.

Disk Usage Detail report

Introduction

The Disk Usage Detail report provides information on disk space usage on the voice storage volumes.

The screen

The following is an example of the Disk Usage Detail report screen.

```
                          Operational Measurements
Disk Usage Detail

                     Volume   Voice Volume   Voice Space   Text Space
Interval Start-End   Name     Size (hh:mm)    Used (%)      Used (%)
5/01  10:00-11:00    VS1          1:51           33           47
                     VS2         33:15           33           17
                     VS202       25:45           10           30
5/01  11:00-12:00    VS1          1:51           33           47
                     VS2         33:15           33           17
                     VS202       25:45           10           30

Select a softkey > _

   Exit        Next
               Report
```

Fields in the Disk Usage Detail report

Interval Start-End

Data are divided into intervals. The length of the interval depends on the entry made in the Traffic Commit Interval field in the Operational Measurement Options screen. The number of intervals displayed depends on the entries made in the Traffic Period Start and Traffic Period End fields in the Operational Measurement Options screen.

Example

If data are collected 24 hours a day (from 01:00 to 01:00), and the commit interval is one hour, the report will divide the data into 24 intervals for each day included in the report. The amount of data displayed in this report depends on the Report Start and Report End entries that were made in the Traffic Reports screen. If no report start and end dates and times were given, all data currently stored on disk are displayed.

Volume Name

This shows the name of the user volume (for example, VS1, VS2, VS202, VS203, and so on). Volumes are sections on Meridian Mail disks. For more information, see "Distributing local voice users evenly over volumes" on page 7-19 of Chapter 7, "User administration—an overview."

Voice Volume Size (hh:mm)

This shows the amount of disk space that has been used, displayed in hours and minutes. One hour of voice storage is equivalent to 8.5 Mbytes.

Voice Space Used (%)

This indicates the percentage of the volume's voice capacity used at the end of the interval.

Text Space Used (%)

This indicates the percentage of the volume's text capacity used at the end of the interval.

Analyzing the Disk Usage Detail report

Voice space

The voice space used will fluctuate, especially if your system has an automatic read-message deletion feature enabled. However, if the Voice Space Used percentage is consistently over your disk usage warning level, then steps should be taken to reduce the amount of voice space used.

> **ATTENTION**
>
> If the system generates a SEER 1103, print this Disk Usage Detail report immediately. This SEER indicates that your system has reached physical or virtual capacity. Check that the nightly audit is functioning. Remove files on the volume in question. If the operation involved VS1, remove directory entries or OM files. The effect of corrective actions may be delayed until the nightly audit is run. Consider redistributing users on multiple nodes, turning on automatic message deletion, or buying a storage upgrade.

Reducing voice space

You can reduce the voice space used by deleting unnecessary mailboxes and ensuring that distribution lists are up to date. If these unnecessary or unused mailboxes are on distribution lists, they may be storing messages sent using outdated distribution lists. With no one logging on to delete the messages, the messages continue to accumulate and use up more disk space. You can also encourage users to delete their messages more frequently, or even reduce the allowable maximum message length (see Chapter 26, “Class of Service administration”).

Reviewing voice menus, forms, and announcements

To lower voice space used, you can also review all voice menus, voice forms, and voice announcements to see if their size can be reduced. For example, unused menu items can be removed. You can also consult the User Usage reports to identify users with excessive storage. This might happen if a user stops accessing his or her mailbox (for example, if the user is on vacation), but callers continue to leave messages.

Are the storage volumes evenly balanced?

If voice space used is high on some volumes but low on others, you may need to move high-usage subscribers to low-usage volumes in order to balance system resources. If the voice space used on all volumes is high, you may need to expand your system.

The text space has changed dramatically

Text space used should not fluctuate greatly from day to day, although it will vary over time. Any large fluctuations or significant steady increases in the text space used should be reported to your technical support organization.

Hospitality Statistics report

Introduction

This report is available only on Hospitality (HVS) systems. Hospitality Statistics include totals for guests checked in and out, as well as statistics on post-checkout mailboxes for each reporting interval.

The screen

This is an example of the Hospitality Statistics report screen.

```
                              Operational Measurements
Hospitality Statistics

                              ------------ Post-Checkout Mailboxes -------------
                      #Guests #Guests #Expired   #New   Total Unread   #Messages
                      Checked Checked  Unread   Unread   Msg Length   Unread Read
Interval Start-End      In      Out   Messages Messages (in minutes)
5/01   07:00-08:00      8       22       2        0         87         12     6
5/01   08:00-09:00     15       17       0        8        104         12     6
5/01   09:00-10:00     23        9       0        4         89         11     7
5/01   10:00-11:00     29        6       0        2         93         11     8
5/01   11:00-12:00     21        6       3        4         93         11     5
5/01   12:00-13:00     17        7       0        0         93          9     4

Select a softkey > _

   Exit        Next
               Report
```

Fields in the Hospitality Statistics report

Interval Start-End	This field indicates the start and end time of each reporting interval within the reporting period.
#Guests Checked In	This field indicates the total number of guests checked in during the interval.
#Guests Checked Out	This field indicates the total number of guests checked out during the interval.
#Expired Unread Messages	This field indicates the total number of unread messages that expired from post-checkout mailboxes which were holding unread messages.
#New Unread Messages	This field indicates the total number of new or unread messages in all post-checkout mailboxes that were created during the interval to hold unread messages.
Total Unread Msg Length (in minutes)	This field indicates the total length (in minutes) of unread messages in all post-checkout mailboxes.
#Messages (Unread, Read)	This field indicates the total number of unread and read messages in all post-checkout mailboxes.

Analyzing the Hospitality Statistics report

Introduction

When looking at the individual columns on the report, you should consider the following information.

#Guests Checked In / #Guests Checked Out

If the hotel's Property Management System (PMS) keeps statistics on how many people were checked in and how many were checked out during a particular time period, these numbers should match the numbers listed in the Hospitality Statistics report. If the numbers do not match, the manual check in and check out functions on the guest administration console (GAC) can be used to reconcile the differences.

If you do not have a PMS, you may wish to use other methods to confirm the checked-in/checked-out values.

#Expired Unread Messages

If the number of post-checkout mailboxes that expire with unread messages is more than three, then you may wish to instruct the checkout clerk and the bellman to remind guests during the checkout process to listen to their messages before checking out. You may want to think about other methods that will help or remind guests to retrieve their messages before they check out of or leave the hotel.

#New Unread Messages

If the number of new post-checkout mailboxes is more than five, you should look at how guests are notified of messages waiting. Consider better methods of informing your guests that they have messages waiting. Also think about how you can help or remind guests to retrieve their messages before they check out.

Total Unread Msg Length / #Messages Unread or Read

If you can find methods that will reduce the number of post-checkout mailboxes (see the previous points), then the unread messages length and the number of unread messages should not be a problem. You should try to keep the numbers in this column as low as possible, since unread messages are an unnecessary strain on your system.

Guest Console Statistics report

Introduction

This report is available only on Hospitality (HVS) systems. The Guest Console Statistics report contains totals for activities that were performed using the Guest Administration Console (GAC) menus for each reporting interval. Refer to the *Guest Administration Console Guide (NTP 555-7001-222)* for descriptions of GAC functions.

The screen

The following is an example of the Guest Console Statistics report screen.

```
                          Operational Measurements
Guest Console Statistics

                    View Updt View PCO Copy Check Check Re-Check  View   Updt
Interval Start-End Mbox Mbox  Mboxes  Mbox  In    Out     In    Status Status
5/01  07:00-08:00   40  20    130     0     0     0       0     70     1
5/01  08:00-09:00   43  19    120     0     0     0       1     65     0
5/01  09:00-10:00   90  47     98     0     0     0       0     53     0
5/01  10:00-11:00   56  31    101     1     0     1       0     58     0
5/01  11:00-12:00   43  19     87     0     0     0       0     78     0
5/01  12:00-13:00   29  11     75     1     0     0       0     58     1

Select a softkey > _

   Exit        Next
               Report
```

Fields in the Guest Console Statistics report

Interval Start-End This field indicates the start and end time of the reporting interval.

View Mbox This field indicates the number of times View/Modify a Mailbox was used to view a guest mailbox.

Updt Mbox This field indicates the number of times View/Modify a Mailbox was used to modify a guest mailbox.

View PCO Mboxes This field indicates the number of times View Post-Checkout Mailboxes was used.

Copy Mbox This field indicates the number of times Copy Mailbox was used.

Check In This field indicates the number of times Manual Mailbox Check In was used.

Check Out This field indicates the number of times Manual Mailbox Check Out was used.

Re-Check In This field indicates the number of times Manual Mailbox Re-Check In was used.

View Status This field indicates the number of times Hospitality System Status was viewed but was not used to change the system status.

Updt Status This field indicates the number of times Hospitality System Status was used to make changes to the system status.

Analyzing the Guest Console Statistics report

Introduction

When looking at the individual columns on the report, you should consider the following information.

The number of View Mbox is high

This should be a minimal number. If it is not, find out why it was necessary to use the view mailbox feature so often. If there was a lot of updating (see the Updt Mbox column), then this may be why the view mailbox feature was used so often.

The number of Updt Mbox is high

If the number of updates is high, investigate what was being updated and why.

For example, if guests' names were being updated, check that the spelling of guest names are always confirmed during the Reservation and Front Desk procedures.

If many of the updates were the result of a forgotten password and you are currently using the check-in date method of generating a password, consider using the last name method. Guests with check-in date passwords may be concerned that their mailboxes are not secure and want to change their password. Also, ensure that guest collateral (such as instruction cards) provide easy instructions on how to change their password.

There are numerous View PCO Mboxes

This number should be low. If it is not, make sure that guests are reminded during the checkout process to retrieve their messages prior to checkout. The guest collateral should also state clearly that guests should retrieve messages prior to checkout.

How to use the Copy Mbox field information

If you have a PMS system, the GAC could have been used to make a manual room change.

If you do not have a PMS, then the number in this field should match the front office room-change records. For every guest who changed rooms, there should have been a Copy Mailbox.

How to use the Check In field information

If you have a PMS system, the GAC could have been used to check in a guest.

If you do not have a PMS, then the number in this field should match the front office check in records. For every guest who checked in, a mailbox should have been activated (and counted in the Check In column).

How to use the Check Out field information

If you have a PMS system, the GAC could have been used to check out a guest.

If you do not have a PMS, then the number in this field should match the front office checkout records. For every guest who checked out, a mailbox should have been deactivated (and counted in the Check Out column).

The Re-Check In number is higher than zero

This number should be zero. If not, check with the front office records to try to determine why guests were checked out and then checked in again.

The Hospitality System is not being checked regularly

It should be part of the hotel staff's procedure to regularly check the Hospitality System status at least once every hour. If no system alarm is installed, you may want to check the system status more often.

The Hospitality System Status has not been updated

Any time the Hospitality System Status is updated (Updt Status), an investigation should be conducted.

Find out if it was a link problem or a human error. If the problem is technical, find the root cause and fix the problem. If the problem is human error, you may need to rewrite procedures or retrain the hotel staff.

Chapter 32

User Usage reports

In this chapter

Overview	32-2
The User Usage Reports screen	32-3
Fields in the User Usage Reports screen	32-4
Generating User Usage reports	32-7
User Usage report	32-9
Fields in the User Usage report	32-11
Analyzing User Usage reports	32-14

Overview

Introduction

The User Usage report provides statistics for local voice messaging usage on a per-user basis. If AMIS Networking or Meridian Networking is installed, then the report also displays users' daily networking activity. To generate User Usage reports, use the User Usage Reports screen.

Note: Check the Operational Measurement Options screen to make sure that the collection of user usage data is enabled. If it is disabled, enable it.

The User Usage Reports screen

Introduction

User Usage reports search criteria are specified in the User Usage Reports screen.

The screen

The following is an example of the User Usage Reports screen.

```
SEVEN CORP.                    Operational Measurements
  User Usage Reports

  Selection Criteria:                  All Lastname Mailbox Department

  Sorted:                              Alphabetical By_Department

  Include Local Usage:                 No Yes

  Include Meridian Network Usage:      No Yes

  Include AMIS Network Usage:          No Yes


  Report Start (mm/dd/yy): ________ (or blank for oldest)
  Report End   (mm/dd/yy): ________ (or blank for newest)

Select a softkey >

     Exit                View Reports   Print Reports
```

Fields in the User Usage Reports screen

Introduction

The following fields appear on the User Usage Reports screen. Select parameters and choose options required to create the type of report you need.

Selection Criteria

The following options are search parameters. Statistics matching your selection are displayed in the report.

All

When this option is selected, user usage data for all local users will be displayed in the report.

Lastname

When this option is selected, you are prompted for the last name of the subscriber whose data you want to view. If the last name is not found, use the Find Users feature in User Administration to verify that the name exists in the system. You may use wildcard characters (“+”, “?”, or “_”) to retrieve a group of users.

Mailbox

When this option is selected, you are prompted for the mailbox number of the user whose data you want to view. You may use wildcard characters (“+”, “?”, or “_”) to retrieve a range of mailboxes. If the mailbox number is not found, use the Find Users feature in User Administration to verify that the mailbox number exists in the system.

Department

When this option is selected, you are prompted for a department name. All users associated with that department will be displayed in the report. The entry you make must correspond to an existing entry in the system. Use wildcard characters (“+”, “?”, or “_”) to retrieve a group of departments.

Note: When searching by department, users with blank department fields will not be displayed.

Sorted

If your selection criterion is All Users, you can choose to sort the user data alphabetically, according to user names, or according to department names.

Note: When sorting by department, users with blank department fields will not be displayed.

Include Local Usage

This field is displayed if Meridian Networking and/or AMIS Networking are enabled. (If networking is not installed, the report displays only local usage.) Set the field to Yes to include user usage data for local voice messaging. This includes information about the number of Express Messaging and logon sessions the user had during the specified interval, the number of messages that were created during the Express Messaging and logon sessions and the total length of those messages, the amount of time that the user was connected to Meridian Mail, and the amount of disk space used by those messages. The default is Yes.

Include Meridian Network Usage

This field is displayed if Meridian Networking is enabled. When this field is set to Yes, the report will include user usage data for Meridian Networking activity. This information includes the number of economy, standard, and urgent messages that users created during the specified interval as well as the total length of the messages created (for each of the three types of messages). The default is No.

Include AMIS Network Usage

This field is displayed if AMIS Networking is enabled. When this field is set to Yes, the report will include user usage data for AMIS Networking activity. This information includes the number of economy, standard, and urgent messages that users created during the specified interval as well as the total length of the messages created (for each of the three types of messages). The default is No.

Report Start (mm/dd/yy)

This is the date on which the selected reports are to start. If Report Start predates the earliest available date, the report starts with the earliest available date. Leave this field blank to retrieve reports for the earliest available data. (The format mm/dd/yy hh:mm is the default. The format can be changed in General Administration, General Options. For more information, see Chapter 13, “General options”.

Report End (mm/dd/yy)

This is the date on which the selected reports are to end. If Report End exceeds the latest available period, the report ends with the last available period. Leave this field blank to report on the most recent data. (The format mm/dd/yy hh:mm is the default. The format can be changed in General Administration, General Options. For more information, see Chapter 13, “General options”.

Generating User Usage reports

Introduction

The following information describes the procedure to generate User Usage reports.

Procedure

To generate User Usage reports, follow these steps.

Starting Point: Main Menu

Step	Action
1	Select Operational Measurements. **Result:** The Operational Measurements screen is displayed.
2	Select User Usage Reports from the Operational Measurements menu. **Result:** The User Usage Reports screen is displayed.
3	Choose the selection criteria by which you want to retrieve data.
4	If the selection criterion is All, select how you want the data to be sorted: alphabetically (by user name) or by department name.
5	Select the type of data you want to view: local usage, Meridian Networking, or AMIS Network usage. You can select all three if required. **Note:** Meridian Networking and AMIS Networking usage are available only if Meridian Networking or AMIS Networking is installed.
6	If you wish to specify a start and stop time for the reporting period, enter the required values in the Report Start and Report End fields.
7	Choose one of the following options.

TO	GO to step
view User Usage reports	8.
print User Usage reports	9.
exit User Usage reports	10.

Step	Action
8	Press [View Reports]. **Result:** The selected report screens are displayed (see the following pages for descriptions of each report). Press [Next Page] to view subsequent pages of the report; press [Exit] to return to the User Usage Reports screen.
9	Press [Print Reports]. **Result:** You are prompted to make sure that your printer is ready and online. Press [Continue Printing] to print the reports, or press [Cancel Printing] at any time to cancel printing. There may be some delay before control is returned to the screen because it waits for the printer to stop printing.
10	Press [Exit]. The Operational Measurements menu is redisplayed.

User Usage report

Introduction

When you view the report on the terminal or from a printout, the data is arranged as shown in the diagram below. These examples show all types of user usage data (local, Meridian Networking, and AMIS Networking).

The screen

The following is an example of the User Usage report.

```
SEVEN CORP.                    User Usage Reports

Last Name          First Name        Department     MailBox              COS
Potts              Brian             Admissions     8050                  0

Local Usage:
           Number of     Connect      Number of      Message     Disk
           Sessions       Time        Messages       Length      Used
Date     EM/Ans Logon    (mm:ss)    EM/Ans Logon    (mm:ss)    (mm:ss)
6/10/96      3     8      5:03         3     4        0:16       0:00
         ------------------------------------------------
Total        3     8      5:03         3     4        0:16
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

Last Name          First Name        Department     MailBox              COS
Lang               Kathy             Records        7000                 15

Local Usage:
           Number of     Connect      Number of      Message     Disk
_____________________________________________________________________
Select a softkey > _

     Exit                                          Next
                                                   Page
```

The following is an example of a User Usage report when Meridian Networking and AMIS Networking is installed.

```
NORTEL CORP.                    User Usage Reports


Meridian Network Usage:
         Number of   Total     Number of   Total     Number of   Total
         Economy    Length     Standard   Length     Urgent     Length
Date     Messages   (mm:ss)    Messages   (mm:ss)    Messages   (mm:ss)
6/10/96    8         2:23        7        11:40       0         00:00
-----------------------------------------------------------------------
Total      8         2:23        7        11:40       0         00:00
AMIS Network Usage:
         Number of   Total     Number of   Total     Number of   Total
         Economy    Length     Standard   Length     Urgent     Length
Date     Messages   (mm:ss)    Messages   (mm:ss)    Messages   (mm:ss)
6/10/96    10        3:10        1         1:30       0         00:00
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
6/10/96    10        3:10        1         1:30       0         00:00
Last Name          First Name        Department     MailBox              COS
 Delray             Marina            Executive     7049                  0

Select a softkey > _

     Exit                                                Next
                                                         Page
```

Fields in the User Usage report

Introduction

These are the fields that are displayed in the User Usage report.

Header fields

Last Name
This is the user's last name.

First Name
This is the user's first name.

Department
This is the user's department name.

Mailbox
This is the user's mailbox number.

COS
This is the class of service number assigned to the user.

Local Usage fields

Date
This is the date of the reporting interval.

Number of Sessions
This is the number of Express Messaging, Call Answering, and logon sessions that occurred during the interval. To check the number of messages that were actually received or created during these sessions, check the Number of Messages field.

- ***EM/Ans*** refers to the total number of sessions created by Express Messaging or Call Answering calls to this mailbox. The number of abandoned calls (where no message is left) can be calculated by subtracting the number of EM/Ans messages from the number of EM/Ans sessions.
- ***Logon*** refers to the number of times the user logged into the mailbox for any reason.

Connect Time (mm:ss)

This is the length of time (in minutes and seconds) that the user was connected to the Voice Messaging service on the given date.

Number of Messages

This is the number of messages that the user received and created on the given date.

- ***EM/Ans*** refers to the number of messages left in the user's mailbox by both the Express Messaging and Call Answering services. The number of abandoned calls (where no message is left) can be calculated by subtracting the number of EM/Ans messages from the number of EM/Ans sessions.
- ***Logon*** refers to the number of messages that the user created on the report date.

Message Length (mm:ss)

This is the total time (in minutes and seconds) of all call answering messages received and messages created by the user or deposited in the user's mailbox on the given date.

Disk Used (mm:ss)

This is the amount of storage used by the user (measured in minutes and seconds) on the given date. This includes storage for greetings and personal verifications (spoken name recordings).

Meridian and AMIS Networking usage fields

Date

This is the date of the reporting interval.

Number of Economy Messages

This is the number of economy messages that the user created on the given date.

Total Length (mm:ss)

This is the total length (in minutes and seconds) of all networking messages created by the user on the given date and tagged as economy.

Number of Standard Messages

This is the number of standard messages that the user created on the given date.

Total Length (mm:ss)

This is the total length (in minutes and seconds) of all networking messages created by the user on the given date and tagged as standard.

Number of Urgent Messages

This is the number of urgent messages that the user created on the given date.

Total Length (mm:ss)

This is the total length (in minutes and seconds) of all networking messages created by the user on the given date and tagged as urgent.

Analyzing User Usage reports

The EM/Ans numbers are high and the logon count is low

The user may be accumulating too many messages before checking the mailbox and thereby contributing to a low disk space problem.

Suggested action

If disk space is already low (check the Disk Usage Detail report), you may need to make the user more aware of the importance of not accumulating messages.

Monitor the length of messages closely. If messages are too long for some users, you may wish to shorten their storage limit to encourage the users to empty their mailboxes more frequently. (For more information, see Chapter 7, "User administration—an overview".) You can also alter the maximum message length parameter (see Chapter 26, "Class of Service administration") to deter callers from leaving long messages.

You can assign a class of service (COS) with a shorter storage limit to encourage the users to empty their mailboxes more frequently (see Chapter 7, "User administration—an overview"). You can also alter the maximum message length parameter (see Chapter 26, "Class of Service administration") to deter callers from leaving long messages.

The number of logons is zero

Suggested action

Check the Time of Last Logon field in the View/Modify Local Voice User screen. If a considerable amount of time has passed since the last successful logon, you may want to contact the user to see if he or she is having any problems logging on. For example, the user may not know how to log on and retrieve messages (especially if this is a new user), or the user may have forgotten the mailbox password and has stopped trying to log on.

Chapter 33

Audit Trail reports

In this chapter

Overview	33-2
Section A: Collecting Audit Trail data	33-3
Section B: Outcalling Audit Trail reports	33-9
Section C: Fax Audit Trail reports	33-29

Overview

Introduction

This chapter describes the two types of Operational Measurement (OM) Audit Trail reports—Outcalling and Fax. These reports are useful for monitoring the use of these two features.

Section A: Collecting Audit Trail data, describes the procedure for enabling the collection of audit trail data.

Section B: Outcalling Audit Trail reports, provides descriptions and analyses for the Outcalling Audit Trail reports.

Section C: Fax Audit Trail reports, provides examples, descriptions, and analyses for the Fax Audit Trail reports.

Section A: Collecting Audit Trail data

In this section

Overview 33-4
Enabling the collection of audit trail data 33-5

Overview

Introduction

This section describes the Operational Measurements Options screen and the procedure for setting up the collection of audit trail data.

Enabling the collection of audit trail data

Introduction

You must explicitly enable the collection of audit trail data, and specify how long this data should be stored before being deleted.

Operational Measurement Options screen

The following is an example of the Operational Measurement Options screen.

```
                    Operational Measurements                    MORE ABOVE
Operational Measurement Options

Traffic Period End (hh:mm):                 01:00

Traffic Commit Interval (hh:mm):            01:00

Number of days of Traffic Data stored:      8

Collect User Usage/Session Trace Data:      Disabled Enabled

Number of days of User Usage Data stored:   31

Collect Audit Trail Data:                   Disabled Enabled

Number of days of Audit Data stored:        7

Shutdown Audit Trail at Volume Full (%):    85 %

   Save        Cancel
```

Fields used to enable audit trail data collection

These fields are used to enable audit trail data collection.

Collect Audit Trail Data	
Description	This field determines whether or not audit trail data is collected.
Options	Enabled and Disabled
Default	Enabled

Number of days of Audit Data stored	
Description	The field determines how long the collected audit trail data will be stored on disk before being overwritten.
Range	1 to 63 days
Default	7

Shutdown Audit Trail at Volume Full (%)	
Description	Use this field to identify the percentage at which you want the collection of audit trail data to stop.
Example	If set to 80%, audit trail data collection is disabled when the volume on which audit data is stored reaches 80% capacity. If set to 100%, collection of data will not stop until the volume is completely full. This is not recommended. ***Note:*** This is a percentage of text space, not voice space.
Default	85%

Procedure

To enable the collection of audit trail data, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Operational Measurements.
2	Select Operational Measurement Options. **Result:** The Operational Measurement Options screen is displayed. Three fields on the screen (Collect Audit Trail Data, Number of days of Audit Data stored, and Shutdown Audit Trail at Volume Full) are used to enable audit trail data collection.
3	Set the Collect Audit Trail Data field to Enabled if currently disabled (Enabled is the default.)
4	Specify the number of days that audit trail data should be stored on disk. **Note:** Detailed field descriptions are provided on the preceding pages.
5	In the Shutdown Audit Trail at Volume Full (%) field, enter the percentage full at which collection of audit trail data should stop. The default is 85%.
6	To save the current configuration, go to step 7. To exit without saving, go to step 8.
7	Press [Save]. **Result:** The outcalling data is saved and you are returned to the Operational Measurements menu.
8	Press [Cancel]. **Result:** Any changes you have made are not saved and you are returned to the Operational Measurements menu.

Section B: Outcalling Audit Trail reports

In this section

Overview	33-10
Generating an Outcalling Audit Trail report	33-11
The Summary Outcalling Audit Trail report	33-15
Fields in the Summary Outcalling Audit Trail report	33-16
Analyzing the Summary Outcalling Audit Trail report	33-18
The Detail Outcalling Audit Trail report	33-19
Fields in the Detail Outcalling Audit Trail report	33-20
Analyzing the Detail Outcalling Audit Trail report	33-28

Overview

Introduction

Outcalling audit trail statistics allow you to monitor how users are using the Remote Notification (RN) and Delivery to Non-User (DNU) features. There are two Outcalling Audit Trail reports that you can generate: a summary report and a detail report. Each report provides outcalling data for a certain period of time as specified by you.

Report types

The following two report types are available for Outcalling.

Outcalling Audit Trail Summary report

The summary report shows each outcall (RN or DNU) that was made during the reporting interval, along with the user who made the call, the user's mailbox number, the target number, and the status of the call. It shows only completed (answered) calls.

Outcalling Audit Trail Detail report

The detail report provides a more thorough account of each outcall request, including the start time and duration of the call, the DN of the channel that was used to place the call, and the number of retries (if any). It shows all outcalls, both successfully completed and unsuccessful.

Generating an Outcalling Audit Trail report

Introduction

The Outcalling Audit Trail Report screen is accessed from the Operational Measurements menu. This is a report selection screen in which you specify the type of report you want to retrieve (summary or detail) as well as the duration of the report period. You must specify whether you want to generate a report for a particular user, mailbox number, phone number, or all. You can either generate a report that includes all of the information currently stored on disk for that user (mailbox number or phone number) or generate a shorter report for a specific time period. The report can either be viewed on your terminal or printed.

The Outcalling Audit Trail Report screen

The following is an example of the Outcalling Audit Trail Report screen.

```
                         Operational Measurements
  Outcalling Audit Trail Report

  Report Type:          Summary Detail

  Selection Criteria:   All Name Mailbox Target_Phone_Number









 Report Start (mm/dd/yy hh:mm): _______________ (or blank for oldest)
 Report End   (mm/dd/yy hh:mm): _______________ (or blank for newest)

Select a softkey >

    Exit                          View Reports   Print Reports
```

Fields in the Outcalling Audit Trail Report screen

The following fields are used to specify the information required to generate an Outcalling Audit Trail report.

Report Type	
Description	Use this field to select the type of report to be generated.
Options	Your options are Summary and Detail. A summary report shows only completed calls. A detail report shows all actions, such as Submission, both successful and unsuccessful.
Default	Summary

Selection Criteria	
Description	All entries in the database can be viewed, or you can view data for a specific user, mailbox number, or phone number.
Options	All, Name, Mailbox, Target_Phone_Number
Default	All

Last Name	
Description	This field is displayed if Selection Criteria is set to Name. To view outcalling data for a particular user, enter that user's last name (and first name in the next field, as there may be more than one user with the same surname).
Limitations	This field does not accept the characters "+", "?", and "_" (underscore).

First Name	
Description	This field is displayed if Selection Criteria is set to Name. To view outcalling data for a particular user, enter that user's full first name (as well as the last name in the previous field).
Limitations	This field does not accept the characters "+", "?", and "_" (underscore).

Mailbox	
Description	This field is displayed if Selection Criteria is set to Mailbox. To view outcalling data for a specific mailbox, enter the full mailbox number.
Limitations	This field accepts numeric data only.
Target Phone Number	
Description	This field is displayed if Selection Criteria is set to Target Phone Number. To view outcalling data for a particular target phone number or pager number (the number entered in the Target DN field in the outcalling schedule), enter the full number in this field.
Limitations	This field accepts numeric data only.
Report Start/End	
Description	Enter the start date and time and end date and time to indicate the reporting period.

Note: If NMS is installed, you may enter a mailbox number for a voice user at another location, prefixed by the appropriate location code. However, if Meridian Networking is installed, you cannot use a remote user's mailbox number as a search criterion.

Procedure

To generate an Outcalling Audit Trail report, follow these steps.

Starting Point: The Main Menu

Step	Action
1	Select Operational Measurements.
2	Select Outcalling Audit Trail Report. **Result:** The Outcalling Audit Trail Report screen is displayed.
3	Specify the report type (Summary or Detail).
4	Specify the selection criteria (Name, Mailbox, Target Phone Number, or All).
5	Fill in the field that corresponds to the selection criteria you choose.

Step	Action
6	Enter the report start and end times. **Note:** If these fields are left blank, all outcalling data that is currently stored on disk will be retrieved.
7	Choose step 8 to view the reports on the terminal or step 9 to print the reports.
8	Press [View Reports]. **Result:** The first Outcalling Audit Trail report is displayed. When viewing the report, press [Next Page] to view the next page of the report. When the last page has been displayed, a prompt appears indicating it is the end of the report. **Note:** For a description of the fields in the summary report, see “Fields in the Summary Outcalling Audit Trail report” in this chapter. For a description of the fields in the detail report, see “Fields in the Detail Outcalling Audit Trail report” in this chapter.
9	Press [Print Reports]. **Result:** You are prompted to ensure the printer is ready and online. Press [Continue Printing] to print the report or [Cancel] if you do not want to print the report. If you selected [Continue Printing], a [Cancel] softkey is displayed that can be used to cancel printing once printing has started. There may be some delay before control is returned to the screen because it waits for the printer to stop printing.
10	Press [Exit]. You are returned to the Outcalling Audit Trail Report screen.

The Summary Outcalling Audit Trail report

Introduction

The Summary Outcalling Audit Trail report is displayed if you select Summary as the report type when you generate the report. This report provides summary information about the use of the Remote Notification (RN) and Delivery to Non-User (DNU) features.

The report

The following is an example of the Summary Outcalling Audit Trail report screen.

```
                          Operational Measurements
Outcalling Audit Trail from start of data to end of data.

Date (mm/dd/yy)
 Name            Mailbox Number
  Start  Duration Target Phone Number          Type  Call Status
 (hh:mm) (mmm:ss)

6/10/96
 Smith, J       7550
  12:40 1:10      91238765                     DNU  Answered
  12:45 0:05      91238765                     DNU  No DTMF Conf.
  13:45 0:18      8051-345643                  RN   Answered
  14:40 0:50      91236789                     DNU  Answered

Select a softkey >
End of Audit Trail report.
     Exit
```

Fields in the Summary Outcalling Audit Trail report

Introduction

The following informational fields are displayed when you generate a Summary Outcalling Audit Trail report.

Date

The date the call was made.

Name

The name of the Meridian Mail user who initiated the call.

Mailbox Number

The mailbox that originated the call.

Start (hh:mm)

The time at which the call was made.

Duration (mm:ss)

The length of the call in minutes and seconds.

Target Phone Number

This is the number called. A maximum of 30 digits can be displayed in this field. For calls placed to paging services (such as SkyPager), the pager identification number (PIN) is also displayed.

Example

In the number 8051-345643, the last six digits are the PIN number. If the full number is longer than 30 digits, the first few digits in the paging service phone number will be truncated.

Type

The Outcalling service that was used: either Remote Notification or Delivery to Non-User.

Call Status

The result of the call. The result status can be one of the following types.

Answered

This indicates that the destination number was answered and the message was heard by the called party.

RN Disabled

This indicates that the called party answered and pressed 3 to disable Remote Notification (RN).

Call Status (cont'd)

No DTMF Conf.

This display indicates that the called party did not press 2 to hear a DNU message (not relevant if DTMF confirmation is not required).

Not Played

This display indicates that the called party disconnected before the DNU message was played.

Analyzing the Summary Outcalling Audit Trail report

Introduction

This report provides a list of the type and result of all outcalling attempts during the specified period.

Invalid RN target

If a particular RN target is associated with RN failures, the RN target may be invalid. Check to see if only one mailbox is associated with the invalid RN target. If so, contact the user and suggest that the target RN be corrected, or correct the RN through the Meridian Mail interface. If multiple mailboxes are associated with the faulty RN target, determine why the RN target is no longer valid.

The Detail Outcalling Audit Trail report

Introduction

The Detail Outcalling Audit Trail report is displayed if you selected Detail as the report type. This report includes the information displayed in the summary report, as well as detailed information regarding the usage of the RN and DNU features.

The report

The following is an example of the Detail Outcalling Audit Trail report screen.

```
                          Operational Measurements
Outcalling Audit Trail from start of data to end of data.

Date (mm/dd/yy)
 Name            Mailbox Number
Transaction   Start  Duration  Device/Target Phone Number          Channel   Re-
(hh:mm)      (hh:mm) (mmm:ss)                                        DN      try
 Request#   Outcall Process    Call Status   Outcall Action

06/10/96
  Howes D.       8050
 00:05        00:05                                                          0
 #00003     RN  Submission                   Continue
 00:05        00:05     0:30   ToneP/7050                            2800    0
 #00003     RN  Call Results   Answered      Remove, User logged in.
 00:06        00:06                                                          0
 #00004     RN  Submission                   Continue
 00:09        00:09                                                          0
 #00005     RN  Submission                   Continue

Select a softkey > _

     Exit                                      Next
                                               Page
```

Fields in the Detail Outcalling Audit Trail report

Introduction

The following fields are displayed when the Detail Outcalling Audit Trail report is chosen.

Date

This is the date the call was made.

Name

This is the name of the Meridian Mail user who initiated the call.

Mailbox Number

This is the mailbox that originated the call.

Transaction (hh:mm)

This indicates the time at which the audit trail record was stored (using 24-hour clock).

Start (hh:mm)

This indicates the time at which the current outcall process started (using 24-hour clock).

Duration (mm:ss)

This indicates the length of the call.

Device/Target Phone Number

This indicates the type of device called followed by the phone/pager number. The device will be one of the following choices:

- Phone
- ToneP (tone pager)
- Voice (voice pager)
- NumPa (numeric pager)
- PaSrv (pager service)

Note: If the device is a paging service, the paging service phone number, followed by the pager identification number (PIN), will be displayed. The maximum length for this field is 30 digits. If this limit is exceeded, the first few digits of the paging service phone number will be truncated.

Channel DN

This indicates the DN associated with the voice channel used.

Retry

This shows the number of retries that have been made at the time of the attempt. This field increments by one whenever

- a DN is busy and is retried
- multiple target DNs are defined and they have all been tried and either not answered or answered with no login

Transaction Request #

This is a unique number identifying the RN or DNU request.

Outcall Process

This shows the type of audit trail entry. This could be one of the following.

Submission
This type indicates that a request has been made for an Outcalling service.

Recovery
This type indicates that messages for outcalling have been detected and submitted after a system reboot.

Cancellation
This type indicates that during recovery, requests for outcalling have been detected but have been cancelled since they are no longer valid.

Logout/Admin
This type indicates that one of two conditions has occurred. The first possibility is that a user has logged out with unannounced messages left in his or her mailbox. Normally, if a user is listening to a message when a new message comes in, the new message is announced after the user has finished listening to the other message. However, if the user hangs up before the message has finished playing, the new message will not be announced. (In this situation, the user will continue to be notified of messages.) The second possibility is that someone (an administrator or you) has modified a user's account while there were unread messages in the user's mailbox.

Validation
This type indicates a checking process just before a call was/is made.

Outcall Process (cont'd)

Call Results

This type indicates information regarding the Call Status and Outcall Action in the adjacent fields to the right.

Call Status

This is a general statement of the results of a call. The following list describes the possible call status results.

Busy

The RN or DNU target DN was busy. A retry attempt will be scheduled if the busy and no answer retries have not been exhausted.

Answered

An outcall to an RN or DNU target DN was placed. The RN call was answered but the user did not log in on the same call to listen to the message. Remote notification will be rescheduled if the answered retries have not been exhausted. The DNU call was answered and the message was successfully delivered.

No Answer

An outcall to an RN or DNU target was placed and the call was not answered. A retry attempt will be scheduled if the no answer retries have not been exhausted.

No DTMF Conf

An outcall to a DNU target DN was placed. The call was answered but the caller did not provide the required DTMF confirmation (in other words, he or she did not press 2 to hear the message). DNU will be rescheduled if the answered retries have not been exhausted.

Reorder

During an outcall, the target DN was dialed, and a reorder tone was detected. The primary reasons for a reorder tone are that an invalid DN was called, there were no resources to complete the call, or there were access restrictions that the DN violated. The call attempt will be treated as a busy attempt, and a retry attempt will be scheduled if the busy and no answer retries have not been exhausted.

Call Status (cont'd)

Resource Delay

The outcall was not completed because the line on which the call was to be made was taken away due to an incoming call that was given priority. The outgoing call is retried on a different channel. If this is a persistent problem, reserve channels for outcalling and make sure no ACD queues terminate on them.

Incomplete

The outcall could not be completed. The call attempt will be treated as a busy attempt, and a retry attempt will be scheduled if the busy and no answer retries have not been exhausted. If there is an accompanying SEER, follow the action described in the *Maintenance Messages (SEERs) Reference Manual* (NTP 555-7001-510).

RN Disabled

During an RN attempt, the target DN was dialed, the call was answered, and 3 was pressed to disable Remote Notification. There will be no further RN attempts for this user until the user logs in to his or her mailbox.

Not Played

During a DNU attempt, the target DN was dialed, and the call was answered and disconnected before DNU could play its message. If the answered retries have not been exhausted, DNU will retry using the answered retry limits and intervals.

Illegal Window

A user attempted to send a DNU message. The message became stale during an illegal time window and could not be delivered. (The stale date parameter defaults to 36 hours. If a message cannot be delivered within this time, a message becomes stale.) The user receives a nondelivery notification.

Call Status (cont'd)

Stale Date

A user attempted to send a DNU message. The message was not delivered immediately (either because it was sent during a restricted time period or the call was not answered and was, therefore, rescheduled). The message became stale during a permitted time period and could not be delivered. (The stale date parameter defaults to 36 hours. If a message cannot be delivered within this time, a message becomes stale.) The user receives a nondelivery notification.

SIT Tone

During an outcall, the target DN was dialed, and a SIT tone was detected. A SIT tone is usually a series of tones followed by a voice message, indicating that this DN is invalid. This causes remote notification for this user to be turned off by disabling all of his or her remote notification schedules. The administrator or user should define a new valid DN and reenable Remote Notification for the user. DNU is cancelled for the message and the user receives a nondelivery notification (NDN).

Bad Called DN

During an outcall, the target DN was dialed, and a bad called DN was detected by the local switch. (In other words, the target DN is invalid for some reason.) This causes Remote Notification for this user to be turned off by disabling all of his or her remote notification schedules. The administrator or user should define a new valid DN and reenable Remote Notification for the user. DNU is cancelled for the message and the user receives a nondelivery notification (NDN).

Outcall Action

This field indicates the action performed on the request. The possible results are described below.

Continue

The validation has been passed and a call attempt is to be made.

Remove, retry limit reached

After the call, the retry was not rescheduled because the retry limit had been reached.

Outcall Action (cont'd)

Remove, another RN exists
The validation step determined that the user has logged on since the last RN attempt and the retry was canceled.

Reset
A problem was encountered retrieving information. Requests will be discarded and recovered from disk.

Delayed 1
A channel could not be obtained on which to call out, and an attempt will be made later to obtain one.

Delayed 2
A channel was obtained but it was taken away before the call was made. An attempt will be made to retry later.

Defer
Another call attempt has been scheduled. RN calls to pagers are always rescheduled, unless the retry limit is reached, because the user may fail to receive the page. (However, if the user logs on before the next retry, the retry will be canceled.)

Outcall Action - Reason Codes for Delivery to Non-User

Reason codes indicate why an action occurred. Possible reason codes follow.

Delivery to Non-User

DNU Interpretation
All OK
Past delivery window
Past system limit (retry, stale date)
Problem reading the message
Stale date time
Problem sending NDN, try again in 5 minutes
Message deleted by utility or file lost
Past system limit (no NDN given)
Outcalling not set up for customer

Outcall Action - Reason Codes for Delivery to Non-User (cont'd)

Delivery to Non-User (cont'd)

DNU Interpretation
Had difficulty determining if the customer had Outcalling; will defer this request for Validation/Results stage and retry
Duplicate call made due to DNU recovery
Duplicate request discarded due to DNU recovery
Indicates invalid DN
No suitable channels
Channels out of service

Remote notification

RN Interpretation
All OK
Notification was cancelled by login
Message arrival is outside the time period
Failed to read personal profile
Outcalling not set up for customer or user
Past retry limit
RN not turned on
RN already active
RN no longer active (RN should still be active)
Message of wrong priority
Reinstated old request
Schedule missing
Failed to read the phone number
Failed to update the personal profile

Outcall Action - Reason Codes for Delivery to Non-User (cont'd)

Remote notification (cont'd)

RN Interpretation
No messages in the user's mailbox
Duplicate recovery entry for user
Notification was cancelled by another request
Non-MM8 profile; no component list
DN no longer valid
Invalid Client ID given
RN disabled by the called party
RN turned off due to multiple retry
Had difficulty determining if the customer had Outcalling; will defer this request for Validation/Results stage and retry
RN disabled by invalid DN
No suitable channels
Channels out of service

Analyzing the Detail Outcalling Audit Trail report

Introduction

This report provides a list of the type and result of all outcalling attempts during the specified interval.

Recurring channel failures on one channel

Recurring outcalling failures on the same channel may indicate problems with the channel hardware.

Suggested Actions

To determine the channel number from the Channel DN, go to Meridian Mail Administrative screen and view the Channel Allocation Table (CAT).

1. If the system is connected to a Meridian 1 system, look under the SCN field and find Channel DN, and then look up the channel number.
2. If the system is connected to a non-Meridian 1 switch, look under the Channel DN field for the Channel DN, and then look up the channel number.

Run the Channel Problem Identification report to see if the channel has unusual traffic patterns. You may need to check the DSP hardware and switch terminal number status as well.

Remote Notification not being received

If a user complains of not receiving Remote Notification, follow the suggested actions.

Suggested actions

Run the Audit Trail with the filter set for the user mailbox over the time interval in question. Then do the following:

- Check to see if RN requests were processed for that user; if none exists, check the Mailbox Session Analysis report to see if any messages arrived during the interval.
- If there was RN activity, check the RN targets used to see if they are valid.

Section C: Fax Audit Trail reports

In this section

Overview	33-30
The Fax Audit Trail Report screen	33-31
The Summary Fax Audit Trail report	33-35
Fields in the Summary Fax Audit Trail report screen	33-36
Analyzing the Summary Fax Audit Trail report	33-37
The Detail Fax Audit Trail report	33-38
Fields in the Detail Fax Audit Trail report screen	33-39
Analyzing the Detail Fax Audit Trail report	33-43

Overview

Introduction

Fax audit trail statistics allow you to monitor how users are using the Fax on Demand features. There are actually two Fax Audit Trail reports that you can generate: a summary report and a detail report. Each report provides fax data for a period specified by you.

Note: Before you can generate a Fax Audit Trail report, the Meridian Mail system must be set so that the collection of audit trail data is enabled (see "Enabling the collection of audit trail data" on page 33-5).

Report types

The following two types of Fax Audit Trail Data reports are available.

Summary report

The summary report shows each fax outcall that was made during the reporting interval, along with the called DN and the status of the call.

Detail report

The detail report provides a more thorough account of each outcall request, including the DN of the channel that was used to place the call and the number of retries (if any).

The Fax Audit Trail Report screen

Overview

The Fax Audit Trail Report screen is accessed from the Operational Measurements menu. This is a report selection screen in which you specify the type of report you want to retrieve (summary or detail) as well as the duration of the report period.

You must specify whether you want to generate a report for a particular billing DN, called DN, or all. You can either generate a report that includes all of the information currently stored on disk for that billing DN or called DN, or generate a shorter report for a specific time period. The report can either be viewed on your terminal or printed.

The screen

The following is an example of the Fax Audit Trail Report screen.

```
                         Operational Measurements
  Fax Audit Trail Report

  Report Type:          Summary Detail

  Selection Criteria:   All Billing_DN Called_DN









 Report Start (mm/dd/yy hh:mm): _______________ (or blank for oldest)
 Report End   (mm/dd/yy hh:mm): _______________ (or blank for newest)

Select a softkey >

    Exit                 View Reports   Print Reports
```

Fields in the Fax Audit Trail Report screen

The following table lists the fields displayed on the Fax Audit Trail Report screen.

Report Type	
Description	Use this field to select the type of report to be generated.
Options	Summary or Detail. For a description of each report type see “Report types” on page 33-30.
Default	Summary
Selection Criteria	
Description	Use this field to select the appropriate report criteria.
Options	Use this field to select the scope of the database search.

SELECT	TO view
All	all entries in the database.
Billing_DN	database entries matching the specified billing DN only.
Called_DN	database entries matching the specified called DN only.

Default	All
Report Start/End	
Description	Use this field to indicate the start and end time period for the report.
Default	Blank

Generating a Fax Audit Trail report

To generate a Fax Audit Trail report, follow these steps.

Starting Point: The Operational Measurements menu

Step	Action
1	Select Fax Audit Trail Report. **Result:** The Fax Audit Trail Report screen is displayed.
2	Specify the report type (Summary or Detail). See “Fields in the Fax Audit Trail Report screen” on page 33-32. for field descriptions.
3	Select the selection criteria (Billing_DN, Called_DN, or All).
4	Enter the report start and end times. **Result:** If these fields are left blank, all fax outcalling data that is currently stored on disk will be retrieved.
5	Press the [View Reports] softkey to view the reports, or the [Print Reports] softkey to print the reports. **Result:** The first Fax Audit Trail report is displayed or printed. **Note:** To cancel the request, press the [Cancel] softkey if you do not want to view or print the reports at this point.
6	Press the [Next Page] softkey to view the next page of the report. When the last page has been displayed, a prompt appears indicating it is the end of the report.
7	Press [Exit]. **Result:** You are returned to the Fax Audit Trail Report screen.

Printing a Fax Audit Trail report

To print a Fax Audit Trail report, follow these steps.

Starting Point: The Operational Measurements menu

Step	Action
1	Select Fax Audit Trail Report. **Result:** The Fax Audit Trail Report appears.
2	Change the selection criteria as desired.
3	Ensure that the printer is online and has paper.
4	Press [Print Reports]. **Result:** A new set of softkeys is displayed: [Cancel Printing] and [Continue Printing]. To cancel printing, press the [Cancel] softkey.
5	Press [Continue Printing] to print the report. **Result:** The report is printed and you are returned to the Operational Measurements menu. **Note:** If you selected [Continue Printing], a [Cancel] softkey is displayed that can be used to cancel printing once printing has started.

The Summary Fax Audit Trail report

Introduction

The Summary Fax Audit Trail report is displayed if the report type chosen is Summary.

The report

The following is an example of the Summary Fax Audit Trail report.

```
                          Operational Measurements
Fax Audit Trail from start of data to end of data.

Date (mm/dd/yy)
 Description            Billing DN
  Sta    Duration    Calle                          Call Status
 (hh:   (mmm:ss)

6/10/96
 FID 2222                3654
  16:42     1:24     7051                           Transmitted
  16:45     0:00     7051                           No Carrier
  16:55     1:19     7051                           Transmit Error

Select a softkey >
End of Audit Trail report.
     Exit
```

Fields in the Summary Fax Audit Trail report screen

Introduction

The Summary Fax Audit Trail report displays the following information.

Date

This indicates the date the call was made.

Description

This is a description of the application.

Billing DN

This indicates the billing DN that originated the call.

Start (hh:mm)

This indicates the time at which the call was made.

Duration (mm:ss)

This indicates the length of the call in minutes and seconds.

Called DN

This indicates the destination DN for the fax delivery.

Call Status

This field displays the result of the call. The allowed values are as follows.

Transmitted
This state indicates that fax transmission was completed without error.

Transmit Error
This state indicates that the fax transmission started but was not completed successfully.

No Carrier
This state indicates that the fax transmission was not started because the call was not answered, or was answered but not by a compatible fax device.

Analyzing the Summary Fax Audit Trail report

Description

This report lists each fax callback call attempt. Use this report to determine which fax delivery attempts are causing the high retry counts and failures that were detected by the Fax Activity report. To explore the cause of the problems in greater detail, run the Detail Fax Audit Trail report.

The Detail Fax Audit Trail report

Introduction

The Detail Fax Audit Trail report is displayed if the report type is Detail.

The report

The following is an example of the Detail Fax Audit Trail report.

```
                          Operational Measurements
Fax Audit Trail from start of data to end of data.

Date (mm/dd/yy)
 Description            Billing DN
Transaction   Start  Duration  Called DN                        Channel DN  Retry
(hh:mm)      (hh:mm) (mmm:ss)
 Request#   Outcall Process    Call Status   Outcall Action

6/10/96
                        3654
 16:42        16:42                                                        0
 #*****     Submission                        Continue
 16:42        16:42     1:24   7051                                  2800     0
 #00003     Call Results       Transmitted   Remove
 16:45        16:45                                                        0
 #*****     Submission                        Continue
 16:45        16:45     0:00   7051                                  2800     0
 #00004     Call Results       No Carrier    Defer
---------------------------------------------------------------------------
Select a softkey > _

     Exit                                    Next
                                             Page
```

Fields in the Detail Fax Audit Trail report screen

Introduction

In addition to the information displayed in the summary report, the detailed report contains the following information fields.

Transaction (hh:mm)

This is the time at which the delivery should have taken place.

Start (hh:mm)

This is the time at which the current outcall process started.

Duration (mm:ss)

This is the length of the call.

Called DN

This is the destination DN for the fax delivery.

Channel DN

This is the DN that was used to originate the call.

Retry

This is the number of retries that were made at the time of the attempt. This field increments by one each time a DN is retried.

Request #

This is the number of the transaction request.

Outcall Process

This is the type of audit trail entry. This could be one of the following.

Submission
This type indicates that a request has been made for an Outcalling service.

Instead of Submission you may also see Recovery.

Recovery
This type indicates that faxes for outcalling have been detected and submitted after a system reboot.

Validation
This type indicates a checking process just before a call was or is made.

Outcall Process (cont'd)

Call Results

This type indicates information regarding the Call Status and Outcall Action in the adjacent fields.

Call Status

This field indicates the status of the call attempt. The possibilities are as follows.

Transmitted

This state indicates that the fax transmission completed without error.

Transmission Error

This state indicates that the fax transmission was started but not successfully completed.

No Carrier

This state indicates that the fax transmission was not started because the call was not answered, or was answered, but not by a compatible fax device.

Illegal Window

This state indicates that the fax became stale during an illegal time window and could not be delivered. (The stale date parameter defaults to 36 hours. If a message cannot be delivered within this time, a message becomes stale.)

Stale Date

This state indicates that the fax was not delivered immediately (either because it was sent during a restricted time period, or the fax was not transmitted and was, therefore, rescheduled). The fax became stale during a permitted time period and could not be delivered. (The stale date parameter defaults to 36 hours. If a fax cannot be delivered within this time, the fax becomes stale.)

Bad Called DN

This state indicates that during an outcall, the target DN was dialed, and a bad called DN was detected by the local switch. (In other words, the target DN is invalid for some reason.) The callback fax is not delivered and is removed.

Call Status (cont'd)

Resource Delay
This state indicates that the outcall was not completed because the line on which the call was to be made was taken away due to an incoming call that was given priority. The outgoing call is retried on a different channel. If this is a persistent problem, reserve channels for fax callback deliveries and make sure no ACD queues terminate on them.

Incomplete
This state indicates that the outcall could not be completed. The call attempt will be treated as a busy attempt, and a retry attempt will be scheduled if the busy and no answer retries have not been exhausted. If there is an accompanying SEER, follow the action described in the *Maintenance Messages (SEERs) Reference Manual* (NTP 555-7001-510).

Outcall Action

This field indicates the action performed on the request. The possibilities are as follows.

Continue
This action indicates that the validation has been passed and a call attempt is to be made.

Remove, retry limit reached
This action indicates that after the call, the retry was not rescheduled because the retry limit had been reached.

Remove
This action indicates that the fax was successfully delivered.

Reset
This action indicates that a problem was encountered retrieving information. Requests will be discarded and recovered from disk.

Delayed 1
This action indicates that a channel on which to call out could not be obtained. Will retry later.

Outcall Action (cont'd)

Delayed 2

This action indicates that a channel was obtained, but it was taken away before the call was made. Will retry later.

Defer

This action indicates that another call attempt has been scheduled.

Outcall Action Reason Codes

Reason codes indicate why an action occurred. Possible reason codes follow.

Reason code
All OK
Past delivery window
Past system limit (retry, stale date, etc.)
Problem reading the message
Stale date time
Problem sending NDN, try again in 5 minutes
Message deleted by utility or file lost
Past system limit (no NDN given)
Fax on Demand not set up for customer
Had difficulty determining if the customer had Fax. Will defer this request for validation/results stage and retry.
Duplicate call made due to FP recovery
Duplicate request discarded due to FP recovery
Indicates invalid DN
No suitable channels
Channels out of service

Analyzing the Detail Fax Audit Trail report

Introduction

Use this information to analyze the Detail Fax Audit Trail report data.

Call Back Status

Check Call Back Status for the failing fax deliveries. For incomplete calls, check to see if a SEER has been produced, and refer to the *Maintenance Messages (SEERs) Reference Manual* (NTP 555-7001-510) for information on solving the problem. For call transmission failure due to resource delay, your system may need more multimedia channels. If faxes are becoming stale (faxes are not being sent before the maximum time for delivery attempts expires), check the time windows to make sure that the faxes are not being sent during illegal time periods.

Fax delivery fails on Bad Called DN

If the fax delivery attempt fails on Bad Called DN, dial the fax phone number to find out if the number is operational. The caller may have provided a wrong number.

Call Back Action field

Check the Call Back Action field for delays (Delay 1 and Delay 2). Delays indicate busy channels. If these problems with delays persist, your system may need more multimedia channels.

Recurring fax deliveries on the same channel

Recurring fax delivery failures on the same channel may indicate problems with the channel hardware. To determine the channel number from the Channel DN, go to the Meridian Mail Administrative screen and view the Channel Allocation Table (CAT):

- If the system is connected to a Meridian 1 system, look under the SCN field and find Channel DN, then look up the channel number.
- If the system is connected to a non-Meridian 1 switch, look under the Channel DN field for the Channel DN, then look up the channel number.

Run the Channel Problem Identification Report to see if the channel has unusual traffic patterns. You may need to check the DSP hardware and switch terminal number status as well.

Chapter 34

Bulk provisioning

In this chapter

Overview	34-2
Section A: Introduction to bulk provisioning	34-3
Section B: Working with bulk provisioning data sets	34-9
Section C: Transferring bulk provisioning data onto tape	34-27
Section D: Provisioning data into a Meridian Mail system	34-33

Overview

Introduction

This chapter contains information on the bulk provisioning feature of Meridian Mail 12. Bulk provisioning allows administrators or distributors to copy voice services such as menus, announcements, and fax items from one Meridian Mail system to another.

Section A: Introduction to bulk provisioning, provides a conceptual overview of bulk provisioning and its uses.

Section B: Working with bulk provisioning data sets, discusses bulk provisioning data sets, including the procedure to create them. As well, procedures for deleting, viewing, and printing data sets are included.

Section C: Transferring bulk provisioning data onto tape, describes the procedure for copying the bulk provisioning data sets onto tape.

Section D: Provisioning data into a Meridian Mail system, provides information about provisioning bulk provisioning data sets to the Meridian Mail system.

Section A: Introduction to bulk provisioning

In this section

Overview 34-4
What is bulk provisioning? 34-5
Using bulk provisioning 34-6

Overview

Introduction

This section includes information on the concept of bulk provisioning—what it is and how it can be used. Included are examples and operational considerations.

What is bulk provisioning?

Introduction

This topic describes and gives examples of bulk provisioning.

Description

Bulk provisioning is a feature that allows the administrator to collect voice service, VSDN, and local user information into data sets, copy them to tape, and have the information copied to other Meridian Mail systems.

Bulk provisioning enables selective distribution of one system's VSDNs and services on another system.

Example

The XYZ Company head office has decided to open a new location in the western region. The new site is obtaining its own Meridian Mail system. The company's president wants his customers in the western region to receive the same greetings and services provided at head office.

In order to provide the same services (for example, menus and announcements) to the new site as they have at head office, the administrator uses bulk provisioning to collect the required services onto tape. The administrator then sends the tape to the western region site. At the new site, the administrator provisions the new system with the information on the tape.

If both sites have Meridian Mail Networking installed, the administrator can use bulk provisioning to collect local user information, copy it onto a tape and send it to the western region site where it is added as remote users. This allows the remote users to have their names played in their own voices, during message compose and when name and dial addressed. This feature helps make the network appear transparent.

Using bulk provisioning

Introduction

This topic describes uses of the bulk provisioning feature.

System setup

Bulk provisioning can be used to initialize a new Meridian Mail system. Selected or all services as well as VSDNs can be collected from the “master” Meridian Mail system into data sets, copied to tape, and provisioned to new Meridian Mail systems.

This allows the administrator to ensure that all services, including menus, announcements, fax items, time of day controllers, and all other services defined using Voice Services Administration (VSA) are distributed and installed on all Meridian Mail systems.

Once the system is set up, the administrator can also save periodic updates to tape and provision them at other Meridian Mail systems. In this way, a group of Meridian Mail systems can always be kept up-to-date with the same services and VSDNs.

Multi-customer administration

Bulk provisioning can be used to copy services (but not VSDNs or users) between customer groups on the same Meridian Mail system. This could save time and reduce errors when setting up common services.

Remote user administration

Bulk provisioning allows the administrator to add remote user information to systems with Meridian Mail networking all at once rather than one user at a time. The users’ spoken names in their own voices are included so that the administrator is no longer required to record them.

The users’ organization directory entries are copied to tape; the administrator uses this tape to provision the users on another Meridian Mail system in the network. If the networking feature is installed, local users may be copied to tape. NMS users are considered local users and may be included on the tape.

Initial setup of temporary remote voice users

Bulk provisioning of the local users information allows the administrator to provide initial setup of temporary remote users on a new system. A sender's name and mailbox information can be propagated across the network along with their messages via Enterprise Networking.

Note: Temporary remote users are subject to a nightly audit. This audit removes the less recently accessed remote users in order to lessen the load on the system. See Chapter 9, "Remote voice users. " Permanent remote users remain on the system until deleted by the administrator.

Addition of remote user attributes: a comparison

The following table compares the addition of remote user attributes by network propagation and bulk provisioning.

Remote User Attribute	Remote user information added by network propagation	Remote user information added by bulk provisioning
Last name, first name	first 18 characters	entire name
Mailbox	yes	yes
Primary DN	=mailbox (if the DN=mailbox convention is set up in the network database)	=mailbox (if the DN=mailbox convention is set up in the network database)
Spoken name	yes, updated with each message sent	yes
Dialable by external callers	yes, default set by administrator	yes, default set by administrator
Department	no	yes
Temporary user flag	temporary	temporary or permanent, as selected by administrator

Bundled applications

A service bureau can create "applications" which, if bundled, could be sold as value-added packages to your mail system. For instance, a recorded front-end menu could be provided on all your systems.

Section B: Working with bulk provisioning data sets

In this section

Overview	34-10
Assembling bulk provisioning data sets	34-11
Creating and modifying bulk provisioning data sets	34-14
Viewing and printing bulk provisioning data sets	34-21
Deleting bulk provisioning data sets	34-25

Overview

Introduction

This section includes information that you need to create and modify bulk provisioning data sets. Also included are instructions on viewing, printing, and deleting data sets.

Assembling bulk provisioning data sets

Introduction

This section provides information required to create new bulk provisioning data sets and modify data sets that currently exist.

Concept of bulk provisioning data sets

Bulk provisioning provides the administrator with the ability to group sets of provisioning data into a catalog. The administrator can select services, VSDNs, and local user information for provisioning to other systems. These selections are saved in a bulk provisioning data set and later copied to tape.

These data sets are the starting point for bulk provisioning. At this point, the tape is created from a data set and is sent to another site where the contents can be duplicated on the target Meridian Mail system.

The administrator can create up to 100 bulk provisioning data sets. The data sets can be stored for future use, and can be modified if required.

Using Wildcards in the Provisioning Data

Using wildcards can be useful when specifying multimedia services or VSDNs. By using wildcards, the administrator can collect much more information than the number of input fields would allow. Also, wildcards provide a means to help organize the items in the data set.

The wildcards available for use are the organization directory wildcards:

- "+" to represent any number of characters
- "_" to represent exactly one character

Example

The administrator in an automotive company can group one set of multimedia services (faxes, menus, announcements) referring to new products with service IDs beginning with the characters 11 (for example, 110001, 110002, 110003, 110004 and so on). By using a wildcard character, these services can be referred to as 11+. Another set of services relating to parts and support could be referred to as 12+. This allows the

administrator to choose specific groupings of services for various sites.

Important considerations

The administrator must be aware of the following important considerations before beginning to collect data for the provisioning data sets.

Support requirements

The administrator must ensure that the target system is correctly set up with support needed for the services and VSDNs that are being bulk provisioned. Included in these considerations are features, hours, networking sites, DNs or TNs, switch connectivity, and system restriction/permission lists.

Dependencies

The administrator must ensure that multimedia services provisioned to a target system do not have references to services that do not exist on the system. For instance, menus or time-of-day controllers typically refer to other services that should be included in the data set as well. VSDNs may also require certain services in order to function properly. Bulk provisioning does not automatically resolve these dependencies. This is the administrator's responsibility.

Hardware-specific information

Hardware-specific information is not propagated to the target system. This information includes

- port names
- link information
- network database information relating to local and remote sites
- the hardware database

Restriction/permission indexes

Restriction and permission indexes associated with specific services on the source system are brought over to the target system. The administrator must take care to ensure that the indexes make sense when preconfiguring systems across area codes on the destination system.

Dialing plan comparison

The system does not do a comparison check of the DNs of the source system against the dialing plan of the target system. This affects

- VSDNs (such as menus, announcements, and time-of-day controllers)
- billing DNs
- revert DNs
- fax confirmation DNs
- attendant DNs

Remapping capability

No capability is provided for remapping of DNs or various service IDs. The target system will have exactly the same DNs and service IDs as the source system.

The administrator should make sure that all revert DNs and service IDs make sense on the target system before beginning the bulk provisioning. If required, the administrator of the target system can use the MMI to correct DNs and service IDs of provisioned services.

System and customer profiles

Information kept in the system or customer profiles is not transferred during bulk provisioning.

Creating and modifying bulk provisioning data sets

Introduction

This section provides information required to create and modify data sets for bulk provisioning.

The Add Data Set screen

The following is an example of the Add Data Set screen.

```
                          Bulk Provisioning
Add Data Set

Data Set Name:   Service01

Local Users:     None All Individual Volume COS Dept
                 Enter individual user mailboxes. Wildcards + and _ permitted.
                 756+

Services:        None All Individual

VSDNs:           None All Individual

Select a softkey >

   Save      Cancel    View Detail   Print Detail
```

The View/Modify Data Set screen

The following is an example of the View/Modify Data Set screen. As you can see, only its title differs from the Add Data Set screen.

```
                          Bulk Provisioning
View/Modify Data Set

Data Set Name:    Service01_____________________

Local Users:      None All Individual Volume COS Dept
                  Enter individual user mailboxes. Wildcards + and _ permitted.
                  756+_____________   _________________
                  _________________   _________________
                  _________________   _________________
                  _________________   _________________
                  _________________   _________________

Services:         None All Individual

VSDNs:            None All Individual

Select a softkey >

   Save      Cancel     View Detail   Print Detail
```

Field descriptions

The following table describes the fields in the Add Data Set and the View/Modify Data Set screens.

Data Set Name	
Description	A descriptive name for the data set. This name is entered by the administrator.
Limitations	Maximum of 30 characters
Default	For the Add Data Set screen, the default is blank. (The data set name must be entered or the data set cannot be saved.) For the View/Modify Data Set screen, the data set name is displayed.

Local Users	
Description	The Local Users field displays only on systems that have Meridian Mail Networking installed. Use this field to add users to the data set. **Note:** Only local users belonging to the networking customer group may be copied to tape.
Description	The Local Users field displays only on systems that have Meridian Mail Networking installed. Use this field to add users to the data set.
Options	None, All, Individual, Volume, COS, Dept.
Limitations	Individual: ten users (use of the wildcards “+” and “_” is allowed to expand the number of local users added). Volume: to maximum number of volumes on the system. COS: 15 classes of service. Dept.: five departments (use of the wildcards “+” and “_” is allowed to expand the number of departments added).
Default	None

Services	
Description	These are the multimedia services.
Options	None, All, Individual.
Limitations	30 services (use of the wildcards “+” and “_” is allowed to expand the number of services added).
Default	None

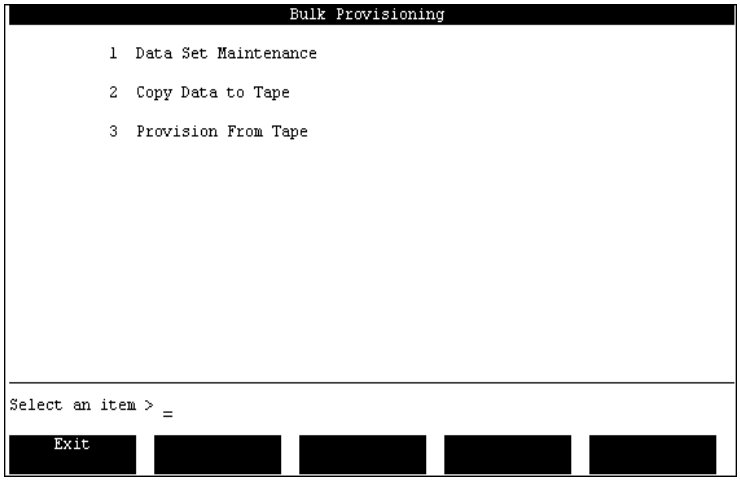
VSDNs	
Description	These are the voice service DNs included in the data set.
Options	None, All, Individual.
Limitations	20 VSDNs (use of the wildcards “+” and “_” is allowed to expand the number of VSDNs added).
Default	None

Creating bulk provisioning data sets

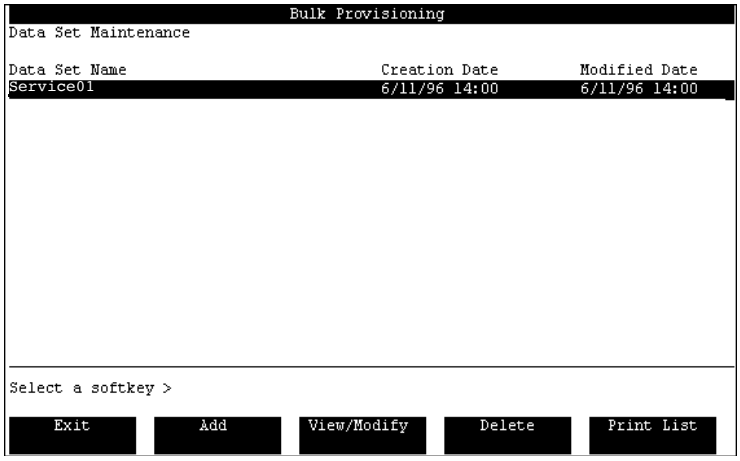
To create bulk provisioning data sets, follow these steps.

Starting Point: The Main Menu screen

Step	Action
1	Select Bulk Provisioning from the Main Menu screen. **Result:** The Bulk Provisioning Menu is displayed.



2	Select Data Set Maintenance. **Result:** The Data Set Maintenance Menu is displayed.



3	Press the [Add] softkey while in the Data Set Maintenance screen. **Result:** The Add Data Set screen displays.

Step	Action
4	Enter a descriptive data set name in the Data Set Name field. This field allows a maximum of 30 characters.
5	Use this table to determine your next action.

IF networking	THEN go to
is installed on your system and you want to add users	step 6.
is not installed on your system	step 8.

6 Choose one of the following options.

IF you want to add	THEN select
no users	None
all users	All
individual users	Individual
users by volume they reside on	Volume
users by COS (Class of Service)	COS
users by department	Dept.

Result: For options Individual, Volume, COS, and Dept., the display is expanded to provide a number of input fields.

7 Complete the input fields as required. See “Field descriptions” on page 34-15 for information on the Local Users fields.

8 To add services and/or VSDNs to the bulk provisioning data set, move the cursor to the Services or VSDNs fields.

IF you want to add	THEN select
no services or VSDNs	None in the appropriate field
all services or VSDNs users	All
individual services or VSDNs	Individual

Result: For the Individual option, the display is expanded to provide a number of input fields.

9 Complete the input fields for Services and/or VSDNs as required. See “Field descriptions” on page 34-15 for information on the Local Users fields.

Step	Action
10	Save the data set by pressing the [Save] softkey. (Before saving the data set, you can view the details by pressing the [View Detail] softkey to make sure that you have chosen the information you require. See “Viewing details of bulk provisioning data sets” on page 34-22.) **Result:** The data set is saved. You are returned to the Data Set Maintenance screen.

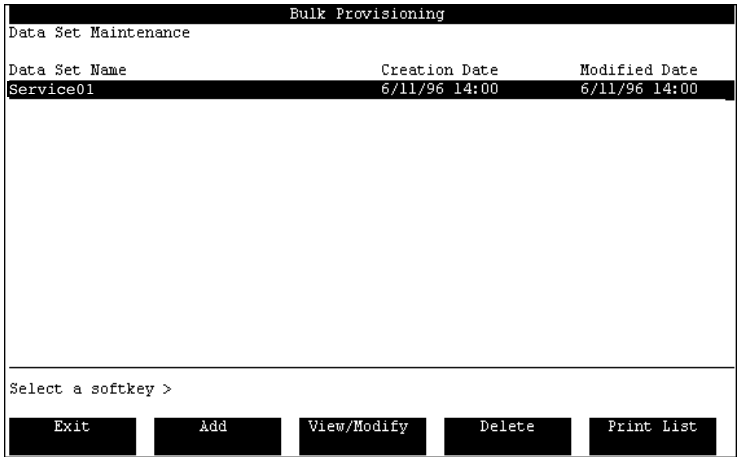
Modifying bulk provisioning data sets

To modify bulk provisioning data sets, follow these steps.

Note: Use the up and down arrows (↑↓) to move between fields and the left and right arrows (← →) to move between options within a field.

Starting Point: The Main Menu

Step	Action
1	Select Bulk Provisioning from the Main Menu screen.
2	Select Data Set Maintenance. **Result:** The Data Set Maintenance Menu is displayed.



3	Move the highlight bar to the data set that you want to modify. **Result:** The data set name is highlighted.
4	Press the [View/Modify] softkey. **Result:** The View/Modify Data Set screen is displayed.

Step	Action
5	Change the input fields as required. See “Field descriptions” on page 34-15 for information on each of the fields.
6	Save the data set by pressing the [Save] softkey. (Before saving the data set, you can view the details by pressing the [View Detail] softkey to make sure that you have chosen the information you require. See “Viewing details of bulk provisioning data sets” on page 34-22.) **Result:** The data set is saved. You are returned to the Data Set Maintenance screen.

Viewing and printing bulk provisioning data sets

Introduction

This section contains the information required to view and print the contents of bulk provisioning data sets.

View/Modify Data Set screen

The following is an example of the View/Modify Data Set screen.

```
                              Bulk Provisioning
View/Modify Data Set

Data Set Name:    Service01_____________________

Local Users:      None All Individual Volume COS Dept
                  Enter individual user mailboxes. Wildcards + and _ permitted.
                  756+_______________    ___________________
                  ___________________    ___________________
                  ___________________    ___________________
                  ___________________    ___________________
                  ___________________    ___________________

Services:         None All Individual

VSDNs:            None All Individual

Select a softkey >

 Save      Cancel     View Detail   Print Detail
```

Field descriptions

The fields in the View/Modify Data Set screen are the same as those in the Add Data Set screen. See page 34-15 for detailed field descriptions.

Viewing details of bulk provisioning data sets

To view details of bulk provisioning data sets, use the following steps. This procedure can be used when modifying existing data sets as well as when adding new data sets.

Starting Point: The Add Data Set or the View/Modify Data Set screen

Step	Action
1	Press the [View Detail] softkey. **Result:** The View Data Set Detail screen is displayed.

```
                                Bulk Provisioning
View Data Set Detail

Data Set Name: Service01

Data     Serv
Class    Type  ID/VSDN/Mbox                    Description
User           7560                            Ulrichte,Lars
User           7561                            Kong,Rex
User           7562                            Turing,Alan
User           7563                            McBain,Arnold
User           7564                            Saget,John
User           7565                            Lee,Roberta
User           7566                            Khan,Faisal
User           7567                            Howell,Wilbur
User           7568                            Gillis,Andrew
User           7569                            Rabbino,Jessica
Service  MS    101                             Main Menu for External Calls
Service  MS    102                             off hours menu

    Exit                                     Next
                                             Page
```

2	Press the [Next Page] softkey (if available) to view additional screens.
3	Press the [Exit] softkey to exit from the View Data Set Detail screen. **Result:** You are returned to the Add Data Set or View/Modify Data Set screen.

Printing bulk provisioning data

To print the detail of bulk provisioning data sets, use the following steps. This procedure can be used when modifying existing data sets as well as when adding new data sets.

Starting Point: The Add Data Set or the View/Modify Data Set screen

Step	Action
1	Press the [Print Detail] softkey. **Result:** The prompt “Please ensure that the printer is ready” is displayed.

```
                          Bulk Provisioning
View/Modify Data Set

Data Set Name:    Service01

Local Users:      None All Individual Volume COS Dept
                  Enter individual user mailboxes. Wildcards + and _ permitted.
                  756+

Services:         None All Individual

VSDNs:            None All Individual

Please ensure that the printer is ready._

                  Cancel Printing          Continue Printing
```

2 Use this table to determine your next action.

IF the printer is	THEN
ready	press the [Continue Printing] softkey to print the contents of the data set.
not ready	ready the printer and return to step 1.

To cancel the printing, press the [Cancel Printing] softkey at any time.

Result: When printing is complete, you are returned to the Add Data Set screen or the View/Modify Data Set.

Printing a list of bulk provisioning data sets

To print a list of bulk provisioning data sets, use the following steps.

Starting Point: The Bulk Provisioning menu

Step	Action
1	Select Data Set Maintenance. **Result:** The Data Set Maintenance screen displays.
2	Press the [Print List] softkey. **Result:** The prompt “Please ensure that the printer is ready” is displayed.
3	Use this table to determine your next action.

IF the printer is	THEN
ready	press the [Continue Printing] softkey to print the list of data sets.
not ready	ready the printer and return to step 2.

Result: The list of data sets is printed.

To cancel the printing, press the [Cancel Printing] softkey at any time.

Deleting bulk provisioning data sets

Introduction

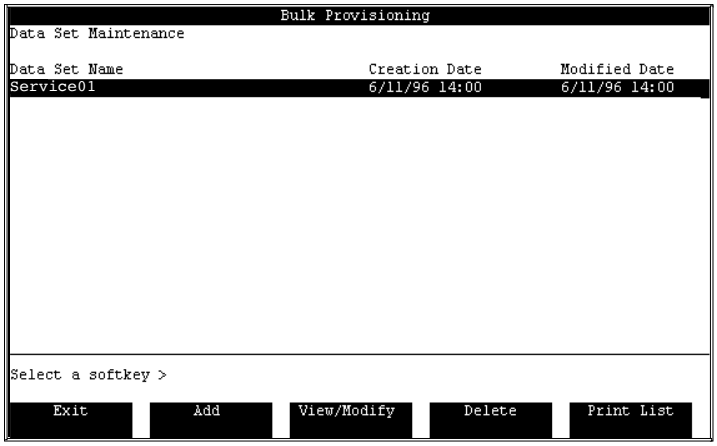
This topic provides information on deleting bulk provisioning data sets.

Procedure

To delete bulk provisioning data sets, use the following steps.

Starting Point: The Bulk Provisioning menu

Step	Action
1	Select Data Set Maintenance. **Result:** The Data Set Maintenance screen displays.



Step	Action
2	Use the up and down arrows (↑↓) to move the cursor to the data set you want to delete, then press the [Delete] softkey. **Result:** The Delete Data Set screen is displayed with a read-only version of the selected data set shown.

```
                                Bulk Provisioning
Delete Data Set

Data Set Name:   Service01_

Local Users:     None All Individual Volume COS Dept
                 Enter individual user mailboxes. Wildcards + and _ permitted.
                 756+



Services:        None All Individual

VSDNs:           None All Individual


Select a softkey >

 OK to Delete      Cancel
```

3	Press the [OK to Delete] softkey to delete the data set. (To abort this procedure, press the [Cancel softkey].) **Result:** The data set is deleted.

Section C: Transferring bulk provisioning data onto tape

In this section

Overview 34-28
Copying provisioning data sets onto tape 34-29

Overview

Introduction

This section provides the procedure for copying bulk provisioning data sets onto tape. Also included is a diagram of the Copy Data to Tape screen and a description of the fields in the screen.

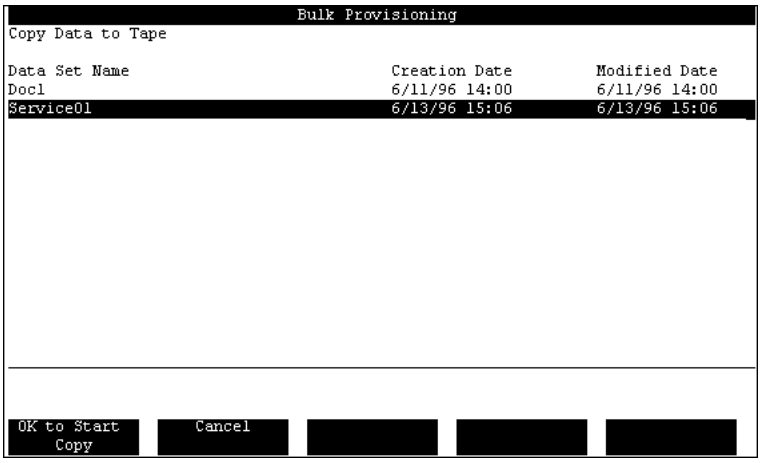
Copying provisioning data sets onto tape

Introduction

This topic explains how to copy provisioning data sets onto tape. Before you begin the procedure, make sure that you have a tape available and that you are able to load the tape when necessary. You must be logged in as system administrator to perform this procedure.

The Copy Data to Tape screen

This is an example of the initial Copy Data to Tape screen.



This is an example of the Copy Data to Tape screen while the copy is in progress.

```
                          Bulk Provisioning
Copy Data to Tape

Data Set Name                          Creation Date        Modified Date
Service01                              6/13/96 15:06        6/13/96 15:06

Status:   Copy in progress, 75% done

                                  Abort
```

Field descriptions

The following fields are contained in the Copy Data to Tape screen.

Data Set Name	
Description	The descriptive name of the data set created by the administrator.
Format	Data set names can be a maximum of 30 characters in length.

Creation Date	
Description	The original creation date and time (24 hour clock) of the data set.
Format	date hh:mm (where date is the system date format as selected under General Administration/General options)

Modified Date	
Description	The date and time (24 hour clock) that the data set was last modified.
Format	date hh:mm (where date is the system date format as selected under General Administration/General options)

Status	
Description	This field shows the status of the copy to tape. This field is viewable only after the tape has been retensioned and the copy to tape begins.
Format	Copy in progress, nn% done or Copy completed successfully **Note:** The percentage done is based on the number of items to be copied.

Before you begin

Ensure that the tape can be read by the destination system. Older systems have Archive tape drives which can only read DC150 and DC250 tapes.

Procedure

To copy provisioning data onto tape, use the following steps.

Starting Point: The Main Menu

Step	**Action**
1	Select Bulk Provisioning from the Main Menu and press <Return>. **Result:** The Bulk Provisioning Menu is displayed.
2	Select Copy Data to Tape and press <Return>. **Result:** The Copy Data to Tape screen is displayed.
3	Using the up and down arrow keys (↑↓), move the highlight bar to the data set you want to copy to tape. **Result:** The data set is highlighted. **Note:** Since one data set can be selected, only one data set can be copied at a time.

Step	Action
4	Load a tape into the tape drive. Make sure that the tape is not write protected.
5	Press the [OK to Start Copy] softkey to begin the copy to tape.

IF the tape is	THEN
in the tape drive in ready status	the copy to tape process begins.
not ready or write protected	the message “Tape drive not ready” or “tape write protected” is displayed. Return to step 4.

Result: The message “The tape is retensioning” is displayed. Retensioning takes approximately four minutes. After the tape has retensioned, the data are copied to the tape. The Status field displays the status of the copy to tape during the process. Press the [Abort] softkey to cancel the copy to tape at any time.

When the copy to tape is complete, the message “Copy completed successfully” displays.

6	Use the [Exit] softkey to return to the Bulk Provisioning menu.

Tip

It is good practice to include a printout of the data set details (from Data Set Maintenance) along with the tape.

Section D: Provisioning data into a Meridian Mail system

In this section

Overview	34-34
Before you start	34-35
Provisioning data	34-37
Viewing and printing data conflicts	34-43

Overview

Introduction

This section provides information on provisioning data sets that were copied from one Meridian Mail system onto the current Meridian Mail system.

Before you start

Introduction

This section provides important information the administrator requires before beginning the provisioning of the bulk provisioning data on the target Meridian Mail system.

How the system responds to users during restore

When provisioning of a system is in progress or completes, services that are *in use* continue to use the previous version of the service as well as the previous set of prompts even after provisioning completes. The new services and prompts are available to users if they are first accessed after the provisioning completes.

Potential conflicts between databases

Two types of conflicts, system level or data, may arise when bulk provisioning data from one Meridian Mail system to another.

CAUTION

Risk of data loss

Check for system level and data conflicts before proceeding with the bulk provisioning. Failure to do so may result in a loss of data.

System level conflicts

System level conflicts will cause provisioning to fail. To overcome a system level conflict, the administrator may have to restrict the choice of data to be provisioned.

System conflicts that cause provisioning to fail include the following:

- a feature is not installed
- an insufficient number of languages are available
- networking sites are not defined

Data conflicts

Data conflicts do not cause provisioning to fail but they can cause data to be overwritten. If a particular VSDN or service is

defined on the bulk provisioning tape and is also defined on the target Meridian Mail system, the target system data will be overwritten if provisioning continues. Provisioning can be continued or canceled if data conflicts exist.

Also, if there are more users on the tape than the target system has room for, temporary users are added up to the system limit only. This may result in some users not being provisioned to the target system.

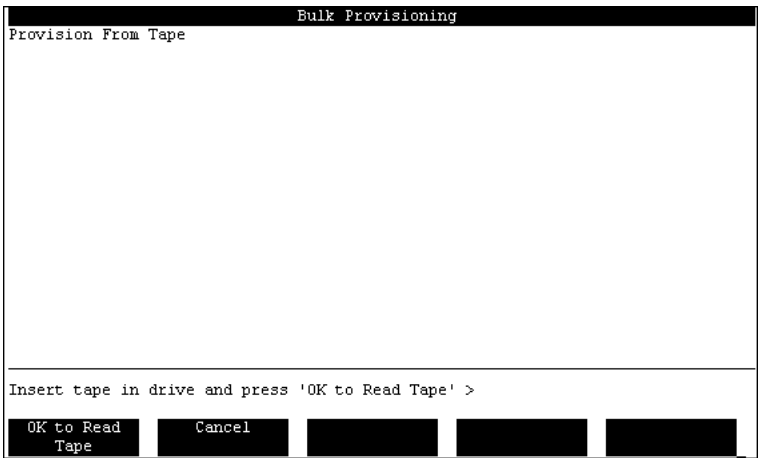
Provisioning data

Introduction

This topic provides information for provisioning the data from the tape to a Meridian Mail system. Also included are diagrams of the screens and descriptions of their fields.

The Provision From Tape initial screen

The following is an example of the Provision From Tape initial screen.



Description

The Provision From Tape initial screen contains no input fields. The [OK to Read Tape] softkey retensions the tape and reads summary information while the [Cancel] softkey returns to the bulk provisioning menu. For more information, see “Provisioning data from the bulk provisioning tape” on page 34-41.

The Provision From Tape screen

The following is an example of the Provision From Tape screen after the contents of the tape have been read.

```
                              Bulk Provisioning
Provision From Tape

Data Set Name:   Service01                        Created On: 06/14/96 09:30

Status:          Provisioning not yet started

Provision remote users as:        Permanent Temporary

Remote Users:    None All Selected
Mailbox                          Provision  Number of Entries
ALL                              No Yes     10

Services:        None All
ServiceID                        Provision  Required Features
ALL                              No Yes     MMUI Fax Forms Menus

VSDNs:           None All
VSDN                             Provision  Required Features
------------------------------------------------------------------------------
Select a softkey >

 Ok to Start      Cancel      View Selected   Print Selected
 Provisioning
```

Field descriptions

The following are the fields in the Provision From Tape screen.

Data Set Name	
Description	This is the descriptive label of the data set on the tape.
Created On	
Description	The date and time that the tape was created, in the date format of the destination system.
Status	
Description	This is the status of the provisioning process.
Provision remote users as	
Options	Permanent or Temporary. Temporary users are subject to the nightly audit. For information on temporary users and the nightly audit, see Chapter 9, “Remote voice users”.
Default	Temporary

Remote Users	
Description	This field appears only if there is user information on the tape and if networking is a feature on the target system.
Options	None, All, or Selected. If the administrator chooses Selected, additional lines display showing the grouping of users as entered in the data set definition. The administrator can then choose the users to be provisioned by using the Yes/No options.
Condition	If the data set was copied to tape by specifying All, then when provisioning from tape the selected option is not available.

Services	
Description	This field appears only if there is service data on the tape. The administrator specifies the services to be provisioned from the tape.
Options	None, All, or Selected. If the administrator chooses Selected, additional lines display showing the grouping of services as entered in the data set definition. The administrator can then choose the services to be provisioned by using the Yes/No options.
Default	All
Condition	If the data set was copied to tape by specifying All, then when provisioning from tape the selected option is not available.

VSDNs	
Description	This field appears only if there is VSDN data on the tape. This field is used to specify the voice service DNs that are to be included in the data set.
Options	None, All, or Selected. If the administrator chooses Selected, additional lines display showing the grouping of VSDNs as entered in the data set definition. The administrator can then choose the VSDNs to be provisioned by using the Yes/No options.
Default	All.
Condition	If the data set was copied to tape by specifying All, then when provisioning from tape the selected option is not available.

Provisioning data from the bulk provisioning tape

To restore data from the bulk provisioning tape to the Meridian Mail system, follow these steps.

Starting Point: The Bulk Provisioning Menu

Step	Action
1	Select Provision from Tape from the menu. **Result:** The Provision from Tape initial screen displays.
2	Insert the tape in the drive and press the [OK to Read Tape] softkey. **Result:** The tape begins to retension. Retensioning takes approximately four minutes.
3	After retensioning is complete, the system checks the tape for bulk provisioning information.

IF the tape	THEN
is not a valid bulk provisioning tape	you are prompted that the tape is not a bulk provisioning tape. Replace the tape and press the [OK to Read Tape] softkey to continue or the [Cancel] softkey to abort the procedure.
is a valid bulk provisioning tape	the Provision From Tape screen displays.

4	View the information on the Provision From Tape screen. Make changes to the Remote Users, Services, and VSDNs fields as necessary. See “Field descriptions” on page 34-38. for information on completing these fields.

Step	Action
5	Before beginning the provisioning process, view or print the potential conflicts between the data set on the tape and the target system. To view or print data set conflicts, see “Viewing and printing data conflicts” on page 34-43. **Note:** If system conflicts exist, [OK to Start Provisioning] will stop. You may wish to restart your choices by using the “Selected” option and toggling Yes to No until the conflicts are resolved.
6	Press the [OK to Start Provisioning] softkey to begin the provision from tape. **Result:** The provisioning begins (if there are no conflicts). During the provisioning process, the status of the process displays in the Status field. The only available softkey during provisioning is [Abort]. The [Abort] softkey aborts the provisioning process at the next logical step. When provisioning is complete, the Status field displays the message “Provisioning in progress, 100% done. Tape rewinding.”
	CAUTION **Risk of data loss** If there are data conflicts, you will be informed of this and prompted to cancel or continue. If you continue, you will overwrite existing data. [Cancel] returns to the Provision from Tape screen. [Continue] will start the provisioning and overwrite conflicting items.
7	Press the [Exit] softkey to return to the Bulk Provisioning Main Menu. **Result:** The provisioned data is ready to use. If necessary the MMI can be used to make corrections, such as changing a revert DN.

Viewing and printing data conflicts

Introduction

This section describes the procedure for viewing and printing data conflicts that may arise during bulk provisioning to another system.

The View Conflicts screen

The following is an example of the View Conflicts screen.

```
                                Bulk Provisioning
View Conflicts

System Level Conflicts
Remote Site 333 does not exist.

Data Conflicts

Data from tape                              Data overwritten on destination
Class Type ID/VSDN/Mbox                     Type Description
Serv   MS  101                               MS  Main Menu for Extern
Serv   MS  102                               MS  off hours menu
Serv   MS  103                               MS  department choice su
Serv   MS  104                               MS  Menu 4
Serv   MS  105                               MS  Main menu in french
Serv   MS  106                               MS  dept choice submenu
Serv   AS  201                               AS  Upcoming product rel
Serv   AS  202                               AS  Upcoming Events
Serv   AS  203                               AS  Security Update

                  _

     Exit                                    Next
                                             Page
```

Field descriptions

These are the fields in the View Conflicts screen.

System Level Conflicts	
Description	This field shows all system level conflicts that would prevent bulk provisioning from proceeding. If there are no conflicts the field will display the word None. For more information, see “Potential conflicts between databases” on page 34-35.

Data Conflicts or All Entries	
Description	The appropriate field displays when either the Conflicts Only or the All Entries option is chosen. This field is divided into two parts: Data from tape on the left side, and Data overwritten on destination on the right side of the screen.
Data from tape	
Description	When the [Conflicts Only] softkey is pressed, this field shows only the data in conflict with the target system. When the [All Entries] softkey is pressed, this field shows all data that is contained on the provisioning tape for the specified selection criteria. The information is shown by Class, Type, and ID/VSDN/MBox. a. Class is the general class of data on the tape. Class is Serv, VSDN, or User. b. Type is the service type represented by the mnemonic used by Voice Service Administration (VSA). This applies to services and VSDNs only. c. ID/VSDN/MBox is the voice service ID for a service, the DN for VSDNs, and the mailbox with a network prefix for users.
Data overwritten on destination	
Description	This field displays any data on the target system that will be overwritten if provisioning proceeds. The data is provided by Type and Description. • Type applies to services and VSDNs only. It is the service type of the service as represented by the mnemonic used by Voice Service Administration (VSA). • Description is the target system's name or the comment field of a data item that will be overwritten. **Note:** This field will be blank if the data item does not yet exist on the target system.

Viewing data conflicts

To view data conflicts before provisioning the data to the new Meridian Mail system, use the following steps.

Starting Point: The Provision From Tape screen

Step	Action
1	Press the [View Selected] softkey. **Result:** The softkeys are replaced by the [Conflicts Only] and [All Entries] softkeys.

```
                                Bulk Provisioning
Provision From Tape

Data Set Name:   Service01                        Created On: 06/14/96 09:30

Status:          Provisioning not yet started

Provision remote users as:        Permanent Temporary

Remote Users:    None All Selected
Mailbox                         Provision  Number of Entries
ALL                             No Yes     10

Services:        None All
ServiceID                       Provision  Required Features
ALL                             No Yes     MMUI Fax Forms Menus

VSDNs:           None All
VSDN                            Provision  Required Features
------------------------------------------------------------------------------
Select a softkey >

                                Conflicts Only  All Entries
```

2 Use the following table to choose the next step.

IF you want to view	THEN press softkey
the conflicts between the data on the tape and the data on the target system only	[Conflicts Only].
all entries on the tape (for the specified criteria) and the conflicts on the target system	[All Entries].

Result: The View Conflicts screen displays with the appropriate information provided.

3 Press the [Exit] softkey to return to the Provision From Tape screen.

Printing data conflicts

To print data conflicts before provisioning the data to the new Meridian Mail system, use the following steps. The printout will go to the reports printer.

Starting Point: The Provision From Tape screen

Step	Action
1	Press the [Print Selected] softkey. **Result:** The softkeys are replaced by the [Conflicts Only] and [All Entries] softkeys.This is an example of the screen.
2	Use the following table to choose the next step.

IF you want to print	THEN press softkey
the conflicts between the data on the tape and the data on the target system only	[Conflicts Only].
all entries on the tape (for the specified criteria) and the conflicts on the target system	[All Entries].

Result: The following screen displays.

```
                              Bulk Provisioning
Provision From Tape

Data Set Name:   Service01                      Created On: 05/06/96 11:35

Status:          Provisioning not yet started

Provision remote users as:        Permanent Temporary

Remote Users:    None All
Mailbox                          Provision  Number of Entries
ALL                              No Yes     10



Please ensure that the printer is ready._

                 Cancel                      Continue
                 Printing                    Printing
```

Step	Action
3	Press the [Continue Printing] softkey to print the conflicts. **Result:** The conflict list is printed. **Note:** At any time, press the [Cancel Printing] softkey to cancel printing.

Appendix A

Integrated Mailbox Administration

In this appendix

Overview	A-2
Section A: Interaction between IMA and Meridian Mail	A-3
Section B: System installation using VMBA	A-15

Overview

Introduction

Section A: Interaction between IMA and Meridian Mail, describes the Integrated Mailbox Administration feature as well as

- the interaction of IMA and Meridian Mail with respect to potential conflicts
- the synchronization of databases
- the implementation and processing differences

In Section B: System installation using VMBA, the procedures describe the installation of a system

- at a new site with no preconfigured database on either the Meridian 1 core or Meridian Mail
- at a new site with sets and VMBs preconfigured on the Meridian 1 core but nothing configured on Meridian Mail
- at an existing site with VMBs configured on Meridian Mail but no VMBs configured on the Meridian 1 core

Section A: Interaction between IMA and Meridian Mail

In this section

Overview	A-4
What is Integrated Mailbox Administration?	A-5
IMA data translations	A-6
Synchronizing IMA and Meridian Mail databases	A-9
IMA and Meridian Mail processing differences and implementation issues	A-10

Overview

Introduction

This section describes Integrated Mailbox Administration and discusses the interactions between IMA and Meridian Mail.

What is Integrated Mailbox Administration?

Description

Integrated Mailbox Administration (IMA) is a feature of Meridian Mail which works in conjunction with the Voice Mailbox Administration (VMBA) feature on the Meridian 1 switch. These features provide a single point for administration of Meridian 1 (M1) sets, Call Party Name Display (CPND), and Meridian Mail mailboxes.

Benefits

IMA/VMBA provides significant time savings for both the installer and the administrator. Set datafile (including CPND) and mailboxes only have to be entered once, in one place (LD 10 for analog sets or LD 11 for digital sets), saving time and the potential for datafill inconsistencies between the two systems.

This feature allows the installer or the administrator to add a user and a mailbox from the Meridian 1 terminal by specifying whether the user requires voice mail capabilities. If the user requires a mailbox, the Meridian 1 core sends a message to Meridian Mail to request that the user be added to the Meridian Mail database. This eliminates the step of adding the user from Meridian Mail.

Prerequisite

In order to use the Integrated Mailbox Administration feature, your Meridian 1 must be running X11 Release 19 or later with the Voice Mailbox Administration feature installed. (VMBA requires X11 Release 19.2x or later.)

IMA data translations

Introduction

The Meridian 1 databases contain a subset of the data that are required to completely configure a voice mail user. When a message is sent by the Meridian 1 to Meridian Mail to add a user, Meridian Mail will use the information with some predefined defaults and rules to add the user to the Meridian Mail database.

Example

By definition, the Primary DN is the same as the mailbox number and the same as the Message Waiting Indication DN. The IMA data translations table below shows the data that are sent by the Meridian 1 and the data that are actually stored for each voice mail user.

Before you begin

Before adding users from the Meridian 1 using VMBA, the following steps must be carried out in Meridian Mail.

1. Define classes of service for the system.

For more information, see Chapter 26, “Class of Service administration”.

2. For added mailbox security, you can define a password prefix.

For more information, see “Password prefix” on page 6-136.

ATTENTION

If VMBA is enabled, do not modify those parameters which are common to both systems in Meridian Mail as this can lead to inconsistencies. The VMBA feature is considered the master and will override these settings. If necessary, you can customize those parameters which appear only in Meridian Mail since there is no chance of conflict.

IMA data translations table

Use the following table to determine which parameters are common to both the VMBA and Meridian Mail, and which can only be customized through Meridian Mail user administration facilities.

Note: Meridian Mail requires three fields to collect the last name, first name, and initials of the user. In VMBA, CPND Name is the only field required to collect all this information. In X11, this information is in the selectable format First Name, Last Name or Last Name, First Name. Commas must be entered between each element; otherwise, Meridian Mail will interpret the whole sequence as the last name.

Meridian Mail field	Meridian 1 field	What Meridian Mail stores
Location Prefix	N/A	Sets to the Local Site ID in Meridian Mail
Mailbox Number	DN	Sets to the Primary DN in Meridian Mail
Volume ID	N/A	Meridian Mail queries all available volumes and selects the least used volume
Class of Service	VMB Class of Service	Value specified from the M1
Last Name	CPND Name	Value specified from the M1, or blank if not supplied ***Note:*** The CPND must be entered in the one of the following selectable formats: • FirstName Initial,LastName Generational_Qualifier • LastName Generational_Qualifier,FirstName Initial A comma is always required before the last name. The initial is optional and can only be one character. The FirstName and LastName cannot contain spaces, or the characters “+”, “_”, or “?”. Generational_Qualifier is optional, and supports Jr, Jr., Sr, Sr., I, II, III, IV.
First Name		
Initials		
Department	N/A	Blank

Meridian Mail field	Meridian 1 field	What Meridian Mail stores
Primary DN	DN (DN fills in the Mailbox Number and Primary DN in Meridian Mail)	Taken from value entered in the DN field
Secondary DN	Second DN (optional field)	Value specified from the M1, or blank if not supplied
Tertiary DN	Third DN (optional field)	Value specified from the M1, or blank if not supplied
MWI DN	N/A	Set to the Primary DN in Meridian Mail
Personal Verification Recorded	N/A	Set to Not Recorded in Meridian Mail. (This field is modifiable from the user's telephone set if the field *Personal Verification Changeable by User* is set to Yes in the assigned COS.)
Logon Status	N/A	Set to Enabled in Meridian Mail
Preferred Language	N/A	Set to the default language
Name Dialable by External Callers	N/A	Set to Yes in Meridian Mail
Hospitality User Class	N/A	If Hospitality is installed, this field is set to Staff in Meridian Mail. (Guest users cannot be added from the M1.)
Remote Notification Schedules	Not datafilled by the M1	Blank (This field is modifiable from the telephone set by the user if the following conditions are met: MMUI is installed on the system. Remote Notification Capability is set to Yes in the user's COS. Remote Notification Keypad Interface is set to Yes in the user's COS If these conditions are not met, remote notification schedules can only be created from the Add or View/Modify Local Voice User screen in User Administration.)
User Password	Not datafilled by the M1	The password will consist of the password prefix (configured in the Voice Security Options screen) and the user's mailbox number.

Synchronizing IMA and Meridian Mail databases

Introduction

The Meridian 1 and Meridian Mail databases are stored on separate systems; however, they can diverge under the following conditions:

- core elements of mailboxes are changed with Meridian Mail user administration
- the X11 VMBA database is loaded while VMBA is disabled
- the X11 VMBA database is updated while the AML link is down or Meridian Mail is out of service

The databases must be synchronized in one of two ways: through automatic or manually invoked audits or through uploading Meridian Mail data to the X11 VMBA database.

Audit synchronization

The two databases are synchronized through the use of automatic or manually invoked audits. If a variance is found during an audit, the result depends on whether DATA_CORRECT is enabled or disabled (X11 LD 17). If enabled, the audit will automatically change the data in Meridian Mail to conform to the X11 VMBA database. If disabled, the audit will flag variances to the Meridian 1 administration printer, allowing the administrator to determine the appropriate corrective action.

Uploading data from Meridian Mail's database to IMA

Another way of synchronizing the two databases is to upload Meridian Mail data to the X11 VMBA database.

Sites upgrading to X11 Release 19 often already have a Meridian Mail system configured. To eliminate manual entry of all the VMBA fields, an upload of existing mailbox data into the VMBA data fields is available. The upload is initiated from X11 LD 48.

See X11 documentation for more details

More detailed information, including overlays, are provided in the *X11 Features and Services* document (NTP 555-3001-305) in the chapter, "Meridian Mail Voice Mailbox Administration."

IMA and Meridian Mail processing differences and implementation issues

Introduction

This section describes a number of feature interactions, name processing differences, and implementation issues that you need to be aware of.

Meridian Mail features interactions

Make note of the following Meridian Mail feature interactions:

- This feature does not support guest users in a Hospitality environment.

  This feature expects that the Meridian 1 User's Primary DN is the user's mailbox number. Staff users will typically have the primary DN equal the mailbox number. However, guest users will not have a room's primary DN the same as their mailbox number.
- If the Network Message Service (NMS) is installed, only users at the local site can be added via the Meridian 1.

  The Location Prefix field defaults to the Local Site ID. Users at satellite locations must be added manually via the Meridian Mail terminal. All NMS administration should be done at the Meridian Mail administration terminal.
- IMA does not support the Meridian Mail Multi-customer feature.
- Configured mailboxes will use the default language of the default customer group on Meridian Mail.

  If the default language is English, all remotely configured mailboxes will be assigned the English language option. Multi-language interaction between the Meridian 1 and Meridian Mail is not supported.
- The IMA feature supports only Local Voice Users.
- IMA should not be run while the Meridian Mail AutoAdmin feature is active.

X11 Meridian Mail database differences

You should be aware of the following X11 Meridian Mail database differences:

- Database audits run every five days.

  If mailbox changes are made directly at the Meridian Mail administration terminal, they may not be detected and corrected for up to five days.
- The combined first and last name is limited to 27 characters on the Meridian 1.

  Meridian Mail supports up to 21 characters for the first name and 41 characters for the last name. This feature overrides these limits to total 27 characters.
- Meridian Mail limits first names to 21 characters.

  If a first name is configured on the Meridian 1 (M1) core and is greater than 21 characters, it will be truncated by Meridian Mail.
- Meridian Mail only supports a subset of the characters supported for names on the Meridian 1 core.

  Meridian Mail does not support the international character set option of X11 (option 211). Meridian Mail only supports North American ASCII characters (excluding +, _, and?) in the name fields. If a name that is configured on the Meridian 1 core contains characters not supported by Meridian Mail, Meridian Mail will reject the name.
- Multiple languages on the Meridian 1 are not supported by the IMA feature.
- When entering the CPND name in X11, the first name and last name (the order of names is selectable) must be separated by commas.

  If commas are not entered, Meridian Mail will interpret the entire sequence of letters as the last name.
- If a mailbox is deleted on the Meridian 1 but not successfully deleted in Meridian Mail, an “orphaned” mailbox will result.

  These mailboxes will be recovered if the same DN is reused in the Meridian 1 (in other words, Meridian Mail will delete the old one and add the new one), but will remain in Meridian Mail if they are not.

X11 VMBA and Meridian Mail IMA interactions

You should be aware of the following X11 VMBA and Meridian Mail interactions:

- Depending on how the VMBA option is set, if a mailbox already exists on Meridian Mail and VMBA requests a mailbox to be created for the DN corresponding to that mailbox, IMA will do one of two things:
  - delete the existing mailbox (including its voice messages) and replace it with the mailbox requested by VMBA
  - keep the mailbox messages but configure the mailbox according to the VMBA data elements
- VMBA is the master database.

  Changes made using VMB will always be copied to Meridian Mail.
- If a DN must be changed on a set on the Meridian 1 core, the mailbox will have to be deleted and added again in Meridian Mail prior to changing the DN on the Meridian 1 core.
- The X11 administrator must set VMBA to off for DNs on the Meridian 1 which should not have mailboxes.
- When making changes to data elements using VMBA, make sure the same mailbox is not open in Meridian Mail user administration.

  If this happens, the download will stay in pending state until the problem is resolved.

X11 VMB limitations

You should be aware of the following X11 VMB interactions:

- Only one Meridian Mail system is supported per Meridian 1 system.
- Only one customer can be configured on the Meridian 1 core for this application.
- Only 500, 2500, SL1, and digital set types are supported in this release.
- The mailbox status that is shown in Overlay 20 in the Meridian 1 indicates the status of the mailbox on the Meridian 1 core and not the status of the mailbox on Meridian Mail.

For example, if a mailbox is disabled on Meridian Mail as a result of a security violation, the state will not be updated in the Meridian 1 core.

- Operator revert is not supported because the revert DN is user-changeable.
- Configuration of Meridian Mail customer numbers, department numbers and mailbox passwords from the Meridian 1 core are not supported in this release.
- Mailboxes cannot be configured for sets served by a remote Meridian Mail subsystem.

Section B: System installation using VMBA

In this section

Overview	A-16
Installing at a new site without a preconfigured database on Meridian Mail or the Meridian 1 core	A-17
Installing at a new site with sets and VMBs preconfigured on the Meridian 1 core but not on Meridian Mail	A-18
Installing at an existing site with VMBs preconfigured on Meridian Mail but not the Meridian 1 core	A-20

Overview

introduction

This section describes the three possible system installation scenarios when using VMBA:

- installation at a new site with no preconfigured database on either the Meridian 1 core or Meridian Mail
- installation at a new site with sets and VMBs preconfigured on the Meridian 1 core but nothing configured on Meridian Mail
- installation at an existing site with VMBs configured on Meridian Mail but no VMBs configured on the Meridian 1 core

Installing at a new site without a preconfigured database on Meridian Mail or the Meridian 1 core

Introduction

Use this procedure to install a system using VMBA at a new site without a preconfigured Meridian Mail or Meridian 1 core database.

Procedure

To install a system using VMBA at a new site with no preconfigured database, follow these steps.

Step	Action
1	Configure and enable the AML link to Meridian Mail.
2	Configure the VMBA application in LD 17 on the VAS associated with Meridian Mail. The data correction and automatic audit options for the VMBA application should be set to On to simplify database maintenance and to ensure database integrity. **Result:** The VMBA application will be enabled automatically following its configuration in LD 17 if the AML link is currently active. If the AML link is not active, the VMBA application will be placed in the link out-of-service (LINKOOS) state.
3	Configure the VMB classes of service on Meridian Mail. A transaction error will result if a class of service is specified on the core that has not been configured on Meridian Mail. For more information, see Chapter 26, “Class of Service administration”.
4	Installation is complete. VMBs can now be added, changed, and deleted in LD 10 and 11. These changes will be downloaded automatically to Meridian Mail if the AML link and VMBA are enabled. If the AML link and/or VMBA application is not enabled when doing VMB administration, the VMBs will be left in the UPDATE PENDING state and downloaded when the AML link is enabled.

See X11 documentation for more details

More detailed installation procedures, including overlays, are provided in the *X11 Features and Services* document (NTP 555-3001-305) in the chapter, “Meridian Mail Voice Mailbox Administration.”

Installing at a new site with sets and VMBs preconfigured on the Meridian 1 core but not on Meridian Mail

Introduction

Use the following procedures to install a system using VMBA where the VMB database is preconfigured on the Meridian 1 core prior to the installation at the customer site (no VMBs should be configured on Meridian Mail). The process is divided into two parts:

- preconfiguring the database
- installing the database at the customer site

Preconfiguring the database

To preconfigure the database, follow these steps.

Step	Action
1	Configure the VMBA application in LD 17 on the VAS associated with Meridian Mail. The data correction and automatic audit options for the VMBA application should be set to On to simplify database maintenance and to ensure database integrity. The AML link does not have to be configured at this point since there is no actual hardware to enable.
2	Configure the sets and associated VMBs. The VMBs will be left in the UPDATE PENDING state.

Installing the database at the customer site

To install the database at the customer site, follow these steps.

Step	Action
1	Ensure that the Meridian Mail database has been configured with the VMB classes of service that were used when preconfiguring the core database. For more information, see Chapter 26, "Class of Service administration". . **ATTENTION** Do not proceed any further until this has been completed.
2	Configure and enable the AML link to Meridian Mail.
3	The VMBA application should be enabled automatically unless it is in the manually disabled state. If it is disabled, then the VMBA application will have to be enabled in LD 48 using the **ENL VMBA <vsid>** command. When the VMBA application has been successfully enabled, the preconfigured mailbox data will begin downloading to Meridian Mail. The VMBs successfully downloaded and configured can be printed using the PRT VMB option in LD 20.
4	When the download has completed, reported errors should be manually corrected.
5	Initiate the database audit by entering **ENL VMBA <vsid> AUDT ALL** in LD 48. This will verify that the VMB and CPND data on the core matches the data on Meridian Mail. The status of the audit can be obtained by entering **STAT VMBA <vsid>** or **STAT VMBA <vsid> AUDT** in LD 48. **Result:** Errors detected by the audit will be corrected automatically. The installation is complete.

See X11 documentation for more details

More detailed installation procedures, including overlays, are provided in the *X11 Features and Services* document (NTP 555-3001-305) in the chapter, "Meridian Mail Voice Mailbox Administration."

Installing at an existing site with VMBs preconfigured on Meridian Mail but not the Meridian 1 core

Introduction

Use this procedure for installing a system using VMBA at an existing site. In most cases, these sites will have the VMBs configured already. The upload command in LD 48 can be used to upload the existing Meridian Mail VMB data to the Meridian 1 core.

Cleanup may be necessary

This command causes name data configured on Meridian Mail to be uploaded; existing names on the core will be overwritten with the names on Meridian Mail. Some name cleanup may be necessary if these names on the core are not the same as those on Meridian Mail. Once this cleanup is complete, name administration becomes easier; it is necessary to change names on the Meridian 1 core only (instead of on the core and on Meridian Mail).

Procedure

To install the system at an existing site with VMBs configured on Meridian Mail but not on the Meridian 1 core, follow these steps.

Step	Action
1	Configure and enable the AML link to Meridian Mail.
2	Configure the VMBA application in LD 17 on the VAS associated with Meridian Mail. The data correction and automatic audit options for the VMBA application should be set to Off until this installation has been completed.
3	The application will be enabled automatically following the configuration of the VMBA application in LD 17 if the AML link is currently active. If the AML link is not active, the VMBA application will be placed in the link out-of-service (LINKOOS) state.
4	Initiate the database upload by entering **ENL VMBA <vsid> UPLD ALL** in LD 48.
5	Periodically check the status of the upload by entering the command **STAT VMBA <vsid>** or **STAT VMBA <vsid> UPLD AUDT** in LD 48.

Step	Action
6	When an UPLOAD COMPLETE message is printed, manually resolve any errors that may have occurred during the upload. **Result:** The upload is complete.
7	Initiate the database audit by entering **ENL VMBA <vsid> AUDT ALL** in LD 48. This will verify that the VMB and CPND data on the core matches the data on Meridian Mail.
8	Manually resolve any errors that may have been uncovered by the audit. **Result:** The audit is complete. The Meridian 1 core and the Meridian Mail databases are synchronized. Perform any cleanup on names, if necessary.
9	Configure the data correction and automatic audit options as desired. These options are recommended to maintain database integrity. **Result:** The installation is complete. Ongoing administration of the VMBs can be performed on the Meridian 1 core from now on.

See X11 documentation for more details

More detailed installation procedures, including overlays, are provided in the *X11 Features and Services* document (NTP 555-3001-305) in the chapter, “Meridian Mail Voice Mailbox Administration.”

Appendix B

Meridian Mail AutoAdmin Utility

In this chapter

Overview	B-2
Introduction	B-3
Meridian Mail AutoAdmin installation	B-5
AutoAdmin Configurator	B-12
AutoAdmin Utility	B-21
The AutoAdmin window	B-25
Using Meridian Mail AutoAdmin	B-34
Troubleshooting	B-51

Overview

Introduction

This chapter explains how to install, configure, and use the Meridian Mail AutoAdmin Utility.

Introduction

What is the Meridian Mail AutoAdmin Utility?

The Meridian Mail AutoAdmin Utility provides a means of propagating user database information from a central system to other local or off-site Meridian Mail systems.

Who should use AutoAdmin?

Large messaging customers of Meridian Mail who often need to administer and manage multiple systems within their organization will benefit from using AutoAdmin. These systems can support thousands of users, and an administrator may have a limited amount of time to get the additions and changes done.

AutoAdmin provides an easy way for customers to get the required information from the local user database and propagate it to any of their other Meridian Mail systems.

Supported platforms

AutoAdmin works on all Meridian Mail platforms supported by MM12, except the Compact Option.

On the windows side, the Meridian Mail AutoAdmin Utility has been developed to use a PC and runs on Microsoft Windows 95 and Windows NT 4.0.

Connecting Meridian Mail and the PC

The connection between Meridian Mail and the PC is called the MSLink (Message server link) and each Meridian Mail system can have only one of these links. The maximum supported port rate on this link is 38.4 Kbytes for the MMP40 systems and 9.6 Kbytes for the MSM and Mod GP systems, subject to the cumulative port rate on each node for these systems.

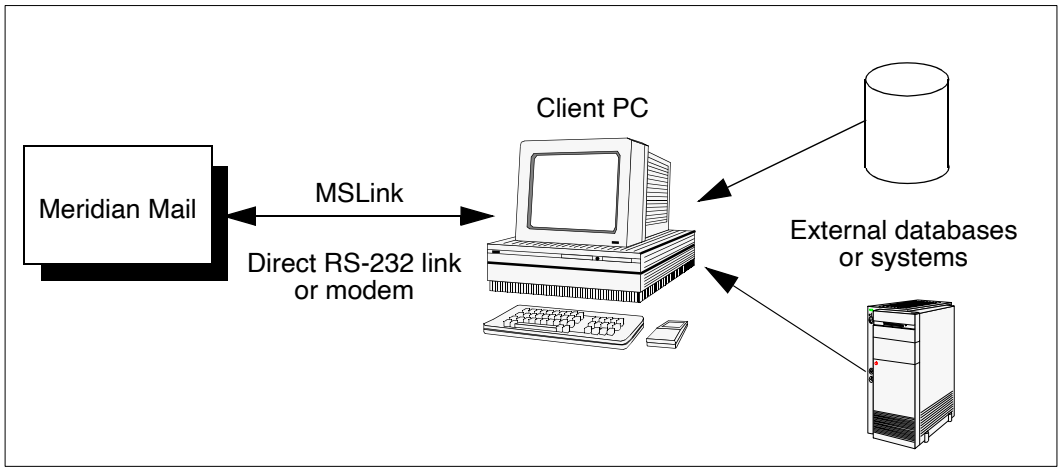
PC minimum hardware requirements

The PC (also known as the client PC) requires the following minimum hardware:

- a Pentium 90 CPU
- an SVGA video card
- a minimum of 16 Mbytes of RAM
- 10 Mbytes of hard disk space
- one 3.5-inch floppy disk drive
- one serial port, with a 16550 UART for connecting to Meridian Mail
- a keyboard
- a mouse

System configuration

The following diagram shows a typical system configuration. This configuration allows the client PC to obtain user information from external databases or computer systems and update them or add them to the Meridian Mail system.



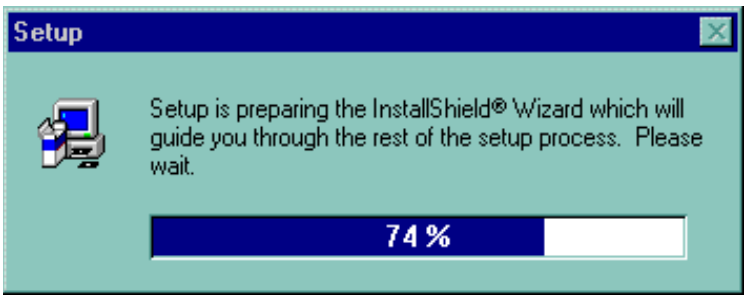
Meridian Mail AutoAdmin installation

Installation procedure

To install Meridian Mail AutoAdmin on the client PC follow these steps.

Note: If this is an upgrade of AutoAdmin see "Upgrade procedure" on page B-10.

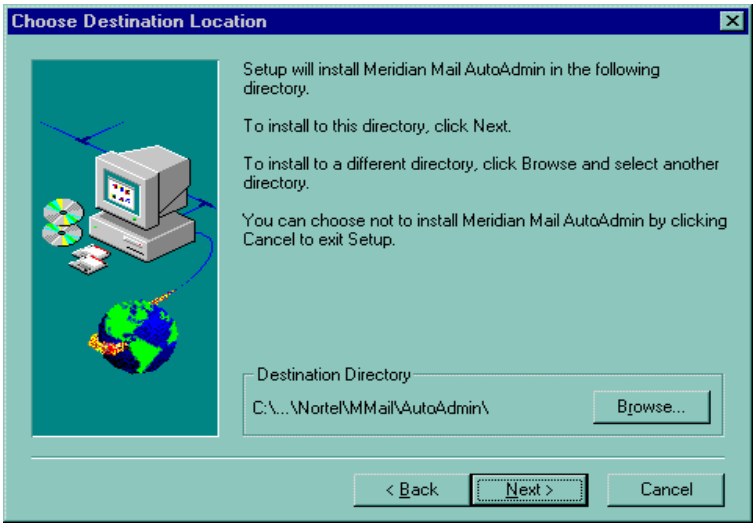
Step	Action
1	Insert the floppy diskette into the appropriate drive.
2	Select the windows Start button and Select Run.
3	Type **q:\setup.exe** where q is the letter of the drive containing the disk. The following screen is displayed:



The InstallShield Wizard displays the standard screens concerning other active Windows programs and the AutoAdmin license agreement.

4	Follow with the appropriate action in each case.

Step	Action
	Result: The following screen is displayed concerning the choices of drive and directory.

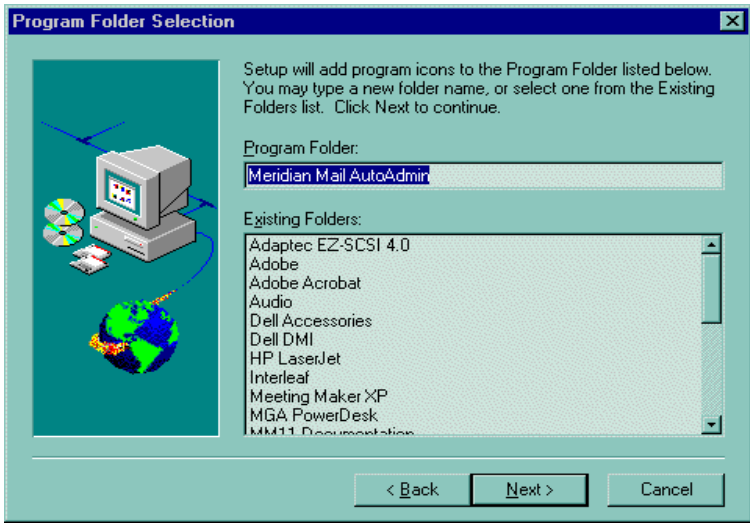


5 If you want the AutoAdmin software package in another directory and/or on another drive, click on the browse button.

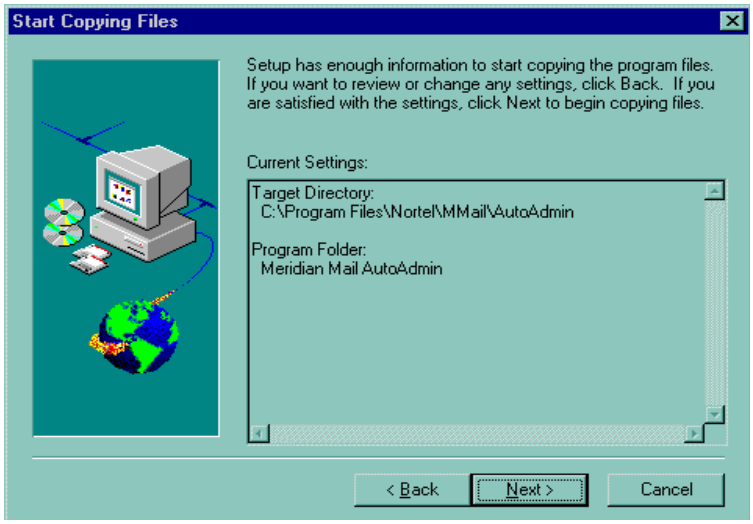
6 Type in or select the desired destination directory and double click on OK.

7 When you are finished, click on Next.

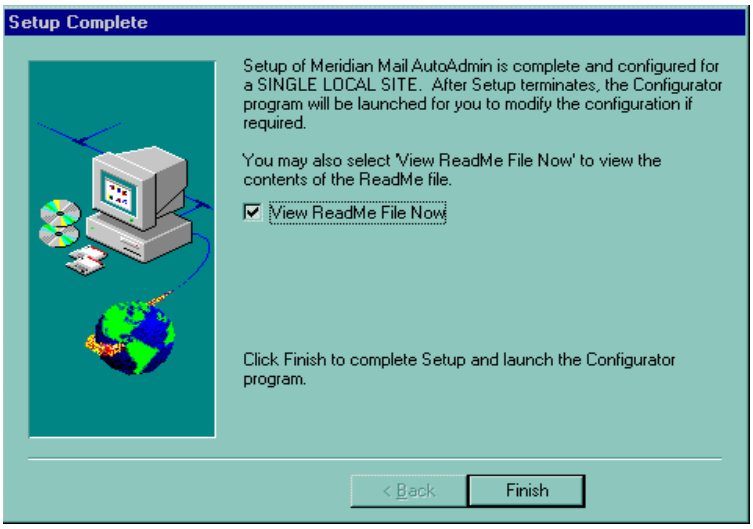
Step	Action
8	Specify the name for the program folder using the following screen. **Note:** It is recommended that you keep the AutoAdmin folder name.
9	Click Next when you have finished.



Step	Action
	Result: The following screen is displayed to verify the information you have input.
10	If you wish to change anything you have entered so far, click Back.



Otherwise, click Next to continue with the installation.

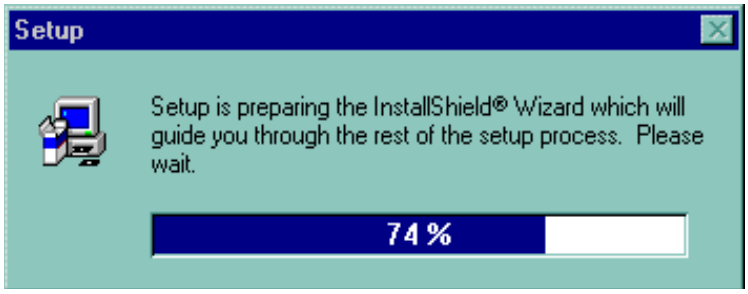
Step	Action
11	Click Finish to complete the installation of AutoAdmin. **Result:** Once you finish the installation, your system is configured for one local site with default settings.  If you require more configuration, or need to modify the existing local site, use the configurator program that follows immediately from the installation. **Note:** You may deselect the View ReadMe file. However, it is recommended that users read the ReadMe file for information on copyright, version, and support.

Upgrade procedure

To upgrade to AutoAdmin, follow these steps.

Note: If you try to upgrade using an older version of AutoAdmin, the procedure will abort.

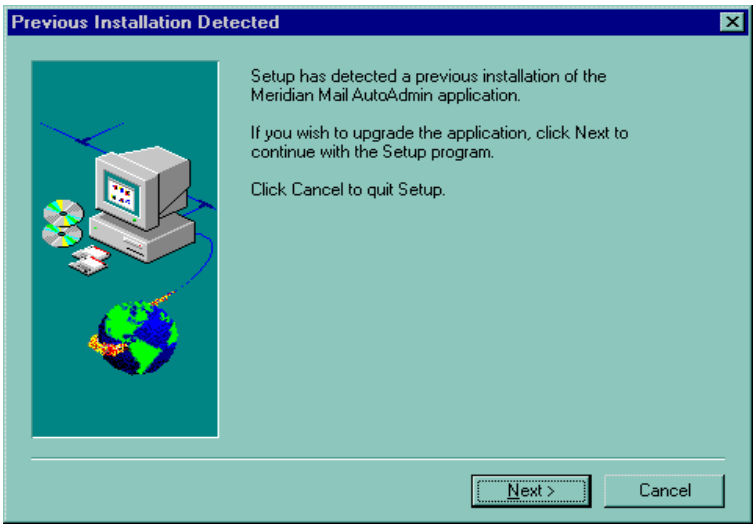
Step	Action
1	Insert the floppy diskette with the AutoAdmin upgrade into the appropriate drive.
2	Select the Windows Start button, and select Run.
3	Type **q:\setup.exe** where q is the letter of the drive containing the disk. **Result:** The following screen is displayed.



The InstallShield Wizard displays the standard screens concerning other active Windows programs.

4	Follow with the appropriate action in each case.

Step	Action
	Result: Once this is done, the following screen is displayed.



5 If you wish to upgrade, select Next and go to step 6, or select Cancel to end the procedure without an upgrade.

6 Click Next.

Result: The upgrade is installed in the same directory as the previous version of AutoAdmin.

Result: When the upgrade is completed, the following message screen is displayed:

7 Click OK to finish the upgrade.

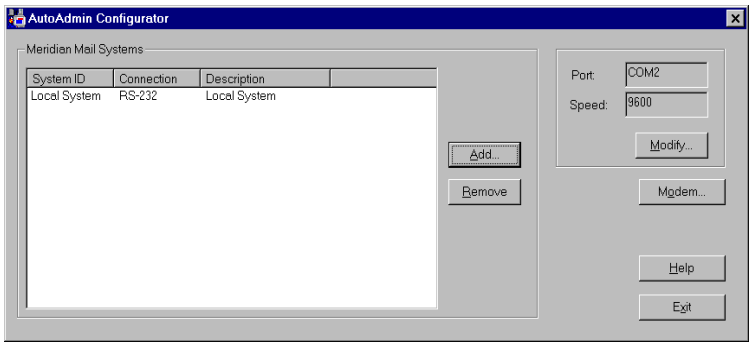
AutoAdmin Configurator

Overview

AutoAdmin Configurator is used to configure your PC connection to Meridian Mail systems. If you need to add Meridian Mail systems that need to be administered by AutoAdmin or need to change port, speed, or modem command settings, AutoAdmin Configurator is required.

Using AutoAdmin Configurator

The following window is displayed when the AutoAdmin installation is complete.



Note: In an upgrade, the configuration from the previous version remains.

Field descriptions

The following table describes the boxes and buttons in the AutoAdmin Configurator screen.

System ID	
Description	Name of the system for administrative purposes only
Maximum length	1 to 25 alphanumeric characters
Default	None
Limit	Up to 150 systems can be defined.

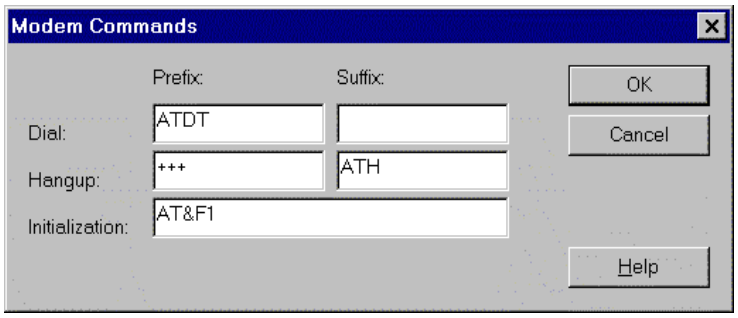
Connection	
Description	The type of connection, which may be a serial (RS-232) connection or the dialing number of a modem
Values	RS-232, dialing number
Description	
Description	Optional field to describe Meridian Mail system
Maximum length	0 to 50 alphanumeric characters
Default	None
Add	
Description	Select this button when you want to add a Meridian Mail site. Type the site information in the System Settings dialog box that is displayed.
Remove	
Description	Select this button when you wish to remove a Meridian Mail site from your site ID list. You must click on the site ID you wish to remove before clicking the Remove button.
Port	
Description	Displays the active serial port on the PC that links AutoAdmin to a Meridian Mail system or to a modem. Although these ports are supported, your PC may or may not have them. This field is read-only. To modify the setting, select the Modify button, and change the setting in the dialog box it presents.
Default	COM 1
Range	COM 1, COM 2, COM 3, COM 4

Speed	
Description	Shows the baud rate of the port linked to the Meridian Mail system, or to the modem. This field is read-only. To modify the setting, select the Modify button, and change the setting in the dialog box it presents.
Default	9600
Values	2400, 4800, 9600, 19200, 38400
Modify	
Description	Sets the selection of port and speed
Modem	
Description	Opens a dialog box that lets you set the commands to a specific modem
Help	
Description	Opens the online help for this dialog box
Exit	
Description	Closes the Configurator.

Modem Commands window

The following window displays the modem commands. Use this dialog box to define the settings for the specific type of modem that connects your PC to the Meridian Mail server.

Note: All the default settings in this dialog box are configured to the values of the U.S. Robotics 14.4 Roadster modem.



Field descriptions

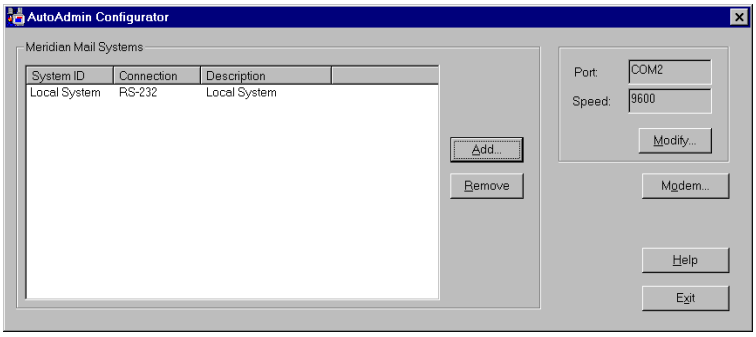
The following table describes the boxes and buttons of the Modem Commands window.

Dial Prefix	
Description	Shows the prefix string for dialing the modem's phone number.
Default	ATDT
Hangup Prefix	
Description	Shows the prefix string for terminating the call.
Default	+++
Dial Suffix	
Description	Shows the suffix string for dialing the modem's phone number.
Default	Blank
Hangup Suffix	
Description	Shows the suffix string for terminating the call.
Default	ATH
Initialization	
Description	Shows the modem initialization string that identifies the specific modem for the PC.
Maximum length	50 alphanumeric characters
Default	AT&F1
OK	
Description	Closes the dialog box and saves the changes.
Cancel	
Description	Closes the dialog box without saving the changes.
Help	
Description	Opens the online help for this dialog box.

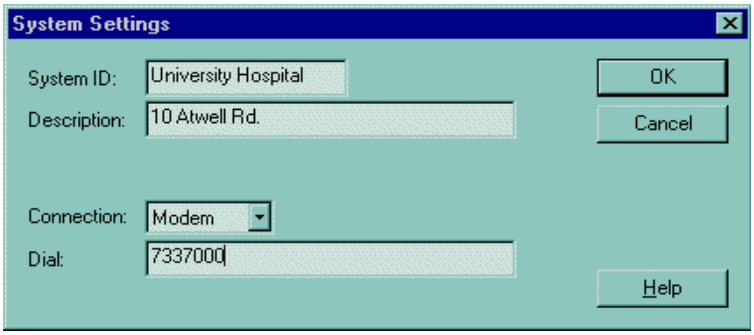
Procedure: Adding a connection to a Meridian Mail system

To add a local or remote Meridian Mail system to the AutoAdmin utility, follow these steps.

Step	Action
1	Open AutoAdmin Configurator. **Result:** The following window is displayed (your display may differ).



2	In the Configurator dialog box, click Add. **Result:** The following window appears.

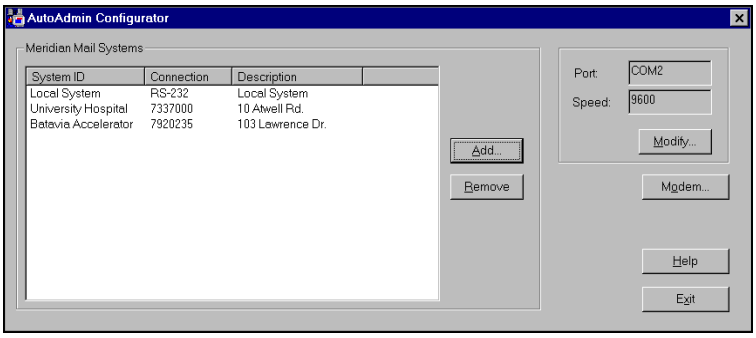


3	Type the System ID and the Description in the system settings window.
4	If you select Modem in the Connection box, type the dial number for the modem connection in the Dial box.
5	When you are done, click OK to save and repeat the steps to add more locations, or Cancel to go back to the Configurator dialog box without saving your settings.
6	Click Exit to end Configurator.

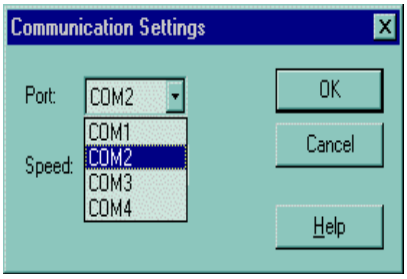
Procedure: Changing settings in Configurator

To change your PC to Meridian Mail (or modem) communication settings, follow these steps.

Step	Action
1	Open AutoAdmin Configurator. **Result:** The following window is displayed (your display may differ).



2	In the Configurator dialog box, click Modify, or double-click the System ID you wish to modify. **Result:** The Communications Settings dialog box appears.
3	Select the port setting from the Port list. **Result:** The following screen is displayed:



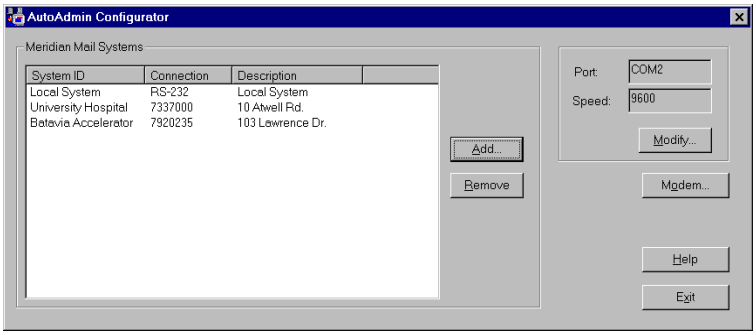
4	To select the baud rate of the connection, select from the Speed list.
5	Click OK to save the settings and return to the Configurator dialog box , or cancel to bring up the Configurator dialog box without saving your newly entered settings.

Procedure: Changing the modem settings

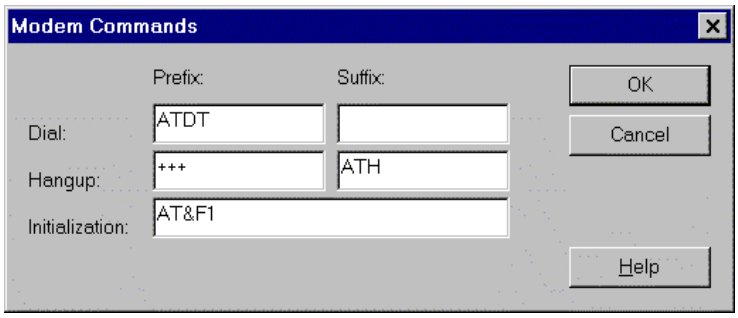
To change your modem settings, follow these steps.

Note: Change the settings for the modem connection if you have changed the modem or if you are not using the default U.S. Robotics modem. Refer to the modem's technical manual.

Step	Action
1	Open AutoAdmin Configurator. **Result:** The following window is displayed (your display may differ).



2	In the Configurator dialog box, click Modem. **Result:** The following screen is displayed (your screen may differ).



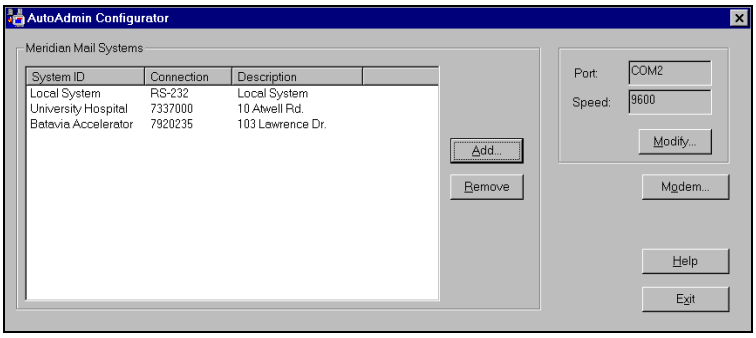
3	In the Modem Commands dialog box, enter the Dial Prefix.
4	To define the suffix string to dial the modem, enter the Dial Suffix.
5	Repeat steps 3 and 4 for the Hangup Prefix and Suffix.

Step	Action
6	To define the initialization string that identifies the particular modem you are using, enter the initialization string.
7	When you have completed your entries, click OK to save the settings or click cancel if you don't want to save. **Result:** In either case, you are returned to the Configurator dialog box.
8	Click Exit to end configurator.

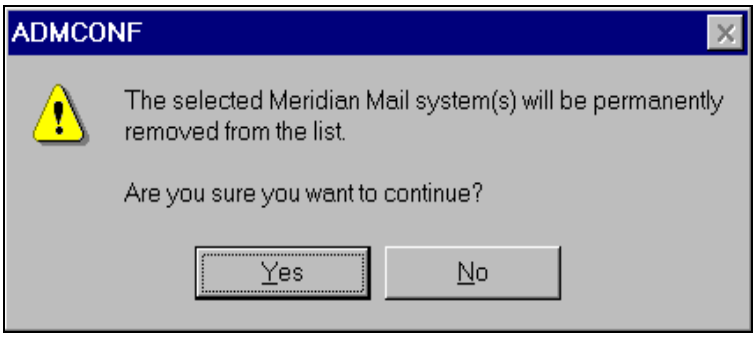
Procedure: Removing a connection to a Meridian Mail system

To remove a local or remote Meridian Mail system from the AutoAdmin utility follow these steps..

Step	Action
1	Open AutoAdmin Configurator. **Result:** The following window is displayed (your display may differ).



2	Click the System ID of the site you wish to remove, then click Remove. **Result:** The following screen is displayed.



Note: More than one system can be removed from the list at one time by selecting all the systems to remove. At least one system has to remain configured.

3	To continue, click Yes, to abort the remove, click No.

AutoAdmin Utility

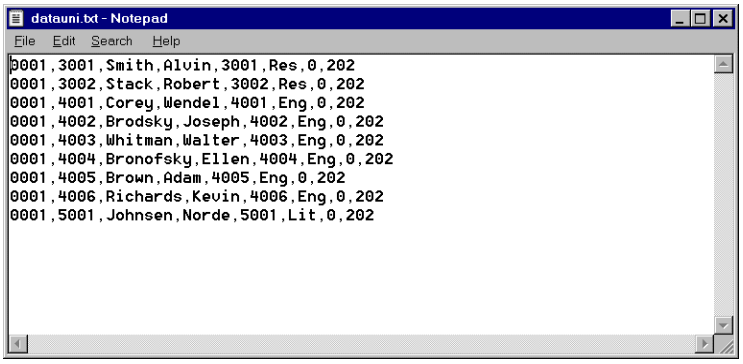
Overview

The Meridian Mail AutoAdmin Utility is the interface that allows you to take large amounts of data from a central system and channel it to your Meridian Mail systems.

Starting with text files

The first thing needed by the AutoAdmin Utility is data in the form of a text file. Simply stated, the text file is used to input the information about mailboxes. The text file is composed of information that an administrator deems necessary for mailbox identification and mailbox access.

Example:
The following illustration lists the data contained in a text file. Each piece of data is separated by a delimiter, in this case a comma. The tags used for this data are (in order of appearance): CN, MN, LN, FN, D1 DP, PL, VI.



Tags

AutoAdmin uses mnemonics or tags to identify the pieces of information entered in the text file.

The following table lists the tags with their descriptions, string length, and values/types.

Local voice user fields	Tags	Length	Valid values/types
Mailbox number	MN	18	Numeric only
Last name	LN	41	Alphanumeric string
Customer number	CD	4	1 to 2000
Mailbox password	MP	16	Numeric only
Location prefix	LP	10	Numeric only
Volume ID	VI	3	1, 2, 202, 203 to 210
First name	FN	21	Letters, numbers, blanks (must be greater than one character, if entered)
Initials	IN	5	Letters and numbers
Department	DP	31	Any string
Class of service	CS	3	1 to 15
Primary DN	PD	30	Numeric only
Extension DN 1	D1	30	Numeric only
Extension DN 2	D2	30	Numeric only
Extension DN 3	D3	30	Numeric only
Extension DN 4	D4	30	Numeric only
Extension DN 5	D5	30	Numeric only
Extension DN 6	D6	30	Numeric only
Extension DN 7	D7	30	Numeric only
Revert DN	RD	30	Numeric only
MWI DN	MD	30	Numeric only
MWI Link	ML	2	0 (for first MWI link); 1 (for second) and so on ...

Local voice user fields	Tags	Length	Valid values/types
Name dialable by external callers	ND	1	1 for true 0 for false
Logon status	LS	1	1 for true 0 for false
Monitor mailbox during monitoring period	MO	1	1 for true 0 for false
Volume level	VL	1	1 for true 0 for false
Preferred language	PL	1	0 (for first language); 1 (for second) and so on ...
Hospitality user class	HC	1	1 for guest 0 for staff
New mailbox number	NM	18	Numeric only
New location prefix	NP	10	Numeric only

Definitions of the applied commands

The following commands are used to perform bulk file requests:

- Add mailbox
- Add/replace mailbox
- Remove mailbox
- Update mailbox

Add mailbox

The Add mailbox command allows the user to perform bulk additions to a local or remote Meridian Mail system. Only one system can be added to at a time.

Add/replace mailbox

The Add/replace mailbox command allows the user to delete all mailboxes if they exist, and information associated with the mailboxes such as greetings, saved messages, personal verifications, and cabinet profiles. The mailbox will then have new information from the text file added to it.

Remove mailbox

The Remove mailbox command is used to delete mailboxes that are listed in the text file.

Update mailbox

The Update mailbox command is used to add new information to each mailbox in the text file. This command does not delete the user profile.

The AutoAdmin window

Overview

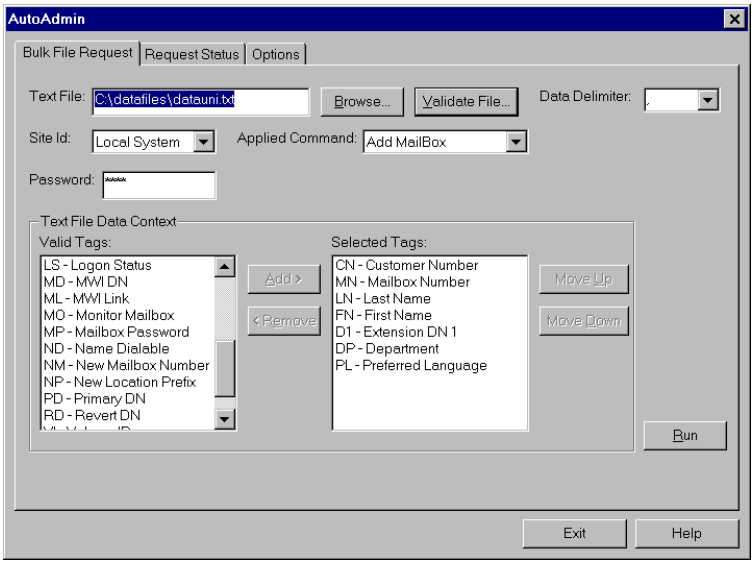
The AutoAdmin window is made up of three tabs

- Bulk file request (default window)
- Request status
- Options

Bulk file request window

The following illustrates the Bulk File Request window.

.



Field descriptions

This table describes the boxes and buttons in the Bulk File Request window.

Text File	
Description	Displays the path and the text file being used
Maximum length	None
Default	None
More information	See “Starting with text files” on page B-21.

Validate file	
Description	This button checks the syntax of the text file. The results of a validation are displayed in the request status window.
More information	See “Request status window” on page B-28.

Data delimiter	
Description	Uses a one-character delimiter that divides the data in the text file
Example	1,555,Smith,Executive
Types	, (comma), tab, /, \, space
Default	, (comma)

Site ID	
Description	This box allows the user to select the site ID of the Meridian Mail system used in the bulk file request. The sites are presented in alphabetical order.
Default	Local System
More information	See “AutoAdmin Configurator” on page B-12.

Applied command	
Description	This box allows the user to select the appropriate operation on the selected text file. The operations are • Add Mailbox • Add/Replace Mailbox • Remove Mailbox • Update Mailbox
Default	Add mailbox
More information	See “Definitions of the applied commands” on page B-23

Password	
Description	When clicked on, this box allows the user to enter a password. The password is indicated by asterisks when typing.
Maximum length	16 characters
Minimum length	The default minimum is 6, but this can be changed with procedures described in **Password Chapter**.

Text File Data Context - Valid tags	
Description	This box lists all the tags that can be used to do a bulk file request.
Default	None

Selected Tags	
Description	This box lists all the tags that will be used to define the mailbox during the bulk file request.
Default	None

Add>	
Description	This button allows the user to add tags to the Selected box. Simply highlight the required tag(s) and click the Add button.

<Remove	
Description	This button allows the user to remove tags from the Selected box. Simply highlight the required tag(s) and click the Remove button.

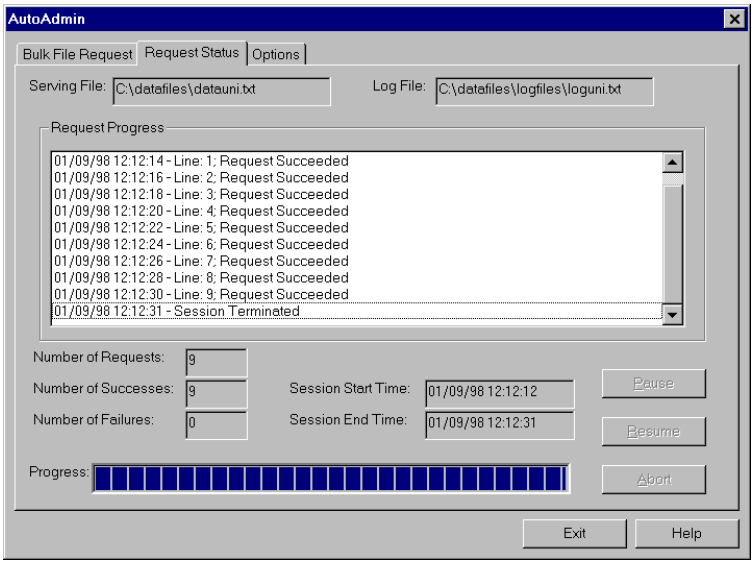
Move Up	
Description	This button allows the user to position the tags by moving them up in the Selected listing. Simply highlight the required tag and click the Move up button.

Move Down	
Description	This button allows the user to position the tags by moving them down in the Selected listing. Simply highlight the required tag and click the Move down button.

Run	
Description	Once the file has been validated, click Run to perform the chosen Applied Command.
Exit	
Description	This button closes down AutoAdmin. If the connection to Meridian Mail is still active, then AutoAdmin cannot be closed down.
Help	
Description	This button provides the user with online help.

Request status window

The following illustrates the Request Status window.



Field descriptions

This table describes the boxes and buttons associated with the request status window.

Serving File	
Description	This box provides the user with the path and name of the file that is presently being run by Bulk File Request and the applied command. If no file is being run, “No file specified” appears in the box.
Default	None
Log File	
Description	This box provides the user with the log file that is used to store verification, errors, and run data. If no file is being used to log the events, “No file specified” appears in the box.
Default	None
Request Progress	
Description	This box provides the user with a view of the text file being processed. For each line of data, a report is issued. If errors occur, a return code (RC) is issued for that line. The window can display only 30 lines of requests at one time.
Default	None
Number of Requests	
Description	Lists the total number of lines in the text file
Default	0
Number of Successes	
Description	Lists the lines that were processed without error
Default	0
Number of failures	
Description	Lists the number of lines not processed because of error
Default	0

Session Start Time	
Description	Displays the time that the connection to Meridian Mail was established
Default	Blank

Session End Time	
Description	Displays the time that the connection to Meridian Mail was terminated
Default	Blank

Pause	
Description	This button is used if the administrator needs to stop but not end the processing of data. **Example:** A large bulk add that is being processed can be paused if an error occurs that the operator wants to note.

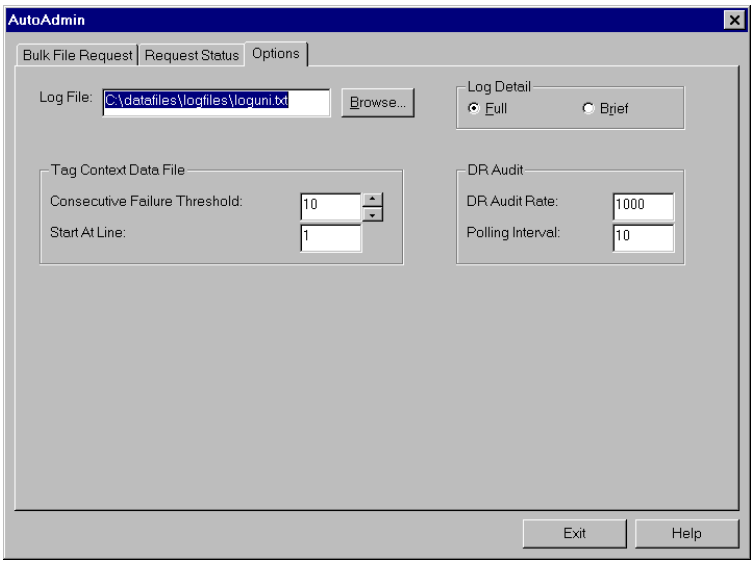
Resume	
Description	This button is used to start processing that has been paused.

Abort	
Description	This button causes AutoAdmin to finish the request currently being processed, then shuts down the connection to Meridian Mail.

Progress	
Description	This box shows the user roughly where the process is at in terms of completing the entire text file.

Options window

The following figure illustrates the options window.



Field descriptions

This table describes the boxes and buttons in the Options window.

Log file	
Description	This box allows users to type in a log file name of their choice. The default directory for the log file is the same location where the.exe for the utility is stored.
Default	None
Browse	
Description	This button is used to navigate to a specific log file in a specific directory or to specify where to create a log file.

Log Detail - Full	
Description	When selected, this button provides a full description of errors that may occur during validation and processing. **Example:** The following is a full error message: Line 1;Tag:MN Data: RC: 20306 INF: Invalid length
Default	Full

Log Detail - Brief	
Description	When selected, this button provides a brief description of information or errors that may occur during validation and processing. **Example:** The following is a brief error message: Line 13;Tag:D1 Data:5024 RC: 9528
Default	Full

Tag Context Data File - Consecutive Failure Threshold	
Description	This box allows the user to provide a number that will stop the processing of a text file after a number of consecutive failures have occurred. **Example:** If 10 is the threshold number, then the processing has to encounter 10 errors in a row, not failures adding up to 10.
Default	10
Range	Use the cursor buttons to increase or decrease the number within a range of 1-100, or use the keyboard to type in a number between 1 and 10,000.

Tag Context Data File - Start at Line	
Description	Shows the line in the text file from which processing will commence.
Default	1
Range	1 to 32,767

DR Audit - DR Audit Rate	
Description	Displays the number of individual requests that have been processed by AutoAdmin before Meridian Mail undergoes a directory audit (DR audit). A directory audit is necessary to maintain optimum processing rates. Processing of the text file is deferred until the audit is complete. The Meridian Mail directory will not be audited if there are 10 or fewer lines in the text file.
Default	1000
Range	500 to 2000

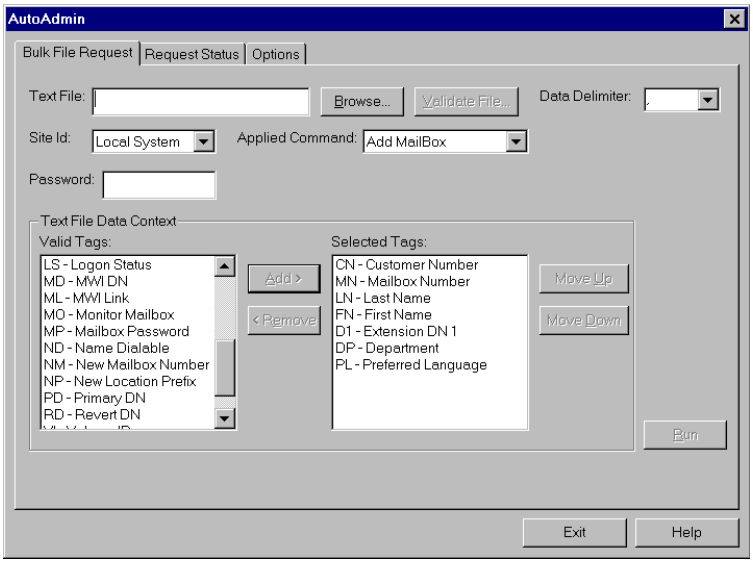
DR Audit - Polling Interval	
Description	Shows the time interval which AutoAdmin waits before checking on Meridian Mail to determine whether the directory audit is processing. The interval applies only after a DR Audit has begun. Once the audit is complete, AutoAdmin continues to process requests. **Note:** The log file will be available once the directory audit is complete.
Default	10 minutes
Range	5 to 30 minutes

Using Meridian Mail AutoAdmin

Procedure: Starting AutoAdmin

To start the Meridian Mail AutoAdmin utility,follow these steps..

Step	Action
1	Click the AutoAdmin icon and open AutoAdmin. **Result:** The following window is displayed.



2	Enter the path of the text file you will be using, or click on Browse and navigate to the appropriate file. When you locate it, double-click. **Result:** The path and the text file name appear in theText File box.
3	Click the Site box to select a site if you have more than one configured.

Step	Action
4	Click the Password box, and type in your Meridian Mail Customer Administrator password. **Note:** A new password will be required every time the site ID is changed.
5	If you wish to keep a log file of all processing, click the Options tab and enter a log file name in the Log File box, then return to the Bulk File Request window.
6	Select the operation you want to perform in the Applied Command box. Use the decision table below to find the procedure you require.

IF you want to ...	THEN go to ...
Add mailboxes	Adding mailboxes, page B-36
Add/replace mailboxes	Adding and replacing mailboxes, page B-40
Remove mailboxes	Removing mailboxes, page B-44
Update mailboxes	Updating mailboxes, page B-48

Procedure: Adding mailboxes

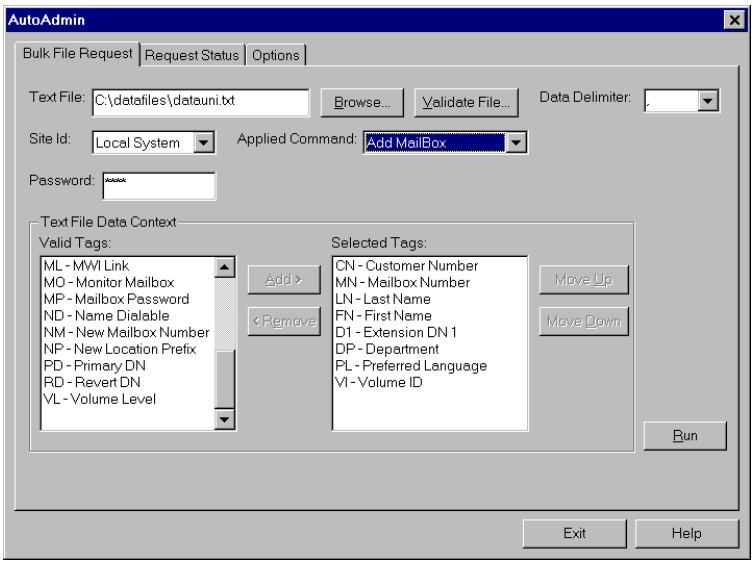
To add mailboxes through a bulk file request using AutoAdmin, follow these steps.

Note: The following procedure assumes you have created and selected an appropriate text file that can be used to process mailbox information, that you have typed in your password, and that you have a logfile to record your events. Refer to the procedure "Starting AutoAdmin" on page B-34 before proceeding with the following instructions

Starting Point: Applied Command window.

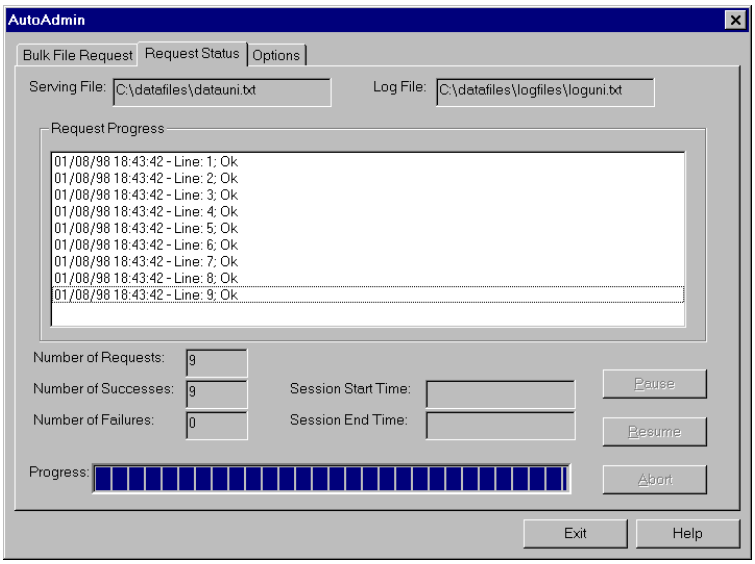
Step	Action
1	Select Add Mailbox.
2	Select the tags you require by first clicking on a desired tag in the Valid Tag box, then clicking the Add button. **Note:** Mandatory tags for adding a mailbox are MN and LN. LN is not mandatory for adding guest mailboxes on an HVS system. For an NMS system, LP is required. **Result:** Each tag is added to the Selected Tag box.

Step	Action
	The following is an example of a screen after tag selections have been completed. Your display may not match due to different requirements.



3 Once all required tags have been selected, click the Move Up or Move Down button to sequence the tags to reflect the text file entries.

Step	Action
4	Click the Validate File button to check that the syntax of the text file you are using is correct. **Result:** The following screen is displayed in the Request Status window (your display may differ).



5

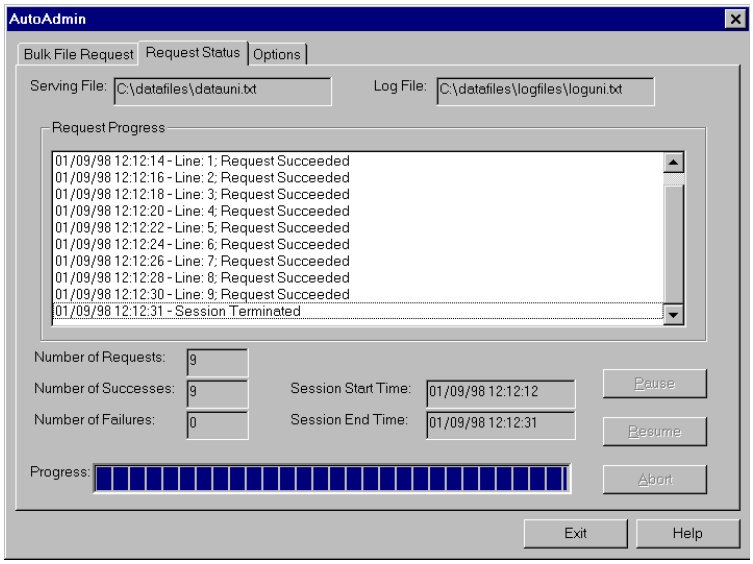
IF your text file is ...	THEN go to ...
invalid	step 6
valid	step 8

6 Read the error message and check the return codes, if any, in the error messages. Look up any RCs in the SEERs Guide (NTP 555-7001-510).

7 Make the required corrections and click Validate File again. Go to step 5.

Note: Most times the error is simply too much data and not enough tags or vice versa, or a delimiter problem.

Step	Action
8	Click Run. **Result:** The following screen is displayed (your display my differ).



9	If you need to perform other bulk file requests with AutoAdmin, see page B-35, step 6.

Procedure: Add/ replace mailboxes

To add/replace mailboxes through a bulk file request using AutoAdmin, follow these steps.

Note: The following procedure assumes you have created and selected an appropriate text file that can be used to process mailbox information. Refer to the "Procedure: Starting AutoAdmin" on page B-34 before proceeding with the following instructions.

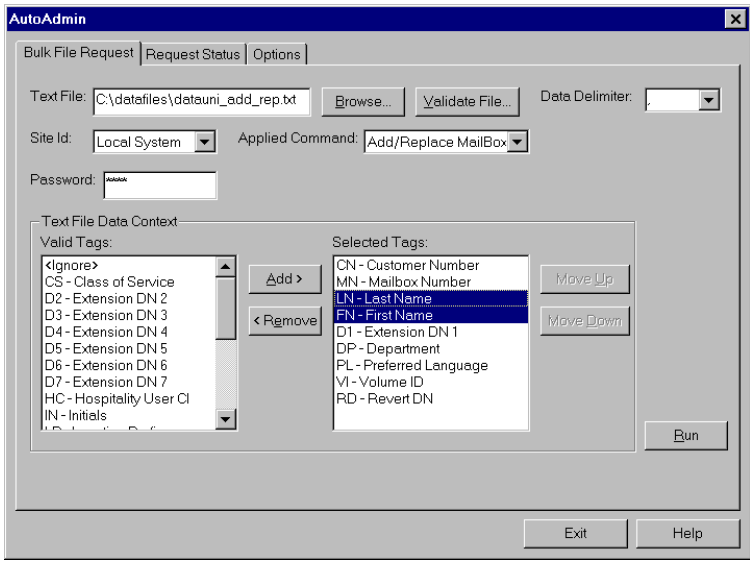
CAUTION

Risk of data loss
Replaced mailboxes cannot be recovered! Use this procedure with care.

Starting Point: Applied Command window

Step	Action
1	Select Add/Replace Mailbox.
2	Select the tags you require by first clicking on a desired tag in the Valid Tag box, then clicking the Add button. **Note:** Mandatory tags for adding/replacing a mailbox are MN and LN. LN is not mandatory for adding guest mailboxes on an HVS system. For an NMS system, LP is required as well. **Result:** The tag is added to the Selected Tag box.

Step	Action
	The following is an example of a screen after tag selections have been completed. Your display may differ due to requirements.

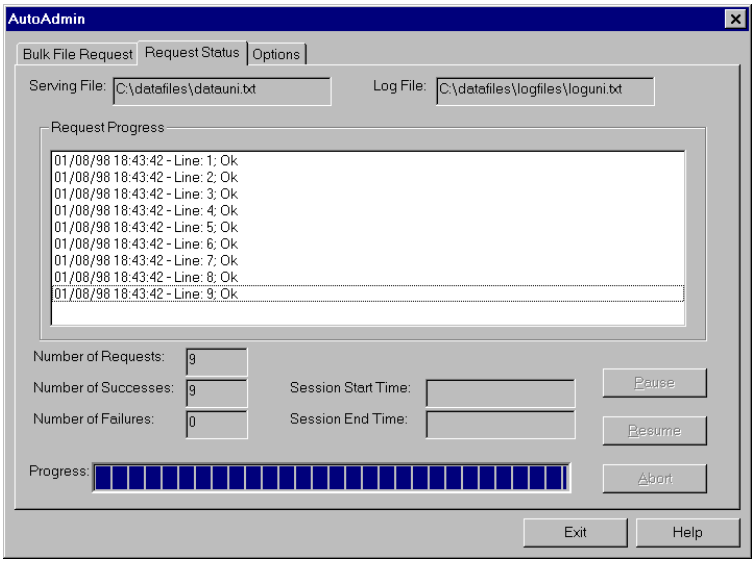


3 Once all required tags have been selected, click the Move Up or Move Down button to sequence the tags to reflect the text file entries.

4 Click the Validate File button to check that the syntax of the text file you are using is correct.

Result: The following screen is displayed in the Request Status window (your display may differ).

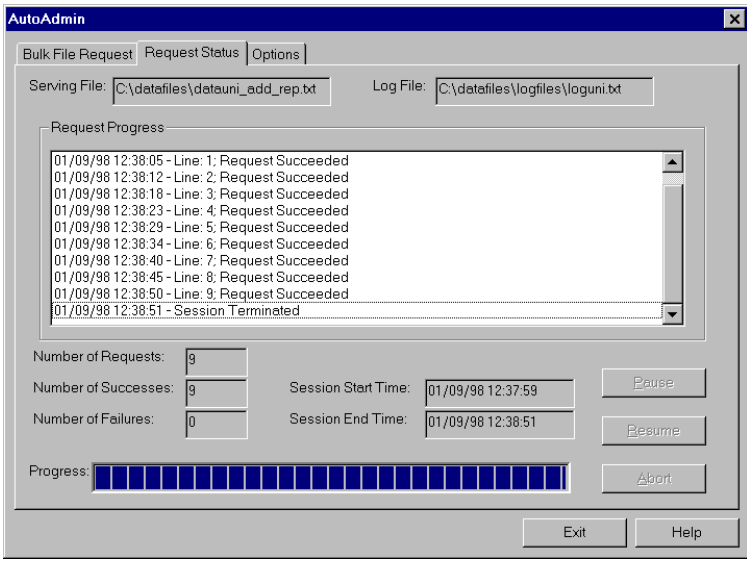
Step Action



5 Use the following decision box for validation.

IF your text file is ...	THEN go to ...
invalid	step 6
valid	step 8

Step	Action
6	Read the error message and check the return codes, if any, in the error messages. Look up any RCs in the SEERs Guide (NTP 555-7001-510).
7	Make the required corrections and click Validate File again. Go to step 5. **Note:** Most times the error is simply too much data and not enough tags, or vice versa, or a delimiter problem.
8	Click Run. **Result:** The following screen is displayed (your display may differ).



9	If you need to perform other bulk file requests with AutoAdmin, see page B-35, step 6.

Procedure: Removing Mailboxes

To remove mailboxes through a bulk file request using AutoAdmin, follow these steps.

Note: The following procedure assumes you have created and selected an appropriate text file that can be used to process mailbox information. Refer to the "Procedure: Starting AutoAdmin" on page B-34 before proceeding with the following instructions.

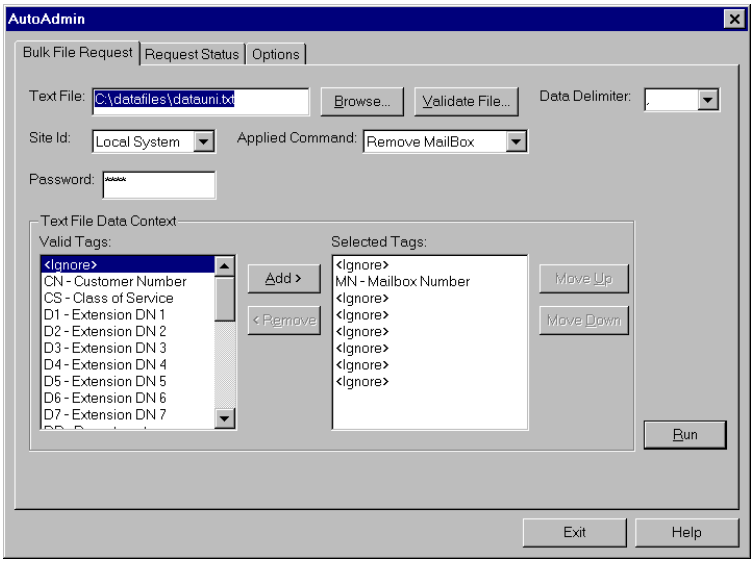
CAUTION

Risk of data loss
Removed mailboxes cannot be recovered! Use this procedure with care.

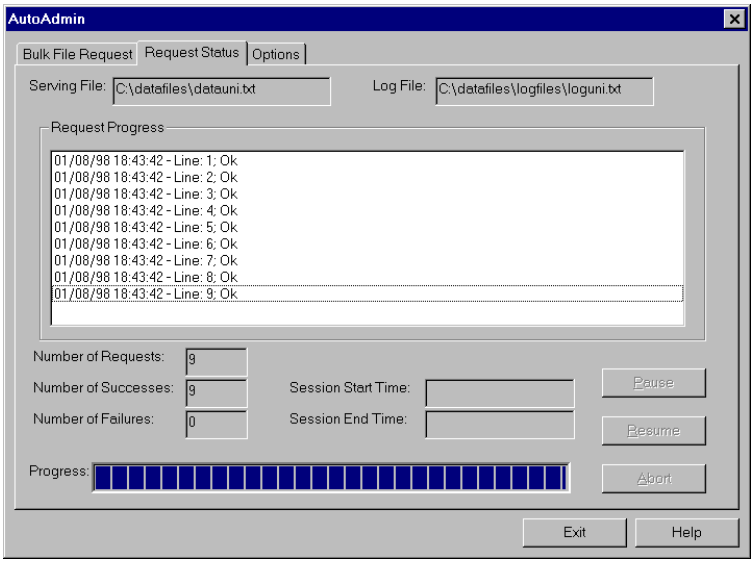
Starting Point: Applied Command window

Step	Action
1	Select Remove Mailbox.
2	Select the MN tag. For an NMS system, select LP as well. **Note:** If information other that the MN is entered in the text file, you can use the <Ignore> tag for each delimited piece of data in the text file. Select <Ignore> tags as necessary. **Result:** The tags are added to the Selected Tag box.

Step	Action
	The following is an example of a screen after tag selections have been completed. Your display may differ.



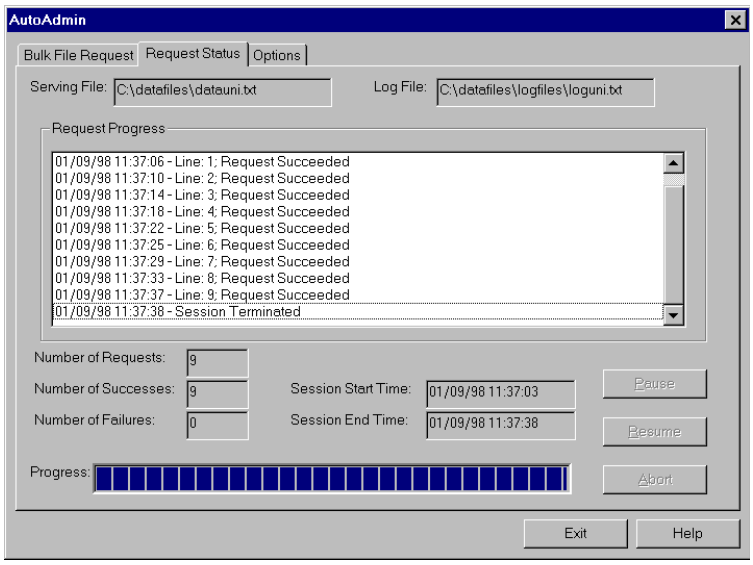
Step	Action
3	Click the Validate File button to check that the syntax of the text file you are using is correct. **Result:** The following screen is displayed in the Request Status window (your display may differ).



4

IF your text file is ...	THEN go to ...
invalid	step 5
valid	step 7

Step	Action
5	Read the error message and check the return codes, if any, in the error messages. Look up any RCs in the SEERs Guide (NTP 555-7001-510).
6	Make the required corrections and click Validate File again. Go to step 4. **Note:** Most times the error is simply too much data and not enough tags or vice versa, or a delimiter problem.
7	Click Run. **Result:** The following screen is displayed (your display may differ).



8	If you need to perform other bulk file requests with AutoAdmin, see page B-35, step 6.

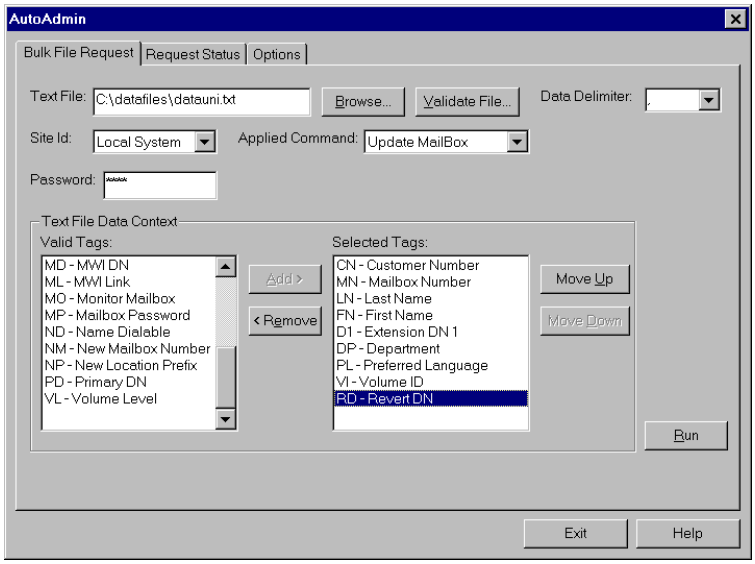
Procedure: Updating mailboxes

To update mailboxes through a bulk file request using AutoAdmin, follow these steps.

Note: The following procedure assumes you have created and selected an appropriate text file which can be used to process mailbox information. Refer to the "Procedure: Starting AutoAdmin" on page B-34 before proceeding with the following instructions.

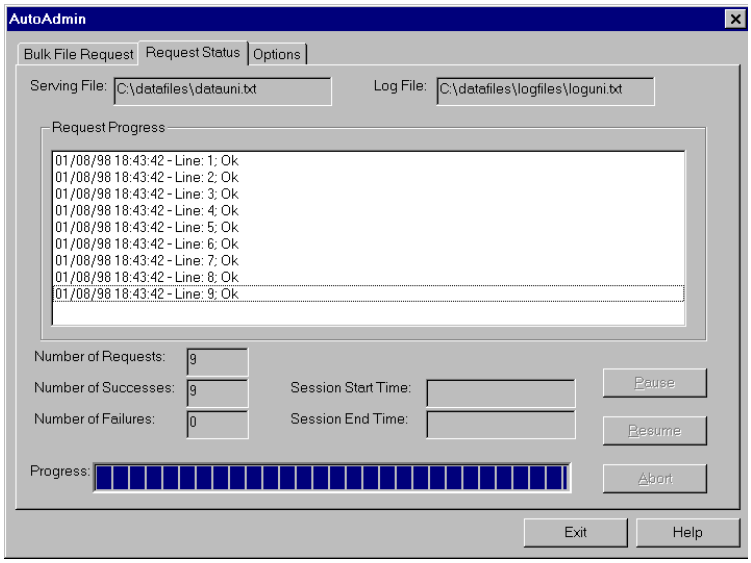
Starting Point: Applied Command window

Step	Action
1	Select Update Mailbox.
2	Select the tags you require by first clicking on a desired tag in the Valid Tag box, then clicking the Add button. **Note:** Mandatory tags for udating a mailbox are MN and LN. LN is not mandatory for adding guest mailboxes on an HVS system. For an NMS system, LP is required as well. **Result:** The tag is added to the SelectedTag box. The following is an example of a screen after tag selections have been completed. Your display may differ due to requirements.



3	Once all required tags have been selected, click the Move Up or Move Down buttons to sequence the tags to reflect the text file entries.

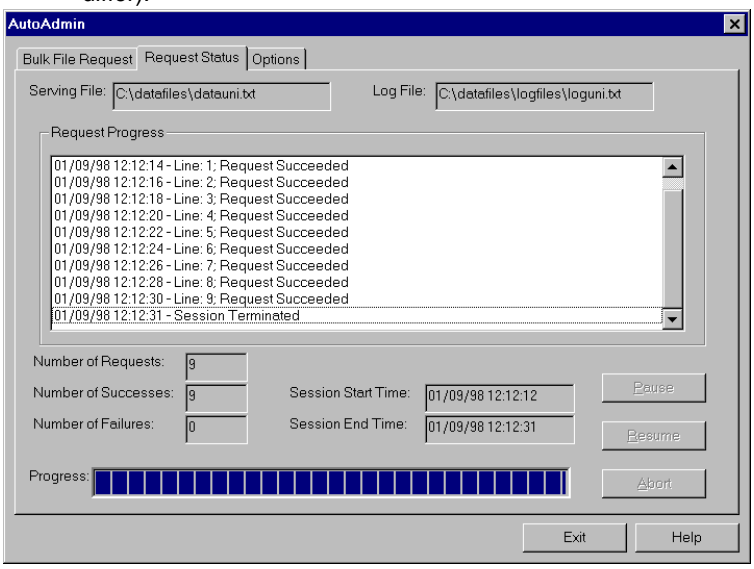
Step	Action
4	Click the Validate File button to check that the syntax of the text file you are using is correct. **Result:** The following screen is displayed in the Request Status window (your display may differ).



5

IF your text file is ...	THEN go to ...
invalid	step 6
valid	step 8

Step	Action
6	Read the error message and check the return codes, if any, in the error messages. Look up any RCs in the SEERs Guide (NTP 555-7001-510).
7	Make the required corrections and click Validate File again. Go to step 5. **Note:** Most times it is simply too much data and not enough tags or vice versa, or a delimiter problem.
8	Click Run. **Result:** The following screen is displayed (your display may differ).



9	If you need to perform other bulk file requests with AutoAdmin, see page B-35, step 6.

Troubleshooting

Overview

In general, if any problems with processing the text files, the user is provided with return codes that are located in the SEERs Guide (NTP 555-7001-510).

Start-up problems

The following information provides possible solutions to start-up problems in AutoAdmin.

AutoAdmin does not start up properly

Check the AutoAdmin folder on your PC, and open it. The following files should be in it:

- cmadf.txt
- cma.dll
- datafile.dll
- Gcl52fw.dll
- pctc.dll
- poweradm.exe

If any of these files are missing from the AutoAdmin folder, reinstall AutoAdmin.

Troubleshooting

The following table provides remedies to problems with AutoAdmin start-up.

Symptom	Error indication	Remedy
AutoAdmin does not start up properly	During start-up, an error box with “data file failure” message appears.	Reinstall AutoAdmin.
	Program starts with error box message: “A required .DLL file, xxx.DLL not found”.	Reinstall AutoAdmin.
	Cannot start AutoAdmin or application with no content	Close other Windows applications.

Symptom	Error indication	Remedy
Persistent communication timeout	Times out on every request	Check cable and redo command.
	Appropriate error codes returned indicating send or receive timeout	Check cable and redo command.
	Both PC COMM port and Meridian Mail dataport are not set up at the same speed	Match PC COMM and Meridian Mail dataport speeds.
	Cable or modem problem	Check both cable connection and modem; redo command

Index

A

ACCESS
  adding a VSDN, 24-36
  class for VSDN, 24-36
accesses to services, 31-13
  numbers of, 31-27
ACD DN
  in CAT, 28-52
Add Local Voice User screen
  accessing, 8-11
adding, 24-16
addressing by name, 20-40
administration context
  setting default for NMS, 8-9
administration menus
  choosing items from, 2-30
administration screens
  layout of, 2-31
  moving around in, 2-33
  selecting an entire line, 2-37
administrator capability
  enabling for mailboxes, 26-19
  locate users with, 8-60
AdminPlus password
  changing, 16-8
agent queues
  adding agents to a queue, 23-58
  configuring (high-level procedure), 23-36
  creating, 23-53
  modifying the CAT after moving agents, 23-64
  modifying the MAXP value, 23-57
  moving agents, 23-62
  removing agents, 23-63
alarms
  description of types, 29-9
  silencing, 29-13
  status of, 28-12, 29-10
allocated ports
  number of, 28-51
AMIS
  act on AMIS initiator tone, 25-9
  adding a VSDN, 24-29
  applying restriction/permission lists, 6-121
  connect time, 31-39
  messages
    failed attempts, 31-39
  number of messages delivered, 31-38
  number of messages received, 31-38
  open network messages
    allowing users to receive, 26-28, 26-46
    allowing users to send, 26-28, 26-47
    restriction/permission lists, 26-29, 26-47
  statistics, 31-38
AMIS networking detail report
  analyzing, 31-40
announcements
  adding a VSDN, 24-41
  finding, 22-11
  maximum prompt sizes, 25-8
  recording, 5-44
announcing callers, 26-40
area/city code
  for local system, 17-35
  translation tables, 17-63
assigning, 6-15
  classes of service to users, 26-64
assigning classes of service to the system, 13-14, 26-49
attendant DN
  modifying, 13-17
audit trail data
  enabling collection of, 31-23, 33-7

number of days stored, 31-23
number of days to store, 33-6
stopping collection of, 33-6
when to stop collection, 31-23
audit trail reports
fax on demand
analyzing, 33-37, 33-43
generating, 33-33
printing, 33-34
authorization code conditionally last
on the M1
implementing, 6-63
authorization codes
on the M1
implementing, 6-24
AutoAdmin, 4-36, 13-11
Bulk file request window, B-25
Connecting Meridian Mail and the PC, B-3
Installation procedure, B-5
Modem Commands window, B-14
Options window, B-31
PC minimum hardware requirements, B-4
Procedure
Add/replace mailboxes, B-40
Adding a connection to a Meridian Mail system procedure, B-16
Changing settings in Configurator, B-17
Changing the modem settings, B-18
Removing a connection to a Meridian Mail system, B-20
Starting AutoAdmin, B-34
Updating mailboxes, B-48
Request status window, B-28
Supported platforms, B-3
System configuration, B-4
Upgrade procedure, B-10
AutoAdmin Configurator, B-12
autologon
for hospitality voice messaging, 24-19
automatic logon to mailboxes, 26-18, 26-36
automatic play of user messages, 26-20

B

backups
checking status of, 15-51
deleting a scheduled backup, 15-45
scheduling, 15-44
selective
of all multimedia services, 15-35
of all users, 15-25
of all users in a department, 15-33
of all users in a particular COS, 15-31
of all users on a volume, 15-29
of individual multimedia services, 15-37
of individual users, 15-27
restoring from, 15-56
to disk
partial, 15-40
to tape
full, 15-19
partial, 15-21
basic service channels
features support by, 23-15
basic service session profile, 24-81
billing DN
defining, 20-52
how used, 20-51
broadcast mailbox
description, 20-47
personal verification
description, 5-5
recording, 5-37, 20-49
setting up, 20-49
broadcast messages
allow users to compose and send, 26-19, 26-37
locate mailboxes with broadcast capability, 8-59
location-specific broadcast messages, 5-40, 5-41
network broadcast messages, 5-39, 5-41, 26-19
locate mailboxes with capability, 8-60
recording and sending, 5-41
bulk provisioning
data sets
assembling, 34-11
copying to tape, 34-31
creating, 34-17
deleting, 34-25
modifying, 34-19
printing, 34-23
printing a list of, 34-24
viewing, 34-22
data sets from tape, 34-41
printing data conflicts, 34-46
viewing data conflicts, 34-45

business hours default, 25-9
busy
notifying callers of, 26-21, 26-37

C

calculating centi-call seconds, 30-27
calculating required OM disk space, 31-16
call answering, 23-18, 24-17
allowing login from, 26-36
applying restriction/permission lists, 6-111
call transferred to mailbox, 5-8
disabling messages from, 26-38
greetings played during, 5-7
language prompts are played in, 20-17, 20-23
messages
maximum length of, 26-22, 26-39
no answer, 5-8
user busy, 5-9
call answering greeting
description, 5-4, 20-29
recording, 20-30
recording from a telset, 5-20
call back
using call sender, 20-60
enabling/disabling, 20-61
call back dialing restrictions
for fax callback services, 24-104
for fax item maintenance, 24-111
call back extension prompt
for callback fax services, 24-102
call back fax delivery, 24-100
call back number treatment
dial as entered, 24-76
ESN, 24-77
for callback fax services, 24-103
for fax item maintenance, 24-111
international, 24-75
national, 24-75
call back options
specifying for fax services, 24-105
call forward all calls
on the M1
implementing, 6-41
call forward external deny
on the M1
implementing, 6-42
call forward to trunk access code
on the M1
implementing, 6-43
call sender
enabling, 26-41
external
applying restriction/permission lists, 6-120
description, 20-60
enabling/disabling, 20-61
restriction/permission lists, 26-24, 26-42
caller choice fax delivery, 24-100
callers
announcing, 26-40
capturing external CLIDs, 17-36
cards
enabling/disabling, 28-27
location, 28-24
number, 28-24
running diagnostics, 28-28
status of, 28-21, 28-26
centi-call seconds
calculating, 30-27
changing the display options, 21-9
Channel Allocation Table
accessing, 28-48
modifying, 28-59
channel allocation table
dedicated channels
overview, 28-56
channel capability
fax item maintenance, 24-110
for session profiles, 24-93
channel usage
statistics, 31-23
channel usage detail report
analyzing, 31-25
channels
dedicating because of mixed port types, 23-24
dedicating to services, 23-26
identifying installed channels, 23-20
checking the installed channels, 23-20
choosing the default language, 20-17
city code. See area/city code
classes of service
adding, 26-10
assigning to the system, 13-14, 26-49
assigning to users, 8-21, 26-64
backing up all users in a COS, 15-31
conversion utility, 26-66

converting from user models, 7-23
creating a personal COS for a user, 8-22, 26-65
deleting, 26-59
finding, listing, printing, 26-51
for dial pulse users, 26-12
modifying, 26-54
on the M1, 6-15
personal, 8-22
reassigning users, 8-73
CLIDs
default translation, 17-36
external
capturing, 17-36
format of CLIDs to monitor, 6-130
monitoring, 6-130, 6-159
code restriction
on the M1
implementing, 6-35
collecting
audit trail data, 31-23, 33-7
session trace data, 31-22
traffic data, 31-21
user usage data, 31-22
compose capability
enabling, 26-44
composed messages
allowing users to receive, 26-23, 26-39
maximum length, 26-16, 26-34
configuring the switch
adding agents to a queue, 23-58
configuring agent queues (high-level procedure), 23-36
configuring dummy queues (high-level procedure), 23-37
creating a dummy queue, 23-60
creating an agent queue, 23-53
high-level procedure, 23-33
modifying the CAT after moving agents, 23-64
modifying the MAXP value in the queue, 23-57
moving agents (high-level procedure), 23-62
removing agents, 23-63
controlled class of service
on the M1
implementing, 6-31
conversion utility
converting from user models to COS, 26-66
country code
for local system, 17-35
courtesy disable
ports, 28-18
courtesy down of system, 28-15
courtesy enable
ports, 28-18
cover sheet
customizing
for fax services, 24-108
for fax items, 24-103
custom revert
applying restriction/permission lists, 6-107
description, 8-26
restriction/permission lists, 26-29, 26-48
custom session profile, 24-109
customizing session profiles, 24-91
fax item maintenance, 24-112
for fax items, time-of-day controllers, voice menus, 24-95

D

data conflicts
printing, 34-46
viewing, 34-45
Data Port Configuration screen
accessing, 27-23
data ports
printing data port information, 27-47
viewing, 27-25
data sets
assembling, 34-11
bulk provisioning from tape, 34-41
copying to tape, 34-31
creating, 34-17
deleting, 34-25
modifying, 34-19
printing, 34-23
printing a list of, 34-24
viewing, 34-22
data storage
percent used, 14-11
dedicated ports
blocking inbound calls, 23-40
blocking outbound calls, 23-43
creating fully dedicated ports, 23-49

dedicating channels
because of mixed port types, 23-24
to services, 23-26
dedicating ports. See dedicating channels
default administration context
setting, 8-9
default dialing prefixes
configuring, 17-37
default language
choosing, 20-17
multilingual systems, 20-13
secondary, 20-19
Definition
Add mailbox, B-23
Add/replace mailbox, B-23
Remove mailbox, B-24
Update mailbox, B-24
Definitions of the applied commands, B-23
delaying delivery of voice messages, 20-40
deleting read messages, 20-57
delivery of network messages
delivery priorities, 20-53
delivery option
for fax services, 24-100
delivery to non-user
applying restriction/permission lists, 6-118
enabling in COS, 26-27, 26-45
detail outcalling audit trail report
analyzing, 33-28
diagnostics
analyzing results of, 28-82
changing the schedule, 28-81
for a disk or disk pair, 28-72
for cards, 28-28
start time, 28-79
dial as entered call back number treatment, 24-76, 24-103
dial pulse
support for, 26-35
dialing by name, 20-40
dialing prefixes
configuring defaults, 17-37
dialing restrictions
for fax callback services, 24-104
for fax item maintenance, 24-111
on the M1
assigning, 6-15
dialing translations
troubleshooting, 17-77
dialing translations. See also translation tables
directory entry users
adding, 10-7
deleting, 10-18
description, 7-9
finding, 10-12
modifying, 10-16
printing, 10-15
recording a personal verification, 10-8
viewing, 10-16
viewing a list of, 10-14
DISA
on the M1
implementing, 6-84
disabing
remote terminal access (non-EC), 3-17
disabling
cards, 28-27
disk shadowing, 28-68
dsp ports
in range mode, 28-43
in single mode, 28-41
external call sender, 20-61
mailboxes, 6-144
name dialing and name addressing, 20-44
nodes, 28-17
ports
with courtesy enable, 28-18
remote terminal access (EC), 3-22
the system, 28-15
unused mailboxes, 6-148
disk, 28-66
diagnostics, 28-72
status of prime disk, 28-66
disk backups, 15-40
disk capacity
checking, 14-12
disk number
for unshadowed systems, 28-66
disk pair
diagnostics, 28-72
status of, 28-67
synching, 28-70
disk pair number
for shadowed systems, 28-66

disk shadowing
disabling, 28-68
disk pair number, 28-66
pair status, 28-67
re-enabling, 28-70
status of shadow disk, 28-67
disk space
calculating requirements for OMs, 31-16
disk status
checking, 28-63
disk usage
checking, 14-12
statistics, 31-53
disk usage detail report
analyzing, 31-54
display options
changing, 21-9
distribution
of volumes across nodes, 14-7
distribution lists
adding, 11-14
deleting, 11-27
description, 7-10
finding, 11-19
listing, 11-19
modifying, 11-23
personal vs. system, 7-10
prefix for personal lists, 20-46
printing, 11-25
recording a title, 11-15
DSP Port Status screen
accessing, 28-31
dsp ports
detailed view of status, 28-38
disabling/enabling in range mode, 28-43
disabling/enabling in single mode, 28-41
location of, 28-36
status, 28-14
status field, 28-36
viewing status of, 28-31
dual language prompting
configuring for call answering, 20-23
description, 20-19
enabling in COS, 26-17
secondary default language, 20-19
dummy queues
configuring (high-level procedure), 23-37
creating, 23-60
duration of mailbox lockout, 26-37

E

economy delivery of networked messages, 20-53
enabling
call sender, 26-41
cards, 28-27
compose capability, 26-44
delivery to non-user, 26-27, 26-45
disabled mailboxes, 8-92
dsp ports
in range mode, 28-43
in single mode, 28-41
external call sender, 20-61
mailboxes (MMUI), 6-144
mailboxes (VMUIF), 6-145
name dialing and name addressing, 20-44
nodes, 28-17
ports
with courtesy disable, 28-18
remote notification, 26-28, 26-45
traffic data collection, 31-21
update logging, 25-9
end time
for traffic period, 31-21
enhanced controlled class of service
on the M1
implementing, 6-32
entering information in fields, 2-36
Enterprise networking
act on Enterprise initiator tone, 25-9
adding a VSDN, 24-34
sharing a DN with a voice service, 24-35
sharing a DN with AMIS, 24-34
error messages
description, 2-41
escalating SEERs, 29-25
ESN call back number treatment, 24-77, 24-103
ESN dialing
default prefix, 17-35
exchange codes
in translation tables, 17-63
expiry date
for temporary absence greetings, 8-90

expiry warning
for mailbox passwords, 6-127
express messaging
adding the VSDN, 24-16
applying restriction/permission lists, 6-111
language prompts are played in, 20-17, 20-20
mailbox ID, 24-15
extension dialing
applying restriction/permission lists, 6-113
restriction/permission lists, 26-29
extension DNs, 8-24
defining, 8-33
external call sender
applying restriction/permission lists, 6-120
description, 20-60
enabling/disabling, 20-61
restriction/permission lists, 26-24, 26-42
external CLIDs
capturing, 17-36
external greetings
how used in call answering, 5-7
external logon
disabling, 6-128
external users
allowing users to send messages to, 26-25, 26-44

F

failed disk
replacing, 28-69
fax audit trail report
generating, 33-33
printing, 33-34
fax delivery detail report
analyzing, 31-50
fax item maintenance
adding a VSDN, 24-64
call back number treatment, 24-111
choosing a session profile, 24-64
customizing the session profile, 24-112
dialing restrictions, 24-111
language of service, 24-65
transmission error handling, 24-110
fax items
adding a VSDN, 24-62
choosing a session profile, 24-61
customizing a session profile, 24-95
maximum number of selections, 24-97
page limit for fax selections, 24-97
fax on demand
applying restriction/permission lists, 6-115
audit trail report
analyzing, 33-37, 33-43
automatic cover sheet, 24-103
call back dialing restrictions, 24-104, 24-111
call back extension prompt, 24-102
customizing a cover sheet, 24-108
customizing the session profile for fax item maintenance, 24-112
fax activity revert DN, 24-98
fax delivery option, 24-100
generating an audit trail report, 33-33
maximum number of fax selections, 24-97
page limit for fax selections, 24-97
page transmission error handling, 24-99, 24-110
printing an audit trail report, 33-34
sender fax number, 24-98, 24-110
sender name display, 24-104
specifying call back options in the session profile, 24-105
specifying fax service options in the session profile, 24-100
sponsor fax item ID, 24-98
statistics, 31-48
treat call back number as, 24-103, 24-111
fax selections
maximum number, 24-97
fax services
finding, 22-11
feature availability
Meridian Mail platforms, 2-46
MMUI and VMUIF, 2-49
features
supported by basic service channels, 23-15
supported by full-service multimedia channels, 23-17
supported by full-service voice channels, 23-16
verifying which are installed, 13-11
fields
entering information in, 2-36
selecting an option, 2-35

filtering SEERs, 29-34
by severity level, 29-31
by type, 29-32
by type and severity, 29-32
Find Local Voice Users screen
accessing, 8-49
Find Remote Voice Users screen
accessing, 9-28
finding
service definitions, 22-11
VSDNs, 22-9
flexible feature codes
on the M1
implementing, 6-33, 6-45
forced charge account
on the M1
implementing, 6-28
forcing regular password changes, 6-141
full backups to tape, 15-19
full mailboxes
calls rejected, 8-89
warning threshold
defining, 20-56
description, 20-55
full service ports
maximum number of, 28-51
full volume
stopping collection of audit trail data, 33-6
full-service multimedia channels
features supported by, 23-17
full-service multimedia session profile, 24-86, 24-89
full-service voice channels
features supported by, 23-16
full-service voice session profile, 24-83
function keys, 2-27

G

General Options screen
accessing, 13-3
generating
user usage reports, 32-7
getting help, 2-40
greetings
call answering, 20-29
recording from a telset, 5-20
external
finding users with greeting recorded, 8-60
for remote sites
recorded verification, 5-5
for VMUIF login
description, 20-33
recordin, 5-52
recording, 20-34
internal
finding users with greeting recorded, 8-60
personal
description, 5-4
maximum length, 26-16, 26-34
recording, 5-25
personal verification
description, 5-4
recording for a local voice user, 8-34
recording for a remote site, 5-35
recording for distribution lists, 5-31
recording for the broadcast mailbox, 5-37
recording from a telset, 5-28
recording from the administration terminal, 5-29
temporary absence
expiry date, 8-90
finding users with greeting recorded, 8-61
greetings service
adding a VSDN, 24-24
guest console
statistics, 31-60
guest console statistics report
analyzing, 31-61

H

Hacker Monitor, 6-151
hardware
monitoring, 18-6
hardware administration menu
accessing, 27-4
hardware location, 28-66
of disk, 28-66
header
replay with message, 26-40
help (online), 2-40
history file
on the M1
implementing, 6-82

holidays, 25-10
hospitality
selecting user class, 8-43
statistics, 31-57
user class, 8-41
hospitality voice messaging
adding the VSDN, 24-21
adding the VSDN for the post checkout mailbox service, 24-22
autologon, 24-19

I

incoming trunk group exclusion
on the M1
implementing, 6-72
initial password change
enforcing, 6-134
installating a system
using VMBA, A-17
installed features
verifying, 13-11
integrated mailbox administration, A-5
data translation tables, A-7
interface type
voice messaging, 26-31
interfaces
for the telset
description, 2-48
internal call forward
on the M1
implementing, 6-44
internal greetings
how used in call answering, 5-7
international call back number treatment, 24-75, 24-103
international dialing
default prefix, 17-34
invalid logon attempts
maximum number per mailbox, 6-127
maximum number per session, 6-126, 6-127
invalid selections
maximum number for voice services, 24-93

K

keeping copies of sent messages, 26-26
keypad functions, 2-27

L

language of service
for fax item maintenance, 24-65
for voice prompt maintenace, 24-52
languages
secondary default language, 20-19
defining, 20-24
setting up, 20-17, 20-24
user's preferred, 8-42, 20-13
overriding, 20-17
length of messages
maximum, 26-16, 26-34
limited access password
on the M1
implementing, 6-78
limited access to overlays
on the M1
implementing, 6-77
link
status of, 28-12
listing
classes of service, 26-51
local area/city code, 17-35
local country code, 17-35
local dialing
default prefix, 17-34
local system defaults
configuring, 17-37
local voice users
adding, 8-6
setting NMS administration context, 8-9
adding large numbers of
guidelines, 7-22
assigning to defined COSs, 8-21
checking status, 8-86
creating a personal COS, 8-22
creating a remote notification schedule
from the administration terminal, 8-37
deleting, 8-97
description, 7-7
distributing evenly over volumes, 7-19
entering user information, 8-18

finding, 8-70
hospitality user class, 8-41
listing, 8-70
modifying, 8-84
moving from a volume, 7-20
name dialing by external callers
allowing, 8-43
number of, 14-12
printing a list of, 8-70
reassigning to another COS, 8-74
recording a personal verification
from the administration terminal, 8-34
selecting preferred language, 8-43
shadowed systems
guidelines for adding, 7-21
volume level, changing, 8-43
without phones
creating a mailbox, 8-25
Location Name, 8-16
Location Prefix, 8-16
location-specific broadcast messages, 5-40, 5-41
locked out mailboxes
checking time of lockout, 8-88
duration of lockout, 26-37
logging on
from a MAT, 3-14
from a remote terminal (EC), 3-21
from a remote terminal (non-EC), 3-17
from the main administration terminal, 3-11
single terminal access
to M1 and Meridian Mail, 3-23
login
allowing from call answering, 26-36
login greeting
for VMUIF
recording/disabling, 5-52
logon
to mailboxes
automatic, 26-18
logon sessions
maximum invalid logon attempts, 6-126, 6-127
Logon/Status screen
redrawing, 3-5
logons
from external phones
disallowing, 6-128
to mailboxes
automatic, 26-36
checking last logon time, 8-88
invalid attempts, 8-56
minimum days since, 8-56
monitoring, 6-153
long distance dialing
default prefix, 17-34

M

mailbox
calls rejected if full, 8-58
mailbox ID
for express messaging, 24-15
mailbox logons
language prompts are played in, 20-16, 20-22
maximum invalid attempts per mailbox, 6-127
maximum invalid attempts per session, 6-126, 6-127
mailbox prompts
enabling delayed prompts, 26-16, 26-34
mailbox thru-dialing
applying restriction/permission lists, 6-113
restriction/permission lists, 26-29
mailboxes
automatic logon to, 26-18, 26-36
broadcast
description, 20-47
recording personal verification, 20-49
setting up, 20-49
calls rejected if full, 8-89
disabled
reenabling, 8-92
disabling, 6-144
enabling administrator capability, 26-19
enabling broadcast capability for, 26-19, 26-37
for users without phones, 8-25
lockout duration, 26-37
mailbox to monitor, 6-152
maximum invalid logon attempts, 6-127
modifying security settings, 6-146
monitoring for logons, 6-153, 8-94
number of, 14-12
passwords, 6-128
changing from administration terminal, 8-93
defining a prefix, 6-137
defining minimum length, 6-138
expiry warning, 6-127

forcing change on first logon, 6-129, 6-134
forcing regular changes, 6-141
maximum days between passwords, 6-127
minimum length, 6-128
suppress telset display, 6-129
suppressing telset display, 6-135
time of last change, 8-90
reassigning to another user, 8-96
reenabling (MMUI), 6-144
reenabling (VMUIF), 6-145
restricting offsite access, 6-147
SEER trigger mailbox, 29-36
time of last lockout, 8-88
unused
disabling, 6-148
volume level
changing, 8-43
warning threshold for full mailboxes
defining, 20-56
description, 20-55
main menu, 2-6
maximum length
of call answering messages, 26-22, 26-39
maximum read message retention
defining, 20-58
description, 20-57
MAXP
modifying its value in the queue, 23-57
menu items
number of accesses, 31-27
menus
choosing items from, 2-30
layout of, 2-28
Meridian Mail AutoAdmin, 4-36, 13-11
Meridian Mail AutoAdmin installation, B-5
Meridian Mail database
synchronizing with Meridian 1, A-9
Meridian Mail Hacker Monitor, 6-151
Meridian Mail hardware
monitoring, 18-6
Meridian Mail menus
choosing items from, 2-30
layout of, 2-28
Meridian Mail platforms
feature availability, 2-46
Meridian Mail screens
layout of, 2-31
moving around in, 2-33
selecting an entire line, 2-37
Meridian Mail telset interfaces
description, 2-48
Meridian networking
adding a VSDN, 24-31
Meridian networking. See also networking
message addressing by name, 20-40
message delivery priority
defining, 20-54
description, 20-53
message header
playing back, 26-40
message length
maximum, 26-16, 26-34
message waiting indication
DN
defining, 8-33
description, 8-29
setting options, 26-23, 26-39
messages
allowing users to compose and send, 26-44
allowing users to send to external users, 26-25, 26-44
AMIS
failed attempts, 31-39
number delivered, 31-38
number received, 31-38
AMIS open network
allowing users to receive, 26-28, 26-46
allowing users to send, 26-28, 26-47
restriction/permission lists, 26-29, 26-47
broadcast
recording and sending, 5-41
call answering
maximum length, 26-22, 26-39
composed
allowing users to receive, 26-23, 26-39
enabling automatic playback, 26-20
from call answering
disabling, 26-38
how long to keep once listened to, 26-25, 26-43
networking
failed attempts, 31-34
number delivered, 31-32
number received, 31-32
playback
skip to first new message, 26-40
playing header, 26-40

retain copy of sent ones, 26-26
setting message waiting indication option, 26-23, 26-39
that have been listened to
when to delete, 20-57
unsent
treatment of, 26-44
MMUI
description, 2-48
feature availability, 2-49
modifying the CAT after moving agents, 23-64
monitoring
CLIDs, 6-130, 6-159
specifying format, 6-130
mailbox logons, 6-153, 8-94
Meridian Mail hardware, 18-6
Meridian Mail operation, 18-4
thru-dials, 6-130, 6-156
monitoring period
for system accesses, 6-129, 6-152
moving agents (high-level procedure), 23-62
multilingual systems
default language, 20-13
overriding user's preferred language, 20-17
user's preferred language, 20-13
multimedia channels
features supported by, 23-17
multimedia ports
minimum number of, 28-51
multiple administration terminals, 2-44
logging on from, 3-14
password
changing, 16-6
multiple appearance DNs
support for, 7-12
multi-user login
on the M1
implementing, 6-80
MWI DN. See message waiting indication DN

N

name dialing
by external callers, 8-41
allowing, 8-43
name dialing and name addressing
description, 20-40
enabling/disabling, 20-44
prefix, 20-41
name display
of sender
for fax services, 24-104
national call back number treatment, 24-75, 24-103
navigating through screens, 2-33
NCOS facility restriction level
on the M1
implementing, 6-57
network broadcast messages, 5-6, 5-39, 5-41
locate mailboxes with capability, 8-60
network broadcast capability, 26-19
network speed call
on the M1
implementing, 6-59
network usage, 31-33
networking
economy delivery, 20-53
failures to send messages, 31-34
message delivery priority
defining, 20-54
description, 20-53
network usage, 31-33
number of messages delivered, 31-32
number of messages received, 31-32
remote sites
recorded verification, 5-5
recording a personal verification for, 5-35
standard delivery, 20-53
statistics, 31-32
networking detail report
analyzing, 31-35
new flexible code restriction
on the M1
implementing, 6-37
new messages
skip to first, 26-40
NMS
location name, 8-16
location prefix, 8-16
location-specific broadcast messages, 5-40, 5-41
setting default administration context, 8-9
node
status, 28-13

Node Configuration screen
accessing, 27-7
nodes
disabling/enabling, 28-17
printing node information, 27-47
type, 28-13
viewing the node configurations, 27-10
notification of specific SEERs, 29-37
notifying callers of busy line, 26-21, 26-37

O

offsite access
to mailboxes
restricting, 6-147
online help, 2-40
operational measurements
calculating disk space requirements, 31-16
setting options, 31-24
Operational Measurements menu
using, 31-14
outcalling
statistics, 31-42
outcalling audit trail report
detail
analyzing, 33-28
generating, 33-13
summary
analyzing, 33-18
outcalling detail report
analyzing, 31-45
out-of-service diagnostics
running, 28-28

P

page limit
for fax selections, 24-97
page transmission error handling
for fax item maintenance, 24-110
paging through screens, 2-33
partial backups to disk, 15-40
partial backups to tape, 15-21
password control
on the M1
implementing, 6-75
password prefix, 6-126
passwords
AdminPlus
changing, 16-8
for mailboxes
changing from administration terminal, 8-93
defining a prefix, 6-137
defining minimum length, 6-138
expiry warning, 6-127
forcing change on first logon, 6-129
forcing regular changes, 6-141
forcing users to change, 6-134
maximum days between changes, 6-127
minimum length, 6-128
minimum number changes before repeats, 6-128
suppress telset display, 6-129
suppressing display, 6-135
time of last change, 8-56, 8-90
for MATs
changing, 16-6
for remote activation, 24-54
system administration
changing, 3-9, 16-3
minimum length, 16-7
recovering, 3-10
setting for first time, 3-7
personal classes of service, 8-22
creating, 26-65
personal distribution lists
auto delete of invalid addresses, 26-20
defining a prefix, 20-46
personal greetings
description, 5-4
how used in call answering, 5-7
locate mailboxes without greetings recorded, 8-59
maximum length, 26-16, 26-34
recording, 5-25
personal verifications
allowing users to change their own, 8-61, 26-15, 26-33
description, 5-4
for broadcast mailbox
description, 5-5
recording, 5-37, 20-49
for directory entry users, 10-8

for distribution lists
description, 5-5
recording, 5-31
for local voice users
recording, 8-34
for remote voice users
recording, 9-19
how used in call answering, 5-7
recording
from a telset, 5-28
from the administration terminal, 5-29
playback of messages
automatic, 26-20
playing message header, 26-40
playback speed, 20-62
port names
for printers
modifying, 13-21
ports
courtesy disable/enable, 28-18
full service
maximum number of, 28-51
maximum number of, 28-50
number currently allocated, 28-51
viewing capability in CAT, 28-54
viewing types in CAT, 28-53
ports, dedicating. See channels
post checkout mailbox service
adding the VSDN, 24-22
preferred language
for local voice users
selecting, 8-43
preferred language of user
overriding, 20-17
prefixes
default dialing prefixes
configuring, 17-37
for ESN dialing, 17-35
for exchange codes in translation table, 17-63
for exchange codes not in translation table, 17-63
for international dialing, 17-34
for local dialing, 17-34
for long distance dialing, 17-34
for mailbox passwords, 6-126
defining, 6-137
for personal distribution lists
defining, 20-46
name dialing and name addressing, 20-41
NMS location, 8-16
personal distribution list
description, 20-46
primary DN, 8-24, 8-31
prime disk
status of, 28-66
printer port names
modifying, 13-21
printers
changing SEER printer port name, 29-41
Procedure
Removing Mailboxes, B-44
prompt played during call answering, 5-8, 5-9
prompts
enabling delayed mailbox prompts, 26-16, 26-34
playing in two languages, 26-17

Q

queues
adding agents to a queue, 23-58
configuring agent queues (high-level procedure), 23-36
configuring dummy queues (high-level procedure), 23-37
creating a dummy queue, 23-60
creating an agent queue, 23-53
modifying the CAT after moving agents, 23-64
modifying the MAXP value, 23-57
moving agents, 23-62
removing agents, 23-63

R

read messages
how long to keep on system, 20-57
retention period, 26-25, 26-43
redrawing
Logon/Status screen, 3-5
reenabling
disabled mailboxes, 8-92
mailboxes (MMUI), 6-144
mailboxes (VMUIF), 6-145

rejected calls
for full mailboxes, 8-89
remapping SEERs, 29-19
remote activation
adding a VSDN, 24-54
password, 24-54
remote notification
applying restriction/permission lists, 6-116
enabling in COS, 26-28, 26-45
finding users with capability, 8-63
schedules
creating from the administration terminal, 8-37
remote sites
recorded verification, 5-5
recording a personal verification for, 5-35
remote terminal (EC)
logging on from, 3-21
remote terminal (non-EC)
logging on from, 3-17
remote terminal access
disabling (EC), 3-22
disabling (non-EC), 3-17
remote voice users
adding
using bulk provisioning, 9-24
using Enterprise Networking, 9-21
using User Administration, 9-17
description, 7-8
finding, 9-35
finding and deleting, 9-46
listing, 9-35
manually deleting, 9-45
modifying, 9-40, 9-44
permanent, 9-8
printing, 9-35
recording a personal verification, 9-19
temporary, 9-9
viewing, 9-40, 9-44
removing agents, 23-63
reports printer port
naming, 13-21
restoring
from selective backup, 15-56
restriction/permission lists
AMIS networking, 6-121
AMIS open network messages, 26-29, 26-47
applying to features, 6-101
call answering, 6-111
custom revert, 6-107, 26-48
custom revert DN, 26-29
defining, 6-99
delivery to non-user, 6-118
express messaging
applying to, 6-111
extension dialing, 6-113, 26-29
external call sender, 6-120, 26-24, 26-42
fax call back, 24-104
fax item maintenance call back, 24-111
fax on demand, 6-115
mailbox thru-dialing, 6-113
remote notification, 6-116
thru-dial on the M1
applying to, 6-114
thru-dial services, 6-109
restrictions
on the M1
assigning, 6-15
retention period
for read messages, 20-57, 26-25, 26-43
revert
user's custom DN
restriction/permission lists, 26-29
revert DN
allowing users to define, 8-27
defining, 8-33
description, 8-26
for ACCESS VSDNs, 24-36
for fax services, 24-98
prohibiting users from defining, 8-28
user's custom DN
restriction/permission lists, 26-48
VMUIF mailbox lockout
defining, 20-46
description, 20-45
revert to operator
applying restriction/permission lists, 6-107
rotary phones
support for, 26-35
routing control
on the M1
implementing, 6-69

S

same call fax delivery, 24-100
scheduled backups
  deleting, 15-45
scheduling
  disk diagnostics, 28-81
scheduling a backup, 15-44
screens
  layout of, 2-31
  moving around in, 2-33
  selecting an entire line, 2-37
scrolling through screens, 2-33
secondary default language
  defining, 20-24
secured messaging, 6-128
security
  for mailboxes
    modifying settings, 6-146
  on the M1
    assigning classes of service, 6-15
    authorization code conditionally last, 6-63
    authorization codes, 6-24
    call forward all calls, 6-41
    call forward external deny, 6-42
    call forward to trunk access code, 6-43
    code restriction, 6-35
    controlled class of service, 6-31
    DISA, 6-84
    enhanced controlled class of service, 6-32
    flexible feature codes, 6-33, 6-45
    forced charge account, 6-28
    history file, 6-82
    incoming trunk group exclusion, 6-72
    internal call forward, 6-44
    limited access password, 6-78
    limited access to overlays, 6-77
    multi-user login, 6-80
    NCOS facility restriction level, 6-57
    network speed call, 6-59
    new flexible code restriction, 6-37
    password control, 6-75
    routing control, 6-69
    single terminal access, 6-79
    station specific authorization codes, 6-26
    supplemental digit recognition, 6-51
    supplemental digit restriction, 6-54
    system speed call, 6-23
    TGAR/TARG, 6-12
    time-of-day routing, 6-66
    user selectable call redirection, 6-46
SEER escalation
  setting, 29-25
SEER printer port
  changing the port name, 29-41
  naming, 13-21
SEER throttling
  setting, 29-22
SEERs
  being notified of specific SEERs, 29-37
  escalating severity level, 29-25
  filtering, 29-34
  filtering by severity level, 29-31
  filtering by type, 29-32
  filtering by type and severity, 29-32
  printing, 29-39
  remapping, 29-19
  retrieving from history file, 29-8
  setting SEER triggering, 29-37
selecting a line in a screen, 2-37
selecting an option in a field, 2-35
selective backup
  of all multimedia services, 15-35
  of all users, 15-25
  of all users in a department, 15-33
  of all users in a particular COS, 15-31
  of all users on a volume, 15-29
  of individual multimedia services, 15-37
  of individual users, 15-27
  restoring from, 15-56
sender name display
  for fax services, 24-104
sender number
  for fax services, 24-98
sent messages
  retain copy, 26-26
service accesses, 31-13
  number of, 31-27
services
  dedicating channels to, 23-26
services detail report
  analyzing, 31-29
services summary report
  analyzing, 31-15
session profiles
  basic service, 24-81

choosing
for fax item maintenance, 24-64
for fax items, 24-61
for time-of-day controllers, 24-48
for voice menus, 24-45
creating a custom session profile, 24-91
custom, 24-109
customizing
for voice menus, fax items, time-of-day controllers, 24-95
customizing the session profile for fax item maintenance, 24-112
full-service multimedia, 24-86, 24-89
full-service voice, 24-83
maximum number of invalid selections, 24-93
session time limit, 24-93
specifying call back options, 24-105
specifying fax service options, 24-100
session time limit
for voice services, 24-93
session trace data
enabling collection of, 31-22
shadow disk
status of, 28-67
silencing alarms, 29-13
single terminal access
on the M1
implementing, 6-79
to M1 and Meridian Mail, 3-23
skipping to first new message, 26-40
softkeys, 2-39
sort order for Choice of Services, 21-11
sort order for Service Definition data menus, 21-11
sort order for VSDN table, 21-10
speed control, 20-62
spoken name. See personal verifications
sponsor fax item ID
for fax services, 24-98
standard delivery of networked messages, 20-53
start time
for traffic period, 31-21
Start-up problems, B-51
station specific authorization codes
on the M1
implementing, 6-26
status
of backups
checking, 15-51
of local voice users
checking, 8-86
storage
amount used, 28-14
of traffic data, 31-22
storage limit
for voice recordings, 26-15, 26-33
submailboxes
maximum number, 26-32
summary fax audit trail report
analyzing, 33-37, 33-43
summary outcalling audit trail report
analyzing, 33-18
supervised transfer delay
modifying, 13-10
supplemental digit recognition
on the M1
implementing, 6-51
supplemental digit restriction
on the M1
implementing, 6-54
suppressing display of telset passwords, 6-135
suppressing telset display of passwords, 6-129
SW7007, 6-147
synching
disk pair, 28-70
synchronizing
Meridian 1 and Meridian Mail databases, A-9
system
disabling/activating, 28-15
system accesses
monitoring period, 6-152
monitoring period for, 6-129
system addressing length
modifying, 13-10
system administration password
changing, 3-9, 16-3
recovering, 3-10
setting for first time, 3-7
system distribution lists. See distribution lists
system name
changing, 13-7
system number
changing, 13-7

system speed call
on the M1
implementing, 6-23
system status, 28-11
System Status screen
accessing, 28-8
system time
changing, 16-10
system volumes, 14-5

T

tape backups
full, 15-19
partial, 15-21
tape drives
cleaning, 18-9
cleaning and maintaining, 15-52
TARG
implementing, 6-12
telset display of passwords
suppressing, 6-129
telset interfaces
description, 2-48
temporary absence greetings
expiry date, 8-90
finding users with greeting recorded, 8-61
how used in call answering, 5-7
terminal number, 28-52
TGAR
implementing, 6-12
The AutoAdmin window, B-25
threshold
for full mailbox warning message
defining, 20-56
description, 20-55
throttling SEERs, 29-22
thru-dial greetings
recording, 5-44
thru-dial on the M1
applying restriction/permission lists, 6-114
thru-dial services
adding a VSDN, 24-43
applying restriction/permission lists, 6-109
thru-dials
monitoring, 6-130, 6-156
timed delivery
description, 20-40
time-of-day controllers
adding a VSDN, 24-50
customizing a session profile, 24-95
time-of-day routing
on the M1
implementing, 6-66
timeouts for voice services, 25-7
toggling a user's COS assignment, 8-73
toggling between M1 and Meridian Mail, 3-23
traffic data
enabling collection of, 31-21
how long to store, 31-22
how often to write to disk, 31-21
traffic period
end time, 31-21
start time, 31-21
traffic reports
descriptions, 31-5
generating, 31-7
traffic statistics
CCS, 31-14, 31-15
transcription service
adding a VSDN, 24-59
defining a voice form ID, 24-58
translation
CLIDs with unkown format, 17-36
translation tables
area/city code, 17-63
configuring, 17-64
deleting, 17-67
exchange codes, 17-63
identifying requirements, 17-45
prefix for exchange codes in table, 17-63
prefix for exchange codes not in table, 17-63
table number, 17-62
troubleshooting, 17-77
transmission error handling
fax item maintenance, 24-110
Troubleshooting, B-51
tutorials
for VMUIF
description, 20-32
recording, 5-50, 20-34

U

UCD groups
determining how many are needed, 23-28
unsent messages
treatment of, 26-44
unused mailboxes
disabling, 6-148
uploading data
from Meridian Mail to M1, A-9
user class
for hospitality
selecting, 8-43
hospitality, 8-41
user flexible call redirection
on the M1
implementing, 6-46
user models
converting from, 26-66
converting to classes of service, 7-23
user usage data
enabling collection of, 31-22
number of days to store, 31-23
user usage reports
analyzing, 32-14
generating, 32-7
report analysis, 32-14
selection criteria, 32-4
selection screen, 32-2
user volumes, 14-6
user's preferred language, 20-13
overriding with default language, 20-17
users. See local voice users, remote voice users, or directory entry users
Using Meridian Mail AutoAdmin, B-34

V

verifying location of voice services, 15-12
View/Modify Local Voice User screen
accessing, 8-80, 8-81
VMBA
installing a system with, A-17
VMUIF
description, 2-48
feature availability, 2-49
VMUIF introductory tutorial
description, 20-32
recording, 20-34
recording/disabling, 5-50
VMUIF login greeting
description, 20-33
recording, 20-34
recording/disabling, 5-52
voice channels
features supported by, 23-16
voice forms
adding a VSDN, 24-56
adding a VSDN for the transcription service, 24-59
finding, 22-11
making recordings, 5-44
transcription service
definining a voice form ID, 24-58
voice menus
adding a VSDN, 24-46
customizing a session profile, 24-95
finding, 22-11
making recordings, 5-44
number of menu item accesses, 31-27
voice messaging
adding the VSDN, 24-13
statistics, 31-19
voice messaging detail report
analyzing, 31-21
voice messaging options
configuring, 20-9
defining for MMUI, 20-38
defining for VMUIF, 20-39
Voice Messaging Options screen
accessing, 20-5
voice path diagnostics, 28-77
maximum duration of, 28-80
maximum number idle channels, 28-80
voice ports
maximum number of, 28-50
voice prompt maintenance
language of service, 24-52
voice prompt maintenance service
adding a VSDN, 24-52
voice services
business hours default, 25-9
enabling update logging, 25-9
holidays, 25-10

making recordings for, 5-44
maximum number of invalid selections, 24-93
maximum prompt sizes for announcements, 25-8
maximum sizes for other recordings, 25-8
modifying the voice services profile, 25-6
session time limit, 24-93
timeouts, 25-7
verifying location of, 15-12
voice storage
percent used, 14-12
Volume and Select Backup screen
accessing, 14-10
volume level
for mailboxes
changing, 8-43
volumes
contents of, 14-5
full
stopping audit trail data collection, 33-6
how they are distributed across nodes, 14-7
how they are named, 14-3
size, 14-11
system, 14-5
user, 14-6
VSDN table
accessing, 24-7
sort order, 21-10
VSDNs
ACCESS, adding, 24-36
AMIS networking, adding, 24-29
announcements, adding, 24-41
calculating how many you need, 23-29
deleting, 24-120
determining how many you need, 24-78
Enterprise networking
adding, 24-34
express messaging, 24-16
fax item maintenance, adding, 24-64
fax items, adding, 24-62
finding, 22-9
greetings service, adding, 24-24
hospitality, adding, 24-21
Meridian networking, adding, 24-31
post checkout mailbox, adding, 24-22
remote activation, adding, 24-54
thru-dial services, adding, 24-43
time-of-day controllers, adding, 24-50
transcription service, adding, 24-59
viewing or modifying, 24-117
voice forms, adding, 24-56
voice menus, 24-46
voice messaging, adding, 24-13
voice prompt maintenance, adding, 24-52

W

waiting messages
setting indication option for, 26-23, 26-39
warning threshold for full mailboxes
defining, 20-56
description, 20-55

List of Fields

Symbols

, B-27
#, 31-57
#Expired Unread Messages, 31-57
#Guests Checked In, 31-57
#Guests Checked Out, 31-57
#Messages (Unread, Read), 31-57
#New Unread Messages, 31-57

A

Abort, B-30
ACCESS class, 24-36
ACD DN, 28-52
Act on AMIS/Enterprise Initiator Tone, 25-9
Add, B-13
Add>, B-27
Administrator Capability, 8-60, 26-19
Alarm Status, 28-12
All Entries, 34-44
Allocated, 28-51
AMIS Open Network Restriction/Permission List, 26-29, 26-47
Announce Caller, 26-40
Announcement ID, 24-41
Applied command, B-26
Area/City Code, 17-63
Attendant DN, 13-15
Attributes (for ports with type = Data), 27-15
Attributes (for ports with type = Device), 27-15
Attributes (for ports with type = Voice or Multi), 27-16
Auto Deletion of Invalid PDL Addresses, 8-61, 26-20
Auto Logon, 8-59, 26-18, 26-36
Auto Play, 26-20
Autologon, 24-19

Automatic Cover Sheet, 24-103
Average Length (in seconds), 31-14

B

Backup Completed, 15-50
Backup frequency, 15-43
Backup Selected, 15-50
Backup start time, 15-43
Backup Started, 15-50
Backup Volumes, 15-50
Baud Rate, 27-29, 27-31, 27-33, 27-37, 27-39, 27-41, 27-43
Billing DN, 20-51, 24-99, 24-110, 33-36
Broadcast Capability, 8-59, 26-19, 26-37
Broadcast Mailbox Number, 20-49
Broadcast Mailbox Personal Verification (Voice), 20-49
Browse, B-31
Business Hours Default, 25-9

C

Call Answering Greeting (Voice), 20-29
Call Answering/Express Messaging Thru-Dial Restriction/
Permission List Number, 6-129
Call Back Dialing Restrictions, 24-104, 24-111
Call Back Extension Prompt, 24-102
Call Sender, 26-41
Call Status, 33-16, 33-22, 33-36, 33-40
Called DN, 33-36, 33-39
Callers Notified of Busy Line, 26-21, 26-37
Calls Rejected after Mailbox Full, 8-89
Calls were Rejected after Mailbox Full, 8-58
Cancel, B-15
Capture External CLID with Unknown Format, 17-36
Card, 27-8
Card #, 28-24
Card_Type, 27-13
C-D-P, 27-13, 28-52
C-D-P (location), 28-36
Channel, 31-23
Channel Capability Required, 24-93, 24-110
Channel DN, 33-20, 33-39
Check In, 31-60
Check Out, 31-60
Class of Service Name, 26-14, 26-31
Class of Service Number, 26-13, 26-31
Class of Service Selections, 13-13

CLID Format—External—CLIDs to Monitor, 6-130
CLID Format—Internal—CLIDs to Monitor, 6-130
CLIDs to Monitor, 6-158
Collect Audit Trail Data, 31-23, 33-6
Collect Traffic Data, 31-21
Collect User Usage/Session Trace Data, 31-22
Comment, 24-10
Comments, 25-10
Compose Capability, 8-59, 26-44
Compose/Send AMIS Open Network Messages, 8-64, 26-28, 26-47
Connect Time (mm:ss), 31-39, 32-12
Connection, B-13
Copy Mbox, 31-60
COS, 8-54
Created On, 34-38
Creation Date, 34-30
Custom Revert Restriction/Permission List, 26-29, 26-48
Customer Number, 29-36

D

Data Conflicts, 34-44
Data delimiter, B-26
Data from tape, 34-44
Data overwritten on destination, 34-44
Data Port Location, 27-28
Data Set Name, 34-15, 34-30, 34-38
Date Format for Administration and Maintenance Reports, 13-18, 13-19
Day of Month, 15-43
Default Language, 20-13
Default Language Overrides User's Preferred Language for Call Answering, 20-14
Default Message Delivery Priority, 20-53
Default sort order for Service Definition data menus, 21-11
Default sort order for VSDN Table data menus, 21-10
Default Translation for CLID with Unknown Format, 17-36
Delayed Prompts, 26-16, 26-34
Delivery to Non-User Capability, 8-62, 26-27, 26-45
Department, 8-18, 9-14, 10-5, 10-11
Description, 27-24, B-13
Device Name, 27-28
Device Type, 27-24, 27-28
Device/Target Phone Number, 33-20
Dial Prefix, B-15
Dial Pulse Support, 26-35
Dial Suffix, B-15
Disk (appears only on Unshadowed systems), 28-66

Disk Pair (appears only on Shadowed systems), 28-66
Disk Used (mm:ss), 32-12
Display Choice of Services/Menu Actions in, 21-11
Display the List in MWI Status Format, 8-66
DN, 24-10
DR Audit - DR Audit Rate, B-33
DR Audit - Polling Interval, B-33
DSP Port Status, 28-14, 28-36
Dual Language Prompting, 26-17

E

Enable Update Logging, 25-9
End Date, 25-10
ESN Dialing, 17-35
Exit, B-14, B-28
Extension Dialing Restriction/Permission List, 26-29
Extension DNs, 8-32, 9-15, 10-6, 10-11
Extension Number (DN), 9-30
External Call Sender Restriction/Permission List, 26-24, 26-42
External Call-Sender Allowed, 20-60
External Logon, 6-128
External Personal Greeting Recorded, 8-60, 8-90

F

Failures, 31-34, 31-39
Fax Activity Revert DN, 24-98
Fax Delivery Option, 24-100
Fax Item ID, 24-62
First Name, 8-17, 10-5, 10-10, 33-12
For each menu item, the number of accesses are, 31-27
Force Password Change on Initial Logon, 6-129

H

Hangup Prefix, B-15
Hangup Suffix, B-15
Help, B-14, B-15, B-28
Holidays, 25-10
hospitality statistics report
  analyzing, 31-58
Hospitality User Class, 8-41
HWLOC, 28-66

I

ID, 31-27
Include AMIS Network Usage, 32-5
Include Local Usage, 32-5
Include Meridian Network Usage, 32-5
Incoming Avg Length (in seconds), 31-23
Information to backup, 15-44
Initialization, B-15
Initials, 8-17
Internal Greeting Recorded, 8-89
Internal Personal Greeting Recorded, 8-60
International Dialing, 17-34
Invalid Logon Attempts, 8-87

J

J4, 27-14
J5, 27-14

L

Language of Service, 24-52, 24-65
Last Access Time, 9-16
Last Event, 28-12
Last Name, 8-17, 9-14, 10-4, 10-10, 33-12
Limit, 28-50
Link Status, 28-12
List Number, 11-12
List Title, 11-13
List Title Recorded (Voice), 11-13
Local Area/City Code, 17-35
Local Country Code, 17-35
Local Dialing, 17-34
Local Users, 34-16
Location Name, 11-11
Location Prefix, 11-11
Lockout Duration, 26-37
Lockout Revert DN, 20-45
Log Detail - Brief, B-32
Log Detail - Full, B-32
Log File, B-29
Log file, B-31
Login from Call Answering, 8-58, 26-36
Login Greeting (Voice), 20-33
Long Distance Dialing, 17-34

M

Mailbox Full Warning Threshold (percentage), 20-55
Mailbox ID, 24-15
Mailbox Number, 8-16, 8-53, 9-13
Mailbox Numbers, 11-13
Mark Channel Faulty if Voice Path Diagnostics Fail, 28-79
MaxFull, 28-51
Maximum CA Message Length (mm:ss), 8-57
Maximum Call Answering Message Length, 26-22, 26-39
Maximum Days Permitted Between Password Changes, 6-127
Maximum Delay for Timed Delivery (days), 20-42
Maximum Duration of Voice Path Diagnostics (hh:mm), 28-80
Maximum Invalid Logon Attempts Permitted per Mailbox, 6-127
Maximum Invalid Logon Attempts Permitted per Session, 6-126
Maximum Message Length, 26-16, 26-34
Maximum Message Length (mm:ss), 8-57
Maximum Number of Fax Selections, 24-97
Maximum Number of Invalid Selections, 24-93
Maximum Number of SubMailboxes, 8-57, 26-32
Maximum Personal Greeting Length, 26-34
Maximum Personal Greeting Length (mm:ss), 8-57
Maximum Prompt Sizes for Announcements (mm:ss), 25-8
Maximum Prompt Sizes for other voice recordings (mm:ss), 25-8
Maximum Read Message Retention (days), 20-57
MaxVoice, 28-50
Message Length (Avg and Max), 31-20
Message Length (mm:ss), 32-12
Message Remote Notification Option, 8-63
Message Trigger, 29-18
Message Trigger Mailboxes, 29-36
Message Waiting Indication DN, 8-32, 8-55
Message Waiting Indication Options, 8-65, 26-23, 26-39
Messages Created (EM/Ans and Log), 31-20
Messages Delivered, 31-32, 31-38
Messages Received, 31-32, 31-38
Minimum Admin Password Length, 16-7
Minimum Number of Days since Last Logon, 8-56
Minimum Number of Days since Pswd Changed, 8-56
Minimum Number of Idle Channels for Voice Path Diagnostics, 28-80
Minimum Number of Invalid Logon Attempts, 8-56
Minimum Number of Password Changes Before Repeats, 6-128
Minimum Password Length, 6-128
MinMulti, 28-51
Modem, B-14
Modified Date, 34-30
Modify, B-14

Monitor All Thru-Dials during Monitoring Period, 6-130, 6-155
Monitor CLIDs during Monitoring Period, 6-130, 6-158
Monitor Mailbox during Monitoring Period, 6-152, 8-40
Monitor this Service during Monitoring Period, 6-155
Move down, B-27
Move up, B-27

N

Name Dialable by External Callers, 8-41, 8-61, 9-15, 10-6
Name Dialing and Name Addressing, 20-42
Network Broadcast Capability, 8-60, 26-19
Network Modem DN, 27-35
Network Usage, 31-33
Node, 27-8, 28-13
Node Type, 28-66
Number of Accesses, 31-13
Number of Attempts, 31-42
Number of Calls (Int and Ext), 31-19
Number of Days of Audit Data stored, 31-23
Number of days of Audit Data stored, 33-6
Number of days of Traffic Data stored, 31-22
Number of days of User Usage Data stored, 31-23
Number of Economy Messages, 32-12
Number of failures, B-29
Number of Incoming Calls, 31-23
Number of Mailboxes, 14-12
Number of Messages, 32-12
Number of New Attempts, 31-48
Number of New Requests, 31-42, 31-48
Number of Outgoing Calls, 31-23
Number of requests, B-29
Number of Retries, 31-48
Number of Sessions, 32-11
Number of Sessions (EM/Ans and Log), 31-19
Number of Standard Messages, 32-13
Number of Successes, 31-43, 31-48
Number of successes, B-29
Number of Urgent Messages, 32-13
Number of Windows, 27-29

O

OK, B-15
OM Collection ACCESS Class, 31-23
Outbound, 28-55
Outcall Action, 33-24, 33-41
Outcall Process, 33-21, 33-39
Outgoing Avg Length (in seconds), 31-23

P

Page Limit for Fax Selections, 24-97
Page Transmission Error Handling, 24-99, 24-110
Pair Status, 28-67
Parity, 27-29
Password, 24-54, B-27
Password Expiry Warning (days), 6-127
Password Last Changed, 8-90
Password Prefix, 6-126
Pause, B-30
Personal Distribution List Prefix, 20-46
Personal Greeting Recorded, 8-59, 8-89
Personal Verific. Recorded, 10-14
Personal Verification Changeable by User, 8-61, 26-14
Personal Verification Recorded (Voice), 9-15, 10-6, 10-11
Personal Verification Status, 8-65, 9-30
Port, B-13
Port Location, 27-24
Port_Type, 27-14
Preferred Language, 8-42, 8-64
Prefix for exchange codes in the table, 17-63
Prefix for Name Dialing and Name Addressing, 20-43
Prefixes for exchange codes NOT in the table, 17-63
Primary DN, 8-31
Primary DN differs from MWI DN, 8-62
Prime Status, 28-66
Progress, B-30
Prompt played During Call Answering, 26-21
Provision remote users as, 34-38

R

Read Message Retention (days), 26-25, 26-43
Receive AMIS Open Network Messages, 8-64, 26-28, 26-46
Receive Composed Messages, 8-59, 26-23, 26-39
Receive Messages for Call Answering, 8-58, 26-38
Re-Check In, 31-60

Remote Notification Capability, 8-62, 26-28, 26-45
Remote Notification Keypad Interface, 8-64
Remote Users, 34-39
Remove, B-13
Replay Header with Message, 26-40
Report, 33-12
Report End (mm/dd/yy), 32-6
Report Start (mm/dd/yy), 32-6
Report Start/End, 29-7, 33-13, 33-32
Report Type, 33-32
Reports Printer Port Name, 13-21
Request #, 33-39
Request Progress, B-29
Resume, B-30
Retain Copy of Sent Messages, 26-26
Retry, 33-21, 33-39
Revert DN, 8-32, 8-55, 24-36
Run, B-28

S

Schedule Diagnostics on the Following Days, 28-79
SCN, 28-53
Secondary Default Language, 20-19
SEER Class, 29-7
SEER Escalation Interval, 29-24
SEER Escalation Threshold Count, 29-24
SEER Filters, 29-33
SEER Printer Output, 29-38
SEER Printer Port Name, 13-20, 29-40
SEER Severity Threshold, 29-33, 29-34
SEER Throttle Interval, 29-22
SEER Throttle Threshold Count, 29-21
SEER Type, 29-7
Selected Tags, B-27
Selection Criteria, 32-4, 33-12
Send Message via DNU if Mailbox Not Found, 8-62
Send Messages to External Users, 26-25, 26-44
Sender Fax Number, 24-98, 24-110
Sender Name Display, 24-104
Service, 24-10
Service Accesses, 31-27
Service Name, 31-13
Services, 34-16
Serving File, B-29
Session end time, B-30
Session Length (Avg and Max), 31-20
Session Profile, 24-45, 24-48, 24-61, 24-64

Session start time, B-30
Session Time Limit (minutes), 24-93
Severity Level, 29-7
Shadow Status, 28-67
Shutdown Audit Trail at Volume Full (%), 31-23, 33-6
Site, 31-32
Site ID, B-26
Skip to First New Message, 26-40
Sort Choice of Services/Menu Actions by, 21-11
Sorted, 32-5
Speed, B-14
Sponsor Fax Item ID, 24-98
Start Date, 25-10
Start Time, 25-10
Status, 27-24, 34-31
Storage Used, 28-14
Storage used, 8-17
Supervised Transfer Delay, 13-8
Suppress Display of Telset Password, 6-129
System Access Monitoring Period, 6-152
System Access Monitoring Period from (hh:mm), 6-129
System Addressing Length, 13-8
System ID, B-12
System Level Conflicts, 34-43
System Name, 13-6
System Number, 13-6
System Status, 28-11

T

Table ID, 17-62
Tag Context Data File - Consecutive Failure Threshold, B-32
Tag Context Data File - Start at Line, B-32
Tape Label, 15-50
Tape label, 15-44
Target Phone Number, 33-13, 33-16
Temporary Absence Greeting Expiry Date, 8-90
Temporary Absence Greeting Recorded, 8-61, 8-90
Text File, B-25
Text File Data Context - Valid tags, B-27
Text Space Used (%), 31-53
The following exchange codes are defined:, 17-63
Thru-Dial ID, 24-43
Time of Last Logon, 8-88
Time of Last Mailbox Lockout, 8-88
Time Remaining, 15-50
Time-of-Day Control ID, 24-50
Timeouts, 25-7

TN, 28-52
Total Length (mm:ss), 32-12, 32-13
Total number of mailboxes on the system, 14-12
Total Unread Msg Length (in minutes), 31-57
Traffic Commit Interval (hh:mm), 31-21
Traffic Period End (hh:mm), 31-21
Traffic Period Start (hh:mm), 31-21
Transaction (hh:mm), 33-39
Transaction Request #, 33-21
Treat Call Back Number As, 24-103, 24-111
Treatment for Unsent Messages if the User Disconnects During Compose, 26-44

U

Updt Mbox, 31-60
Updt Status, 31-60
Usage (% Full) Data, 14-11
Usage (% Full) Voice, 14-12
Use, 14-11
User Type, 9-16, 9-31

V

Validate file, B-26
View Mbox, 31-60
View PCO Mboxes, 31-60
View Status, 31-60
VMUIF Introductory Tutorial (Voice), 20-32
VMUIF Introductory Tutorial for Dial Pulse (Voice), 20-33
Voice Form ID, 24-56, 24-58
Voice Mail Usage (in CCS), 31-14, 31-23
Voice Menu ID, 24-46
Voice Message Playback Speed, 20-63
Voice Messaging Interface Type, 26-31
Voice Path Diagnostics, 28-79
Voice Services Volume, 25-7
Voice Space Used (%), 31-53
Voice Storage Limit, 26-15, 26-33
Voice Storage Limit (minutes), 8-55, 8-56, 8-58, 8-62, 8-63
Voice Storage Limit Exceeded, 8-62
Voice Volume Size (hh:mm), 31-53
Volume ID, 8-16, 8-53
Volume Level, 8-41
Volume Name, 14-11, 31-53

Volume Size Data (Kbytes), 14-11
Volume Size Voice (hh:mm), 14-11
Volume Size Voice (Kbytes), 14-11
VSDNs, 34-16

W

Wait Time, 31-44, 31-48
Weekly, 15-43
Window Height, 27-29
Window Width, 27-29

NORTEL
NORTHERN TELECOM

Reader Response Form

Meridian Mail 12
System Administration Guide
555-7001-301

Tell us about yourself:

Name: _____

Company: _____

Address: _____

_____

Occupation: _____ **Phone:** _____

1. What is your level of experience with this product?

   ☐ New User ☐ Intermediate ☐ Experienced ☐ Programmer

2. How do you use this book?

   ☐ Learning ☐ Procedural ☐ Reference ☐ Problem solving

3. Did this book meet your needs?

   ☐ Yes ☐ No

   If you answered No to this question, please answer the following questions.

4. What chapters, sections, or procedures did you find hard to understand?

   _____

   _____

   _____

5. What information (if any) was missing from this book?

   _____

   _____

   _____

6. How could we improve this book?

   _____

   _____

   _____

Please return your comments by fax to (416) 597-7104, or mail your comments to:
Toronto Information Products, Nortel, 522 University Avenue, 14th Floor, Toronto, ON, Canada M5G 1W7.

NORTEL
NORTHERN TELECOM

Reader Response Form

Reader Response Form

Meridian 1

Meridian Mail
System Administration Guide

Toronto Information Products
Nortel
522 University Avenue, 14th Floor
Toronto, Ontario Canada
M5G 1W6

© 1993, 1994, 1995, 1996, 1997, 1998 Northern Telecom
All rights reserved

Information is subject to change without notice.
Northern Telecom reserves the right to make changes
in design or components as progress in engineering
and manufacturing may warrant.

Meridian 1, Meridian, and Nortel are trademarks of
Northern Telecom.

Publication number: 555-7001-301
Product release: 12
Document release: Standard 1.0
Date: January 1998

Printed in the United States of America

NORTEL
NORTHERN TELECOM