System Releases
7.15, 7.16, 7.17, 7.17.2
ASTRO® 25
INTEGRATED VOICE AND DATA

Enhanced Telephone Interconnect Feature Guide

MARCH 2019

MN004321A01-B

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Furthermore, the purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a specific system, or may be dependent upon the characteristics of a specific mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

Contact Us

Motorola Solutions Support Center

The Solutions Support Center (SSC) is the primary contact for technical support included in your organization's service agreement with Motorola Solutions.

Service agreement customers should be sure to call the SSC in all situations listed under Customer Responsibilities in their agreement, such as:

- Before reloading software.
- To confirm troubleshooting results and analysis before taking action.

Your organization received support phone numbers and other contact information appropriate for your geographic region and service agreement. Use that contact information for the most efficient response. However, if needed, you can also find general support contact information on the Motorola Solutions website, by following these steps:

- Enter motorolasolutions.com in your browser.
- Ensure that your organization's country or region is displayed on the page. Clicking or tapping the name of the region provides a way to change it.
- Select "Support" on the motorolasolutions.com page.

Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number.
- The page number or title of the section with the error.
- A description of the error.

Document History

Version	Description	Date
MN004321A01-A	Original release of the *Enhanced Telephone Interconnect Feature Guide*	November 2017
MN004321A01-B	• Carrier system for the maximum number of phone lines corrected in Enhanced Telephone Interconnect Call Capabilities on page 37. • Ethernet LAN switch models supported in the zone core outlined in Enhanced Telephone Interconnect Planning on page 60 • Prerequisites and postrequisites revised in Mounting the Telephone Media Gateway Hardware on page 65. • Step 10 added in Upgrading to UNIVERGE 3C Version 8.5.2.3 Service Pack 3 on page 172.	March 2019

Contents

Copyrights.. 2

Contact Us... 3

Document History.. 4

List of Figures...12

List of Tables.. 13

List of Processes.. 14

List of Procedures..15

About Enhanced Telephone Interconnect.. 18

What Is Covered In This Manual?... 18

Helpful Background Information... 19

Related Information.. 19

Chapter 1: Enhanced Telephone Interconnect Description...................................21

1.1 Enhanced Telephone Interconnect Introduction..21

1.2 Enhanced Telephone Interconnect Physical Description...................................... 21

1.2.1 Telephone Media Gateway...23

1.2.2 IP PBX Server...24

1.2.2.1 NEC UNIVERGE 3C Software...24

1.2.3 IP PBX Media Gateway.. 24

1.2.3.1 NEC BranchHub Media Gateway...27

1.2.3.2 NEC COHub Media Gateway..28

1.2.4 Third-Party Media Gateways.. 28

1.2.5 Telephony Firewall...29

1.2.6 Additional Motorola Equipment Interfacing the Enhanced Telephone Interconnect Subsystem.. 30

1.3 Enhanced Telephone Interconnect Components and the ASTRO 25 System......................30

1.3.1 Call Types Support.. 32

1.3.2 Audio Formats Support...32

1.4 Enhanced Telephone Interconnect Terminology..32

1.5 Enhanced Telephone Interconnect Functionality...36

1.5.1 Enhanced Telephone Interconnect Capabilities.. 36

1.5.1.1 Enhanced Telephone Interconnect Call Capabilities................................. 37

1.5.2 Enhanced Telephone Interconnect Feature Limitations.. 38

1.5.3 Enhanced Telephone Interconnect and Dynamic System Resilience..................... 38

Chapter 2: Enhanced Telephone Interconnect Theory of Operation.................. 39

2.1 Enhanced Telephone Interconnect Operation in an ASTRO 25 Trunked System.................39

2.2 Enhanced Telephone Interconnect Architecture Components.. 41
2.2.1 Zone Controller... 42
2.2.2 Network Time Protocol Server and ETI.. 42
2.2.3 Syslog and ETI...42
2.2.4 Domain Name Services and ETI...42
2.2.5 Service Laptop and ETI.. 42
2.2.6 Unified Event Manager and ETI...42
2.2.7 Unified Network Configurator and ETI.. 43
2.2.8 RADIUS and ETI...43
2.2.9 Key Management Facility and ETI...43
2.2.10 Key Variable Loader and ETI...43
2.2.11 Radio Network Infrastructure-Demilitarized Zone Firewall and ETI......................43
2.3 Call Control and ETI.. 44
2.4 Audio/Tone Generation and ETI...44
2.5 Audio Connections and ETI...44
2.6 Enhanced Telephone Interconnect Subsystem Initialization.. 44
2.7 Dynamic Call Mode Determination... 44
2.8 Mobile-to-Land Calls in the ASTRO 25 System...45
2.8.1 Mobile-to-Land Call Request in the ASTRO 25 System... 45
2.8.2 Mobile Functionality in Mobile-to-Land Call.. 45
2.8.3 Site Response During Mobile-to-Land Call...46
2.8.4 Mobile-to-Land Call Mobile Registration Verification.. 46
2.8.5 Mobile-to-Land Call Mobile Interconnect Authorization Verification........................46
2.8.6 Mobile-to-Land Call Service Options Check... 46
2.8.7 Mobile-to-Land Call Routing Determination...46
2.8.7.1 Mobile-to-Land Call Routing Mode - Local Interconnect Preferred............47
2.8.7.2 Mobile-to-Land Call Routing Mode - Use Default Interconnect Only......... 47
2.8.7.3 Mobile-to-Land Call Routing Mode - Local Interconnect Only....................47
2.8.7.4 Mobile-to-Land Call Exclusion Class and Dialing Restrictions...................47
2.8.8 Mobile-to-Land Call Resource Reservation and Busy Queuing...............................48
2.8.8.1 Table-Driven and Dynamic Shared Service..48
2.8.9 Mobile-to-Land Call IP PBX Server Notification...48
2.8.10 Mobile-to-Land Call IP PBX Server Phone Number Validation..............................48
2.8.11 Mobile-to-Land Call Global Dialing Privileges..48
2.8.12 Mobile-to-Land Call IP PBX Check for Trunk Resources..................................... 49
2.8.13 Mobile-to-Land Call Initiation of Call to PSTN...49
2.8.14 Mobile-to-Land Call Alerting..49
2.8.15 Mobile-to-Land Call Landline Answers... 49
2.9 Land-to-Mobile Calls...49

2.9.1 Land-to-Mobile Voice Announcement..50

2.9.2 Land-to-Mobile Call Request through Overdial for Non-DID Interface to PSTN......50

2.9.3 Land-to-Mobile Call Answer Supervision..51

2.9.4 Land-to-Mobile Call Request with DID Interface to PSTN...................................... 51

2.9.4.1 Direct Inbound Dialing Database and Related Parameters....................... 51

2.9.4.2 Direct Inbound Dialing Call Initiation.. 52

2.9.4.3 Land-to-Mobile Call Target Radio Authorization, Registration Checks 53

2.9.4.4 Land-to-Mobile Call Secure/Clear Mode Determination............................53

2.9.4.5 Land-to-Mobile Call Contention Checking...54

2.9.4.6 Land-to-Mobile Call Radio System Resource Reservation and Busy Queuing..54

2.9.4.7 Land-to-Mobile Call Target Mobile Notification and Ringing......................54

2.9.4.8 Land-to-Mobile Call Radio User Answering Call.......................................55

2.9.5 Active Interconnect Calls Maintenance...55

2.9.5.1 Voice Channel..55

2.9.5.2 Control Channel Grant Updates..55

2.9.5.3 Maximum Interconnect Call Duration..56

2.9.5.4 Overdial Support.. 56

2.9.5.5 Radio Secure Upgrade/Downgrade Requests...56

2.9.5.6 Go-Ahead Tone for Half-duplex Operation... 56

2.9.6 Interconnect Call Termination..57

2.9.6.1 Mobile-Initiated Call Termination During Active Interconnect Call............ 57

2.9.6.2 Mobile Power Off During Interconnect Call...57

2.9.6.3 Landline-Initiated Call Termination During Active Interconnect Call.......... 57

2.9.6.4 Mobile “Hangs up” Before Landline Answers Mobile-to-Land Call.............57

2.9.6.5 Landline “Hangs up” Before Mobile Answers Land-to-Mobile Call.............57

2.9.6.6 Interconnect Call Termination Due to Maximum Call Timeout Expiration..57

2.9.6.7 End-of-Call Alert Tone...58

2.9.6.8 Call Teardown...58

2.9.6.9 Individual Interconnect Timeout Expiration (No Mobile Activity)................ 58

2.9.6.10 Interconnect Call Termination and Expiration of Call Setup Timers.........58

2.9.6.11 Interconnect Ring Timer...58

2.9.6.12 Interconnect Mobility.. 59

2.9.6.13 Location Registration at New Site by Roaming Radio............................ 59

2.9.6.14 Radio Roaming During Active Interconnect Call.....................................59

2.9.6.15 Radio Roaming During Busy Interconnect Call.......................................60

2.9.6.16 Radio Roaming While Ringing for Land-to-Mobile Call............................60

2.9.6.17 Radio Roaming While Answering Land-to-Mobile Call, Before Receiving Response... 60

2.9.6.18 Zone Controller Receives No Answer Response at Old Site...................60

2.10 Enhanced Telephone Interconnect Planning....60

Chapter 3: Enhanced Telephone Interconnect Installation....62

3.1 Enhanced Telephone Interconnect Installation Prerequisites....62

3.2 Telephone Media Gateway Installation....62

3.2.1 Installing the Telephone Media Gateway Requirements.... 62

3.2.2 Installing the Telephone Media Gateway....64

3.2.3 Mounting the Telephone Media Gateway Hardware....65

3.2.4 Telephone Media Gateway Power Distribution Installation....66

3.2.5 Software Download Manager Installation and Data Transfer.... 66

3.2.6 Telephone Media Gateway Initial Configuration.... 67

3.2.6.1 Provisioning the Telephone Media Gateway Serial Connection Parameters....67

3.2.6.2 Configuring the Telephone Media Gateway in the CSS (Ethernet Connection)....68

3.2.6.3 Setting the Software Download Manager Transfer Mode.... 70

3.2.6.4 Setting the Telephone Media Gateway Local Password Configuration..... 70

3.2.6.5 Setting the Date and Time on the Telephone Media Gateway.... 72

3.2.6.6 Setting the Serial Security Services....72

3.2.6.7 Changing SNMPv3 Configuration and User Credentials on the Telephone Media Gateway.... 73

3.2.6.8 Adding or Modifying an SNMPv3 User....75

3.2.6.9 Verifying an SNMPv3 Connection in the CSS....76

3.2.6.10 Network Services Configuration in the CSS....77

3.2.7 Connecting the Telephone Media Gateway to the Network....78

3.2.8 Installing Telephone Media Gateway Software 78

3.2.8.1 Discovering the Telephone Media Gateway Devices with the UNC.... 78

3.2.8.2 UNC Server Application Logon Using PuTTY....80

3.2.8.3 Loading the Telephone Media Gateway OS Images to the UNC....80

3.2.8.4 Loading OS Software to Telephone Media Gateway Devices.... 81

3.3 NEC UNIVERGE 3C System Installation....84

3.3.1 Preparing for NEC UNIVERGE 3C System Installation....84

3.3.2 Mounting the Dell Server and Optional Media Gateways.... 86

3.3.2.1 Establishing the Telco Connection for the NEC BranchHub Media Gateway....87

3.3.2.2 Establishing the Telco Connection for the NEC COHub Media Gateway.. 87

3.3.3 Installing the UNIVERGE 3C Software Process.... 89

3.3.4 Installing the UNIVERGE 3C Software on the IP PBX Server....89

3.3.4.1 Installing Service Pack 3 on the IP PBX Server....91

3.3.4.2 Setting Permissions for the UCM Server.... 93

3.3.4.3 Commissioning the UNIVERGE 3C Software of the Console of the IP PBX Server.... 94

3.3.5 NEC UNIVERGE 3C Application Configuration.. 95

3.3.5.1 Configuring the IP PBX Media Gateway Addresses and Password.......... 95

3.3.5.2 Configuring the IP Address of the Unified Communications Manager Server...97

3.3.5.3 Joining the Unified Communications Manager Server to the ASTRO 25 Domain...98

3.3.5.4 Configuring Syslog Messaging..98

3.3.5.5 McAfee Anti-Malware Client Configuration.. 99

3.3.5.6 Configuring Remote Desktop for the Unified Communications Manager...99

3.3.5.7 Sharing the UNIVERGE 3C File System...99

3.3.6 Commissioning the UNIVERGE 3C Unified Communications Manager................100

3.3.7 Updating the UNIVERGE 3C License File..101

3.3.8 Installing the Auto Attendant Voice Prompt File...102

3.4 Firewall Hardware Installation...102

3.4.1 Telephony Firewall Installation..103

3.4.2 RNI-DMZ Firewall Installation... 103

3.4.3 Zone Core Protection Firewall Installation... 103

Chapter 4: Enhanced Telephone Interconnect Configuration........................... 104

4.1 Telephone Media Gateway Configuration Overview.. 104

4.1.1 Configuring the Telephone Media Gateway..104

4.1.2 Telephone Media Gateway Network Management Configuration......................... 104

4.1.2.1 Telephone Media Gateway Configuration in the UNC............................ 104

4.2 PRNM Interconnect Subsystem Configuration... 106

4.2.1 Enabling Telephone Interconnect on the ASTRO 25 System in the UNCW Process.. 107

4.2.1.1 Configuring Interconnect Calls in the UNCW 107

4.2.1.2 Configuring Disallowed Dialing Patterns...108

4.2.2 Interconnect Subsystem Configuration in the Provisioning Manager.................... 108

4.3 Configuring the NEC UNIVERGE 3C System.. 109

4.3.1 UNIVERGE 3C Administrator Settings... 110

4.3.1.1 General System Settings... 110

4.3.1.2 Media Gateway Configuration...118

4.3.1.3 Voice Announcement Configuration...127

4.3.1.4 MOTOPATCH Updates on the IP PBX Server.......................................130

Chapter 5: Enhanced Telephone Interconnect Optimization.............................131

5.1 Optimizing Access to Interconnect Services...131

5.1.1 Interconnect through Radio and User Configuration Optimization.........................131

5.1.2 Individual Interconnect Profiles... 131

5.1.3 Interconnect through Infrastructure Configuration Optimization........................... 131

5.1.4 Interconnect Control through the Shared Service Algorithm.................................132

5.1.5 Limit Interconnect Time at the Zone Level....132
5.2 Dynamic Shared Service Algorithm....132
Chapter 6: Enhanced Telephone Interconnect Operation....133
6.1 Telephone Media Gateway Operation....133
6.1.1 Turning on the Telephone Media Gateway....133
6.1.2 Turning off the Telephone Media Gateway....133
6.1.3 Rebooting the Telephone Media Gateway by Power Cycling the Hardware....133
6.1.4 Rebooting the Telephone Media Gateway in the CSS....134
6.1.5 Rebooting the Telephone Media Gateway in the UEM....134
6.1.6 Telephone Media Gateway Logon....134
6.1.7 Telephone Media Gateway Accounts Administration....135
6.1.8 Telephone Media Gateway Back Up....135
6.1.9 Telephone Media Gateway Status....136
6.1.9.1 ETI Status in the UEM....136
6.1.9.2 Viewing Status in the UNC....136
6.1.10 Telephone Media Gateway Removal....136
6.2 NEC UNIVERGE 3C System Use....137
6.2.1 Launching the NEC UNIVERGE 3C System....137
6.2.2 NEC UNIVERGE 3C Hardware Operation....137
6.2.3 UNIVERGE 3C System Database Back Up....137
6.2.3.1 Backing Up the UNIVERGE 3C System Database....138
6.2.3.2 Formatting a DVD-R on Windows Server 2008 R2....138
6.2.3.3 Scheduling Automatic Database Backup....139
6.2.3.4 Restoring the UNIVERGE 3C 7.1 System Database....139
6.2.3.5 Restoring the UNIVERGE 3C 8.5.2.3 System Database....140
Chapter 7: Enhanced Telephone Interconnect Maintenance....141
7.1 Enhanced Telephone Interconnect Hardware Maintenance....141
7.1.1 Replacing the TMG Battery....141
7.2 TMG Software Maintenance....142
Chapter 8: Enhanced Telephone Interconnect Troubleshooting....143
8.1 Enhanced Telephone Interconnect Failures....143
8.2 Troubleshooting Tools....143
8.2.1 Unified Event Manager....144
8.2.2 ZoneWatch Raw Display....145
8.2.3 Enhanced Telephone Interconnect Call Events....146
8.2.4 NEC UNIVERGE 3C Administration....147
8.2.4.1 DNS Record Settings for Unified Communication Manager to Zone Controller SIP Trunk Failover....148
8.2.4.2 Verifying SRV Records on the Domain Controller....148

8.2.4.3 Adding or Deleting UNIVERGE 3C Active Directory User/Group Accounts.......... 148
8.2.4.4 UNIVERGE 3C System Troubleshooting.......... 149
8.2.4.5 Call Processing Problems.......... 151
8.2.5 Motorola Solutions Equipment Administration.......... 151
8.2.5.1 ETI Troubleshooting in the UEM.......... 152
8.2.5.2 Using IP PBX Group Objects for Auditing and Security.......... 152
8.3 Software Download to TMG Troubleshooting.......... 153
8.4 Passwords and SNMPv3 Passphrases.......... 153
Chapter 9: Enhanced Telephone Interconnect FRU/FRE.......... 155
9.1 ETI Hardware Replacement.......... 155
9.1.1 Replacing the Telephone Media Gateway.......... 155
9.1.2 IP PBX Server Replacement.......... 156
9.1.3 IP PBX Media Gateway Replacement.......... 156
9.2 TMG Component Disposal.......... 156
9.3 ETI FRU/FRE Parts List.......... 157
Chapter 10: Enhanced Telephone Interconnect Reference.......... 158
10.1 Telephone Media Gateway Hardware Information.......... 158
10.1.1 Telephone Media Gateway Ports and Connector Diagrams.......... 158
10.1.2 Telephone Media Gateway LEDs.......... 159
10.1.2.1 TMG Power LED.......... 160
10.1.2.2 TMG Status LEDS.......... 160
10.1.2.3 TMG Security Alarm LED.......... 161
10.1.2.4 TMG KVL Interface Enabled LED.......... 161
10.1.2.5 TMG Ethernet Activity LEDs.......... 161
10.2 NEC UNIVERGE 3C Hardware Information.......... 161
10.3 SIP Messages between the ZC and IP PBX Server.......... 161
10.4 NEC UNIVERGE 3C System Initialization Settings.......... 162
Chapter 11: Enhanced Telephone Interconnect Disaster Recovery.......... 166
11.1 Recovery Sequence for Enhanced Telephone Interconnect Devices.......... 166
11.1.1 Recovering the Telephone Media Gateway.......... 166
11.1.2 Recovering the IP PBX Server.......... 167
11.1.3 Recovering an IP PBX Media Gateway.......... 169
11.1.4 Recovering the Telephony Firewall.......... 170
Chapter 12: Enhanced Telephone Interconnect Software Upgrade from 7.1 to 8.5.2.3 SP3.......... 171
12.1 Upgrading to UNIVERGE 3C Version 8.5.2.3.......... 171
12.2 Upgrading to UNIVERGE 3C Version 8.5.2.3 Service Pack 3.......... 172

List of Figures

Figure 1: Enhanced Telephone Interconnect Subsystem with Telephony Firewall 22

Figure 2: Enhanced Telephone Interconnect Subsystem without Telephony Firewall 22

Figure 3: Telephone Media Gateway Front View.. 23

Figure 4: Telephone Media Gateway Rear View 23

Figure 5: IP PBX Server Front View.. 24

Figure 6: NEC BranchHub Media Gateway Front View..28

Figure 7: NEC COHub Media Gateway Front View..28

Figure 8: Fortinet FortiGate 100D Front View.. 29

Figure 9: Enhanced Telephone Interconnect Subsystem with Telephony Firewall................................ 31

Figure 10: Enhanced Telephone Interconnect Subsystem without Telephony Firewall......................... 32

Figure 11: The Enhanced Telephone Interconnect Network Configuration with a Telephony Firewall 40

Figure 12: The Enhanced Telephone Interconnect Network Configuration without a Telephony Firewall 41

Figure 13: Password Configuration Window... 71

Figure 14: KVL Loader Port and the Key Erase Button..158

Figure 15: Voice Processor Module Port Mapping...159

Figure 16: TMG LEDs..160

List of Tables

Table 1: Media Gateway Equipment Public Switched Telephone Network Type Approvals by Country....25

Table 2: Certifications for IP PBX Media Gateways....27

Table 3: Certifications for Third-Party Media Gateways....29

Table 4: Percentage of Calls Queued 1%....37

Table 5: Percentage of Calls Queued 5%....37

Table 6: Percentage of Calls Queued 10%....37

Table 7: Ethernet LAN Switch Models....61

Table 8: RJ21X Connector Pinouts....87

Table 9: 8 Pin Modular Connector Pinout....88

Table 10: Changing NEC System Passwords....126

Table 11: Telephone Media Gateway Accounts....135

Table 12: Battery Replacement Time....141

Table 13: UEM Troubleshooting Scenarios for the TMG....144

Table 14: UEM Troubleshooting Scenarios for the ETI Feature....145

Table 15: ZoneWatch Troubleshooting Scenarios....145

Table 16: Telephone Interconnect Call Raw Display Messages....147

Table 17: Local Password and SNMPv3 Passphrase Troubleshooting....153

Table 18: Enhanced Telephone Interconnect Parts List....157

Table 19: Status Definitions for the Telephone Media Gateway Status LEDs....160

Table 20: TMG Ethernet Activity LEDs....161

Table 21: Common SIP Messages Exchanged between the ZC and the IP PBX Server....161

Table 22: System Initialization Settings....162

List of Processes

Installing the Telephone Media Gateway Requirements 62
Installing the Telephone Media Gateway 64
Installing Telephone Media Gateway Software 78
Loading OS Software to Telephone Media Gateway Devices 81
Preparing for NEC UNIVERGE 3C System Installation 84
Installing the UNIVERGE 3C Software Process 89
Configuring the IP PBX Media Gateway Addresses and Password 95
Configuring the Telephone Media Gateway 104
Enabling Telephone Interconnect on the ASTRO 25 System in the UNCW Process 107
Configuring the NEC UNIVERGE 3C System 109
Enabling the Enhanced Telephone Interconnect Voice Announcement Feature 128
Recovering the Telephone Media Gateway 166
Recovering the IP PBX Server 167
Recovering an IP PBX Media Gateway 169

List of Procedures

Mounting the Telephone Media Gateway Hardware 65
Provisioning the Telephone Media Gateway Serial Connection Parameters 67
Configuring the Telephone Media Gateway in the CSS (Ethernet Connection) 68
Setting the Software Download Manager Transfer Mode 70
Setting the Telephone Media Gateway Local Password Configuration 70
Setting the Date and Time on the Telephone Media Gateway 72
Setting the Serial Security Services 72
Changing SNMPv3 Configuration and User Credentials on the Telephone Media Gateway 73
Adding or Modifying an SNMPv3 User 75
Verifying an SNMPv3 Connection in the CSS 76
Customizing the Login Banner in the CSS 77
Connecting the Telephone Media Gateway to the Network 78
Discovering the Telephone Media Gateway Devices with the UNC 78
Loading the Telephone Media Gateway OS Images to the UNC 80
Enabling FTP Service in Telephone Media Gateway Devices 81
Transferring and Installing the OS Image to Telephone Media Gateway Devices 81
Inspecting Device Properties for Software Transferred and Installed to Telephone Media Gateway Devices 83
Disabling FTP Service 83
Mounting the Dell Server and Optional Media Gateways 86
Establishing the Telco Connection for the NEC BranchHub Media Gateway 87
Establishing the Telco Connection for the NEC COHub Media Gateway 87
Installing the UNIVERGE 3C Software on the IP PBX Server 89
Installing Service Pack 3 on the IP PBX Server 91
Setting Permissions for the UCM Server 93
Commissioning the UNIVERGE 3C Software of the Console of the IP PBX Server 94
Configuring the IP PBX Media Gateway Addresses 96
Configuring the IP PBX Media Gateway Password 97
Configuring the IP Address of the Unified Communications Manager Server 97
Joining the Unified Communications Manager Server to the ASTRO 25 Domain 98
Configuring Syslog Messaging 98
Configuring Remote Desktop for the Unified Communications Manager 99
Sharing the UNIVERGE 3C File System 99
Commissioning the UNIVERGE 3C Unified Communications Manager 100
Updating the UNIVERGE 3C License File 101
Installing the Auto Attendant Voice Prompt File 102

Establishing the TDMA Interconnect Mode 105
Loading Encryption Keys 105
Configuring Interconnect Calls in the UNCW 107
Configuring Disallowed Dialing Patterns 108
Creating Mapping Lists for Non-DID Calls 110
Creating Mapping Lists for DID Calls 111
Creating a Number Range for Mapped Non-DID Numbers 112
Creating a Number Range for Mapped DID Numbers 113
Creating the Auto Attendant Extension 113
Setting the Auto Attendant Greeting and Schedule 114
Replacing the American English Greeting 115
Adding Restricted Numbers to the Number Range Lists 116
Configuring Automatic Route Selection for Restricted and Non-Restricted Calls 116
Configuring Dialing Rule Overrides 117
Activating Automated Route Selection 117
Configuring the BranchHub Media Gateway 118
Configuring the COHub Media Gateway 119
Creating the Zone Controller SIP Trunk User Agent 121
Creating and Configuring a ZC SIP Trunk 123
Reading the License File 125
Changing the Computer Name 125
Enabling Music On Hold 128
Enabling Voice Announcements 129
Customizing Voice Announcements 129
Turning on the Telephone Media Gateway 133
Turning off the Telephone Media Gateway 133
Rebooting the Telephone Media Gateway by Power Cycling the Hardware 133
Rebooting the Telephone Media Gateway in the CSS 134
Rebooting the Telephone Media Gateway in the UEM 134
Viewing Status in the UNC 136
Launching the NEC UNIVERGE 3C System 137
Backing Up the UNIVERGE 3C System Database 138
Formatting a DVD-R on Windows Server 2008 R2 138
Scheduling Automatic Database Backup 139
Restoring the UNIVERGE 3C 7.1 System Database 139
Restoring the UNIVERGE 3C 8.5.2.3 System Database 140
Replacing the TMG Battery 141
Verifying SRV Records on the Domain Controller 148
Adding or Deleting UNIVERGE 3C Active Directory User/Group Accounts 148

Modifying the DB Level to Resolve Mobile to Land Call Issues 151
Using IP PBX Group Objects for Auditing and Security 152
Replacing the Telephone Media Gateway 155
Upgrading to UNIVERGE 3C Version 8.5.2.3 171
Upgrading to UNIVERGE 3C Version 8.5.2.3 Service Pack 3 172

About Enhanced Telephone Interconnect

The ASTRO® 25 Enhanced Telephone Interconnect feature provides a way to connect the radio communication system to the Public Switched Telephone Network (PSTN) or an external IP network, so that a subscriber radio user can dial fixed telephones (cellular phones included) and initiate a half duplex phone conversation. Likewise, a landline telephone user can dial ASTRO® 25 system radios using one of two methods detailed in this manual when the Enhanced Telephone Interconnect feature is employed on the system.

What Is Covered In This Manual?

This manual is organized into the following chapters:

- Chapter Enhanced Telephone Interconnect Description on page 21 provides a high-level description of the Enhanced Telephone Interconnect feature and the function it serves on your system.
- Chapter Enhanced Telephone Interconnect Theory of Operation on page 39 explains how the Enhanced Telephone Interconnect feature works in the context of your system.
- Chapter Enhanced Telephone Interconnect Installation on page 62 details hardware and software installation procedures, as well as the initial configuration required for connectivity to the network for Enhanced Telephone Interconnect.
- Chapter Enhanced Telephone Interconnect Configuration on page 104 details configuration procedures and fault management application discovery relating to Enhanced Telephone Interconnect.
- Chapter Enhanced Telephone Interconnect Optimization on page 131 is for optimization procedures and recommended settings relating to the Enhanced Telephone Interconnect.
- Chapter Enhanced Telephone Interconnect Operation on page 133 is for tasks performed once Enhanced Telephone Interconnect is operational on your system.
- Chapter Enhanced Telephone Interconnect Maintenance on page 141 describes maintenance instruction for Telephone Interconnect.
- Chapter Enhanced Telephone Interconnect Troubleshooting on page 143 provides fault management and troubleshooting information relating to Enhanced Telephone Interconnect.
- Chapter Enhanced Telephone Interconnect FRU/FRE on page 155 describes Field Replaceable Units (FRU) and Field Replaceable Entities (FRE) relating to the Enhanced Telephone Interconnect feature.
- Chapter Enhanced Telephone Interconnect Reference on page 158 describes additional reference information on the Voice Processor Module (VPM) hardware ports, cabling, LEDs, and more when used as a Telephone Media Gateway (TMG).
- Chapter Enhanced Telephone Interconnect Disaster Recovery on page 166 provides disaster recovery information for the Enhanced Telephone Interconnect feature.
- Enhanced Telephone Interconnect Software Upgrade from 7.1 to 8.5.2.3 SP3 on page 171 provides upgrade procedures for systems running UNIVERGE 3C Server software 7.1 to move to version 8.5.2.3 with Service Pack 3 (SP3).

Helpful Background Information

Motorola offers various courses designed to assist in learning about the system. For information, access http://www.motorolasolutions.com/training to view the current course offerings and technology paths.

Related Information

See the following documents for information about the radio system.

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known as R56 manual. This document may be purchased by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
System Overview and Documentation	Provides an overview of the ASTRO® 25 new system features, documentation set, technical illustrations, and system-level disaster recovery that support the ASTRO® 25 radio communication system.
Call Processing and Mobility Management Feature Guide	Describes the behavior of various ASTRO® 25 system infrastructure components and subscriber radios as they process calls and manage subscriber mobility.
Core Security Management Server Feature Guide	Provides information relating to implementation and management of basic network security software components in an ASTRO® 25 system. This includes server functions and client functions that support multi-factor RADIUS authentication for remote users accessing the system through a modem and terminal server. Information is also included about the server functions for managing system-wide antivirus protection. The CSMS is also a host for the firewall management user interface (details are available in the *Fortinet Firewall Manager User Guide*.)
Fortinet Firewall Feature Guide	Provides information about the Fortinet firewall hardware appliances including installation, replacement, and LEDs.
Fortinet Firewall Manager User Guide	Provides information relating to the implementation of server software and user interface software supporting firewall management using Fortinet hardware in an ASTRO® 25 system.
Information Assurance Reference Guide	Provides an overview of Information Assurance features for ASTRO® 25 systems, including a description of each feature and their impact on system implementation and management. Additionally, the manual contains details about Motorola Solutions services related to Information Assurance and physical security considerations for ASTRO® 25 systems.
Key Management Facility User Guide	Provides information regarding the Secure Communications features of the ASTRO® 25 system.
KVL 3000 Key Variable Loader User Guide	Provides information for the KVL 3000 Key Variable Loader equipment.

Related Information	Purpose
KVL 3000 Plus User Guide	Provides information for the KVL 3000 Plus Key Variable Loader equipment.
KVL 4000 Key Variable Loader ASTRO 25 User Guide	Provides instructions for using the Key Variable Loader (KVL) to create and store encryption keys, and then load them into other Motorola Solutions secure equipment, such as radios, fixed encryption units, digital interface units (DIUs), and others, in ASTRO® 25 operating mode.
Master Site Infrastructure Reference Guide	Provides site-level information required to install and maintain equipment at the ASTRO® 25 system master site/zone core.
MCC 7500 Dispatch Console with VPM User Guide	Provides information about the VPM hardware as it is being used as the audio interface for the MCC 7500 console subsystem.
SmartX Site Converter Feature Guide	Provides information about the VPM hardware as it is being used as the interface between SmartZone® , OmniLink, and SMARTNET® 3600 systems and the ASTRO® 25 system. This application also requires a site gateway.
Voice Processor Module User Guide	Provides additional information on the VPM hardware platform, which is used for the Telephone Media Gateway.
Windows Supplemental Configuration Setup Guide	Provides additional configuration information for the IP PBX server using the Windows 2008 Server Operating System, which is also referred to as a Telephony Server on the *Windows Supplemental* media Graphical User Interface.
Zone Controller Feature Guide	Covers the zone controller, a key component of the ASTRO® 25 system master site/zone core. Includes information on the installation, configuration, and management of this software application.

This table provides non-Motorola documentation required to install and configure the NEC equipment used in the ASTRO® 25 system for the Enhanced Telephone Interconnect feature.

Document	Purpose
NEC Install and Configure the UNIVERGE 3C System	NEC UNIVERGE 3C software documentation for the installation and configuration of the NEC UNIVERGE 3C IP PBX used in the ASTRO® 25 system Enhanced Telephone Interconnect solution. Designated as Book 2 in the UNIVERGE 3C documentation suite.
NEC Integrate UNIVERGE 3C Partner Technologies	NEC UNIVERGE 3C software documentation for the operation of the NEC UNIVERGE 3C IP PBX used in the ASTRO® 25 system Enhanced Telephone Interconnect solution. Designated as Book 4 in the UNIVERGE 3C documentation suite.
NEC BranchHub Installation Manual	NEC documentation that provides all specifications, operational, and installation information on the NEC BranchHub Media Gateway hardware.
NEC COHub Installation Manual	NEC documentation that provides all specifications, operational, and installation information on the NEC COHub Media Gateway hardware.

Chapter 1

Enhanced Telephone Interconnect Description

This chapter provides a high-level description of the Enhanced Telephone Interconnect subsystem and the function it serves on your system.

1.1 Enhanced Telephone Interconnect Introduction

The Enhanced Telephone Interconnect (ETI) subsystem is a Voice-over-IP (VoIP) solution that provides individual subscriber radios the ability to access the Public Switched Telephone Network (PSTN) using Internet Protocol (IP) Private Branch Exchange (PBX) equipment.

The ETI subsystem allows a subscriber radio user the ability to dial telephones (fixed or cellular phones) from an ASTRO® subscriber radio to initiate a half-duplex phone conversation. It also allows a telephone user the ability to dial subscriber radios directly using a telephone number reserved for the ASTRO® subscriber radio (Direct Dial Number) or indirectly by dialing a central number to access the home zone of the subscriber followed by over-dialing to access the subscriber by entering in the subscriber ID to initiate the call.

When integrated into the ASTRO® 25 trunked radio system, the ETI solution provides high quality telephone interconnect features. The ETI subsystem can be integrated per zone or per system.

For a list of terms associated with this feature, see Enhanced Telephone Interconnect Terminology on page 32.

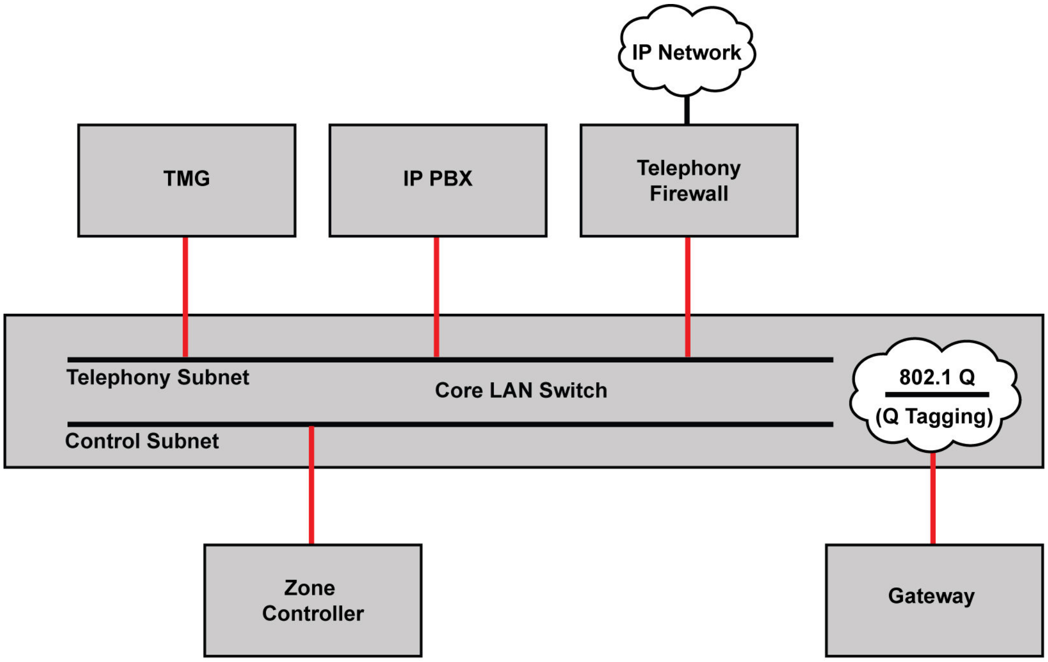
1.2 Enhanced Telephone Interconnect Physical Description

The Enhanced Telephone Interconnect (ETI) subsystem consists of the:

- Telephone Media Gateway (TMG)
- NEC UNIVERGE 3C system, which may consist of two types of components: the IP Private Branch Exchange (PBX) server and the IP PBX media gateways (if telephony firewall is not used).
- Telephony firewall, which connects to the IP network (IP PBX server or third party media gateway)

Figure 1: Enhanced Telephone Interconnect Subsystem with Telephony Firewall

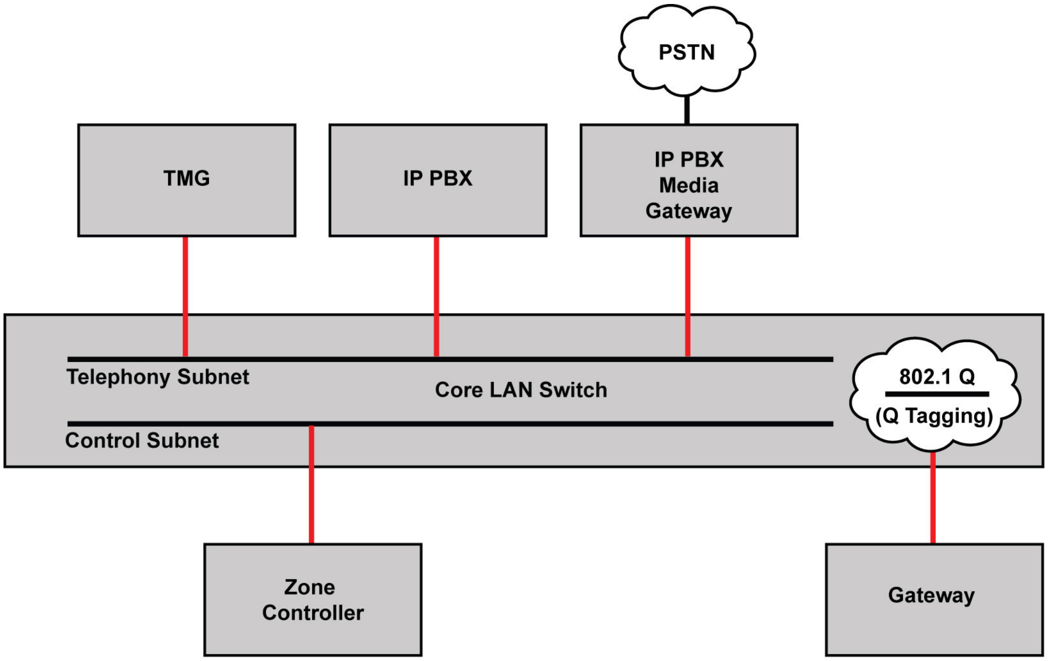
The following illustration shows the ETI subsystem with the telephony firewall, which is used for IP connectivity. A firewall is required only when a non-NEC media gateway (COHub or BranchHub) is used or when no media gateway is used at all (Session Initiation Protocol (SIP) connection to a third-party switch).



Zone_Core_ETI_subsystem_w_telephony_firewall_B

Figure 2: Enhanced Telephone Interconnect Subsystem without Telephony Firewall

The following illustration depicts the ETI subsystem with the IP PBX media gateway, which is used in place of the telephony firewall and provides E1, T1, and analog connectivity to the Public Switched Telephone Network (PSTN).



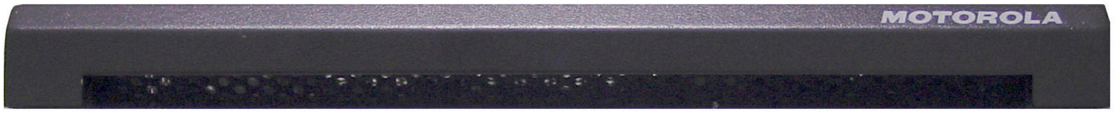
Zone_Core_ETI_subsystem_B

1.2.1 Telephone Media Gateway

The Telephone Media Gateway (TMG) is based on the Voice Processor Module (VPM) hardware platform. Specialized software allows the VPM to perform the tasks required for TMG operation. This hardware requires one rack unit (RU) of space at the zone core. For specifications on the hardware see the *Voice Processor Module User guide*.

The following figure shows the front of the TMG.

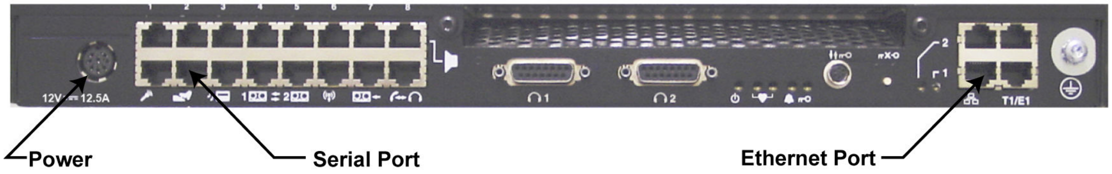
Figure 3: Telephone Media Gateway Front View



Telephone_Media_Gateway_front

The following figure illustrates the rear of the TMG with the ports illustrated. Note that the Serial port, which is used for the device configuration, has a foot switch icon below it.

Figure 4: Telephone Media Gateway Rear View



Telephone_Media_Gateway_rear1

The TMG translates audio between the ASTRO® 25 AMBE audio and IP Private Branch Exchange (PBX) G.711 audio. The TMG supports both encrypted and clear audio to and from the ASTRO® 25 network. All audio exchanged with the IP PBX is clear. If encryption is required, sending encryption keys from the Key Management Facility (KMF) to the TMG consoles can be accomplished either by using the Key Variable Loader (KVL) device or by sending it through the network with the Over-the-Ethernet-Keying (OTEK).

The TMG performs the following functionality under the control of a Zone Controller (ZC) and Key Management Subsystem (KMS):

- Converts a P25–compliant media stream (vocoded w/ AMBE) to standard IP telephony media stream (G.711).
- Generates tones in the media stream sent to the IP PBX media gateway to enable DTMF overdial from the subscriber radio, generates a go-ahead tone to the landline to facilitate a half-duplex conversation, and generates the Final Alert tone to both the landline and radio users (replaces the Tone Generation Service used in the previous ASTRO® 25 telephone interconnect solution).
- Generates ringback to the subscriber radio during radio-to-landline calls (North America ringback only).
- Encrypts/decrypts audio to support secure communication between ASTRO® 25 subscribers and the TMG. The supported encryption algorithms include: Data Encryption Standard-Output Feedback (DES-OFB), Data Encryption Standard (DES-XL), Digital Voice International (DVI-XL), Digital Voice Protection (DVP-XL), Advanced Encryption Standard (AES), and Advanced Digital Privacy (ADP). However, the encryption algorithms loaded on a TMG has a direct impact on number of simultaneous calls that a TMG can support:
  - 6 calls when using DVI-XL and DVP-XL
  - 12 calls when using DES-XL
  - 15 calls when using DES-OFB, AES, ADP, or no encryption

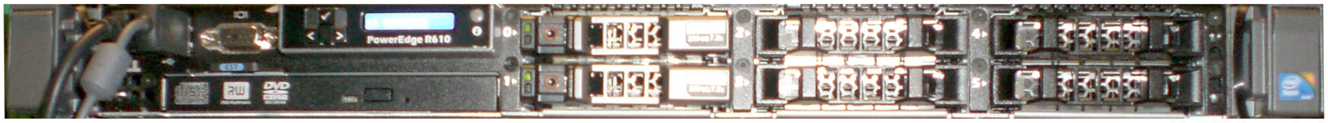
Multiple algorithms can be loaded, but the capacity is always the lowest of the algorithms present in the system.

NOTICE: The algorithms that the various Motorola subscriber radio models support are restricted. Consult the user guides for the radios used within your system.

1.2.2 IP PBX Server

The IP Private Branch Exchange (PBX) server is a Dell PowerEdge R 610 computer server using the Windows Server 2008 R2 operating system that requires one Rack Unit (RU) of space at the zone core.

Figure 5: IP PBX Server Front View



IP_PBX_Server_front

The IP PBX server, also called the NEC Unified Communications Manager, provides call control and administration through a network management application that provides configuration and fault management of the IP PBX server and IP PBX media gateways. The Unified Communications Manager connects to the external IP network (through a telephony firewall) when connecting to an external VoIP network (your enterprise IP PBX or a non-NEC media gateway).

The IP PBX server can be accessed locally or through Remote Desktop Protocol (RDP) from a computer that is within the ASTRO 25 radio network.

NOTICE: NEC documentation that ships with these products provides all the NEC UNIVERGE 3C system hardware and software specifications. You can also download the documentation at the manufacturer Web site.

1.2.2.1 NEC UNIVERGE 3C Software

The NEC UNIVERGE 3C architecture relies on the 3C Administrator software application, which resides on a computer running Windows 2008 Server. The 3C Administrator application provides a standard Windows GUI environment for users. The NEC UNIVERGE 3C application ships pre-installed on the server.

1.2.3 IP PBX Media Gateway

IP Private Branch Exchange (PBX) media gateways convert signals (both signaling and voice) between IP and non-IP networks, under the control of the IP PBX server. Multiple media gateways may be required based on the capacity your ASTRO® 25 system requires, and each one takes one Rack Unit (RU) of space. An IP PBX media gateway is not needed if landline telephones are connected through an IP network, for example, a non-NEC media gateway or your enterprise IP PBX media gateway.

An IP PBX media gateway is needed if landline telephones are connected though T1/E1 or analog lines. IP PBX media gateways are automatically discovered and partially configured by the Unified Communications Manager. The IP addresses for the IP PBX media gateways is manually set using the Command Line Interface (CLI) through the serial port. All other maintenance procedures can be done through the Administrator utility. The IP PBX media gateways covered in this document include NEC BranchHub media gateway and NEC COHub media gateway. Both are for domestic US market and some international countries where they meet the line type approvals. Additional third-party media gateways are available from Network Equipment Technologies (NET) for use in locations where the NEC equipment is not approved. See Table 1: Media Gateway Equipment Public Switched Telephone Network Type Approvals by Country on page 25 for details on the NEC and third party (that is, NET development gateways) hardware approvals by country.

NOTICE: Network Equipment Technologies equipment may also be referred to by the NET Quintum or NET Tenor names in other documentation.

Table 1: Media Gateway Equipment Public Switched Telephone Network Type Approvals by Country

Country	NEC BranchHub	NEC COHub	NET AXT800 - Analog Trunk Gateway - Development Gateway	NET DX2024 - Digital Telephony Media Gateway T1 - Development Gateway	NET DX2030 - Digital Telephony Media Gateway E1 - Development Gateway
United States	✓	✓	✓	✓	✓
Canada	✓	✓	✓	✓	✓
Mexico	✗	✓	✓	✓	✓
Puerto Rico	✓	✓	✓	✓	✓
Uruguay	✗	✗	✗	✗	✗
Chile	✗	✗	✗	✓	✓
Brazil	✗	✗	✓	✓	✓
Peru	✗	✗	✓	✓	✓
Barbados	✗	✗	✓	✓	✓
Columbia	✗	✗	✓	✓	✓
Uzbekistan	✗	✗	✗	✗	✗
Saudi Arabia	✗	✗	✗	✗	✗
Russia	✗	✗	✓	✓	✓
Latvia	✗	✗	✓	✓	✓
Turkey	✗	✗	✓	✓	✓
Qatar	✗	✗	✗	✗	✗
Australia	✗	✗	✓	✓	✓
New Zealand	✗	✗	✓	✓	✓
Malaysia	✗	✗	✓	✓	✓
India	✗	✗	✗	✗	✗
Indonesia	✗	✗	✗	✗	✗
Thailand	✗	✗	✗	✓	✓

Country	NEC Branch-Hub	NEC COHub	NET AXT800 - Analog Trunk Gateway - Development Gateway	NET DX2024 - Digital Telephony Media Gateway T1 - Development Gateway	NET DX2030 - Digital Telephony Media Gateway E1 - Development Gateway
Taiwan	✗	✗	✓	✓	✓
South Korea	✗	✗	✗	✗	✗
Sri Lanka	✗	✗	✗	✗	✗
Vietnam	✗	✗	✗	✗	✗
Philippines	✗	✗	✗	✓	✓
Bangladesh	✗	✗	✓	✓	✓
Brunei	✗	✗	✗	✗	✗
Japan	✗	✗	✓	✓	✓
Germany	✗	✓	✓	✓	✓
United Kingdom	✗	✓	✓	✓	✓
Italy	✗	✓	✓	✓	✓
Spain	✗	✓	✓	✓	✓
France	✗	✓	✓	✓	✓
Netherlands	✗	✓	✓	✓	✓
Luxemburg	✗	✓	✓	✓	✓
Belgium	✗	✓	✓	✓	✓
Denmark	✗	✓	✓	✓	✓
Austria	✗	✓	✓	✓	✓
Switzerland	✗	✓	✓	✓	✓
Norway	✗	✓	✓	✓	✓
Sweden	✗	✓	✓	✓	✓
South Sudan	✗	✗	✗	✗	✗
Poland	✗	✓	✓	✓	✓
Slovakia	✗	✓	✓	✓	✓
Czech Republic	✗	✓	✓	✓	✓
Israel	✗	✗	✓	✓	✓

The following table provides the certification types for the NEC IP PBX media gateways. If your system requires an alternate solution, see Table 3: Certifications for Third-Party Media Gateways on page 29 for the third-party media gateway certification types.

Table 2: Certifications for IP PBX Media Gateways

IP PBX Media Gateway	Part Number	Certification Types
NEC BranchHub	TT05502AA	FCC Part 15, WEEE, RoHS, FCC Part 68 (reg. # 5INT06ABH1830), TUV-R (reg. # 72080978), UL STD 60950.1 2003, CAN/CSA STD C22.2 No 60950.103 reg. # IC: 3057A-BH1830
NEC COHub	TT05503AA	CE, FCC Part 15, WEEE, RoHS, FCC Part 68 (reg. # 5INDDANCH2430), TUV-R (reg. # 72080539), UL STD 60950 2000, CAN/CSA STD C22.2 No 60950 reg. # IC: 3057A-CH2430

If the COHub and/or BranchHub media gateway do not have the line type approvals required for a particular installation, a common solution is to connect the COHub and/or BranchHub media gateway to another PBX. In some instances, a PBX is already deployed by the end user and is connected to the PSTN (and has the line type approvals required). The COHub or BranchHub media gateway can then be connected to this PBX (which in most cases alleviates the requirement for the COHub or BranchHub media gateway to have the local line type approval). Alternately, if a local PBX is not available, other third-party IP PBX media gateways can be deployed. See Table 3: Certifications for Third-Party Media Gateways on page 29. Contact Motorola for assistance in selecting a third-party IP PBX media gateway that has the local line type approvals and is compatible with the Enhance Telephone Interconnect (ETI) subsystem.

IMPORTANT: This documentation supports the NEC UNIVERGE 3C solution for the IP PBX media gateways though alternative media gateways exist that work with this system. Any media gateway used must support the Session Initiation Protocol (SIP) protocol and comply to line type approvals for a given country.

Each ETI subsystem supports up to four IP PBX media gateways. The individual call capacity for the IP PBX media gateway is six simultaneous calls on BranchHub MG (analog) and 23 (T1 ISDN)/24 (T1 CAS) or 30 (E1) on the COHub MG (digital). Thus, an ETI subsystem supports a maximum of 24 calls, if four BranchHub media gateways are installed. An ETI subsystem can support up to a maximum of 120 simultaneous calls, if four COHub media gateways are installed with E1 interfaces. BranchHub and COHub media gateways may be installed in the same ETI subsystem.

NOTICE: The NEC documentation that ships with these products provides all NEC UNIVERGE 3C system hardware and software specifications. You can also download the documentation at the manufacturer Web site.

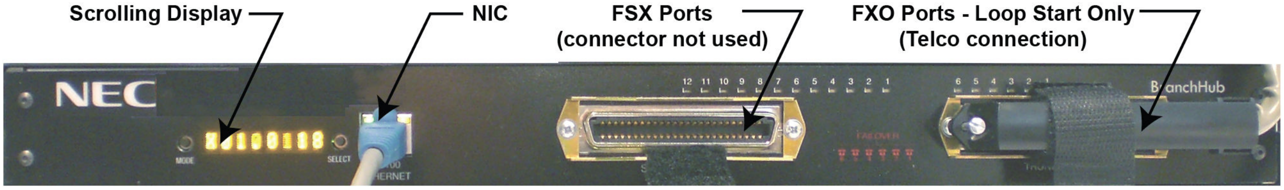
1.2.3.1 NEC BranchHub Media Gateway

An NEC BranchHub IP Private Branch eXchange (PBX) media gateway connects to both the ASTRO® 25 radio network and telephone lines. The BranchHub media gateway supports a maximum of six analog loop start trunk lines using a single 50-position connector wired per USOC RJ-21X configuration. This media gateway uses a broadband Ethernet connection to communicate with the rest of the IP Private Branch Exchange (PBX) server/Unified Communications Manager and the ASTRO® 25 system.

The BranchHub Media Gateway requires one Rack Unit (RU).

Figure 6: NEC BranchHub Media Gateway Front View

The following photograph shows the front of the NEC BranchHub media gateway mounted in a rack.



NEC_MG_BranchHub_front1

NOTICE: If your system requires ground start trunk lines, commercial ground start/loop start converter products are available.
The BranchHub media gateway does not support Direct Inward Dialing (DID) over an analog connection.

1.2.3.2

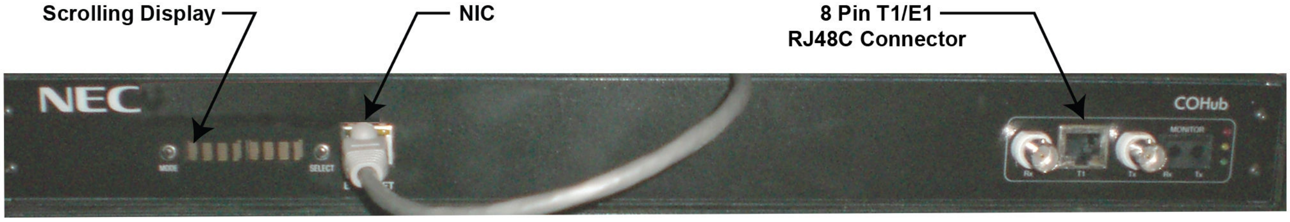
NEC COHub Media Gateway

An NEC COHub IP Private Branch Exchange (PBX) media gateway contains the hardware and software to interface a digital Time-Division Multiplexing (TDM) circuit to a private network. T1 Channel Associated Signaling (CAS) and Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) and E1 PRI circuits are supported. The digital TDM circuit and a network media stream pass 23 ISDN channels, 24 CAS channels, 30 E1 ISDN channels, and 30 E1/R2 channels of voice communication between them in real time. This media gateway uses industry standard RJ48 connector. The COHub media gateway also uses a broadband Ethernet connection to communicate with the rest of the Unified Communications Manager and the ASTRO® 25 system.

The COHub media gateway requires one Rack Unit (RU) of space.

Figure 7: NEC COHub Media Gateway Front View

The following photograph shows the front of the NEC COHub media gateway mounted in a rack.



NEC_MG_COHub_front1

1.2.4

Third-Party Media Gateways

If the NEC COHub and/or BranchHub do not have the line type approvals required for a particular installation, other third-party IP Private Branch Exchange (PBX) media gateways can be deployed. Contact Motorola for assistance in selecting a third-party IP PBX media gateway that has the local line type approvals and is compatible with the Enhanced Telephone Interconnect (ETI) subsystem.

NOTICE: If your system is using a third-party IP PBX media gateway, a telephony firewall is required. See Telephony Firewall on page 29 for more information.

Options include the NET AX (analog) or DX (digital T1 or E1) Series Development Gateway. These alternative IP PBX media gateways can be ordered through Motorola. See Table 1: Media Gateway

Equipment Public Switched Telephone Network Type Approvals by Country on page 25 and Table 3: Certifications for Third-Party Media Gateways on page 29 for details.

Table 3: Certifications for Third-Party Media Gateways

Third Party Media Gateway	Part Number	Certification Types
NET AXT800 - Analog Trunk Gateway - Development Gateway	TT05504AA	CE, WEEE (officially in UK, France, Netherlands), RoHS, FCC, UL
NET DX2024 - Digital Telephony Media Gateway T1 - Development Gateway	TT05505AA	CE, WEEE (officially in UK, France, Netherlands), RoHS, FCC, UL
NET DX2030 - Digital Telephony Media Gateway E1 - Development Gateway	TT05506AA	CE, WEEE (officially in UK, France, Netherlands), RoHS, FCC, UL

1.2.5

Telephony Firewall

The Fortinet FortiGate 100D is the default hardware model.

Figure 8: Fortinet FortiGate 100D Front View

In configurations where the NEC IP Private Branch Exchange (PBX) server is connected to an external IP network (as opposed to connection to T1/E1 or analog circuits), a telephony firewall is needed to safeguard the ASTRO® 25 network from outside threats including worms, virus, Trojans, spam, and emerging malware. The connection to an external IP network can be either a Customer Enterprise Network (CEN) containing an IP PBX server or a third-party media gateway.

The telephony firewall is also required for customers who need a third-party media gateway for country specific line type approvals not met by NEC UNIVERGE 3C solution. if the telephony firewall is not used, the other brands of Media Gateways are accessed through IP (Session Initiation Protocol) and could pose a risk to the system.

The telephony firewall is managed by Network and Security Manager software residing on a firewall management server, with a graphical user interface located on a Windows server at the zone core. See the *Fortinet Firewall Feature Guide* for more information on the FortiGate 100D hardware and the *Fortinet Firewall Manager User Guide* for the firewall management system software information and instructions for adding firewalls to the firewall management system.

NOTICE: If your system has an intersystem firewall in the zone where Enhanced Telephone Interconnect is present, that ISG 1000 firewall can also serve as the telephony firewall.

1.2.6
Additional Motorola Equipment Interfacing the Enhanced Telephone Interconnect Subsystem

The following ASTRO® 25 system infrastructure devices interface with the Enhanced Telephone Interconnect (ETI) subsystem components:

Gateways

Provides transport between zone controllers and Telephone Media Gateways (TMGs) using 100Base-T interfaces. To reduce the impact of potential gateway failures, when more than one TMG is installed, TMGs may be evenly split among gateways (up to two gateways per zone). This arrangement ensures that, in the event of a gateway failure, all control traffic between the zone controller and TMG is not lost. The gateways also provide transport between the zone controller and the IP Private Branch Exchange (PBX) server. In the event of a gateway failure, the control traffic between the zone controller and the IP PBX server is not lost.

Zone Controller

Supports and manages resource allocation (RF channel, TMG) for telephone interconnect calls. Each redundant zone controller is connected to the ETI subsystem through an IP interface.

Zone Core Local Area Network (LAN) switch

Establishes the connections between the zone controllers (and the sites) and the ETI subsystem equipment. Also known as the master site LAN switch.

Private Radio Network Management

Includes the Motorola system and zone level network management server functionality in the zone core, as well as the configuration and fault management applications. See the following manuals for more information:

- *Master Site Infrastructure Reference Guide*
- *Private Network Management Client Feature Guide*
- *Private Network Management Servers Feature Guide*
- *Unified Network Configurator User Guide*
- *Provisioning Manager User Guide* (for subscriber radios)
- *Unified Event Manager User Guide*

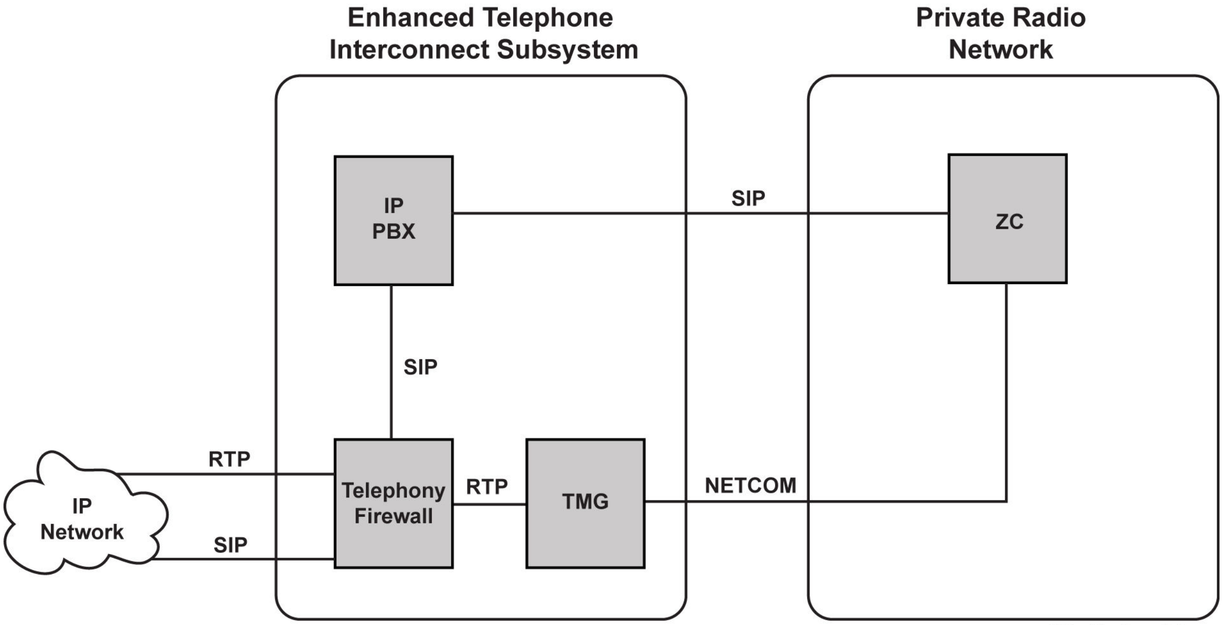
1.3
Enhanced Telephone Interconnect Components and the ASTRO 25 System

The ASTRO® 25 Enhanced Telephone Interconnect (ETI) subsystem provides a means to connect the radio system to the Public Switched Telephone Network (PSTN) or external IP network. This subsystem enables a subscriber to initiate and receive calls through the PSTN or external IP network using one of two configurations:

- Telephony firewall for IP connectivity
- IP PBX media gateway for circuit connectivity

Figure 9: Enhanced Telephone Interconnect Subsystem with Telephony Firewall

The following figure illustrates the ASTRO® 25 ETI configuration with a telephony firewall and shows only Real-time Transport Protocol (RTP) audio within the ETI subsystem. Also audio (AMBE/XIS) comes in from the ASTRO® 25 network to the TMG.



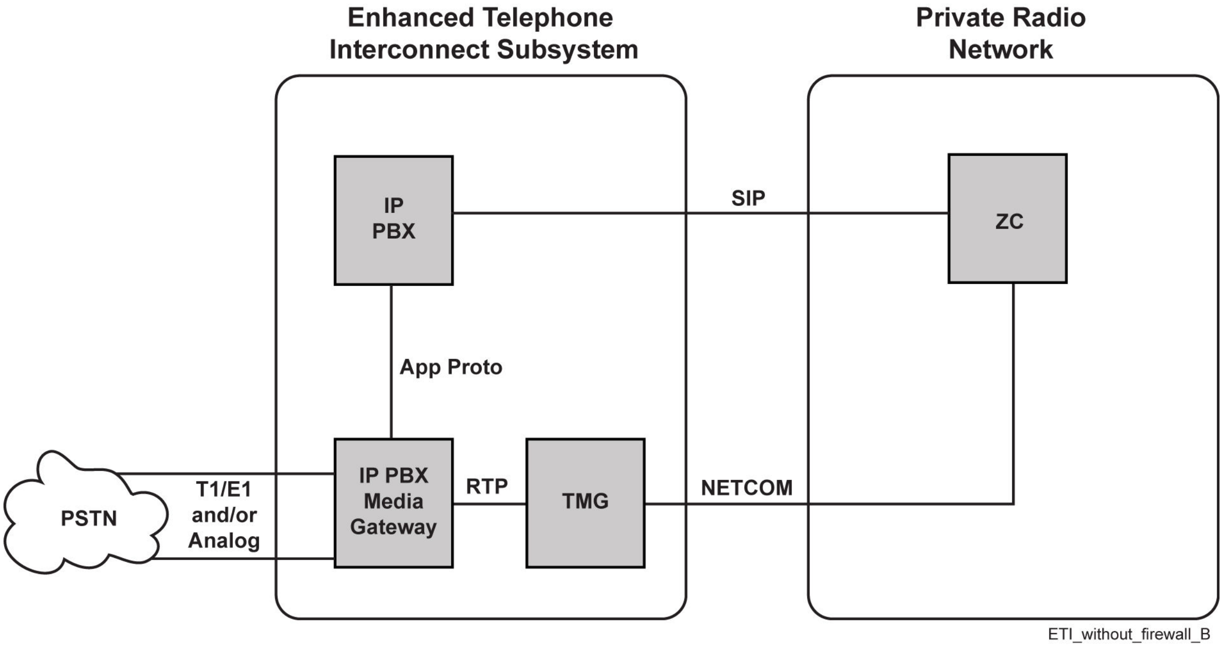
ETI_with_firewall_B

IMPORTANT: A system with an NET Media Gateway is considered outside the ASTRO® 25 zone core, and a telephony firewall must be present.

NOTICE: In a system with an intersystem firewall in the zone where ETI is present, that ISG 1000 firewall can also serve as the telephony firewall.

Figure 10: Enhanced Telephone Interconnect Subsystem without Telephony Firewall

The following figure illustrates the ASTRO® 25 configuration without a telephony firewall and shows only Real-time Transport Protocol (RTP) audio within the ETI subsystem. There is also audio (AMBE/XIS) coming in from the ASTRO® 25 network to the TMG.



The ASTRO® 25 system supports mobile-to-land and land-to-mobile interconnect calls. It does not support interconnect calls to and from talkgroups.

1.3.1 Call Types Support

A telephone user is able to dial subscriber radios using one of two techniques:

- A telephone user is able to directly dial a subscriber radio using a telephone number explicitly reserved for the ASTRO® subscriber radio Direct Inward Dial (DID).

  NOTICE: DID is only supported using a COHub set for a T1 CAS circuit emulating EM signaling.

- A telephone user is able to dial a central number for the ASTRO® system and then use Dual-Tone Multi-Frequency (DTMF) overdialing to enter the subscriber ID to initiate a call.

1.3.2 Audio Formats Support

Enhanced Telephone Interconnect in an ASTRO® 25 system supports G.711 encoded audio on the media plane between the Telephone Media Gateway (TMG) and IP Private Branch eXchange (PBX) media gateway or from the TMG through the firewall to a Voice over IP (VoIP) endpoint.

1.4 Enhanced Telephone Interconnect Terminology

The Enhanced Telephone Interconnect (ETI) subsystem references the following terms.

802.1Q

An IEEE networking protocol for the sharing of a physical Ethernet network connection by multiple independent logical networks Virtual LANs (VLANs) within a LAN switch. This protocol allows devices on different VLANs to communicate with one another through a single physical connection to a router. This scheme replaces the need for a dedicated physical connection between each VLAN in the LAN switch and a router. IEEE 802.1Q is also known as *VLAN Tagging* or *Q Tagging*.

Automated Attendant (AA)

Allows land-to-mobile calls to be handled without the use of a human attendant position. AA is a functionality of the IP Private Branch eXchange (PBX) server. A type of voice announcement.

Active Directory (AD)

Windows Active Directory.

Advanced Multi-Band Excitation (AMBE)

A speech coding standard.

Answer Supervision

The functionality for a Private Branch eXchange (PBX) to be signaled the exact moment when the called party has answered. Used mainly for billing purposes.

Answer Threshold

A timer used for determining when a call is considered to be active (in the conversation state). Answer threshold is used when answer supervision is not available.

Automatic Route Selection (AARS)

Allows the outbound mobile-to-land calls to specific numbers to be routed out specific trunks in a pre-determined order.

BranchHub

A media gateway that is part of the NEC Sphere IP PBX solution for ETI, which interfaces analog FXS and FXO ports with the IP media stream. Only FXO ports are used for Enhanced Telephone Interconnect.

Committee European for Postal and Telecommunications (CEPT)

An agency that deals with regulatory matters in the field of posts and telecommunications in Europe. The Electronic Communications Committee (ECC) develops radio communications policy and coordinates frequency, regulatory and technical matters concerning radio communications.

Central Office (CO)

Houses the telephone company equipment.

COHub

A media gateway that is part of the NEC Sphere IP PBX solution for ETI, which interfaces digital circuits with the IP media stream. The COHub is software configurable for T1 or E1 operation and can support Channel Associated Signaling (CAS) or various types of Integrated Services Digital Network (ISDN).

Core Security Management Server (CSMS)

Distributes the latest McAfee anti-malware updates to all subscriber devices using the CSMS McAfee Anti-Malware Client software.

Demarc

Demarcation Point. The point up to where the local Telco service provider is responsible for providing service at the customer location

Direct Inward Dialing (DID)

A calling method that allows land line subscribers to reach a target mobile for an interconnect call by only having to dial a pre-assigned directory telephone number instead of requiring intervention of an operator.

DS0

Digital Service level 0. An individual 64 Kbps timeslot within a T1 or E1 aggregate link.

DS1

Digital Service level 1. A circuit-based link comprising 24 DS0s. Traditionally, an E1 link is not described as a DS1 link but the term is often used interchangeably in the field.

Dual Tone Multiple Frequencies (DTMF)

The industry term for Touch Tone (Touch Tone was released to the public by ATT and is no longer a trademarked name).

E1

A 2.048 Mbps aggregate link comprised of 32 DS0s used for voice and data primarily in Europe. Also known as CEPT1.

Enhanced Telephone Interconnect (ETI)

Provides individual subscriber radios the ability to access the Public Switched Telephone Network (PSTN) using Internet Protocol (IP) PBX equipment in an ASTRO® 25 radio system. The ETI subsystem can be integrated per zone or per system.

FXO

Foreign eXchange Office. An FXO port interfaces the BranchHub MG with analog loop start service provided by the serving telephone company.

Ground start

A type of two-wire telephone service where the status of the line is positively indicated. The COHub MG supports ground start emulation while the BranchHub MG does not.

IP

Internet Protocol carries packets of data primarily in Ethernet-based systems. The IP is used by both User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). IP operates below UDP and TCP in the TCP/IP Internet layer. IP routes packets across interconnected networks and performs packet segmentation and reassembly functions.

IP PBX

A Private Branch eXchange that switches calls between Voice over Internet Protocol (VoIP) users on local lines while allowing all users to share some external phone lines. The typical IP PBX can also switch calls between a VoIP user and a traditional telephone user, or between two traditional telephone users in the same way that a conventional PBX does.

Integrated Services Digital Network (ISDN)

A type of service over a T1 or E1 circuit for providing voice, video, and data services. ISDN is not widely deployed domestically in the US, but is still popular in international countries.

JITC

Joint Interoperability Task Command. An initiative that defines interoperability between switching equipment and other IT-based equipment from different manufacturers.

Loop start

A common type of service found in residential and dial-up modem applications. A description of loop start operation is given in the BranchHub media gateway configuration section of this document. Commonly referred to as a Plain Old Telephone Service (POTS) line.

Media Gateway (MG)

The IP PBX MG is a physical hardware component of the softswitch architecture that converts traditional analog or digital media into RTP media streams using IP as the transport mechanism. However, the Telephone Media Gateway is another media gateway component of the ETI subsystem used to process audio.

Media Gateway Controller (MGC)

The service part of the softswitch application responsible for controlling the MGs.

Media Gateway Control Protocol (MGCP)

Rules MGCs use to control MGs.

Mobile
An alternative name for an ASTRO® 25 subscriber radio. ETI enables mobiles to make and receive landline calls within the ASTRO® 25 system.

Music On Hold (MOH)
Part of the Voice Announcement option used for land-to-mobile calls.

Nippon Electric Corporation (NEC)
A division of Western Electric founded in 1899.

Private Branch Exchange (PBX)
A telephone switching system within an enterprise.

Plain Old Telephone Service (POTS)
An industry term describing typical loop start residential service. A ground start line is not considered a POTS line.

Push-to-Talk (PTT)
This button on the subscriber radio is used to transmit to a landline user during an enhanced telephone interconnect call.

Q Tagging
See *802.1Q*.

Real-time Transport Protocol (RTP)
A UDP-based protocol for transporting media streams.

Session Initiation Protocol (SIP)
A protocol used for setting up, tearing down, or modifying an existing media connection for VoIP calls. RTP is used for media.

SIP trunk
A logical session between two SIP endpoints. In ETI, the SIP trunks run between the IP PBX server and the zone controller, the IP PBX server and the telephony firewall, as well as the telephony firewall and the IP network. SIP trunks can be used to restrict dialed digits.

Softswitch
A switching architecture where network hardware is separate from network software, used primarily for VoIP applications.

Soft trunk
A virtual trunk. In ETI, a SIP trunk is established as a soft trunk to restrict dialed digits from the subscribers on the ASTRO® 25 system (also called an “inactive trunk”).

Service Record (SRV)
A Service record in the Domain Name System (DNS) specifying the location of zone cores in the system. For ETI, there are two SRVs for the two zone cores per zone.

T1
A 1.544 Mbps aggregate link comprising 24 DS0s commonly used in the US and Japan. A T1 is also referred to as a DS1.

Telco
Telephone Company.

Telephone Media Gateway (TMG)
The device used to process audio in an ETI subsystem.

Trunk
A single phone line or multiple phone lines that share operational characteristics.

Uniform Resource Identifier (URI)
A SIP URI is used to identify an entity addressed through SIP, much like an e-mail address identifies the e-mail recipient.

Universal Service Ordering Code (USOC)
A code used when obtaining telephone service.

Voice over IP (VoIP)
A broad term used to describe using IP as a transport mechanism for voice applications.

X-Zone Infrastructure Signaling (XIS)
An audio protocol. The TMG is responsible for translating XIS packets with AMBE encoded audio into RTP packets with G.711 (A-law or ulaw) voice encoding.

Zone Controller (ZC)
The server application responsible for performing call processing.

Zone Network Management (ZNM)
An ASTRO® 25 subsystem that includes Virtual Management Server (VMS) 1 (ZC1, Zone Statistics Server, Air Traffic Router), VMS2 (ZC2, Unified Event Manager), Network Management Client, CSMS, and more.

1.5 Enhanced Telephone Interconnect Functionality

Enhanced Telephone Interconnect (ETI) provides ASTRO® 25 radio system customers with the following functionality:

- Mobile-to-land interconnect calls: Allows a subscriber radio user to dial telephone numbers using the interconnect feature to initiate a half-duplex phone conversation.
- Land-to-mobile interconnect calls: Allows a telephone user to initiate calls to subscriber radios using one of two methods: Direct Inbound Dialing (DID) and non-DID.
- Standards-based Session Initiation Protocol (SIP) connection to IP network from IP Private Branch eXchange (PBX) server
- E1/T1/analog connections to Public Switched Telephone Network (PSTN) through IP PBX media gateways
- DID functionality over T1/E1 with up to 4000 DID numbers
- Up to 120 simultaneous calls per ETI subsystem
- Dual-Tone Multi-Frequency (DTMF) (touch tone) overdialing
- Flexible, configurable dialing plan
- Support of Loop Start over analog trunks
- Interconnect call continuation after radio roaming
- Interconnect call timeout after maximum call duration
- Support for voice traffic encryption between ASTRO® 25 subscribers and Telephone Media Gateways (TMGs)
- Integrated ASTRO® 25 network management functionality, for both configuration and fault management of the TMG
- Voice announcements (for example, Automated Attendant)
- Call barring for preventing individual subscribers from dialing specific numbers
- Echo cancellation

1.5.1 Enhanced Telephone Interconnect Capabilities

The ASTRO® 25 system supports a maximum of one Enhanced Telephone Interconnect (ETI) subsystem per zone. The ETI subsystem is at a prime site and is directly connected to the zone core.

The maximum number of simultaneous calls supported by the ETI subsystem is 120, provided enough Telephone Media Gateways and other telephony resources are available (for example, IP Private Branch eXchange (PBX) media gateways).

1.5.1.1 Enhanced Telephone Interconnect Call Capabilities

Different configurations of the Enhanced Telephone Interconnect (ETI) subsystem support different call capacities. Because each added line adds an incremental cost, the end customer should purchase enough phone lines to support the anticipated call load. The following tables provide estimates for the call capacity supported during the busy hour based on the number of phone lines and desired grade of service.

Table 4: Percentage of Calls Queued 1%

Number of Phone Lines	Supported Call Volume (Erlangs)	Calls per Hour
4	0.6	36
8	3.0	180
12	5.4	324
16	7.8	468
20 (DS1)	10.8	648
24 (DS1)	13.8	828
30 (E1)	18.6	1116

Table 5: Percentage of Calls Queued 5%

Number of Phone Lines	Supported Call Volume (Erlangs)	Calls per Hour
4	1.2	72
8	3.6	216
12	6.6	396
16	9.6	576
20 (DS1)	13.2	792
24 (DS1)	16.2	972
30 (E1)	21	1260

Table 6: Percentage of Calls Queued 10%

Number of Phone Lines	Supported Call Volume (Erlangs)	Calls per Hour
4	1.8	108
8	4.2	252
12	7.8	468
16	10.8	648

Number of Phone Lines	Supported Call Volume (Erlangs)	Calls per Hour
20 (DS1)	14.4	864
24 (DS1)	17.4	1044
30 (E1)	22.8	1368

1.5.2 Enhanced Telephone Interconnect Feature Limitations

The Enhanced Telephone Interconnect (ETI) solution does not support the following:

- Phone calls to Talkgroups - only calls to individual subscribers are supported
- Audio Logging
- Analog conventional
- Digital conventional
- SmartX Site Converter (for 3600 remote sites)
- Inter SubSystem Interface (ISSI), which is a Project 25 network gateway interface
- Caller ID on subscriber radios

1.5.3 Enhanced Telephone Interconnect and Dynamic System Resilience

An Enhanced Telephone Interconnect (ETI) subsystem may not be deployed on a backup core for a zone deployed as a part of a Dynamic System Resilience (DSR) master site. The result is that telephone interconnect service is not available when a zone controller in a backup core is actively processing voice calls for that zone.

Chapter 2

Enhanced Telephone Interconnect Theory of Operation

This chapter explains how the Enhanced Telephone Interconnect works in the context of your ASTRO® 25 system.

2.1 Enhanced Telephone Interconnect Operation in an ASTRO 25 Trunked System

The Enhanced Telephone Interconnect (ETI) subsystem consists of Telephone Media Gateways (TMGs), IP Private Branch eXchange (PBX) server, and optional IP PBX media gateways (NEC COHub, NEC BranchHub media gateways) or optional telephony firewall .

The two ETI network configurations are described in terms of being with and without the telephony firewall.

Figure 11: The Enhanced Telephone Interconnect Network Configuration with a Telephony Firewall on page 40 illustrates the ETI network configuration where the telephony firewall is used for IP connectivity. A telephony firewall is required when supporting either of the following:

- A third-party (non-NEC) IP PBX media gateway
- A Session Initiation Protocol (SIP) interface to an external IP network

NOTICE: In a system with an intersystem firewall in the zone where ETI is present, that ISG 1000 firewall can also serve as the telephony firewall.

Figure 11: The Enhanced Telephone Interconnect Network Configuration with a Telephony Firewall

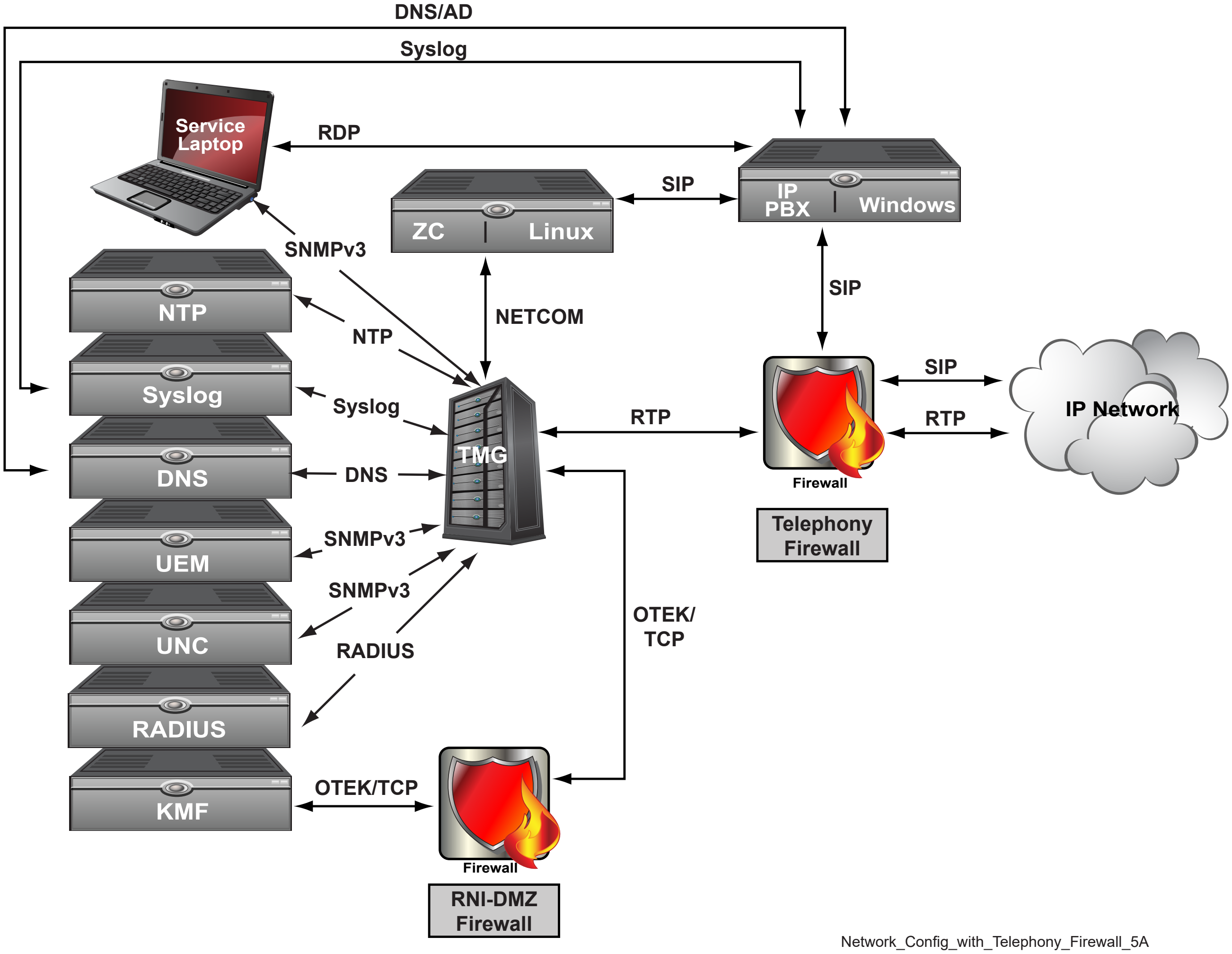
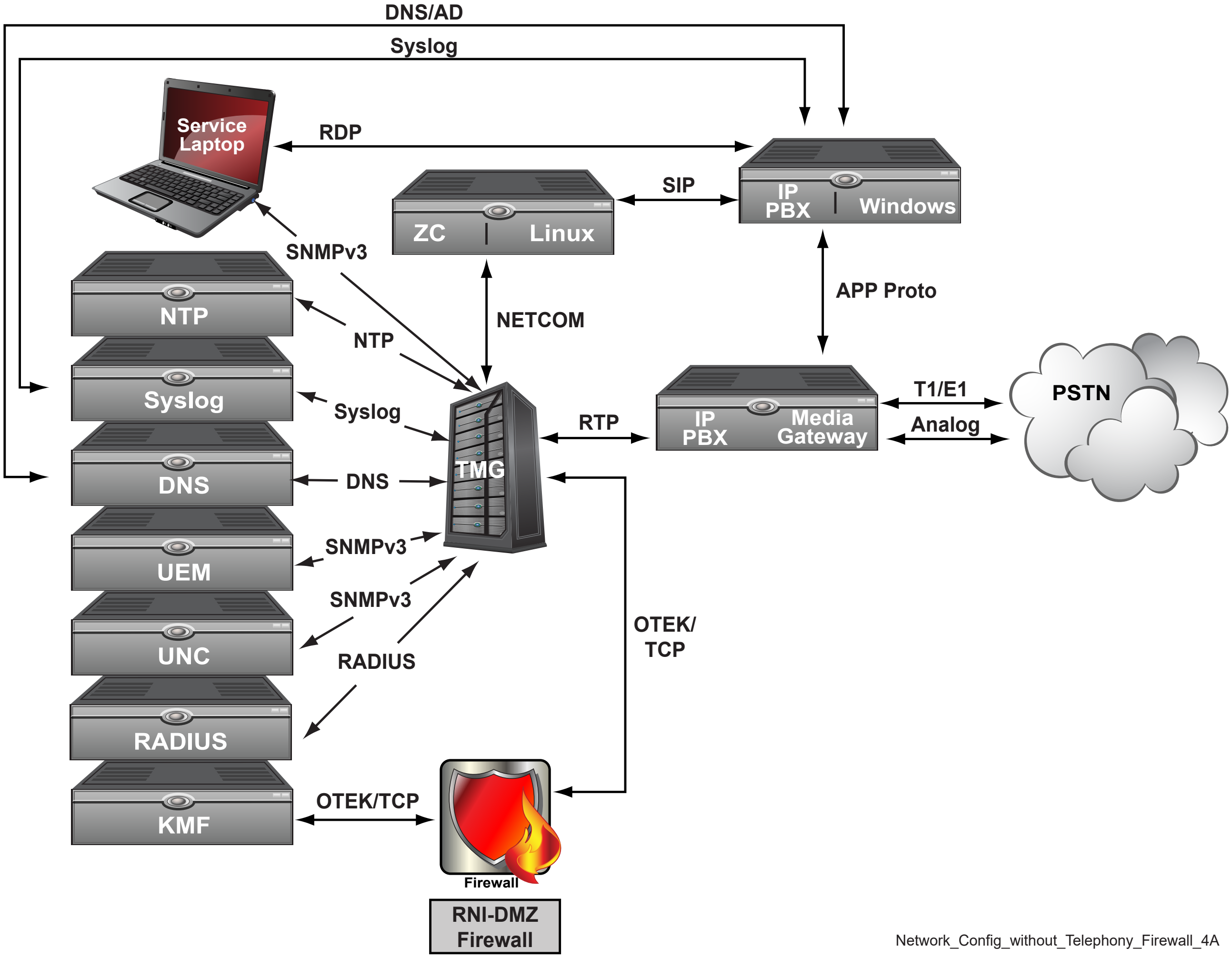


Figure 12: The Enhanced Telephone Interconnect Network Configuration without a Telephony Firewall on page 41 illustrates the ETI network configuration where the IP PBX media gateway is used for T1/E1 or analog connectivity to the Public Switched Telephone Network (PSTN). The IP PBX media gateway can be a NEC BranchHub or NEC COHub.

Figure 12: The Enhanced Telephone Interconnect Network Configuration without a Telephony Firewall



Network_Config_without_Telephony_Firewall_4A

NOTICE: Figure 11: The Enhanced Telephone Interconnect Network Configuration with a Telephony Firewall on page 40 and Figure 12: The Enhanced Telephone Interconnect Network Configuration without a Telephony Firewall on page 41 only show Real-time Transport Protocol (RTP) audio within the ETI subsystem. Audio (AMBE/XIS) is also coming in from the ASTRO® 25 network to the TMG.

2.2 Enhanced Telephone Interconnect Architecture Components

The Enhanced Telephone Interconnect (ETI) subsystem components that are important to successful interconnect call processing within the ASTRO® 25 radio communication system infrastructure are:

- Zone Controller (ZC)
- Network Time Protocol Server (NTP)
- Syslog (optional)
- Domain Name Services (DNS)
- Service Laptop
- Unified Event Manager

- Unified Network Configurator
- RADIUS
- Key Management Facility
- Key Variable Loader
- Radio Network Infrastructure-Demilitarized Zone (RNI-DMZ) Firewall

2.2.1 Zone Controller

The Zone Controller (ZC) is responsible for managing calls on the Radio Network Interface (RNI) and a Telephone Media Gateway (TMG), and sets up the media streams on the TMGs which get passed to the IP Private Branch eXchange (PBX) server using Session Initiation Protocol (SIP). See Table 21: Common SIP Messages Exchanged between the ZC and the IP PBX Server on page 161.

The ZC notifies the TMG to set up media streams and passes the TMG information (IP address, port number, supported codecs) to the IP PBX server in the SIP INVITE message (for mobile-to-land calls) and in the SIP 200 OK message (for land-to-mobile calls).

2.2.2 Network Time Protocol Server and ETI

Relating to the Enhanced Telephone Interconnect (ETI) subsystem, the Network Time Protocol (NTP) server shares time-of-day information between networked devices, such as the servers and Telephone Media Gateway (TMG) in a zone.

2.2.3 Syslog and ETI

Relating to the Enhanced Telephone Interconnect (ETI) subsystem, the Syslog server provides the optional Centralized Event Logging (CEL) to the Telephone Media Gateway (TMG). The CEL feature captures Operating System (OS) events generated by the TMG.

2.2.4 Domain Name Services and ETI

Relating to the Enhanced Telephone Interconnect (ETI) subsystem, the Domain Name Services (DNS) provides hostname-to-IP address resolution to the Telephone Media Gateway (TMG) through the Domain Controller, which is also called an authentication server. It is also used by the TMG and the IP Private Branch eXchange (PBX) server to resolve the zone controller IP addresses. DNS is used by network devices to find out about other network devices in the ASTRO® 25 radio system.

2.2.5 Service Laptop and ETI

Relating to the Enhanced Telephone Interconnect (ETI) subsystem, the service laptop communicates with the Telephone Media Gateway (TMG) using SNMPv3. The TMG is initially configured using a serial connection and the Configuration/Service Software (CSS) application on the service laptop.

2.2.6 Unified Event Manager and ETI

Relating to the Enhanced Telephone Interconnect (ETI) subsystem, the Unified Event Manager (UEM) application provides fault management information on the Telephone Media Gateway (TMG) and discovers the TMG using SNMPv3.

2.2.7 Unified Network Configurator and ETI

The Unified Network Configurator Wizard (UNCW) is used to discover the Telephone Media Gateway (TMG) devices and establish telephone interconnect service through the Interconnect Sub-System (ISS) tab. If a Key Management Facility (KMF) is used for encryption, the KMF must be created before the TMG is discovered in the UNCW. After the TMG is discovered, you can set the **Contains Interconnect Sub-System** field in the **AEB Switch and ISS Configuration** tab to establish Enhanced Telephone Interconnect (ETI).

The UNC discovers and manages the TMG using SNMPv3. There are System Level Configuration and Zone Level Configuration parameters associated with telephone interconnect are set up in the UNCW.

See the *UNC Wizard Online Help* for descriptions of the parameters and the *Unified Network Configurator User guide* for procedural information related to these settings.

2.2.8 RADIUS and ETI

Remote Access Dial In User Service (RADIUS) is an authentication method where access control is implemented through user identifiers. This service is provided by the Domain Controllers, which provide RADIUS services to the Telephone Media Gateway (TMG) for Enhanced Telephone Interconnect (ETI).

2.2.9 Key Management Facility and ETI

Relating to the Enhanced Telephone Interconnect (ETI) subsystem, the Key Management Facility (KMF) server and application provide encryption to the Telephone Media Gateway (TMG) to enable encrypted calls.

Key loading on the TMG from the KMF is done through Store and Forward using a Key Variable Loader (KVL) or through the Over-the-Ethernet-Key Management (OTEK) feature.

If centralized key management is being used with the TMG, the KMF must be added in the Unified Network Configurator (UNC) before the TMG is discovered in the system. To delete a KMF from the system, you must remove the TMG association using the UNC application.

2.2.10 Key Variable Loader and ETI

The encryption key provisioning and key loading can be accomplished using a Motorola Key Variable Loader (KVL). The KVL is a hand-held device that can be used to manually load keys into the Telephone Media Gateway (TMG) or as a transfer method between the Key Management Facility (KMF) and the TMG using Store and Forward for key management for the Enhanced Telephone Interconnect (ETI) subsystem.

2.2.11 Radio Network Infrastructure-Demilitarized Zone Firewall and ETI

Relating to the Enhanced Telephone Interconnect (ETI) subsystem, the Telephone Media Gateway (TMG) does not physically connect to the Radio Network Infrastructure Demilitarized Zone (RNI-DMZ) Firewall. The TMG physically connects to the gateway then through the DMZ firewall to the Key Management Facility (KMF) in the Customer Enterprise Network (CEN) when the TMG is centrally key managed.

2.3 Call Control and ETI

For the Enhanced Telephone Interconnect (ETI) subsystem, the zone controller sends control messages to the IP Private Branch eXchange (PBX) server using the Session Initiation Protocol (SIP) (standard) protocol and to the Telephone Media Gateway (TMG) using a proprietary control protocol. The IP PBX server sends control messages to the zone controller using SIP and to its media gateways using either a proprietary protocol (NEC COHub, NEC BranchHub media gateways) or SIP (other third-party media gateways).

2.4 Audio/Tone Generation and ETI

For the Enhanced Telephone Interconnect (ETI) subsystem, the zone controller instructs the Telephone Media Gateway (TMG) to inject a specified tone into the audio stream of an existing media session with the IP Private Branch eXchange (PBX) media gateway or IP endpoint. This tone is used to support radio user-initiated Dual-Tone Multi-Frequency (DTMF) signaling. This functionality is also used to generate the end-of-call warning (final alert) tone to the IP PBX media gateway and the radio user, the Go-Ahead tone to the IP PBX media gateway, and local ringback to the radio user during the start of a mobile-to-land call.

2.5 Audio Connections and ETI

The Enhanced Telephone Interconnect (ETI) subsystem supports T1/E1 and analog FXO interfaces to the Public Switched Telephone Network (PSTN). It also supports a Session Initiation Protocol (SIP)/ Real-time Transport Protocol (RTP) (VoIP) interface to an external IP network. The Telephone Media Gateway (TMG) is the media gateway between the ASTRO® 25 system and the IP Private Branch eXchange (PBX) media gateway or external IP network. An IP PBX media gateway expects G.711 encoded audio wrapped in RTP voice packets. The TMG is responsible for translating X-Zone Infrastructure Signaling (XIS) packets with AMBE encoded audio into RTP packets with G.711 (A-law or ulaw) voice encoding.

2.6 Enhanced Telephone Interconnect Subsystem Initialization

When the Enhanced Telephone Interconnect (ETI) subsystem initializes, the following events must take place before interconnect calls can be processed:

- The zone controller registers with the IP Private Branch eXchange (PBX) server using Session Initiation Protocol (SIP) messaging over User Datagram Protocol (UDP). If the registration is accepted, then the zone controller can place and receive calls to/from the IP PBX server.
- The Telephone Media Gateway (TMG) establishes a connection through a reliable protocol over UDP with the zone controller and reports to the zone controller the number of interconnect calls that it can process. The zone controller can then assign this TMG to interconnect calls.

2.7 Dynamic Call Mode Determination

The zone controller dynamically determines the mode of the call based on the capabilities of the resources needed to support the call at the time it is set up. The call mode is Time Division Multiple Access (TDMA) if the following conditions are true:

- The subscriber radio is registered at a site that supports TDMA.
- The subscriber radio supports TDMA

If either of these conditions is not met, the call mode is P25 Phase 1 (Frequency Division Multiple Access (FDMA).

The subscriber radio may roam after the call has been initiated. Once the call becomes active, the mode of the call cannot change. If the subscriber roams into a site that cannot support the mode of the call, the call is terminated. This termination could occur if a TDMA-capable subscriber radio roams from a TDMA-capable site to a site that supports only P25 Phase 1 (FDMA).

2.8 Mobile-to-Land Calls in the ASTRO 25 System

The following is a high-level overview of a mobile-to-land call setup:

1. The system verifies that the IP Private Branch eXchange (PBX) server is available and that the mobile is authorized for interconnect service.
2. The system verifies that dialed digits are allowed (not restricted) for the mobile.
3. The system sends the dialed digits to the IP PBX server, which also validates the digits and selects a trunk resource to place the call to the Public Switched Telephone Network (PSTN).

2.8.1 Mobile-to-Land Call Request in the ASTRO 25 System

In an ASTRO® 25 Trunking system, mobile-to-land calls are initiated with a control channel request. The control channel request includes all dialed digit information for the call, allowing the system to check dialing restrictions before granting the voice channel for the call. This check allows the system to deny interconnect call requests made to restricted phone numbers by sending a deny message over the control channel.

Delayed buffered dialing operation (that is, subscriber radio user enters digits or selects a number from a list and then hits Push To Talk (PTT) to send the call request with the digits) is the only initial dialing mode supported. The ASTRO® 25 system does NOT support mobile-to-land trunked calls initiated using live dialing operation.

2.8.2 Mobile Functionality in Mobile-to-Land Call

When a subscriber radio user presses a pre-programmed interconnect activation button, the mobile enters Phone mode, allowing access to interconnect functionality. A properly programmed mobile is capable of supporting an alternate one-touch method of initiating interconnect calls, in which a request to a single pre-programmed phone number is automatically sent when the subscriber radio user presses a single button. One-touch interconnect functionality allows mobiles not equipped with a display to initiate interconnect calls.

The mobile allows a subscriber radio user to enter digits directly into a scratchpad, or select the desired phone number from a pre-programmed list of phone numbers in addition to one-touch dialing. These methods represent the most common methods that radio users follow to select or dial phone numbers for mobile-to-land call initiation.

Based on the programmed interconnect dialing method, the subscriber radio user request for a Mobile-to-Land call may be triggered by a Push To Talk (PTT) after the desired number has been selected or entered (delayed buffered dialing), or by pressing a key programmed to activate the one-touch interconnect feature.

2.8.3 Site Response During Mobile-to-Land Call

A site must be operating in wide-area trunking mode for interconnect call requests to be supported at that site. Sites operating in site trunking mode deny any interconnect requests received. Sites operating in wide-area mode forward interconnect requests received to the zone controller. Enhanced Telephone Interconnect (ETI) does not work with SmartX (3600) sites.

2.8.4 Mobile-to-Land Call Mobile Registration Verification

A mobile must be registered on the system before the system allows the mobile to initiate a mobile-to-land interconnect call. The registration includes information on the Time Division Multiple Access (TDMA)/Frequency Division Multiple Access (FDMA) mode capabilities of the mobile. If the system receives a mobile-to-land interconnect request from a mobile not currently registered on the system, the call is denied, and the system requests that the mobile perform registration.

2.8.5 Mobile-to-Land Call Mobile Interconnect Authorization Verification

The system allows a system manager to control which subscriber radio users are allowed to use the interconnect feature. If a subscriber radio user attempting to initiate a mobile-to-land interconnect call is configured with the interconnect capability disabled, the system denies the call request.

2.8.6 Mobile-to-Land Call Service Options Check

Mobile-to-land calls can be initiated in clear/secure mode, determined by the service option protection information included in the call request. The zone controller determines if the call request is allowed or denied by checking the subscriber radio configured secure communications mode.

2.8.7 Mobile-to-Land Call Routing Determination

The ASTRO® 25 trunking system allows mobile-to-land calls to be initiated from anywhere in the system, even if the subscriber radio is registered to a zone without an Enhanced Telephone Interconnect (ETI) subsystem.

To improve availability of the interconnect feature, a dynamic mobile-to-land call routing mechanism takes into consideration certain failures of an ETI subsystem in systems with more than one ETI subsystem. If the zone controller determines that based on the radio user-configured call routing information, the mobile-to-land call is to be routed through the local ETI subsystem, and the zone controller knows that the local ETI subsystem is failed such that it can no longer support interconnect calls, the zone controller can decide to route the call to the ETI subsystem in the radio user-specified Alternate/Default Interconnect Subsystem. This strategy improves the chance that the call attempt is successful.

NOTICE: The zone controller does not reroute the call in the event that the ETI subsystem in the radio user Alternate/Default zone has also failed.

This dynamic Mobile-to-Land call routing mechanism means that calls may be placed through different ETI subsystems without the knowledge of subscriber radio user. Therefore, it may not be obvious to the subscriber radio user where the call is being routed. For systems with more than one zone with an ETI subsystem, the subscriber radio should be instructed to always dial the area code, even when placing local calls. In this type of system, configure the IP Private Branch eXchange (PBX) dialing plan tables to accommodate the call accordingly (stripping off the area code when it is not necessary).

The subscriber radio user interconnect profile is a Network Management feature that allows a system manager to define a different profile for each unique set of interconnect capabilities settings. Each subscriber radio is then assigned one of the defined interconnect profiles. The following sections describe the feature settings.

2.8.7.1 Mobile-to-Land Call Routing Mode - Local Interconnect Preferred

If the Mobile-to-Land Call Routing Mode parameter in the interconnect profile of the requesting radio assigned is configured for **Local Interconnect Preferred**, and the subscriber radio is registered to a zone with a functional Enhanced Telephone Interconnect (ETI) subsystem, the zone controller routes the call to the ETI subsystem in the subscriber radio registered zone for the call request. Otherwise, the zone controller routes the call to the ETI subsystem in the zone specified by the **Alternate/Default Interconnect Subsystem** parameter.

2.8.7.2 Mobile-to-Land Call Routing Mode - Use Default Interconnect Only

If the **Mobile-to-Land Call Routing Mode** parameter in the assigned interconnect profile of the requesting mobile is configured for **Use Default Interconnect** only, the zone controller routes the call to the Enhanced Telephone Interconnect (ETI) subsystem in the zone specified by the A**lternate/Default Interconnect Subsystem** parameter.

2.8.7.3 Mobile-to-Land Call Routing Mode - Local Interconnect Only

If the **Mobile-to-Land Call Routing Mode** parameter in the requesting subscriber radio assigned interconnect profile is configured for **Local Interconnect Only**, the zone controller routes the call to the Enhanced Telephone Interconnect (ETI) subsystem in the registered zone of the subscriber radio. The **Local Interconnect Only** operation is included in the Mobile-to-Land feature to accommodate those users wanting to minimize interconnect inter-zone traffic by following a “no Mobile-to-Land call routing” design.

NOTICE: This feature does not prevent the subscriber radio from roaming to a new zone after the call has started, nor does it prevent a multi-zone land-to-mobile call from being initiated to the same radio.

2.8.7.4 Mobile-to-Land Call Exclusion Class and Dialing Restrictions

Dialing restrictions on a mobile subscriber basis may be configured on and screened by the zone controller using the Provisioning Manager application.

In the **Radio User Interconnect** profile, you can identify which **Exclusion Class** applies to a specific radio user for call barring. When this field is set to 0, no call barring is available to the user.

If the **Exclusion Class Number** in the requesting radio assigned interconnect profile is non-zero, the zone controller screens the dialed digits against the numbers in the **Disallowed Dialing Patterns** field associated with that exclusion class. If the dialed digits match a disallowed pattern, the call request is denied.

NOTICE: The dialed digits are screened against the numbers in the **Disallowed Dialing Patterns** field associated with the exclusion class in the zone where the used Enhanced Telephone Interconnect (ETI) subsystem resides (which may be different than the zone where the call originated).

2.8.8 Mobile-to-Land Call Resource Reservation and Busy Queuing

Many considerations factor into the zone controller mechanism to obtain resources for a call attempt. The zone controller can determine that various required resources are available, busy, or not capable of supporting the request. Resources may not be capable of supporting a request due to a failure condition, or users may control resource usage. For example, users may configure the Shared Service algorithm to minimize busies for group and private calls due to channels being used for excessive interconnect activity.

2.8.8.1 Table-Driven and Dynamic Shared Service

The two types of Shared Service are Table-Driven and Dynamic. Shared Service is a feature that allows the system manager control over the number of channels used for interconnect compared to dispatch calls for each site at any given time. The zone controller uses information provided by the network management subsystem (the zone controller is not aware of Table-Driven versus Dynamic Shared Service).

Table-Driven Shared Service is a standard feature that allows the customer to specify how many interconnect calls are allowed at any given time at each site, per two-hour time period throughout the day. Dynamic Shared Service is an optional feature that goes beyond the Table-Driven Shared Service functionality by providing an automatic adjustment to the configured Table-Driven Shared Service tables according to current system loading. The Dynamic Shared Service algorithm provides an interconnect usage that approximates the user-desired interconnect versus dispatch balance.

When a mobile-to-land interconnect call is initiated, before the call request is sent to the IP Private Branch eXchange (PBX) server, radio system resources are reserved for the call. If no channel is available, the call is placed in a busy queue. After a channel becomes available for the call, the call request is sent to the IP PBX server.

If Telephone Media Gateway (TMG) or trunk resources are unavailable (busy), the call is denied, not queued. The subscriber radio user has to re-initiate the call request later.

2.8.9 Mobile-to-Land Call IP PBX Server Notification

After radio system resources are obtained for a mobile-to-land interconnect call request, the zone controller notifies the IP Private Branch eXchange (PBX) server about the call, including dialed digit information.

2.8.10 Mobile-to-Land Call IP PBX Server Phone Number Validation

The IP Private Branch eXchange (PBX) server can be configured with information defining a valid phone number, such as the phone number length and format (for example, 1 + 10-digit number). This capability allows the IP PBX server to deny mobile-to-land calls initiated to phone numbers not considered valid.

2.8.11 Mobile-to-Land Call Global Dialing Privileges

Global dialing restrictions/privileges (that is, those that apply to all mobile-to-land calls at that Enhanced Telephone Interconnect (ETI) subsystem) may be configured on and screened by the IP Private Branch eXchange (PBX) server. If the IP PBX server determines that the dialed number is disallowed, the system rejects the call.

2.8.12 Mobile-to-Land Call IP PBX Check for Trunk Resources

When the IP Private Branch eXchange (PBX) server determines that the dialed number is valid, it determines if an available Public Switched Telephone Network (PSTN) interface is available. If the IP PBX server determines that no trunks are available for the call, the call is rejected.

2.8.13 Mobile-to-Land Call Initiation of Call to PSTN

If the IP Private Branch eXchange (PBX) server determines that a Public Switched Telephone Network (PSTN) interface is available, it initiates the call to the PSTN.

2.8.14 Mobile-to-Land Call Alerting

Session Initiation Protocol (SIP) calls take longer to set up, so the ASTRO® 25 trunking system may provide local ringback to the subscriber radio user, generated by the Telephone Media Gateway (TMG), to let the radio user know that the call attempt is progressing. This strategy may be confusing if the call fails at the Public Switched Telephone Network (PSTN), because the subscriber radio user may hear a few seconds of ringback before the call is torn down. The PSTN may provide ringback. The radio user may hear ringback provided by the TMG, followed by ringback provided by the PSTN. The user experience may vary depending on the landline termination (analog, IP, and so forth.).

NOTICE: The TMG only supports North American ringback tone. So if both local ringback and ringback from the PSTN are provided, the subscriber radio user may experience two different ringback tones within a single call attempt. Also, Motorola has observed ringback experience varies depending on the service provider. In addition to ringback duration (that is, truncated ringback), gaps (that is, silence) of varying length between ringback tones may appear.

2.8.15 Mobile-to-Land Call Landline Answers

The zone controller is notified of a connection being made between the IP Private Branch eXchange (PBX) media gateway and the Public Switched Telephone Network (PSTN). At this point, an audio path is established and the zone controller marks the call start time, for billing purposes. This does not necessarily mean the landline user has answered. The PSTN could be providing ringback tone or a voice announcement. When the landline answers, no signaling is provided to the ASTRO® 25 system. The terminating end handles any audio changes between tones/announcements and voice.

At the end of an interconnect call, billing information is forwarded to the Network Management subsystem for the Air Time Information Access (ATIA) feature, also known as billing.

The zone controller in the zone with the Enhanced Telephone Interconnect (ETI) subsystem is responsible for keeping track of the interconnect call duration for billing purposes.

2.9 Land-to-Mobile Calls

The following list is a high-level overview of a Land-to-Mobile (L-M) call setup.

Initial call setup events for Direct Inbound Dialing (DID) operation:

1. The IP Private Branch eXchange (PBX) media gateway detects an incoming call. It receives DID digits from the Public Switched Telephone Network (PSTN).
2. The IP PBX media gateway notifies the radio system (through the IP PBX server) about the call, and provides the system with the received DID number information.

3 The IP PBX media gateway plays ringback tone for the landline user, in the direction of the PSTN interface.

4 The radio system performs a DID database lookup using the DID number information to determine the mobile being targeted for the call.

Initial call setup events for non-DID (land-to-mobile through overdial) operation:

1 The IP PBX media gateway detects an incoming call. It notifies the IP PBX server, which recognizes this call as a non-DID call. The IP PBX server invokes the Auto Attendant service. The Auto Attendant answers the call, returning answer supervision to the PSTN interface as required by PSTN interface type.

2 The Auto Attendant plays a voice announcement, prompting the landline user to enter DTMF overdial digits reflecting the target mobile ID.

3 After the Auto Attendant collects the overdial digits, it forwards the information to the IP PBX server. The IP PBX server notifies the radio system about the call, and provides the system with the overdial digits, which reflect the target radio ID.

4 The IP PBX media gateway plays ringback tone for the landline user, in the direction of the PSTN.

Call setup events applying to DID as well as non-DID (overdial) call initiation:

1 The system verifies that target subscriber radio is registered and authorized for interconnect service.

2 The radio system resources, Radio Frequency (RF) and Telephone Media Gateway (TMG), are reserved for the call.

3 The system sends a control channel message to the subscriber radio registered site to notify the subscriber radio of the incoming call.

4 Radio monitoring the control channel responds to this message and starts alerting the subscriber radio (ringing) for the call.

5 When the subscriber radio user answers the call, radio system resources are granted for the call.

2.9.1 Land-to-Mobile Voice Announcement

To instruct the landline user to enter the radio ID when initiating a land-to-mobile call, the IP Private Branch eXchange (PBX) Auto Attendant service plays an appropriate voice announcement when a call is received on a non-Direct Inbound Dialing (DID) interface.

The IP PBX server ships with a standard American English recording. This announcement is a .wav file that may be replaced with a custom `.wav` file. If a customized announcement is required, a plan to record an announcement should be created before the Enhanced Telephone Interconnect (ETI) subsystem installation.

⚠ **CAUTION:** When creating a custom `.wav` file for the Auto Attendant functionality, the `.wav` file must be named the same as the file it is replacing or the land line caller hears silence.

2.9.2 Land-to-Mobile Call Request through Overdial for Non-DID Interface to PSTN

Land-to-mobile call initiation using overdial allows a landline user to initiate a land-to-mobile call over non-Direct Inbound Dialing (DID) trunks to the Public Switched Telephone Network (PSTN). The system allows the landline user to enter the target radio ID through Dual-Tone Multi-Frequency (DTMF) overdial digits to place a call to any radio registered on the system that is provisioned for interconnect. The system prompts the landline user to enter the digits and once the digits have been collected, the system proceeds with the call setup. This scheme is sometimes referred to as two-stage dialing because the landline user is initiating the call in two stages by first entering the phone number of the trunk connected to the IP Private Branch eXchange (PBX) media gateway, and then by entering the target radio ID.

NOTICE: DID is only supported using a COHub set for a T1 CAS circuit emulating EM signaling.

2.9.3
Land-to-Mobile Call Answer Supervision

When the IP Private Branch eXchange (PBX) media gateway receives an incoming call on a non-Direct Inbound Dialing (DID) Public Switched Telephone Network (PSTN) interface, it notifies the IP PBX server, which recognizes this as a non-DID call. The IP PBX server invokes the Auto Attendant service. The Auto Attendant answers the call and provides answer supervision to the PSTN as appropriate for the PSTN interface type. Answer Supervision must be provided immediately for calls received on non-DID PSTN interfaces (as opposed to waiting until the target radio answers the call, as can be done for DID interfaces) since Answer Supervision is required before the overdial digits from the landline user can be passed through the PSTN.

When the Auto Attendant answers the call, it automatically plays a voice announcement, prompting the landline user to enter overdial digits reflecting the target radio ID. After the Auto Attendant plays the voice announcement, it collects the overdial digits received from the PSTN. When the Auto Attendant receives a # digit, it stops collecting overdial digits, and forwards the digits on to the IP PBX server.

The IP PBX server sends the overdial digits along with a prefix indicating that this is a non-DID call to the zone controller. Non-DID calls are forwarded to the zone controller after the receipt of a “#” or the interdigit timer expires (if no “#” is received).

Upon receiving the dialed digits for a non-DID call, if the zone controller determines that the called party number received is not a valid radio ID on the system, the zone controller sends an error response to the IP PBX server.

The IP PBX server, upon receiving an error response from the zone controller, terminates the call and the IP PBX media gateway plays an appropriate tone (fast busy) to inform the landline user.

2.9.4
Land-to-Mobile Call Request with DID Interface to PSTN

The ASTRO® 25 Trunking system supports land-to-mobile calls received on Direct Inbound Dialing (DID) Public Switched Telephone Network (PSTN) interfaces, allowing a landline user to place a call to a target radio directly, by entering the target radio assigned DID number. The DID database associating a subscriber radio user with a DID number is kept in the zone controller.

2.9.4.1
Direct Inbound Dialing Database and Related Parameters

Each zone controller supports up to 4000 Direct Inbound Dialing (DID) numbers, for assignment to individual radio users.

The Provisioning Manager application allows a system manager to configure the **Number of DID Digits** parameters for each Enhanced Telephone Interconnect (ETI) subsystem in the trunking system. The range of this parameter is two to five. The IP Private Branch eXchange (PBX) server is configurable to expect a specified number of digits from the Public Switched Telephone Network (PSTN) or IP network.

The DID digits parameter value, the IP PBX server configuration for the expected number of DID digits, and the DID digits received from the PSTN as ordered from the phone company must be identical in order for DID calls to be routed correctly through the system. For each radio user record, the

Provisioning Manager application allows the system manager to configure a DID number and select which ETI subsystem is used for DID calls placed to the subscriber radio.

NOTICE: This feature is optional. A subscriber radio user does not need a DID number if Land-to-Mobile service using overdial is desired.

The DID number assigned to a subscriber radio user in the Provisioning Manager application can be as long as 15 digits, which allows a system manager to enter the entire DID phone number (if desired) instead of only entering the DID digits from the central office.

The Provisioning Manager application performs a uniqueness check to ensure that the last X digits of the subscriber radio user DID number are unique for all radio users with same assigned ETI subsystem, where X is the setting of the **Number of DID digits** parameter. For example, if the DID number entered in the Provisioning Manager for a subscriber radio is 5760001, and the **Number of DID digits** parameter is set to **three**, the subscriber radio user actual DID number is **001**. With this configuration, the system ensures that no other subscriber radio with the same assigned ETI subsystem for DID is assigned actual DID number 001. The network management subsystem sends DID database records (DID number mapped to radio user) to the zone controller in the zone with the subscriber radio assigned ETI subsystem for DID operation. When sending the DID database records to the zone controller, the network management subsystem sends only the last X digits of the subscriber radio user assigned DID number, where X is the setting of the **Number of DID digits** parameter.

The zone controller retains radio ID to DID number assignment information. If the Number of DID digits parameter is increased, the network management subsystem updates the associated zone controller with new DID numbers for all configured radio users, according to the new Number of DID digits parameter setting.

To prevent non-unique entries in the DID database, the network management subsystem does not allow the Number of DID digits parameter value to be decreased.

As DID numbers are assigned to radio users, the network management subsystem ensures that the entries are unique per ETI subsystem, according to the last X digits, where X is the **Number of DID digits** parameter setting. If the **Number of DID digits** parameter were decreased, this could result in non-unique DID number assignments. Therefore when the system manager attempts to increase the value of the **Number of DID digits** parameter, the network management subsystem provides a warning, explaining that once increased, the parameter value cannot be decreased.

DID numbers must be configured on the IP PBX server using **DID Mapping Lists**. Wild cards can be used. The entry in the **DID Mapping List** must match the DID digits that are received from the phone company, with leading 0s, if necessary.

2.9.4.2 Direct Inbound Dialing Call Initiation

The IP Private Branch eXchange (PBX) media gateway collects Direct Inbound Dialing (DID) digits from the Public Switched Telephone Network (PSTN) and forwards these to the IP PBX server. After the IP PBX server receives the Direct Inward Dialing (DID) digits, it determines if it has received the required number of digits from the PSTN. If it determines that it has not received enough DID digits, an appropriate tone (fast busy) is played and the call is terminated.

NOTICE: The IP PBX server is configured with information regarding the number of DID digits it should receive from the PSTN. If the IP PBX server does not receive the correct number of DID digits, the IP PBX server operates as described above. Thus, it is critical that the number of expected DID digits as configured in the IP PBX server matches the DID operation as ordered from the phone company.

If the IP PBX server determines that it has received the correct number of DID digits, it sends these digits along with a prefix indicating that this is a DID call to the zone controller.

Upon receiving the digits, the zone controller accesses its DID database to look up the target radio ID associated with the DID digits received in the request.

Upon accessing the DID database, if the zone controller determines that the DID number received is not configured in the DID database (this means no radio ID has been assigned this DID number), the zone controller sends an error response message to the IP PBX server.

The IP PBX server, upon receiving an error response from the zone controller, terminates the call and the IP PBX media gateway plays an appropriate tone (fast busy) to inform the landline user.

2.9.4.3 Land-to-Mobile Call Target Radio Authorization, Registration Checks

The system determines if the target radio is authorized for interconnect service and registered on the system before proceeding to set up a land-to-mobile call.

When a land-to-mobile call is initiated, the zone controller checks the target mobile registration status. Because land-to-mobile calls can be routed across zones to wherever the target radio is located, the zone controller checks to see if the target radio is registered at any site/zone in the system.

In any of the following scenarios, the zone controller sends an error response to the IP Private Branch eXchange (PBX) server:

- Target subscriber radio is not registered on the system.
- Target subscriber radio is registered to a site for which it is not valid for individual services.

The IP PBX server, upon receiving an error response from the zone controller, terminates the call and the IP PBX media gateway plays an appropriate tone (fast busy) to inform the landline user.

The network management subsystem allows the system manager to enable/disable interconnect functionality, per radio user record. When the zone controller has the target radio ID, the zone controller looks up the configured interconnect capability in the subscriber radio user assigned interconnect profile to determine if the target radio is authorized for interconnect service.

If the zone controller determines that the target radio is either not authorized for interconnect service, or the target ID is actually a console device or not allowed to use the system (radio user capability of disabled), the zone controller sends an error response to the IP PBX server.

2.9.4.4 Land-to-Mobile Call Secure/Clear Mode Determination

Land-to-mobile calls can be initiated in clear or secure mode. Because the landline user requesting the call has no way to select clear or secure mode on the telephone itself, the system allows a manager user to pre-configure the initial secure mode of land-to-mobile calls, for each radio (Secure Land to Mobile Start Mode). The zone controller sets up the call in the mode according to the latest configuration of this parameter.

After the call has been granted, the target radio user has the option of requesting an upgrade or downgrade by sending in a request over the control channel. The zone controller determines if the request is allowed by checking the configured secure communications mode in the subscriber radio user record.

NOTICE: Interconnect calls cannot actually be downgraded from secure to clear. If the mobile configured secure-communications mode allows the subscriber radio to transmit in clear mode, the subscriber radio is allowed to transmit clear, but the outbound transmission to the subscriber radio remains secure.

2.9.4.5 Land-to-Mobile Call Contention Checking

The system checks if the target radio is involved in another interconnect call before the land-to-mobile call is set up. The system does not perform contention checking across services, that is, check to determine if the target radio is involved in a group or unit-to-unit call before setting up the land-to-mobile call.

When a land-to-mobile call is initiated, the zone controller determines if the target radio is involved in another interconnect call. If the target radio is involved in another interconnect call, the zone controller sends an error response message to the IP Private Branch eXchange (PBX) server.

The IP PBX server, upon receiving an error response from the zone controller, terminates the call and the IP PBX media gateway plays an appropriate tone (fast busy) to inform the landline user.

2.9.4.6 Land-to-Mobile Call Radio System Resource Reservation and Busy Queuing

After the radio system determines that the land-to-mobile call request is allowed, before the call request is sent to the target subscriber radio, radio system resources are reserved for the call. If an RF channel is not available at the subscriber radio registered site (busy), the call is placed in a busy queue and the landline user hears ringing, however the target radio is not notified about the call until all required radio system resources have been reserved for the call. After a channel becomes available for the call, the call request is sent to the target radio over the control channel.

If a Telephone Media Gateway (TMG) resource is not available (busy), the zone controller sends an error response to the IP Private Branch eXchange (PBX) server. The IP PBX server, upon receiving an error response from the zone controller, terminates the call and the IP PBX media gateway plays an appropriate tone to inform the landline user.

After the zone controller reserves all required radio system resources for the call, in the unlikely event that the reserved RF channel is preempted for an Emergency call at the site, the zone controller also sends an error response to the IP PBX server.

2.9.4.7 Land-to-Mobile Call Target Mobile Notification and Ringing

After radio system resources have been reserved for the call, the radio system notifies the target radio about the call request. The call request notification is sent repeatedly on the control channel in case the target radio is temporarily away from the control channel, monitoring a voice channel for a group or unit-to-unit call. The zone controller starts an Interconnect Ring timer when the target radio is being contacted for the call.

When the subscriber radio starts ringing for the call and responds to the zone controller, the zone controller restarts the timer. If the Interconnect Ring timer expires and the target radio user has not responded, the call is ended and the call request notification stops being repeated on the control channel.

The target radio continues to ring until the subscriber radio user answers the call, the subscriber internal timer expires, or the radio system cancels the unanswered call. The mobile radio internal timer serves as a safety timer to prevent the subscriber radio from ringing forever in the event the subscriber radio misses the zone controller deny message when the zone controller ring timer expires. If the internal timer expires, and the subscriber radio user enters phone mode, the subscriber radio does not notify the zone controller, even if the call is still pending in the zone controller. For this reason, set the mobile radio internal timer to a value slightly larger than the system Interconnect Ring timer.

2.9.4.8
Land-to-Mobile Call Radio User Answering Call

After the subscriber radio user answers the call, the radio system grants the previously reserved radio system resources for the call and the billing record is created.

With a land-to-mobile interconnect call request pending (radio ringing), the subscriber radio user enters “phone mode,” and the subscriber radio stops generating ring tone and sends the site a message to proceed. The site then sends a message to the zone controller notifying the zone controller that the subscriber radio user has answered the land-to-mobile call.

After the zone controller receives the message that the subscriber radio user has answered the call, the zone controller grants resources to begin the call.

The zone controller uses the **Secure Land to Mobile Start Mode** parameter setting in the subscriber radio user assigned interconnect profile (configured in the Provisioning Manager application) to determine if the call is started in secure or clear mode. The zone controller sends a beginning of transmission message to the Telephone Media Gateway (TMG) that includes the outbound transmission mode (secure or clear). If the call is to be secure, or is clear but capable of being upgraded, the zone controller also includes a Common Key Reference (CKR) in the beginning of transmission message.

The subscriber radio, upon receiving a channel grant leaves the control channel, moves over to the voice channel, and un-mutes. In addition to sending messages to the site and TMG, the zone controller notifies the IP Private Branch eXchange (PBX) server of the answer. This notification includes audio information, such as the assigned TMG IP address and UDP port number.

When the IP PBX server receives the answer notification, it connects the audio path between the Public Switched Telephone Network (PSTN) interface and the TMG.

At the end of an interconnect call, billing information is forwarded to the Network Management subsystem for the Air Time Information Access (ATIA) feature, also known as billing. The billing information contains only the radio ID, not the associated Direct Inward Dialing (DID) number.

2.9.5
Active Interconnect Calls Maintenance

When an interconnect call is established, the subscriber radio moves over to the assigned voice channel for the duration of the call, only moving over to the control channel to perform functions such as a secure upgrade or downgrade request or a call termination request, in the event of a fade.

2.9.5.1
Voice Channel

Control information, as well as voice, is sent on the interconnect voice channel, both inbound (sent by the subscriber radio) and outbound (sent by the system). This control information is sent in a Link Control Word (LC). Interconnect LCs sent during active interconnect calls include information about the subscriber radio participating in the call, its Working Unit ID (WUID), and whether the call is clear or secure. Adjacent channel status and site status information is also sent on the voice channel during active interconnect calls.

NOTICE: Subscriber radios do not scan for talkgroup activity while participating in interconnect calls. Therefore, the site does NOT send Priority Monitor LC information on voice channels assigned to interconnect calls.

2.9.5.2
Control Channel Grant Updates

After the initial channel grant is sent over the control channel at the beginning of an interconnect call (multiple times for reliability), channel grant updates are sent over the control channel periodically throughout the duration of the call. During an active interconnect call, if the subscriber radio enters a fade and leaves the voice channel, when the subscriber radio is able to recover from the fade condition and can monitor the control channel, the channel grant update allows the subscriber to rejoin the active call.

2.9.5.3 Maximum Interconnect Call Duration

When an interconnect call is answered, the zone controller starts the Maximum Interconnect Call Duration timer, which limits the total duration of an interconnect call. A different timer, the Individual Interconnect Call timer, limits the amount of time an interconnect call remains active with no radio activity. For example, the Individual Interconnect Call Timer works to terminate calls left hanging when a subscriber radio goes out of range.

2.9.5.4 Overdial Support

To allow a subscriber radio user participating in an interconnect call to send additional digits to the Public Switched Telephone Network (PSTN) after the call is established, for example, to access voice mail functionality, the system supports overdial functionality. Because the APCO® 25 air interface standard allows a subscriber to send overdial information on either the voice channel or the control channel, the system handles overdial requests received on either the control channel or voice channel, to accommodate radios from other manufacturers. The system routes overdial requests received on the control and voice channels to the zone controller over the control path. The zone controller then instructs the Telephone Media Gateway (TMG) to generate the requested Dual-Tone Multi-Frequency (DTMF) digits to the Public Switched Telephone Network (PSTN).

NOTICE: Motorola subscriber radios support both live and buffered overdial, which is selectable through Customer Programming Software (CPS).

Problems may be encountered when a subscriber radio from another manufacturer performs live overdial on the control channel. While the subscriber radio user is entering the digits one after another, the subscriber radio is looking for a grant confirming that each digit is received after each digit is sent. If the subscriber radio transmits to send another digit before receiving the acknowledgement for the previous digit, the subscriber radio may miss the grant sent to acknowledge that digit.

2.9.5.5 Radio Secure Upgrade/Downgrade Requests

If a subscriber radio user involved in an active interconnect call wishes to upgrade or downgrade the secure mode of the call, the subscriber radio moves over to the control channel and sends another interconnect call request indicating the desired secure/clear state. The zone controller evaluates the request and either allows or denies the request based on the subscriber radio configured secure communications mode setting.

Interconnect calls cannot be downgraded from secure to clear. If a subscriber radio user requests to downgrade a call, the subscriber radio may be allowed to transmit clear, but the outbound transmission from the landline user to the subscriber radio remains secure.

2.9.5.6 Go-Ahead Tone for Half-duplex Operation

The ASTRO® 25 trunking system supports “Go Ahead Tone” functionality during an interconnect call, informing a landline user when the half-duplex radio has de-keyed. This action allows the landline user to know when to speak since the subscriber radio user can now hear the landline user audio.

2.9.6 Interconnect Call Termination

The system allows an interconnect call to be terminated either by the subscriber radio user or landline user. Either party is able to terminate the interconnect call. In addition, the system can initiate termination of the interconnect call in various call time-out scenarios.

2.9.6.1 Mobile-Initiated Call Termination During Active Interconnect Call

Motorola ASTRO® 25 radios send call termination requests on the control channel, but because the APCO® 25 air interface standard specifies that call termination requests may be sent on the voice channel, the system handles call termination requests received on either the control channel or voice channel, to accommodate radios from other manufacturers. The system routes call termination requests received on the control and voice channels to the zone controller over the control path.

2.9.6.2 Mobile Power Off During Interconnect Call

If an ASTRO® 25 subscriber radio is turned off during an interconnect call, the subscriber radio automatically cancels the interconnect call before deregistering from the system and powering down.

2.9.6.3 Landline-Initiated Call Termination During Active Interconnect Call

When the landline user hangs up during an active interconnect call, the IP Private Branch eXchange (PBX) media gateway detects this condition and notifies the system. However, loop start lines may not provide disconnect supervision when the land line user hangs up. In these instances, the IP PBX media gateway may keep the trunk seized if the UNIVERGE 3C application does not terminate the call.

2.9.6.4 Mobile “Hangs up” Before Landline Answers Mobile-to-Land Call

When a mobile-to-land interconnect call has been initiated and the landline party is being alerted (ringing), the call is active from the system perspective (since the RF channel is assigned to the mobile). Therefore, a billing record may be generated even if the landline has not answered the call.

2.9.6.5 Landline “Hangs up” Before Mobile Answers Land-to-Mobile Call

After a land-to-mobile interconnect call has been initiated and the subscriber radio is being alerted (ringing) if the IP Private Branch eXchange (PBX) media gateway detects that the landline party hangs up, the zone controller is notified and the call is terminated.

2.9.6.6 Interconnect Call Termination Due to Maximum Call Timeout Expiration

The system can be configured to control the duration of interconnect calls. The Maximum Interconnect Call Duration timer is not the only mechanism that controls the duration of interconnect calls. The Shared Services algorithm modifies the interconnect call duration limit according to the Shared Services configuration, as well as the current system loading.

2.9.6.7 End-of-Call Alert Tone

When the Maximum Interconnect Call Duration timer (either configured in network management subsystem or modified by Shared Services, whichever has the smaller timer value) or the Individual Interconnect Call timer expires, the zone controller instructs the Telephone Media Gateway (TMG) to generate the end of call alert tone in the direction of both the landline and radio user and starts the Interconnect Final timer. If the Interconnect Final timer expires before either the mobile or the landline terminates the call, the call is torn down by the zone controller.

2.9.6.8 Call Teardown

To terminate the call, the zone controller notifies the IP Private Branch eXchange (PBX) server of the termination. The IP PBX server notifies the IP PBX media gateway to end the call with the Public Switched Telephone Network (PSTN) and free up resources. The zone controller also sends control messages to the Telephone Media Gateway (TMG) and Site to free up these resources for assignment to other call requests.

2.9.6.9 Individual Interconnect Timeout Expiration (No Mobile Activity)

The system can be configured to control how long an interconnect call lasts without any activity from the participating radio. If the system does not detect a subscriber radio Push To Talk (PTT) within the configured Individual Interconnect Call duration, the system terminates the call. This feature is useful to limit the impact of “hung call” scenarios where a subscriber radio roams out of range, and perhaps the landline party either does not hang up (landline is not being monitored by a person, but a voice mail computer).

2.9.6.10 Interconnect Call Termination and Expiration of Call Setup Timers

The system controls the length of time a land-to-mobile interconnect call remains pending in various call setup states. Because subscriber radio system resources are reserved before the system attempts to notify a subscriber radio about a land-to-mobile call request, limiting the amount of time the call can remain in a setup state is desired.

NOTICE: The Maximum Interconnect Call Duration, Individual Interconnect Call, Interconnect Ring, and Interconnect Final timers are configurable through the Unified Network Configurator (UNC) and apply to all interconnect calls that use the zone interconnect subsystem. The Maximum Duration Interconnect timer is also applicable when using Table-Driven Shared Service.

2.9.6.11 Interconnect Ring Timer

When the answer request message is sent over the control channel to notify the target radio for the call, a timer is started. If the subscriber radio does not respond to the control channel message before the timer expires, the system terminates the call request. Upon receiving a response, the timer resets and then operates during ring, until either the subscriber radio user answers, or the timer expires.

2.9.6.12 Interconnect Mobility

Roaming impacts active interconnect calls. Several possibilities can occur after the subscriber radio has roamed to the new site, depending on variables such as resource availability at the new site, and whether the subscriber radio is valid for individual call activity at the new site.

The system allows active interconnect calls in progress to be continued if the subscriber radio roams to a new site within the same zone, or to a new site within a different zone, provided the subscriber radio is valid at the new site. The subscriber radio is valid for individual services at the new site, and the site is considered to be interconnect capable, according to shared services.

2.9.6.13 Location Registration at New Site by Roaming Radio

If a subscriber radio registered on the system roams to a new site, the subscriber radio must send in a request for Location Registration on the control channel. The zone controller evaluates the subscriber radio and group ID in the request to determine if the subscriber radio and group are valid at the new site. Based on the system Site Access Denial configuration, the zone controller determines if the subscriber radio is allowed to register at the site, or if the subscriber radio is forced to leave the site in search of another control channel.

If the subscriber radio is allowed to register at the new site, the zone controller sends a control channel message to the subscriber radio, indicating that the registration has been accepted. The subscriber radio then waits on the control channel for further messages, or retries sending a message that was not acknowledged at its previously registered site.

When the subscriber radio has successfully performed location registration, the subscriber radio retries any unanswered request messages, including any request messages sent for interconnect service. After the subscriber radio has successfully performed location registration, if the subscriber radio had been participating in an interconnect call, the system automatically attempts to continue the interconnect call at the new site.

If the subscriber radio is not allowed to register at the new site, according to the systems Site Access Denial configuration, the subscriber radio resumes control channel search procedures and looks for a different site. If the subscriber radio was participating in an interconnect call at the original site and the new site is within the same zone as the original site, the call is not ended, but continues at the original site until the subscriber radio is able to successfully register at a new site, or the applicable call duration or call setup timeout timer expires.

2.9.6.14 Radio Roaming During Active Interconnect Call

When a radio roams during an active interconnect call, after the zone controller determines that the subscriber radio is valid for individual services at the new site, and that the new site is capable of supporting the interconnect call, the zone controller allows the call to continue at the new site. If the required resources at the new site are available, the zone controller grants the call at the new site immediately. If the required resources at the new site are busy, the zone controller places the call in a busy queue until the busy resource becomes available (during the busy the landline user hears silence). If the site does not have the resources to support the current call, the zone controller terminates the call.

According to the zone controller, a mobile-to-land call is active as soon as the voice channel is granted for the call, though the landline user has not yet answered the call.

2.9.6.15 Radio Roaming During Busy Interconnect Call

When the zone controller determines that the required resources are not available during the setup of a mobile-to-land or land-to-mobile call, the call is busy until the required resources are available. If the subscriber radio involved in this “busy” call roams to a new site, after the subscriber radio successfully performs location registration, the zone controller determines if the required resources are now available, or if the call must remain in the busy queue.

2.9.6.16 Radio Roaming While Ringing for Land-to-Mobile Call

When a subscriber radio roams while ringing for a land-to-mobile call, the subscriber radio continues to generate the ringing indication for the subscriber radio user. If the subscriber radio roams to a new site in the same zone, the zone controller Interconnect Ring timer continues to count down during mobile roaming and location registration. If the subscriber radio roams to a site in another zone, the zone controller in the new zone starts its Interconnect Ring timer after the mobile successfully registers.

2.9.6.17 Radio Roaming While Answering Land-to-Mobile Call, Before Receiving Response

When a subscriber radio sends in a request, it expects to receive a response from the system within a certain amount of time. If the subscriber radio does not receive a response within the time limit, the subscriber radio retries the request. After a predetermined number of retries, the subscriber radio attempts to find another control channel.

If a subscriber radio is attempting to answer a land-to-mobile call and does not receive a response, the subscriber radio roams to a new site. After the subscriber radio has successfully performed location registration, the subscriber radio resends the response for the interconnect call at the new site.

If the zone controller does not receive the response at the original site, when the zone controller receives the response at the new site, it works to set up the call at the new site, provided the subscriber radio is valid for individual call activity at the new site.

2.9.6.18 Zone Controller Receives No Answer Response at Old Site

If the zone controller does not receive the response from the old site, the call is continued at the new site in its previous call setup state. After subscriber radio performs location registration at the new site, the zone controller determines if the subscriber radio is valid for interconnect activity at the new site, and attempts to reserve the required resources at the new site. Once the subscriber radio retries, the zone controller grants the required resources for the call, assuming they are available.

2.10 Enhanced Telephone Interconnect Planning

This section provides recommendations based on the presence of the Enhanced Telephone Interconnect (ETI) feature within an existing ASTRO® 25 system.

First, identify your systems telephony needs (capacity, phone line type, and so forth.) Then, identify the number of Telephone Media Gateways (TMGs) needed (based on call capacity and encryption needs), keeping in mind that:

- Digital Voice International (DVI-XL), Digital Voice Protection (DVP-XL) algorithms max capacity = 6 calls/TMG
- Data Encryption Standard (DES-XL) algorithm max capacity = 12 calls/TMG

- DES-Output Feedback (OFB) algorithm max capacity = 15 calls/TMG
- Advanced Digital Privacy (ADP), Advanced Encryption Standard (AES) (rc4) algorithms or unencrypted max capacity = 15 calls/TMG

NOTICE: Even during a clear call, the system is limited by the lowest capacity algorithm loaded on the TMG. You can load multiple algorithms and your call capacity is the lowest value listed above for both clear or secure calls.

Up to 20 TMGs are permitted, but you must calculate the number required by determining the number of phone lines currently deployed. However, the TMG capacity varies when encryption is being used. If more than eight TMGs are required, the Ethernet switches deployed at the zone core must be the following models:

Table 7: Ethernet LAN Switch Models

System Release	Switch Model
A7.17.2	• Aruba 2930F 48G • HP 3500 • HP 3800–48
A7.17 and earlier	• HP 3500 • HP 3800–48

If the appropriate models are not deployed at the zone core, replace all Ethernet LAN switches at the zone core. If more than eight TMGs are required and the appropriate models are deployed at the zone core, evaluate the number of available ports on the Core LAN Switches, as these ports may be used for other dynamically assigned hosts (that is, network management clients and MCC 7500 Dispatch positions). While TMGs are supported only on the Core LAN switches, network management clients and MCC 7500 Dispatch positions could be re-deployed as remote sites, providing more Core LAN switch ports for core-only hosts, such as TMGs. Alternatively, you may opt to deploy an additional Core LAN Ethernet switch at the zone core to provide additional capacity.

The IP Private Branch eXchange (PBX) server comes with a standard American English recording; however, you can record a custom `.wav` file to change the greeting. Make this recording before installing the IP PBX server.

Load new configurations provided by Motorola for the Zone Core Protection (ZCP) firewall if one is in the system when Enhanced Telephone Interconnect (ETI) is installed.

Chapter 3

Enhanced Telephone Interconnect Installation

This chapter covers the installation of the following devices:

- Telephone Media Gateway
- NEC UNIVERGE 3C system
- Firewalls

3.1 Enhanced Telephone Interconnect Installation Prerequisites

The Enhanced Telephone Interconnect (ETI) installation information in this chapter is based on two assumptions:

- The ASTRO® 25 system is installed and operational.
- The system has been updated to the appropriate level of hardware and software and all previous Telephone Interconnect equipment has been decommissioned.

The following prerequisites must be met before installing the Telephone Media Gateway (TMG), IP Private Branch eXchange (PBX) server, and IP PBX media gateways or telephony firewall:

- Install configuration files on the gateway and core routers.
- Obtain T1/E1/analog lines and capacity with the Central Office (CO) before installing the media gateways.

3.2 Telephone Media Gateway Installation

This section provides the processes and procedures necessary for the initial Telephone Media Gateway (TMG) installation, which is based on the Voice Processor Module (VPM) hardware. The Telephone Media Gateway (TMG) is deployed in the zone core.

3.2.1 Installing the Telephone Media Gateway Requirements

Prerequisites:
The following prerequisites must be met before installing the Telephone Media Gateway (TMG):

- Install configuration files on the gateway and core routers.
- Obtain T1/E1/analog lines and capacity with the Central Office (CO) before installing the media gateways.

When and where to use:
This process provides a list of items you must have access to before you can complete the installation and configuration procedures for the Telephone Media Gateway (TMG).

Process:

1. Obtain the Motorola Telephone Media Gateway CD to load the Telephone Media Gateway OS images to the UNC.

2 Install applications from the *Windows Supplemental* CD.

   a Insert the Windows Supplemental CD.

   b Log on with administrator privileges and open the command window.

   c Change to \WIF directory on the CD/DVD drive, then execute the following command:
   ```
   WindowsInstallFramework.exe /e /i "Motorola PuTTY.xml"
   ```

   This media installs PuTTY, which can be used to initiate secure sessions with other devices that support secure protocols. For more information on using Secure SHell (SSH) to communicate with the Unified Network Configurator (UNC) server application, see the *Securing Protocols with SSH Feature guide*.

3 Obtain a License Key CD to install the EMC Smarts™ Network Configuration Manager license key on the network management client for the UNC. See the *Unified Network Configurator User guide*.

   The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

4 Obtain the *MOTOPATCH for Windows (OS)* CD for the latest Windows OS updates and *Motorola Virtual Appliance* DVD.

   The MOTOPATCH requirement does not apply to the K core or Express Trunking configurations except if your organization purchased Security Update Service (SUS). Then MOTOPATCH media is available for deployment in your system. SUS is available for K core, but not Express Trunking configurations.

5 Obtain the Centralized Event Logging Server (Syslog Server) software media .

6 Contact your system administrator to verify the user names, passwords, and procedures you need to access the devices on the network.

7 Obtain the following values from the system administrator:

   - Telephone Media Gateway Box ID
   - Telephone Media Gateway Zone ID
   - Telephone Media Gateway IP address
   - Primary, secondary, and tertiary Domain Name Services (DNS) IP addresses, as well as the DNS Domain Name
   - Primary and secondary NTP IP addresses
   - Primary SYSLOG server Fully Qualified Domain Names (FQDN), optional
   - RADIUS FQDN parameter value
   - RADIUS Row Status parameter value
   - RADIUS Service Time Out (sec) parameter value
   - RADIUS Service Retransmits Attempts parameter value
   - RADIUS Service Dead Timer (min) parameter value
   - RADIUS Specific Key parameter value
   - RADIUS Service Global Key parameter value
   - Host name to access the UNC server application with SSH (<username>@<IP address> format)

8 Contact your system administrator to obtain the default credentials (local accounts, central authentication, and SNMPv3) for the device being installed, as well as updated passwords for those types of accounts (so that you can change the password once you install the device). See the *SNMPv3 Feature guide* for more information.

9 Ensure that the TMG device is configured as a Remote Authentication Dial-In User Service (RADIUS) client on the RADIUS server. See the *Authentication Services Feature guide* for more information.

10 Set up the Unified Network Configurator (UNC) to use the EMC Smarts™ Network Configuration Manager/VoyenceControl component of the Motorola centralized configuration application for any of the remote site device. Depending on your organizations policies, you may also need to implement a secure protocol between the UNC and the device. Before performing any procedures using EMC Smarts™ Network Configuration Manager/VoyenceControl, discover the Telephone Media Gateway in VoyenceControl and pull the configuration into the Unified Network Configurator database. See the following ASTRO® 25 system documentation:

- *Unified Network Configurator User guide*
- *Securing Protocols with SSH Feature guide*

11 Various tools are required to install and service the equipment. If information is needed regarding where to obtain any of the equipment and tools listed, contact the Motorola Solution Support Center (SSC). The following is a list of general recommended tools for installing and servicing the hardware:

- One service laptop with the Configuration/Service Software (CSS) application installed. See the instructions in the CSS CD-ROM jewel box for instructions on loading the CSS application on a service laptop or computer
- Three Rack Units (RUs) of space for the TMG hardware and power supply tray
- One screwdriver
- One Ethernet cross-over cable
- One DB9F to RJ-45 VPM programming adapter
- One RS232 cable

3.2.2 Installing the Telephone Media Gateway

Follow this process to install the Voice Processor Module (VPM) hardware and configure it as a Telephone Media Gateway (TMG).

Prerequisites:
The following prerequisites must be met before installing the Telephone Media Gateway (TMG):

- Install configuration files on the gateway and core routers.
- Obtain T1/E1/analog lines and capacity with the Central Office (CO) before installing the media gateways.

Process:

1 Install the Voice Processor Module (VPM) hardware. See Mounting the Telephone Media Gateway Hardware on page 65.

2 Configure the startup parameters with the Configuration/Service Software (CSS). See Provisioning the Telephone Media Gateway Serial Connection Parameters on page 67.

3 Enable secure credentials.

   a Set the Software Download (SWDL) transfer mode in the CSS. See Setting the Software Download Manager Transfer Mode on page 70.

   b Set up the local Password Configuration in the CSS.See Setting the Software Download Manager Transfer Mode on page 70.

   c. Set the current date and time in CSS. See Setting the Software Download Manager Transfer Mode on page 70.
   d. Set the serial security services. See Setting the Software Download Manager Transfer Mode on page 70.
   e. Change the SNMPv3 configuration and user credentials from CSS on a selected device in the remote site. See Setting the Software Download Manager Transfer Mode on page 70.
   f. Create, update, or delete an SNMPv3 user. See Setting the Software Download Manager Transfer Mode on page 70.

4. Verify the SNMPv3 credentials. See Verifying an SNMPv3 Connection in the CSS on page 76.
5. Set the Network Services Configuration in the CSS.
   a. Configure DNS using the CSS. For instructions on using CSS to configure DNS on devices, search on “Network Services” in *CSS Online Help*. Also, see the *Authentication Services Feature guide*.
   b. Configure the Telephone Media Gateway for Secure SHell (SSH). See the *Securing Protocols with SSH Feature guide* , “Configuring SSH for RF Site Devices and VPMs Using CSS - Overview” section in the SSH Configuration chapter.
   c. Configure the local cache size for the Telephone Media Gateway. See the *Authentication Services Feature guide*.
   d. Enable Centralized Authentication in the CSS. See the *Authentication Services Feature guide*.
   e. Optional: Customize the login banner text in the CSS. See Customizing the Login Banner in the CSS on page 77.
   f. Enable RADIUS Authentication in the CSS. See the *Authentication Services Feature guide*.
   g. Optional: Enable Centralized Event Logging in the CSS. See the *Centralized Event Logging Feature guide*.
   h. Enable Network Time Protocol (NTP) in the CSS. Search on Network Services in the *CSS Online Help*.
6. Connect the TMG to the gateway router. See Installing Telephone Media Gateway Software on page 78.
7. Install the software on the TMG in the Unified Network Configurator (UNC). See Installing Telephone Media Gateway Software on page 78 for the procedures involved in the software installation on the TMG.
8. Discover the TMG in the Unified Event Manager (UEM). After the TMG is added to the ASTRO® 25 system, the UEM discovers the device as part of the site. See the *Unified Event Manager User guide* and online help for more information on the discovery process, as well as the software’s fault management capabilities.

3.2.3 Mounting the Telephone Media Gateway Hardware

This procedure describes how to install the Voice Processor Module (VPM) hardware in the chassis.

Prerequisites:
Verify that the power source, the site router, and the site equipment are located near the planned position of the Telephone Media Gateway (TMG), and that adequate rack space is available.

NOTICE: Each TMG uses one rack unit (RU) of space. The TMG uses a power supply, which sits on a two-RU high tray. Each power supply tray can hold up to three power supplies. So each TMG requires three RUs for the VPM hardware and power supplies, and three TMGs would require five RUs (three RUs for TMGs plus two for the power supply tray.) The TMG must be deployed in the zone core.

If more than eight TMGs are deployed in the system, ensure that the appropriate models of Ethernet LAN switches are deployed in the zone core. For more information, see Enhanced Telephone Interconnect Planning on page 60.

If you do not have enough open ports at the zone core, consider adding switches and/or redeploying network management clients and MCC 7500 dispatch consoles as remote sites.

Procedure:

1. Place the VPM hardware in the mounting rack.

   NOTICE: To easily access the ports and view the LEDs, mount the front of the TMG facing the rear of the rack.

2. Fasten the grounding wire from the hardware to the rack, then tighten the grounding lug.
3. Connect the DC power cable to the round port on the chassis (left side) and the power supply.
4. Plug the AC power line cord to power supply and then into the AC power source.
5. Verify that the Power LED illuminates on the chassis (right side).

Postrequisites: After the VPM hardware is installed at the site, you can install the software and configure the device to function as a TMG within your ASTRO® 25 system.

3.2.4 Telephone Media Gateway Power Distribution Installation

The basic power distribution is the Telephone Media Gateway (TMG) hardware, a power supply, and a power line cord.

For more information on the hardware specifications, see the Mounting the Telephone Media Gateway Hardware on page 65, Enhanced Telephone Interconnect Reference on page 158, and the *Voice Processor Module User guide* for more information.

3.2.5 Software Download Manager Installation and Data Transfer

The Software Download (SWDL) Manager is an application that can transfer only, install only, or transfer and install new software to devices. The new software can be installed either locally at a site or on the Network Management subsystem. Individual devices not connected to the system can be downloaded using single device mode.

Data transfer can be performed by:

Clear SWDL

Transfer operations without security, based on the File Transfer Protocol (FTP). This setting is the default for VPM-based devices.

Secure SWDL

Transfer operations are encrypted, based on the Secure File Transfer Protocol (SFTP).

NOTICE: Configuration/Service Software (CSS) can be used to configure the device SWDL transfer mode, using the Remote Access/Login Banner Screen, on one device at a time. Unified Network Configurator (UNC) can be used to schedule and configure all devices in the system at once. After the SWDL credentials are initially configured, user intervention is not required during the SWDL process.

For information on how to configure the secure or clear SWDL transfer mode, see the *Unified Network Configurator User guide* and Device Security Configuration in the *CSS Online Help*.

SWDL operation can be fault managed through Unified Event Manager (UEM), syslog, local SWDL log files, user messages, and device reports. For further information on SWDL, see the *Software Download Manager User guide*.

3.2.6 Telephone Media Gateway Initial Configuration

During the initial configuration, you must provide the IP addressing and enable the SNMP credentials, so that the Unified Network Configurator (UNC) can identify the Telephone Media Gateway (TMG) within the ASTRO® 25 system.

A laptop computer with the Configuration/Service Software (CSS) provides the Voice Processor Module (VPM) hardware with the necessary parameters to function as a TMG within an ASTRO® 25 radio system.

Generally, you can use two applications to configure the TMG: CSS and Unified Network Configurator (UNC) (not applicable for the serial port procedures which must be done using the CSS software). This manual focuses on the CSS procedures . If you want to configure the TMG using the UNC, see the *Authentication Services Feature guide* or the *Unified Network Configurator User guide* for the necessary procedures.

The CSS procedures in this manual assume CSS is loaded on your computer. See the *Private Network Management Client Feature guide*, if necessary.

3.2.6.1 Provisioning the Telephone Media Gateway Serial Connection Parameters

This procedure describes how to set up the Telephone Media Gateway (TMG) startup parameters.

IMPORTANT: Changing the device IP address causes the SNMPv3 configuration and user credentials to be reset.

NOTICE: The serial port uses the DB-9F to RJ-45 Voice Processor Module (VPM) programming adapter and an RS232 cable.

Procedure:

1 Power on the VPM hardware.

The Power LED on the front of the TMG illuminates.

2 Connect the laptop with the Configuration/Service Software (CSS) serial port to the TMG serial port using an RJ–45 to female DB9 pin serial converter.

NOTICE: The serial port is designated by a foot switch icon on the VPM hardware. See Telephone Media Gateway on page 23 for the location of the serial port.

The laptop and TMG chassis are connected.

3 Launch the CSS application and connect to the device using a serial connection.

NOTICE: If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the Username, Password, and Elevated Privileges Password fields, as they cannot be left blank.

The **CSS** main window appears.

4 To connect to the device using a serial connection, choose **Tools** → **Connection Configuration**.

The **Connection Screen** dialog box appears.

5 Set the following serial connection parameters, then click **Connect**.

- Select Serial from the **Connection Type** field.
- Select a Baud rate of **19200**.
- Select the appropriate **Com** port (usually Com Port 1).

A confirmation dialog box appears telling you that CSS has connected with the device.

6 Click **OK**. If authentication on the device is enabled, a login screen appears. Provide all required credentials. Click **OK**.

7 Select **Tools** → **Set IP Address and Box Number**.

The **Set IP Address and Box Number** dialog box appears.

8 Set the following parameters:

- Set the device IP address by entering the value. Press **Set IP Address**.
- Set the Netmask by entering the value. Press **Set Netmask**.
- After setting the other values, press **Reset** to reboot the hardware.

NOTICE: After a VPM device reset, the SNMPv3 user credentials and configuration are reset to defaults. You can reconfigure SNMPv3 user credentials or settings only after the device is reset.

The TMG reboots with the new IP address and Netmask assignments. The SNMPv3 user credentials reset to their factory default values.

9 Proceed to Setting the Software Download Manager Transfer Mode on page 70 to reconfigure the SNMPv3 credentials.

3.2.6.2
Configuring the Telephone Media Gateway in the CSS (Ethernet Connection)

This procedure describes how to set the Telephone Media Gateway (TMG) Box ID and Zone ID.

NOTICE: During initial installation, setting these IDs is done through an Ethernet cable connected directly to the Ethernet port of the TMG. After installation this procedure may be performed from a remote Configuration/Service Software (CSS).

Procedure:

1 Connect the CSS Ethernet port to the TMG Ethernet port using a cross-over Ethernet cable.

The laptop and Voice Processor Module (VPM) chassis are connected.

2 Set the Ethernet to 100 MB full duplex on the CSS laptop.

3 Set the IP address of the CSS laptop to have an IP address on the same subnet as the TMG is configured. For example, if the TMG is configured with IP address 10.101.1.203, an IP on the same subnet is 10.101.1.XXX.

4 Launch the CSS application and connect to the device using a serial connection.

NOTICE: If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the **Username**, **Password**, and **Elevated Privileges Password** fields, as they cannot be left blank.

The **Configuration/Service Software** main window appears.

5 To connect to the device using a Ethernet connection, choose **Tools** → **Connection Configuration**.

The **Connection Screen** dialog box appears.

6 Select **Ethernet** from the **Connect Type** field.

7 Type the IP address of the device.

8 Click **OK**.

The SNMPv3 passphrase prompt appears. If the connection fails, a message appears.

9 Select appropriate security level. Click **OK**.

- **NoAuthNoPriv** does not require authentication passphrase or encryption passphrase
- **AuthNoPriv** requires authentication passphrase
- **AuthPriv** requires authentication passphrase and encryption passphrase

NOTICE: During initial installation, **NoAuthNoPriv** may be selected.

10 Choose **File** → **Read Configuration From Device**.

A message window states that an Ethernet connection must be established.

11 If Centralized Authentication is enabled, an FTP Login Screen opens. See “Device Security Configuration - Remote Access Login (Ethernet)” in the *CSS Online Help* for details. Provide the required credentials.

NOTICE: If Authentication Services is enabled in the **Security Services Configuration** window, enter a **Username** and **Password**. Also, enter an **Elevated Privileges Password** if the chosen security level requires these credentials. If Authentication Services is not enabled, enter any alphanumeric value for **Username**, **Password**, and **Elevated Privileges Password**, as they cannot be left blank.

12 Click **OK**.

The **Connection Screen** appears.

13 In the navigation pane, click the **Configuration** folder.

A **Box ID** dialog box appears.

14 Enter the **Box ID** number for the TMG.

15 In the navigation pane, click the **Zone** folder.

The **Zone** dialog box appears.

16 Type the **Zone ID** number for the TMG zone.

A green mark appears indicating the Zone ID has changed.

17 Save the configuration data to an archive file.

18 Choose **File** → **Write Configuration to Device** to download the configuration data to the TMG.

The Zone ID and Box ID are set for the TMG.

3.2.6.3 Setting the Software Download Manager Transfer Mode

This procedure describes how to set the Software Download (SWDL) Manager transfer mode to FTP (clear) or SFTP (secure) for the device.

Procedure:

1. Connect to the device using CSS through an Ethernet port link. See Configuring the Telephone Media Gateway in the CSS (Ethernet Connection) on page 68.
2. From the **Security** menu, select **Device Security Configuration** → **Remote Access/Login Banner (Ethernet)**.

   The **Remote Access/Login Banner** screen appears displaying the **Remote Access Configuration** tab.

3. In the **Software Download Transfer Mode (Requested)** field, choose either **Ftp** (clear) or **Sftp** (secure). Click **OK**.

   NOTICE: Secure Shell Service and Secure FTP service are automatically set to Enabled and grayed out when you choose Sftp.

3.2.6.4 Setting the Telephone Media Gateway Local Password Configuration

This procedure describes how to set the complexity requirements and controls for the local service account password. The updated password criteria is enforced on the next password change for the device local service account. Password Configuration is an optional feature. For information, see “Password Configuration” in the *CSS Online Help*.

Procedure:

1. Launch the Configuration/Service Software (CSS) application.

   NOTICE: If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the **Username**, **Password**, and **Elevated Privileges Password** fields, as they cannot be left blank.

2. Choose **File**, **Read Configuration From Device**.

   A message window states that an Ethernet connection must be established.

3. If Centralized Authentication is enabled, an FTP Login Screen opens. See “Device Security Configuration - Remote Access Login (Ethernet)” in the *CSS Online Help* for details. Provide the required credentials.

   NOTICE: If Authentication Services is enabled in the **Security Services Configuration** window, enter a **Username** and **Password**. Also, enter an **Elevated Privileges Password** if the chosen security level requires these credentials. If Authentication Services is not enabled, enter any alphanumeric value for **Username**, **Password**, and **Elevated Privileges Password**, as they cannot be left blank.

4. Click **OK**.

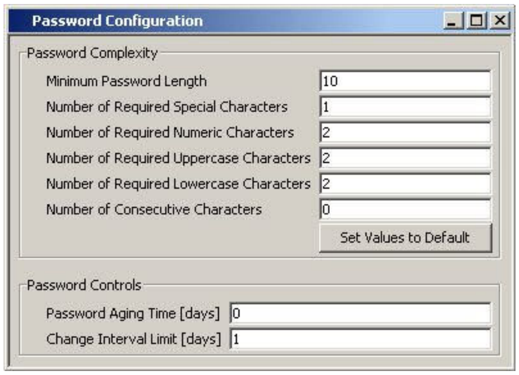
   The **Connection Screen** appears.

5. Enter the `<IP address>` of the Telephone Media Gateway (TMG) you want to access. Click **Connect**.

NOTICE: If an authentication window appears, enter your credentials. A message window appears displaying the `CSS Successfully Connected to this Device` message.

6 In the navigation pane, click the **Password Configuration** element.

Figure 13: Password Configuration Window



Password Complexity

Minimum Password Length	10
Number of Required Special Characters	1
Number of Required Numeric Characters	2
Number of Required Uppercase Characters	2
Number of Required Lowercase Characters	2
Number of Consecutive Characters	0

Password Controls

Password Aging Time [days]	0
Change Interval Limit [days]	1

The **Password Configuration** window appears.

7 Complete the following fields:

- **Minimum Password Length**: This field allows you to enter a value as the minimum length for the password. The minimum can be between 8 and 255 characters, with a default of 10 characters.
- **Number of Required Special Characters**: This field allows you to enter a value for the required number of special characters which must be included in the password. The value can be between 0 and 255, with a default of 1.
- **Number of Required Numeric Characters**: This field allows you to enter a value for the required number of numeric characters which must be included in the password. The value can be between 0 and 255, with a default of 2.
- **Number of Required Uppercase Characters**: This field allows you to enter a value for the required number of uppercase alphabetic characters which must be included in the password. The value can be between 0 and 255, with a default of 2.
- **Number of Required Lowercase Characters**: This field allows you to enter a value for the required number of lowercase alphabetic characters which must be included in the password. The value can be between 0 and 255, with a default of 2.
- **Number of Consecutive Characters**: This field allows you to enter the maximum number of consecutive repeated characters that are permitted in the password.
- **Set Values to Default**: This returns all fields to their system default values.
- **Password Aging Time [days]**: This field allows you to enter a value between 0 and 65535 for the maximum number of days a devices local password is valid. After the Password Aging Time has elapsed, the devices password must be changed. The default value is 0.
- **Change Interval Limit [days]**: This field allows you to enter a value between 0 and 65535 for the number of days which must elapse before a devices local password can be changed. The default value is 1.

8 Select **File** → **Save** to save the configuration changes.

9 Select **File** → **Write Configuration to Device** to download the configuration changes on the TMG.

3.2.6.5
Setting the Date and Time on the Telephone Media Gateway

This procedure provides the date and time to the Telephone Media Gateway (TMG). If there is a power outage, the TMG does not retain the date and time settings.

NOTICE: During installation, these procedures are done through an Ethernet cable connected directly to the Ethernet port of the TMG. After installation this procedure may be performed from a remote Configuration/Service Software (CSS).

Procedure:

1 Connect the laptop with CSS to the TMG through the Ethernet cross-over cable.

2 Set the Ethernet to 100 MB full duplex.

3 Set the IP address of the CSS laptop to have an IP address on the same subnet as the TMG is configured. For example, if the TMG is configured with IP address 10.101.1.203, an IP on the same subnet is 10.101.1.XXX.

4 Launch the CSS application and connect to the device using a serial connection.

NOTICE: If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the **Username**, **Password**, and **Elevated Privileges Password** fields, as they cannot be left blank.

The CSS main window appears.

5 To connect to the device using a Ethernet connection, select **Tools** → **Connection Configuration**.

The **Connection Screen** dialog box appears.

6 From the **Connect Type** field, select **Ethernet** .

7 Set the IP address to the TMG IP address, then choose **Connect**.

8 Choose **Tools** → **Set Date and Time**.

9 Enter the current date and time. Click **OK**.

3.2.6.6
Setting the Serial Security Services

This procedure describes how to enable the secure services and change the device password. Perform these steps before changing the SNMPv3 configuration and user credentials from Configuration/Service Software (CSS) on a selected device in the remote site.

Procedure:

1 Connect the CSS serial port to the Telephone Media Gateway (TMG) Serial port through an RJ-45 to female DB9 pin serial converter.

IMPORTANT:
Obtain the required credentials information (local service account password and elevated privileges password) to configure the site devices before proceeding. The user credentials information includes both the current and new credentials. Without the current credentials, you cannot access the device and cannot change the user credentials.

Changing to the incorrect user credentials may lead to not being able to access the device through CSS or Secure SHell (SSH). See Passwords and SNMPv3 Passphrases on page 153

2 Launch the CSS application and connect to the device using a serial connection.

NOTICE: If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the **Username**, **Password**, and **Elevated Privileges Password** fields, as they cannot be left blank.

The **CSS** main window appears.

3. To connect to the device using a Serial connection, select **Tools** → **Connection Configuration**.

   The **Connection Screen** dialog box appears.

4. Set the following serial connection parameters, then click **Connect**.
   - Select Serial from the **Connection Type** field.
   - Select a Baud rate of **19200**.
   - Select the appropriate **Com** port (usually Com Port 1).

   A confirmation dialog box appears telling you that CSS has connected with the device.

5. Click **OK**. If authentication on the device is enabled, a login screen appears. Provide all required credentials. Click **OK**.
6. Select **Security** → **Device Security Configuration** → **Security Services (Serial)** from the menu.

   The **Security Services Configuration** dialog box opens.

7. Set the **Authentication Services** field to **Enabled**. This field enables local authentication services and must be enabled as a prerequisite for centralized authentication.
8. Set the **Password Reset Mechanism** field. This field allows a user to reset the passwords for two built-in device accounts to their default values.
9. To update the password for the device, select either **Service Account** or **Elevated Privilege** from the drop-down list and click **Update password**.
10. Enter the old password, then enter a new password and confirm the new password before clicking **Change Password**.
11. Click **OK** to save the new password.

3.2.6.7 Changing SNMPv3 Configuration and User Credentials on the Telephone Media Gateway

This procedure changes the SNMPv3 configuration and user credentials from Configuration/Service Software (CSS) on a selected device in the remote site. For more information on this feature, see the *SNMPv3 Feature guide*.

NOTICE: During installation, this procedure is done through an Ethernet cable connected directly to the Ethernet port of the Telephone Media Gateway (TMG). After installation this procedure may be performed from a remote CSS.

Procedure:

1. Connect the laptop with CSS to the TMG through the Ethernet cross-over cable.

IMPORTANT:
Obtain the required SNMPv3 credentials information (Authentication passphrase, Encryption passphrase, and Authoritative Engine ID) to configure the device before proceeding. The user credentials information includes both the current and new credentials. Without the current credentials, you cannot access the device and cannot change the user credentials.

Changing to the incorrect user credentials may lead to not being able to access the device from the Unified Network Configurator (UNC) or for the device to not be able to send alarms to the Unified Event Manager (UEM) (for fault management).

2 Set the Ethernet to 100 MB full duplex.

3 Set the IP address of the CSS laptop to have an IP address on the same subnet as the TMG is configured. For example, if the TMG is configured with IP address 10.1.234.1, then an IP on the same subnet is 10.1.234.XXX.

4 Launch the CSS application and connect to the device using a serial connection.

NOTICE: If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the **Username**, **Password**, and **Elevated Privileges Password** fields, as they cannot be left blank.

The **CSS** main window appears.

5 To connect to the device through an Ethernet connection, specifically for configuring the SNMPv3 User Credentials on the device, choose **Security** → **SNMPv3 Configuration** → **Configure SNMPv3 Users (Ethernet)**.

The **SNMPv3 Login/Connection** dialog box appears with MotoAdmin as the selected SNMPv3 user.

6 Enter the appropriate authentication and encryption passphrases/passwords in the fields.

NOTICE: When accessing the device for the first time, if the default passphrases do not work, the passphrases may have been set to default values by a different system release of software. See the *CSS Online Help* section “Reset SNMPv3 Configuration (Serial)” to reset the passphrases to the current software release defaults.

7 Enter: `<IP address>`

8 Click **OK**.

A connection is made with the selected device, and the entered SNMPv3 admin passphrases/passwords are authenticated and the **Configure SNMPv3 Users** dialog box appears. If the connection fails, a message appears.

9 To choose the SNMPv3 user whose credentials are to be updated, select **Username** from the **Username** list in the **User Information** form of the **Configure SNMPv3 Users** dialog box.

NOTICE: Depending on the user selected, some fields on this dialog box become Read-Only or disabled. Click **Cancel** on the **Configure SNMPv3 Users** dialog box at any time to discard changes made to the selected user.

The CSS retrieves the current credentials from the device for the selected user.

10 To change or update the SNMPv3 security level for the selected user, select the security level from the **Security Level** list in the **User Information** form of the **Configure SNMPv3 Users** dialog box. The security level options are:

- **NoAuthNoPriv**: Neither the Authentication Password nor Encryption Password is needed for communicating with the device.
- **AuthNoPriv**: Authentication Password is needed; but no Encryption Password is needed for communicating with the device.

- **AuthPriv**: Both Authentication Password and Encryption Password are needed for communicating with the device.

NOTICE: The **User Status** field on the **Configure SNMPv3 Users** dialog box reflects the current operational status of the selected SNMPv3 User. The **Status Types** include:

- **Active**: User configured on device; **Update** and **Delete** selections are enabled.
- **Not in service**: User configured on device; **Update** and **Delete** selections are enabled.
- **Not ready**: User configured on device; **Update** and **Delete** selections are enabled.
- **Not present**: Not present on the device; **Create** selection is enabled.

The security level of the selected user is set.

11 To change the authentication password/passphrase for the selected SNMPv3 user (if applicable to the selected security level), type the password into the **Old Password Field** in the **Authentication Password** form of the **Configure SNMPv3 Users** dialog box.

NOTICE: If you do not know the password, select the **I do not remember old password** check box.

12 Type the new password/passphrase into the **New Password** field.

NOTICE: Password must be between 8 and 64 characters in length and must consist of upper or lowercase alphanumeric characters (excluding the @ # $ ^ or _ characters).

13 Type the same new password/passphrase into the **Confirm New Password** field.

14 To change the encryption password/passphrase for the selected SNMPv3 user (if applicable to the selected security level), type the old password/passphrase into the **Old Password Field** in the **Encryption Password** form of the **Configure SNMPv3 Users** dialog box.

NOTICE: If you do not know the password, select the **I do not remember old password** check box.

15 Type the new password/passphrase into the **New Password** field, then type the same new password/passphrase into the **Confirm New Password** field.

16 To change the **Authoritative Engine Identifier** (applicable to MotoInformA and MotorInformB users only), select the desired current engine ID from the **Current Engine ID List** in the **Authoritative Engine ID** Section of the **Configure SNMPv3 Users** dialog box.

17 Type the new engine ID into the **New Engine ID** field.

NOTICE: The new engine ID must be between 1 and 27 characters and comply with the Engine ID Domain Name Syntax.

The authoritative engine ID is assigned.

18 To create, update, or delete SNMPv3 users, continue with Adding or Modifying an SNMPv3 User on page 75.

3.2.6.8

Adding or Modifying an SNMPv3 User

This procedure describes how to create, update, or delete an SNMPv3 user from the Configure SNMPv3 Users Screen dialog box.

Procedure:

1 In the Configuration/Service Software (CSS), log in using the appropriate credentials.

2 To create, delete, or update the selected SNMPv3 user, use one of the following steps:

- If you want to create a user when the status is Not Present, click **Create**

- If you want to update an existing user, click **Update**
- If you want to remove an existing user, click **Delete**

A **Confirmation** dialog box appears and asks if you want to continue.

3 Click **Yes**.

The **Processing Requests** dialog box appears and processes the request. A green square indicates OK and a red square indicates failure.

4 After reviewing the processing status, click **OK**.

NOTICE: If you encounter any errors, go back to the appropriate step and correct the information entered.

5 Repeat these steps for any SNMPv3 users you wish to create, update, or delete.

6 In the **Configure SNMPv3 Users** dialog box, click **Cancel**.

The **Configure SNMPv3 Users** dialog box closes, and the **CSS** main window returns.

7 Select **File** → **Exit**. Click **OK**.

The **CSS** application closes.

3.2.6.9
Verifying an SNMPv3 Connection in the CSS

When and where to use:
When the SNMPv3 user credentials have been created, modified, or deleted, you can verify the device is properly configured for SNMPv3. This procedure describes how to verify the SNMPv3 connection.

IMPORTANT: This procedure requires that you know the IP address or the Fully Qualified Domain Name (FQDN) for the device. If you do not, you can see the *SNMPv3 Feature guide* for more information on the **Fetch DNS** option.

Procedure:

1 Connect a service laptop or network management client with Configuration/Service Software (CSS) to the Telephone Media Gateway (TMG), then launch the CSS application using an Ethernet connection.

NOTICE: If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the **Username**, **Password**, and **Elevated Privileges Password** fields, as they cannot be left blank.

2 When the passphrase prompt screen opens, select configured security level and enter the required passphrases.

A confirmation dialog box appears indicating that the CSS has connected with the device.

3 Click **OK** if the connection was successful. This step indicates your SNMPv3 configuration is valid.

NOTICE: If you fail to connect or login to the device in SNMPv3 mode, then the device is not properly configured for SNMPv3.

4 On the main **CSS** window, select **File** → **Exit**. Click **OK** to confirm that you want to exit.

3.2.6.10 Network Services Configuration in the CSS

The Configuration/Service Software (CSS) is used to configure the Site, Network Services Configuration, and Password Configuration screens for the Telephone Media Gateway (TMG). The Zone ID and TMG ID are configured for the TMG in Configuring the Telephone Media Gateway in the CSS (Ethernet Connection) on page 68 and the Password Configuration procedure is provided in Setting the Telephone Media Gateway Local Password Configuration on page 70.

The Network Services Configuration window allows you to configure the network Domain Name Services (DNS), RADIUS, and Syslog services for this TMG. This window contains three tabs to configure all parameters. Each tab is its own procedure in this section; however, you do not need to launch CSS and save the configuration on each tab if you are performing all of these steps at the same time. You just need to fill in the fields on each tab, then save the file to the archive and write to the device once.

See the *CSS Online Help* and the following manuals for the CSS procedures to perform the following:

- Configuring DNS in the CSS. See the *Authentication Services Feature guide*.
- Configuring the TMG for SSH. See “Configuring SSH for RF Site Devices from CSS” section in the SSH Configuration chapter of the *Securing Protocols with SSH Feature guide*.
- Configuring the local cache size for the TMG. See the *Authentication Services Feature guide*.
- Enabling Centralized Authentication in the CSS. See the *Authentication Services Feature guide*.
- Enabling RADIUS Authentication in the CSS. See the *Authentication Services Feature guide*.
- Enabling Centralized Event Logging in the CSS (optional). See the *Centralized Event Logging Feature guide*.
- Enabling Network Time Protocol (NTP) in the CSS. Search on Network Services in the *CSS Online Help*.

NOTICE: You can also use the *CSS Online Help* in the software application to complete these tasks during the device configuration.

3.2.6.10.1 Customizing the Login Banner in the CSS

This procedure describes how to edit the login banner security notice.

Procedure:

1. Connect to the device using Configuration/Service Software (CSS) through an Ethernet port link. See Configuring the Telephone Media Gateway in the CSS (Ethernet Connection) on page 68.
2. Select **Security** → **Device Security Configuration** → **Remote Access/Login Banner (Ethernet)** .

   The **Remote Access/Login Banner** screen appears displaying the **Remote Access Configuration** tab.
3. Click the **Login Banner** tab.
4. Edit the text of the banner.
5. Click one of the following options:
   - **Refresh**: To re-read the original Login Banner text.
   - **Apply**: To save your changes and keep the screen open .
   - **OK**: To save your changes and close the screen.
   - **Close**: To close the screen without saving your changes.

3.2.7

Connecting the Telephone Media Gateway to the Network

When and where to use:
When the Telephone Media Gateway (TMG) is installed in the mounting rack and the initial startup configuration and security credentials are set, perform this procedure to connect the TMG to the existing gateway.

Procedure:

1. Connect a cross-over Ethernet cable to the Ethernet port on the gateway router.
2. Connect the opposite end of the Ethernet cable into the Ethernet port on the TMG.

   The TMG shares an Ethernet cable with the gateway.
3. Verify the connection by accessing the site from the remote Configuration/Service Software (CSS).

3.2.8

Installing Telephone Media Gateway Software

The Unified Network Configurator (UNC) is the Network Manager used to load Operating System software to the Telephone Media Gateway (TMG) devices. This process lists the basic steps involved in the software installation on the device.

NOTICE: You can also use either the UNC or Software Download Manager (SWDL) application to load software on the TMG.

Process:

1. Discover the TMG device in the UNC. See Discovering the Telephone Media Gateway Devices with the UNC on page 78.
2. Log in to the UNC Server Application with PuTTY. See “Logging in to the UNC Server Application Using PuTTY” in the *Unified Network Configurator User guide* for this procedure.
3. Load the Operating System images to the UNC. See Loading the Telephone Media Gateway OS Images to the UNC on page 80.
4. Enable FTP services on the UNC. See Enabling FTP Service in Telephone Media Gateway Devices on page 81.
5. Transfer and install the OS image to the TMG. See Transferring and Installing the OS Image to Telephone Media Gateway Devices on page 81.
6. Inspect the TMG properties for the transferred and installed software. See Inspecting Device Properties for Software Transferred and Installed to Telephone Media Gateway Devices on page 83.
7. Disable FTP services for the UNC. See Disabling FTP Service on page 83.
8. Loading encryption keys on the TMG. See Loading Encryption Keys on page 105.
9. Discover the TMG in the Unified Event Manager (UEM). When the TMG is added to the ASTRO® 25 system, the UEM discovers the device as part of the site. See the *Unified Event Manager User guide* and online help for more information on the discovery process, as well as the software fault management capabilities.

3.2.8.1

Discovering the Telephone Media Gateway Devices with the UNC

When and where to use:

The discovery process allows site devices to be managed by the Unified Network Configurator (UNC). After the Telephone Media Gateway (TMG) is installed, configured through the Configuration/Service Software (CSS), and security parameters are enabled, use this procedure to discover the device and then you can update configuration information using this configuration management application.

The UNC network management solution consists of two applications, and both the UNC Wizard and the EMC Smarts™ Network Configuration Manager applications are used in this procedure.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

When the device is discovered in the UNC, the OS images and TMG configuration files can be loaded to add a TMG to a 3600 site, which then connects the 3600 site to the current ASTRO® 25 zone core.

NOTICE: To re-discover a replacement device in the system, replace the previous TMG in the UNC. See Chapter 4, “Replacing a Device” in the *Unified Network Configurator User guide*.

Procedure:

1. Ensure that Domain Name Services (DNS) is functional on your system. DNS is supplied by a specific server application, which also needs to be operational before you can discover the TMG.
2. Log on to the UNC Wizard from the network management client, by double-clicking the **Internet Explorer** icon on the desktop.
3. Type `http:ucs-unc0<Y>.ucs:9080/UNCW` in the **Address** field, where <Y> is the number of the UNC server (01 for primary core UNC server, and 02 for backup core UNC server). Press ENTER.

   The **UNC Wizard** launches and a login dialog box appears.
4. Type the administrative username and password. Click **OK**.
5. From the list of available wizards on the left side, select **Subnet Discovery**.

   The right side of the window is updated with the **Subnet Discovery** form.
6. Select **Master Site** by clicking on the **Discovery Type** drop-down list.
7. Enter the **Zone ID**. Click **Submit**.

   An auto-discovery job is created in the **UNC Schedule Manager**. You are finished using the **UNC Wizard** now.
8. Log on to the UNC from the NM client, by typing `http:ucs-unc0<Y>.ucs` in the **Address** field, where <Y> is the number of the UNC server (01 for primary core UNC server, and 02 for backup core UNC server). Press ENTER.

   NOTICE: When logging on to the UNC, the first screen displays the name EMC Smarts™ Network Configuration Manager instead of VoyenceControl.

   The UNC client launches and a login dialog box appears.
9. Type the administrative username and password. Click **OK**.

   The **EMC Smarts Network Configuration Manager** launches.
10. Press F7 (Schedule Manager).

    The **Schedule Manager** window appears in the UNC with the discovery jobs.
11. Verify that the **Zone** and **Master Site** containers include TMGs just discovered.

    NOTICE: No sites should be in the **Lost and Found** folder. If so, use the *Unified Network Configurator User guide* for troubleshooting guidance.

3.2.8.2

UNC Server Application Logon Using PuTTY

Log on to the Unified Network Configurator (UNC) server application using a Secure SHell (SSH) session and your Active Directory account that is a member of the user group with privileges to load new Operating System (OS) images and update an OS. See the *Authentication Services Feature Guide* and *Private Network Management Servers Feature Guide* for more information on this procedure.

3.2.8.3

Loading the Telephone Media Gateway OS Images to the UNC

This procedure loads the Operating System (OS) images for the routers, switches, terminal servers, Telephone Media Gateway (TMG), and other Voice Processor Module (VPM) devices for distribution through the Unified Network Configurator (UNC). This procedure requires the TMG and VPM OS Image CDs.

When OS images are distributed to the UNC, you can update the TMG configuration files to the UNC.

Procedure:

1 Launch an Secure SHell (SSH) terminal server session in PuTTY to access the **UNC Server Administration** menu.

   The **UNC Server Administration** menu appears.

2 Select the **Application Administration** menu.

3 Select **OS Images Administration** from the menu. Press ENTER.

4 Select **Load new OS images** from the menu. Press ENTER.

   A message appears indicating there are two methods for loading OS Images.

5 Insert the OS Images CD into the CD/DVD-ROM drive of the server.

   The drive light starts blinking on the server.

6 When the drive light stops blinking, press ENTER.

   NOTICE: The Transport OS Image media is packaged with the Network Management DVDs when an ASTRO® 25 system ships.

   The OS images load on the UNC.

7 Select **Eject CD** from the menu. Press ENTER.

   The media ejects from the drive on server.

8 Remove the OS Image CD from the CD/DVD-ROM drive of the server.

   The User Configuration Server Administration menu appears.

9 Select **quit**. Press ENTER again.

3.2.8.4

Loading OS Software to Telephone Media Gateway Devices

These procedures describe how to load software images onto Unified Network Configurator (UNC), and download and install this software to the Telephone Media Gateway (TMG).

Process:

1. Before you begin to install the software, enable FTP as described in Enabling FTP Service in Telephone Media Gateway Devices on page 81.
2. Download the OS from the Unified Network Configurator (UNC) to the Telephone Media Gateway (TMG). See Transferring and Installing the OS Image to Telephone Media Gateway Devices on page 81.
3. When the software has been transferred and installed, use this procedure to inspect the device properties before assuming the installation was a success and disabling FTP service. See Inspecting Device Properties for Software Transferred and Installed to Telephone Media Gateway Devices on page 83.
4. After the transfer and installation of the software, the FTP service must be disabled. Follow Disabling FTP Service on page 83.

3.2.8.4.1

Enabling FTP Service in Telephone Media Gateway Devices

Before you begin to install the software into the Telephone Media Gateway (TMG), you must enable FTP as described in this procedure.

Procedure:

1. Launch an Secure SHell (SSH) terminal server session in PuTTY to access the **UNC Server Administration** menu.

   The **UNC Server Administration** menu appears.

2. Select **Unix Administration** from the menu. Press ENTER.
3. Select **FTP Services** from the menu. Press ENTER.
4. Select **Enable FTP Service** from the menu. Press ENTER.

   The FTP Services are enabled and available for software transfer and install operations.

3.2.8.4.2

Transferring and Installing the OS Image to Telephone Media Gateway Devices

This procedure describes how to download the OS from the Unified Network Configurator (UNC) to the Telephone Media Gateway (TMG).

Procedure:

1. Log on to the UNC from the network management client, by typing `http:ucs-unc0<Y>.ucs` in the **Address** field

   where ***<Y>*** is the number of the UNC server (`01` for primary core UNC server, and `02` for backup core UNC server).

2. Press ENTER and log in using the admin account.
3. In the left navigation pane, expand **Networks** → **Astro 25 Radio Network** → **Views**.

   The list of options expands.

4. Double-click **Motorola Telephone Media Gateway** from the navigation pane.

   The view opens and all currently discovered TMG devices appear.

5. Select **Tools** → **OS Inventory**.

   NOTICE: You can also press the F9 key to select the OS Inventory.

   A list of the OS images appears.

6. Verify OS images loaded on the UNC server appear in the OS inventory.

   NOTICE: These images were automatically created during Loading the Telephone Media Gateway OS Images to the UNC on page 80.

7. Under **Networks** in the navigation pane, select one or more devices from the same device class, right-click the selections. Choose **Update OS Image** from the menu.

8. Select **Software Image**. Click **Next**.

9. Select each device that appears in the **Selected Devices** section.

   NOTICE: In most cases, the summary of device partitions are set up and you only need to verify the values in step 9 to step 11.

   This associates a version to a device instance.

10. Select **nvm partition** from the **Manage Partition for Device** section.

    NOTICE: This is the only choice for TMG device.

    This defines where the OS image is transferred.

11. Select the image for this device from the **Selected Image** section.

    NOTICE: Ignore the **Install** and **Copy** check boxes.

    This populates the **Image Info** tab and informs the application which image to use.

12. Select the **Device Options** section, **Software Operations**, then choose

    - **transfer**
    - **install**
    - **both**

    NOTICE: If you choose **transfer**, select the install option later to complete the installation. If you choose **both**, the software is transferred and then installed. Up to two resets of the TMG/Voice Processor Module (VPM) may be performed during installation.

    This step indicates which operations occur when the job is executed.

13. Click **Schedule**.

14. Configure the schedule information and click **Approve and Submit**.

    NOTICE: If you choose **Submit**, you are asked to approve the job later.

    This step approves the job and you can view it in the **Schedule Manager** window.

15. Verify the job status by pressing F7 (Schedule Manager).

    The **Schedule Manager** window appears in the UNC with the discovery jobs.

3.2.8.4.3

Inspecting Device Properties for Software Transferred and Installed to Telephone Media Gateway Devices

After the software has been transferred and installed, use this procedure to inspect the device properties before assuming the installation was a success and disabling FTP service.

Procedure:

1. From the **Device** view, right-click the device, select **Pull** → **Pull Hardware Spec**.

   NOTICE: You can skip this step if a **Pull All** or **Pull Hardware Spec** has occurred.

   The current software version information is updated in the Unified Network Configurator (UNC).

2. From the **Device** view, right-click the device, then choose **Properties**.

   NOTICE: If you select the **Properties** icon, you can view the device properties appear directly within the **Device** view.

   The **Device Properties** window appears.

3. Choose the **Configuration** tab, then the **Hardware** tab.
4. Double-click the **Chassis** object from the **Physical Hardware** properties.

   The **Chassis** property tree expands.

5. View the following properties and their values:
   - **Telephone Media Gateway**: Installed and Running Software.
   - **Bnk1:Telephone_Media_Gateway**: Transferred software in bank 1.
   - **Bnk2:Telephone_Media_Gateway**: Transferred software in bank 2.

   NOTICE: You can use the Table format (instead of the Diagram format) to view the Installed and Running Software in the Device view.

3.2.8.4.4

Disabling FTP Service

After the transfer and installation of the software, the FTP service must be disabled. Follow this procedure to disable FTP service.

Procedure:

1. Launch an Secure SHell (SSH) terminal server session in PuTTY to access the Unified Network Configurator (UNC) **Server Administration** menu.

   The **UNC Server Administration** menu appears.

2. Select **Application Administration** from the menu. Press Enter.

   The **Application Administration** menu appears.

3. Select **FTP Services** from the menu. Press Enter.

   The **FTP Services** menu appears.

4. Select **Disable FTP Service** from the menu. Press Enter.

   The FTP Services are disabled and unavailable for software transfer and install operations.

5. Back out of the menus by pressing q three times.

6 At the prompt, type `exit` to return to the previous menu.

7 Type `exit` again.

   You have successfully logged out of the application.

8 Close the PuTTY connection.

3.3 NEC UNIVERGE 3C System Installation

This section describes the NEC UNIVERGE 3C system, which includes the IP Private Branch eXchange (PBX) server, the 3C Administrator application, and optionally the COHub and BranchHub media gateways, which are only used when a Telephony Gateway is not implemented.

In addition to this manual, see the following NEC documentation for more information on the UNIVERGE 3C system:

- NEC *BOOK 2: Install and Configure the UNIVERGE 3C System*
- NEC *BOOK 4: Integrate UNIVERGE 3C Partner Technologies*
- NEC *BranchHub Installation Manual*
- NEC *COHub Installation Manual*

You can also access the NEC documentation suite at `C:\Program Files (x86)\Sphere\Documents\System Install and Management` folder. This documentation requires Adobe Acrobat Reader, which is available for free online and on your ASTRO® 25 system Supplemental CD.

3.3.1 Preparing for NEC UNIVERGE 3C System Installation

This procedure provides a list of items required before you can complete the installation and configuration procedures for the IP Private Branch eXchange (PBX) server and optional IP PBX media gateways.

Process:

1 ASTRO® 25 system media must be available. Specifically, obtain the Windows Server 2008 OS media.

2 Install applications, as needed, from the Windows Supplemental CD. Insert the *Windows Supplemental* CD, log in with administrator privileges, open the command window, change to `\WIF` directory on the CD/DVD drive, then execute the following command:

```
WindowsInstallFramework.exe /e /i "Motorola PuTTY.xml"
```

3 Obtain the *MOTOPATCH for Windows* media for the latest Windows OS updates.

   NOTICE: The MOTOPATCH requirement does not apply to the K core or Express Trunking configurations except when your organization purchased Security Update Service (SUS). Then the MOTOPATCH media is available for deployment in your system. SUS is available for K core, but not Express Trunking configurations.

4 Obtain the Centralized Event Logging Server (Syslog Server) software media (optional).

5 Locate copies of the NEC UNIVERGE 3C software DVD and UNIVERGE 3C License Key CD.

   NOTICE: Contact your Motorola Field representative to have a license issued by NEC in your domain name.

6 Obtain the user names, passwords, and procedures required to access the devices on the network. For specific user names and passwords to access devices on the network, contact your system administrator.

7 Determine the type of service to obtain from the Telco service provider if using the NEC media gateways/without telephony firewall configuration.

> **NOTICE:** Time slots designated for bi-directional service (land-to-mobile and mobile-to-land) can emulate loop start or ground start signaling. Loop start, ground start, and EM signaling are available only on T1 trunks configured as CAS. Only PRI ISDN is supported for T1 or E1. Inbound only Direct Inward Dial (DID) service must use EM signaling.

8 Obtain the following values from the system administrator:

- The IP address and Domain Name Services (DNS) settings for the IP PBX server
- PBX User username and password used for Session Initiation Protocol (SIP) link authentication (must be the same as the PBX User password for the zone controller)
- Computer name for the IP PBX server (that is, `Z00<zone number>IPPBX01.zone<zone number>`. For example, Z00xIPPBX01.zone***<x>***, where ***<x>*** is the actual zone number. If that zone number is 6, the IP PBX server is `Z006IPPBX01.zone6`.
- IP address and port to send Syslog messages (zone Syslog server), optional
- The IP Address of any optional BranchHub or COHub media gateways
- Total capacity, inbound capacity, and outbound capacity values (where Inbound and Outbound values added together should equal the total capacity)
- Realm field (domain of the IP PBX server)
- User Agent parameters (for zone controller SIP trunk)
- Unified Network Configurator Wizard (UNCW) parameters for the IP PBX SIP URI Domain Name (which is `zone<zone number>`, for example `zone6`) and IP PBX URI User Name (`zcsiptrunk`)
- MG_number (the particular BranchHub or COHub media gateway number), optional
- Active Directory domain name, and AD Domain Administrator user names and password
- UNIVERGE 3C license file (must be licensed by NEC in your domain name)
- Wireshark software (optional, open-source packet analyzer that can be used for troubleshooting the UNIVERGE 3C system. Available at http://www.wireshark.org).

9 Ensure that you have the default credentials (local accounts, central authentication) for the device being installed, as well as updated passwords for those types of accounts (so that you can change the password once you install the device). Contact your system administrator, if you do not have this information.

10 Purchase blank DVD-Rs to back up the UNIVERGE 3C database configuration.

11 Various tools are needed to install and service the equipment. For information regarding where to obtain any of the equipment and tools listed, contact the Motorola Solution Support Center (SSC). The following is a list of general recommended tools for installing and servicing the hardware:

- One service laptop with the Configuration/Service Software (CSS) application installed. See the instructions in the CSS CD-ROM case for instructions on loading the CSS application on a service laptop or computer
- A keyboard, mouse, and monitor for the Dell server
- One Rack Unit (RU) of space for the server hardware. Extra one RU of space for each IP PBX media gateway
- One screwdriver
- One Ethernet cross-over cable
- IP cables (NIC connection)

- One 25 pair RJ21X cable (for each BranchHub media gateway requiring Telco connection)
- One type 66 punchdown block (for a demarcation point for each BranchHub media gateway requiring Telco connection)
- One 8–pin modular connector (for each COHub media gateway requiring Telco connection)
- One Smart Jack (for a demarcation point/troubleshooting for each COHub media gateway requiring Telco connection)
- One null modem cable (per DB9 EIA-232 serial port) for each media gateway

3.3.2 Mounting the Dell Server and Optional Media Gateways

When and where to use:
Mount the IP Private Branch eXchange (PBX) media gateways above the Dell server for easy reading of the scrolling marquee displays on the front panel of the media gateways for troubleshooting purposes. This procedure provides details on mounting the NEC UNIVERGE 3C system hardware.

Before starting the installation, determine the physical location of each component on the rack or cabinet.

Procedure:

1 Determine whether to mount the server in a rack or cabinet.

If…	Then…
If you want to rack mount the hardware,	perform the following actions: **a** Remove the four screws that fasten the mounting ears of the device. **b** Rotate the metal mounting ears 180 degrees. **c** Reinstall the mounting ears for each server/media gateway so it mounts in the middle of the rack.
If you want to cabinet mount the hardware,	proceed to the next step.

2 Using the mounting rails and instructions that ship with the Dell server, mount the server in the lowest point of the cabinet/rack that the NEC equipment is going to occupy.

3 Mount any optional BranchHub or COHub media gateways immediately above the server in a stacked manner.

NOTICE: This equipment does not require a minimal vertical clearance.

4 Connect a keyboard, mouse, and monitor to the Dell server.

5 Connect the IP cables to the NIC on each media gateway and the Dell server.

IMPORTANT: The Dell server uses the first NIC on the left when viewed from the back. Whereas, the BranchHub MG and COHub MG NICs are on the left side of the front panel.

6 Connect the power cables and power up the equipment.

3.3.2.1 Establishing the Telco Connection for the NEC BranchHub Media Gateway

This procedure provides the initial connection steps for the BranchHub media gateway.

Two 25 pair RJ21X connectors are on the front panel of the BranchHub media gateway. The one on the right is used for connecting the BranchHub media gateway to the Telco service provider. Use a type 66 punch block as a demarcation point for ease of connection.

Table 8: RJ21X Connector Pinouts

The following table details the pinout for the 25 pair RJ21X connectors.

NOTICE: The FXO ports on the BranchHub media gateway only support Loop Start lines.

FXO Port Number	Ring Lead	Tip Lead
1	26	1
2	27	2
3	28	3
4	29	4
5	30	5
6	31	6

Procedure:

1 Connect the BranchHub media gateway to either a punch down block or wiring panel using the Trunk Lines 50-position connector on the right side of the front of the BranchHub media gateway.

2 Connect the Public Switched Telephone Network (PSTN) trunks to the punch down block or wiring panel based on premise wiring.

3 Connect the AC power cord to the BranchHub media gateway and an AC outlet.

4 Press the ON/OFF switch on the back panel.

IMPORTANT: NEC recommends supporting all UNIVERGE 3C system equipment with an uninterruptible power supply backup unit.

Verifies that the Power LED illuminates.

5 Verify that the BranchHub media gateway initializes. See Chapter 2 of the NEC *BranchHub Installation Manual* for more information.

3.3.2.2 Establishing the Telco Connection for the NEC COHub Media Gateway

This procedure provides the initial connection steps for the COHub media gateway.

Several options are available for connecting the COHub media gateway to the Telco service provider. If you use the 8-pin T1/E1 RJ48C modular connector on the right side of the front panel, a Smart Jack can be used as a demarcation point and is useful for troubleshooting purposes. When you order T1 services from the Public Switched Telephone Network (PSTN) Central Office (CO), reach an agreement on how the services are delivered to the COHub media gateway.

IMPORTANT: You must agree on the type of service obtained from the Telco service provider before installation. Time slots designated for bi-directional service (land-to-mobile and mobile-to-land) can emulate loop start or ground start signaling. Inbound only Direct Inward Dial (DID) service must use EM signaling. Agree on these details with the service provider for a successful installation of the COHub media gateway. DID is only supported using a COHub set for a T1 CAS circuit emulating EM signaling.

Table 9: 8 Pin Modular Connector Pinout

The following table describes the functions for the COHub media gateway 8–pin modular connector.

Pin Number	Function
1	Receive RING (RX A)
2	Receive TIP (RX B)
3	Not Used
4	Transmit RING (TX A)
5	Transmit TIP (TX B)
6	Not Used
7	Not Used
8	Not Used

Procedure:

1. Connect a UTP-5 cable from the T1/E1 Interface port (8-position modular jack wired per RJ-48C configuration) to the T1/E1 NIU at the demarcation point.
2. Install a device commonly known as a smart jack to allow the T1/E1 to be placed into a loop-back mode for remote diagnostic testing by the CO. Use a wired straight-through cable.
3. Connect the Network Interface Port on the front of the COHub media gateway using the straight-through Ethernet cable to the switch.
4. If you are connecting the COHub media gateway to other network devices, such as a legacy PBX or channel bank unit, obtain a cross-over cable. See Chapter 2 of the *NEC COHub Installation Manual* for more information.

   NOTICE: For information on tandem trunking using the COHub media gateway, see the Advanced Connections chapter of *NEC BOOK 2: Install and Configure the UNIVERGE 3C System*.
5. Connect the AC power cord to the COHub media gateway and an AC outlet.
6. Press the ON/OFF switch on the back panel.

   IMPORTANT: NEC recommends supporting all UNIVERGE 3C system equipment with an uninterruptible power supply backup unit.

   Verify that the Power LED illuminates
7. Verify that the COHub media gateway initializes. See Chapter 2 of the NEC *COHub Installation Manual* for more information.

3.3.3 Installing the UNIVERGE 3C Software Process

The following process provides details on installing the NEC UNIVERGE 3C v8.5 software on the IP PBX server.

Prerequisites: This process requires that you have the following items:

- A formatted DVD-R to back up the existing database. See “How to Format a DVD-R on Windows Server 2008 R2” in the *Enhanced Telephone Interconnect Feature guide* to format the media.
- Two UNIVERGE 3C™ v8.5 software DVDs: 8.5.2.3 (disk 1) and 8.5.2.3_SP3 (disk 2).
- A UNIVERGE 3C™ v.8.5 license. Contact NEC to obtain this license if you do not have it.
- Service Pack 2 with the Windows Server 2008 Server R2 operating system on the IP PBX server.
- A test number for a mobile (ASTRO® 25 subscriber radio) calling within the radio system and a landline telephone.

When and where to use: Use this process to install UNIVERGE 3C™ v8.5 software for use with the Enhanced Telephone Interconnect feature in an ASTRO® 25 system.

Process:

1. If a database exists, back up the data to DVD-R as described in Backing Up the UNIVERGE 3C System Database on page 138.
2. Install the UNIVERGE 3C™ v8.5 software on the IP PBX server. See Installing the UNIVERGE 3C Software on the IP PBX Server on page 89, Installing Service Pack 3 on the IP PBX Server on page 91, then Commissioning the UNIVERGE 3C Software of the Console of the IP PBX Server on page 94.
3. Install the UNIVERGE 3C™ v8.5 software on the IP PBX server. See Installing the UNIVERGE 3C Software on the IP PBX Server on page 89.
4. Commission the Unified Communications Manager (UCM) application. See Commissioning the UNIVERGE 3C Unified Communications Manager on page 100.
5. Verify that the system is operational by making land-to-mobile and mobile-to-land test calls.

3.3.4 Installing the UNIVERGE 3C Software on the IP PBX Server

The NEC UNIVERGE 3C software provides more functionality for the Enhanced Telephone Interconnect feature in an existing ASTRO® 25 radio system. Follow this procedure to install the UNIVERGE 3C software on the IP PBX server.

Prerequisites: Obtain the following items:

- A formatted DVD-R to back up the existing database. See Formatting a DVD-R on Windows Server 2008 R2 on page 138.
- Two UNIVERGE 3C v8.5 software DVDs: 8.5.2.3 (disk 1) and 8.5.2.3_SP3 (disk 2).
- A UNIVERGE 3C v.8.5 license. Contact NEC to obtain this license if you do not have it.
- The Windows Server 2008 Server R2 with Service Pack 2 Operating System on the IP PBX server.

When and where to use: Use this procedure to install the IP PBX server software application.

Procedure:

1. Insert the UNIVERGE 3C software DVD in the DVD drive of the IP PBX server.

2 In Windows Explorer, navigate to the DVD drive and double-click `Launch.exe`.

Unless the User Account Control (UAC) is disabled, a UAC message appears. The software installation begins.

3 Perform one of the following actions:

If…	Then…
If UAC is disabled,	Go to the next step.
If the UAC is not disabled,	Enter the domain account credentials. Press **OK**.

4 Choose **Install Prerequisites**.

A warning message appears.

5 Click **Install**.

The prerequisites install on the IP PBX server.

6 Click **Finish**.

7 After the prerequisite software installs, click **Yes** to reboot the server.

The IP PBX server restarts.

8 In Windows Explorer, navigate to the DVD drive and double-click `Launch.exe`.

9 Click **Install Unified Communications Manager** to install the 3C Manager, Desktop, and the Administrator application.

10 Click **Yes, Continue**.

The **3C Installation** window appears.

11 Click **Next**.

12 If prompted, select **United States** for the country and **English** for the language.

The License Agreement appears.

13 Read and click **Yes** to accept the License Agreement.

14 Click **Yes** or **OK** to acknowledge any warning or confirmation dialog boxes.

15 Click **Next** on the **Setup Welcome** window.

16 Choose **Typical** installation. Click **OK**.

The UNIVERGE 3C™ installation process begins.

17 When the **Windows Security** window appears, select **Install this driver software anyway**. Repeat this step as needed.

18 Click **Yes** to restart the computer.

The IP PBX server restarts.

The UNIVERGE 3C software is installed on the console of the IP PBX server. Proceed with Installing Service Pack 3 on the IP PBX Server on page 91, Setting Permissions for the UCM Server on page 93, and then Commissioning the UNIVERGE 3C Software of the Console of the IP PBX Server on page 94 to make the server operational in the ASTRO® 25 system.

3.3.4.1 Installing Service Pack 3 on the IP PBX Server

Follow this procedure to install the UNIVERGE 3C Service Pack 3 software on the IP PBX server after software version 8.5.2.3 is installed.

Prerequisites: Ensure that the following conditions are met:

- The Windows Server 2008 Server R2 with Service Pack 2 Operating System on the IP PBX server.
- Server is joined to the ASTRO® 25 domain.
- Ensure that the domain Group Policy Objects have been applied.

When and where to use:
Service Pack 3 is a mandatory software upgrade for the Enhanced Telephone Interconnect feature in an ASTRO® 25 radio system. This procedure requires a 8.5.2.3 Service Pack 3 installation DVD. SQL Server Authentication must not be used in a Joint Interoperability Test Command (JITC) certified installation, so during this procedure you configure the server for Windows Authentication mode only.

Procedure:

1. Once the computer restarts, insert the UNIVERGE 3C 8.5.2.3 Service Pack 3 disk, run `setup.exe`, and follow prompts.
2. To ensure JITC compliance, change the SA password by connecting to the SQL Server instance with **SQL Server Management Studio**.
3. Expand the **Security** and **Logins** folders.
4. Right-click **sa user**.
5. Select **Properties**.
6. Enter a new password that meets your local complexity requirements in the **Password** field.
7. Re-enter the password in the **Confirm Password** field.
8. To change the SA user name, right-click **sa user**.
9. Select **Rename**.
10. Enter the new name.
11. Click **OK**.
12. To add the **Sphericall Admins** group to the SQL Server instance, in the **SQA Server Management** window, right-click the **Logins** folder.
13. Select **New Login**.
14. In the Login name edit control, enter `<3C system domain name>\Sphericall Admins`.

    NOTICE: When using **Search**, Groups must be added to the searchable object types by clicking **Object Types** and selecting **Group**. Once the new user is added to the SQL Server instance, add them to **Server Roles**.

15. Highlight the user name, right-click, then select **Properties and Server Roles**.
16. To navigate to the users mapped to this login, check the **Database** settings as follows in the Users mapped to the list login:
    - calls
    - master
    - PBX
17. Highlight and verify selection of the **db_owner** and **public** check boxes for all three databases.
18. Click **OK** to save and exit.

19. To change the SQL Server authentication mode, right-click on the server name, select **Security → Properties → Windows Authentication mode**.
20. To configure the Windows Sphericall Service login as the domain user `SRV3CDatabase`, run the **Services** applet from the **Administrative Tools** group.
21. Right-click **Windows Sphericall Service** and select **Properties**.
22. On the **Log On** tab, select **This account**. Enter ***<3C system Domain>***`\SRV3CDatabase`.
23. In the **Password** and **Confirm password** fields, enter the desired password for the SRV3CDatabase. Click **OK**.
24. To configure the CallLogger process for Windows Authentication connect to SQL Server using a trusted connection by changing the registry keys listed using `regedit`. Change all the following instances:

```
\\HKLM\SOFTWARE\Wow6432Node\Sphere\CallLogger\CfgTrustedConnection to
“yes”
```

```
\\HKLM\SOFTWARE\Wow6432Node\Sphere\CallLogger\CallsAdminPassword to “”
```

```
\\HKLM\SOFTWARE\Wow6432Node\Sphere\CallLogger\CallsAdminUserName to “”
```

```
\\HKLM\SOFTWARE\Wow6432Node\Sphere\CallLogger\CallsUserPassword to “”
```

```
\\HKLM\SOFTWARE\Wow6432Node\Sphere\CallLogger\CallsUserUserName to “”
```

NOTICE: When editing the registry, “” indicates an empty null stream.

25. To configure the DBServer process to connect to SQL, connect to SQL Server using a trusted connection by changing the registry keys listed using `regedit`. Change all the following instances:

```
\\HKLM\SOFTWARE\Wow6432Node\Sphere\DbServer\CfgTrustedConnection to
“yes”
```

```
\\HKLM\SOFTWARE\Wow6432Node\Sphere\DbServer\CfgAdminPassword to “”
```

```
\\HKLM\SOFTWARE\Wow6432Node\Sphere\DbServer\CfgAdminUsername to “”
```

```
\\HKLM\SOFTWARE\Wow6432Node\Sphere\DbServer\SystemAdminPassword to “”
```

```
\\HKLM\SOFTWARE\Wow6432Node\Sphere\DbServer\SystemAdminUsername to “”
```

26. To remove the CallLogger SQL accounts, connect to the calls database by expanding the following folders:
    - Databases
    - Calls
    - Security
    - Users
27. Expand the following folders:
28. Right-click **CallDBAdmin**. Select **Delete**.
29. If present, remove **CallDBUser**.
30. To remove DbServer SQL account, connect to the PBX database and remove the CfgDBAmin user by expanding the following folders:
    - Databases
    - PBX
    - Security
    - Users

31 Right-click **CfgDBAdmin**. Select **Delete**.

32 If present, remove **CfgDBUser**.

33 To grant permission to required Sphericall Admins, open a command window and navigate to `Program Files (x86)\Sphere\Data`.

34 Enter `"spgrantpermission "`***`<DOMAIN>`***`\sphericall admins"`

where ***`<DOMAIN>`*** is the 3C system domain name.

NOTICE: The quotation marks are part of this command.

35 Exit the **Command** window.

36 Repeat this task for any other UCM in the system.

3.3.4.2

Setting Permissions for the UCM Server

Follow this procedure to complete the installation of the Unified Communications Manager (UCM) server.

Prerequisites: Ensure that the following conditions are met:

- UNIVERGE 3C 8.5.2.3 and Service Pack 3 software are installed on the IP PBX server.
- The IP PBX server is running correctly.

Procedure:

1 On the IP PBX server, apply the JITC policy and enter: `gpupdate /force`

2 Place the UCM server into the new domain.

3 Log in to server using the local administrator account.

4 Change the server domain to the new Motorola domain.

5 Reboot the server.

6 Log in to server using the local administrator account.

7 To add the **Sphericall Admins** group to the SQL Server instance, in the **SQA Server Management** window, right-click the **Logins** folder.

8 Select **New Login**.

9 In the Login name edit control, enter `<new domain>\Sphericall Admins`.

NOTICE: When using **Search**, Groups must be added to the searchable object types by clicking **Object Types** and selecting **Group**. Once the new user is added to the SQL Server instance, add them to **Server Roles**.

10 Highlight the new user, right-click, then select **Properties and Server Roles**.

11 To navigate to the users mapped to this login, check the **Database** settings as follows in the Users mapped to the list log in:

- calls
- master
- PBX

12 Highlight and verify selection of the **db_owner** and **public** check boxes for all three databases.

13 Click **OK** to save and exit.

14 Close the **SQL Server Management Studio** application.

15 Open the command prompt window.

16 Enter "***<new domain>***`\Sphericall Admins"`

> **NOTICE:** The quotation marks are required in this command, but the brackets indicate a variable dependent the specific name of the new domain for your site.

17 Close the command prompt window.

18 Run the **Services** applet from the **Administrative Tools** group.

19 Right-click on **Sphericall Service**. Select **Properties**.

20 On the **Log On** tab, enter ***<new domain>***`\SRV3CDatabase` in the **This Account** field.

21 Enter the password for SRV3CDatabase in the **Password** and **Confirm password** fields.

22 Click **Apply**, then **OK**.

23 Run the **Server Manager** applet from the **Administrative Tools** group.

24 Open **Configuration** → **Local Users and Groups** → **Groups**.

25 Double-click **Administrator**.

26 Click **Add**.

27 Enter the ***<new domain>***`\Sphericall Admins` account.

28 Highlight ***<old domain>***`\Sphericall Admins`. Click **Remove**.

29 Highlight ***<old domain>***`\SRC3CMediaServer`. Click **Remove**.

30 Click **Apply**, then **OK**.

31 Reboot the server.

32 Log in to the server using an account that is a member of the Sphericall Admins group.

33 Launch the **AdminGUI** application.

34 Re-commission the UCM. See Commissioning the UNIVERGE 3C Unified Communications Manager on page 100.

The Unified Communications Manager (UCM) server is functional.

3.3.4.3 Commissioning the UNIVERGE 3C Software of the Console of the IP PBX Server

Follow this procedure to complete the installation of the UNIVERGE 3C software on the IP PBX server.

When and where to use:
Use this procedure to provision the IP PBX server software application to use more telephone interconnect features, such as voice prompts.

Procedure:

1 Once the computer restarts, double-click **3C Administrator** to begin the commissioning process.

> **NOTICE:** During the commissioning process, several dialog boxes may appear indicating password lengths are too short, prompting for software upgrades for SIP phones, and other features that are not being used in the Enhanced Telephone Interconnect solution, so these warnings can be ignored. Select the default setting where appropriate or acknowledge any warning messages that appear by clicking OK during this installation.

2. In the **Select Default Domain for RIA Clients** window, double-check the domain name.

   The **IP Phone Upgrade** window appears.

3. Select **Run IP Phone**. Click **OK**.
4. Click **OK** on any warning messages that appear.
5. Click **OK** on the completion window.

   The **NEC IP Phone Upgrade** window appears.

6. Click **OK**.

   The **Default Polycom Boot Rom** window appears.

7. Select the appropriate phone types.

The UNIVERGE 3C software is operational on the console of the IP PBX server. Proceed with the commissioning of the Unified Communications Manager (UCM) application.

3.3.5 NEC UNIVERGE 3C Application Configuration

In the NEC UNIVERGE 3C application, the items under the **General** tab are the primary system-level components to administer. Each component can be expanded to show the individual items under each component. The other tabs contain more specific topics, such as Number Plan and Trunks.

When the NEC UNIVERGE 3C application launches, six processes are automatically started and are listed under the **Unified Communications Manager - Primary Server** window:

1. dbserver
2. calllogger
3. webserver
4. desktopmanager
5. mgc
6. mediaserver

The **Primary Server** window can be minimized to the Windows tools tray, but it can never be closed out completely. These six processes collectively work in parallel to create the primary softswitch environment.

3.3.5.1 Configuring the IP PBX Media Gateway Addresses and Password

The BranchHub and COHub media gateways IP addresses are set using the Command Line Interface (CLI) over their serial port using the same procedure.

Process:

1. Configure the IP PBX Media Gateway Addresses as described in Configuring the IP PBX Media Gateway Addresses on page 96.
2. Configuring the IP PBX Media Gateway Password. See Configuring the IP PBX Media Gateway Password on page 97.

3.3.5.1.1 Configuring the IP PBX Media Gateway Addresses

Follow this procedure to configure the IP Private Branch eXchange (PBX) media gateway addresses.

Procedure:

1. Connect a terminal to the DB9 EIA-232 serial port on the back of the IP PBX Media Gateway using a null modem cable (that is, 38,400 baud, N, 8, 1, hardware flow control).
2. Press ENTER until a prompt for a password appears.
3. Type the administrative password. Press ENTER. Consult with your system administrator if you are not sure of the Media Gateway credentials.
4. Enter: `ip device add ether ether 10.<zone>.234.<MG_number>`

   where:

   `<zone>` is the zone the IP PBX media gateway is located in (1 7).

   `<MG_number>` is the particular IP PBX media gateway number (11 14).
5. Enter: `ip route add default 0.0.0.0 10.<zone>.234.254`

   The IP address is added and the prompt returns.
6. Enter: `config save` to save the configuration. Type `restart` when the prompt returns to reboot the hardware.

   The IP PBX media gateway restarts.
7. Validate that the media gateway establishes a connection with the UNIVERGE 3C application and that the Media Gateway software is updated to the correct version.
8. Disconnect the Ethernet connection.
9. At the prompt, enter `ip set ipv4 10.<zone>.234 <MG_number>/24`

   The prompt returns.
10. Type `del all routes`. Press ENTER.
11. Enter: `ip add ipv4 route 0.0.0.0/0 10.<zone>.234.254 1`
12. Enter: `config save`

    The Media Gateway IP address is set.
13. Reconnect the Ethernet connection.
14. When the media gateway finishes saving the configuration, type `restart`. Press ENTER to reboot.

    IMPORTANT: When the media gateway finishes rebooting an `Incomplete Configuration` message may appear. This message clears when the media gateway has its full configuration data entered in the 3C Administrator.
15. Change the IP PBX media gateway password. See Configuring the IP PBX Media Gateway Password on page 97.

3.3.5.1.2

Configuring the IP PBX Media Gateway Password

Use this procedure to change the default password for the IP Private Branch eXchange (PBX) media gateway.

Procedure:

1. Connect a terminal to the DB9 EIA-232 serial port on the back of the IP Private Branch eXchange (PBX) media gateway using a null modem cable (that is, 38,400 baud, N, 8, 1, hardware flow control).
2. Press Enter until a prompt for a password appears.
3. Type the administrative password. Press Enter. Consult with your system administrator if you are not sure of the media gateway credentials.
4. Type `Password`. Press Enter.

   The system prompts you for the new password.
5. Enter the new password in the **Password** and **Verify** fields. Press Enter.

   The IP PBX media gateway stores the new password.

3.3.5.2

Configuring the IP Address of the Unified Communications Manager Server

This procedure describes how to configure the address of the IP Private Branch eXchange (PBX) server, as well as the network connection.

Procedure:

1. Log on to the **Unified Communications Manager** server as the local administrator.
2. Click the **Server Manager** icon in the lower-left corner of the system tool tray.
3. Click **View Network Connections**.
4. Double-click the active connection with the IP address you want to change.

   NOTICE: Only one connection is active all inactive connection icons have a large red X on them.
5. Highlight **Internet Protocol Version 4**. Click **Properties**.
6. Set the Unified Communications Manager IP address to the default `10.<zone>.234.9`. Press Enter.
7. Type `255.255.255.0` in the **Subnet** mask field.
8. Type `10.<zone>.234.254` in the **Default Gateway** field.
9. Enter the preferred (`10.<zone>.233.163`) and alternate (`10.0.0.226`) DNS server addresses.
10. Click **Advanced**. Add the IP address and default gateways entered above, and check the **Automatic metrics** box.
11. On the **DNS** tab, set the DNS server address order and append the zone and UCS suffixes.
12. Click **OK**. Click **Close**. Click **Close** again.
13. Close the **Network Connections** window.
14. From **Start**, select **Control Panel** → **Hardware** → **Device Manager** → **Network Adapters**.

15 Select **Broadcom NetXtreme II Gig** → **Advanced** → **Speed Duplex**.

16 Set to **100 MB Full** (100 Megabytes Full Duplex). Click **OK**.

17 Right-click the unused port and select **Disable**. Repeat for all unused ports.

18 Restart the **Unified Communications Manager**.

3.3.5.3 Joining the Unified Communications Manager Server to the ASTRO 25 Domain

This procedure describes how to join the server to the ASTRO® 25 domain. See “Adding Windows-Based Devices to an Active Directory Domain – Overview” in the *Authentication Services Feature guide* for more information.

NOTICE: Log in to the Active Directory account, if available. After a device joins the domain, its applications that have Roles Based Access Control in Active Directory are not usable by the local Windows administrator or the domain administrator that is not a member of the group associated with the application for that device unless the administrator accesses the application by entering its executable path and filename at an elevated Windows command line. The path and filename can be seen in the properties for the application desktop shortcut. For information on how to run the elevated Windows command line, see “Starting the Windows Command Line as Administrator” in the *Authentication Services Feature guide*. The local Windows administrator account “Motosec” is set up by Motorola supplemental configuration for devices operating on Windows Server 2003 and 2008.

Procedure:

1 Log on to the **Unified Communications Manager** server as the local administrator.

2 Perform Changing the Computer Name on page 125 to change the computer name.

   NOTICE: Do not change the computer name or domain name if not required (that is, rejoining an existing domain).

3 On the Windows Supplemental CD, navigate to the `Join_Domain\OtherWindowsOS` directory.

4 Double-click `JoinADomain.exe`.

   NOTICE: By joining the domain, you are applying the Windows 2008 Security Group Policy to the server.

   The **Join Active Domain Directory** screen appears.

5 Type the Domain default administrator credentials. Press ENTER.

6 Enter the custom `<AD Domain Name>` (for example, `newyork.prne`).

7 Select **Telephony Server** as the **Organizational Unit (OU)** for the Unified Communications Manager server.

8 Click **Join** and verify that the join was successful.

   A `SUCCESS` message appears in green on the screen.

9 Restart the Unified Communications Manager server for the new domain to take affect.

3.3.5.4 Configuring Syslog Messaging

Centralized Event Logging (CEL) through the Syslog server is an optional feature. If you choose to enable CEL, the Sphericall system Syslog messages are forwarded to the ASTRO® 25 system Syslog server for the zone. This action requires setting two system initialization settings, Syslog server IP address (ASTRO® 25 system Syslog server) and Syslog server IP port (514). Set only the Syslog server IP address because the Syslog Server IP Port value was set during the software installation. This procedure describes how to set the IP address for the Syslog server. For more information on Syslog messaging and log files, see the *Centralized Event Logging Feature guide*.

Procedure:

1. In the Sphericall Administrator main window, double-click **System - Motorola Astro25**.

   The **System Properties** window opens.

2. Click the **System Initialization Settings** tab.
3. Click **Add**.

   A list box appears in the **Name** column.

4. Select **Syslog IP Address** from the pull-down list.
5. Enter: `10.<zone>.233.249`

   The Syslog IP address is set.

6. Click **OK** to save the IP address.

3.3.5.5 McAfee Anti-Malware Client Configuration

The ASTRO® 25 system *Core Security Management Server Feature Guide* McAfee application is used to update the Unified Communication Manager server with the latest anti-malware updates. Install McAfee Anti-Malware Client software on the Unified Communication Manager to access the latest anti-malware updates.

See Chapter 5: “CSMS – Deploying McAfee Client Software to Anti-Malware Clients” in the *Core Security Management Server Feature guide*.

3.3.5.6 Configuring Remote Desktop for the Unified Communications Manager

Remote Desktop allows remote access capabilities for configuration and maintenance of the Unified Communications Manager. This procedure describes how to enable this setting in Windows.

Procedure:

1. From **Start**, select **Control Panel** → **System and Security** → **System**.
2. Click **Remote Settings**.
3. Click **Allow connections from computers running any version of Remote Desktop (less secure)**.
4. Click **OK**.

   The Windows server hosting the Unified Communications Manager is now accessible remotely.

3.3.5.7 Sharing the UNIVERGE 3C File System

This procedure describes how to set up file sharing in Windows.

When and where to use:

To allow local users and administrative access to the Sphere folder, the UNIVERGE 3C file system must be shared.

Procedure:

1. From **Start**, select **Computer** → **C:\Program Files(x86)**.
2. Right-click **Sphere**. Select **Properties**.
3. Select **Advanced Sharing** → **Share this folder** → **Permissions**.
4. Choose **Add**. Add the following users and assign Read permissions to the Sphere file system:
   - Local administrator account
   - Domain\Sphericall Admins group account
   - Domain built-in admin account
5. Click **OK** to save the settings.

3.3.6 Commissioning the UNIVERGE 3C Unified Communications Manager

Once you install the NEC UNIVERGE 3C v.8.5 software on the IP PBX server, you can commission the Unified Communications Manager (UCM) using the UCM Commissioning wizard.

Prerequisites: Obtain the following items:

- UNIVERGE 3C v8.5 software installed on the IP PBX Server (Telephony server).
- A test number for a mobile (ASTRO® 25 subscriber radio) calling within the radio system and a landline telephone.

When and where to use: Use this procedure to complete the upgrade of the IP PBX server software application to use additional telephone interconnect features, such as voice prompts.

Procedure:

1. Log on to the Unified Communications Manager (UCM) with the domain administrator account.

   The **UCM Commissioning** wizard begins.

2. In the User Account Control (UAC) window, enter the domain account credentials. Press **OK**. If UAC is disabled, go to the next step.
3. Read and click **I accept this agreement** to accept the Software License Agreement.
4. Click **Next**.
5. Choose **Primary UCM**. Click **Next**.
6. Click **Next** without choosing any third-party voice mail options.
7. Browse to the location of the license file. For example, `C:\Program Files(x86)\Sphere\data\license.xml` or the location on the DVD drive.
8. Select **Finish completing commissioning and starting the Sphericall service**. This step takes several minutes to configure the Distributed File System (DFS) and File Transfer Protocol (FTP) components.
9. Verify the database user account name, domain, and password match the previous UNIVERGE 3C settings.
10. By default the system performs a daily backup of the database at 1 AM and is sufficient for most installations. If a periodic backup is desired, select the check box and specify a time in minutes to perform a periodic backup. Click **Next**.

11 Click **Next** without specifying any FTP/HTTPS server information.

12 Specify the local **Country Code**, **Area Code**, and **PBX phone number**, and the appropriate dialing template for the given area of operation. The PBX phone number can be any value. For example, the main number for your agency. Click **Next**.

13 Click **Finish**.

A warning message appears since various warning and options were dismissed during the commissioning process.

14 Close the window.

The UNIVERGE 3C software is ready for use.

15 Verify the items previously specified in the **General**, **Number Plan**, and **Trunks** tabs are present.

16 Configure the software. Go to Configuring the NEC UNIVERGE 3C System on page 109.

17 Launch the **UNIVERGE 3C** software on the console and verify that all services are running.

18 Configure the UNIVERGE 3C system. See Configuring the NEC UNIVERGE 3C System on page 109.

19 Make a test land-to-mobile (ASTRO® 25 subscriber radio) call to verify that the system is operational.

20 Make a mobile-to-land call to verify that the system is operational.

The NEC UNIVERGE 3C software is operational on the console of the IP PBX server.

3.3.7

Updating the UNIVERGE 3C License File

Contact your Motorola Field representative to have a license issued in your domain name. After you have the license file CD, perform this procedure to update an existing license file when required.

When and where to use:
The NEC Unified Communications Manager server is delivered with software loaded. The UNIVERGE 3C 8.5 software must be commissioned and the license file added for the application to function. You might need to update the UNIVERGE 3C license file to:

- Set the domain names during the initial deployment.
- Add more phone lines (sold in bundles of three)

NOTICE: The license domain name must match your domain name or the UNIVERGE 3C Services cannot start. The number of supported trunks must be at least six to support three simultaneous calls. Any additional call capacity requires an updated license from NEC with the number of trunks to support the desired simultaneous calls (two trunks per simultaneous call). Contact the Motorola Solution Support Center (SSC) to order a new license.

IMPORTANT: The Unified Communications Manager server must successfully join the domain before starting this procedure. See Joining the Unified Communications Manager Server to the ASTRO 25 Domain on page 98.

Procedure:

1 In the **3C Administrator**, select **Tools** → **View License Summary**.

2 Click **Load New License**.

3 Click **Browse** to navigate to the location of the new license file, select the file. Click **OK**.

4 Click **Load**.

The license file loads on the system.

5 Restart the **Unified Communications Manager**.

6 To verify the new parameters, click **Tools** → **View License Summary**.

3.3.8

Installing the Auto Attendant Voice Prompt File

When installing the UNIVERGE 3C software, the default voice prompt asks for an extension. This procedure describes how to replace that file with a custom voice prompt that asks for a radio ID.

Prerequisites: Locate the `.wav` file you want to use to replace the default Auto Attendant announcement.

NOTICE: The language used depends on the template selected in the **Telephony Area** of the **3C Administrator**.

When and where to use: Execute this procedure to install the Auto Attendant recording file at the end of the software installation.

Procedure:

1 Navigate to the `c:/Program Files(x86)/Sphere/MediaServer/AA` folder.

2 Right-click `AAPrompt0000.wav` and choose **Rename**.

3 Add `.old` to the end of the file name(AAPrompt0000.wav.old). Press **Enter**.

4 Navigate to the subfolder for the language you want to use (Example: **en** for English, **fr** for French, and so on).

5 Copy the replacement `*.wav` file into the language folder you wish to use and name the file `AApropmpt0000.wav`.

6 Close any open instances of **3C Administrator**.

7 From `Start`, select **Administrative Tools** → **Services**.

8 Highlight **Sphericall Services** and select **Restart** from the left pane.

9 After the system restarts, call a mobile radio in the ASTRO® 25 system and verify that the correct announcement is played to the land line caller.

3.4

Firewall Hardware Installation

Three firewalls related to the Enhanced Telephone Interconnect feature require installation and additional configuration if they are part of the Enhanced Telephone Interconnect (ETI) implementation:

- Telephony firewall - required for connectivity to the IP network (in lieu of NEC BranchHub or COHub media gateways)
- RNI-DMZ firewall - required if Telephone Media Gateway (TMG) is encrypted
- Zone Core Protection firewall - requires additional configuration if already deployed when ETI is installed.

3.4.1 Telephony Firewall Installation

Fortinet FortiGate 100D firewalls are used as a telephony firewall for the Enhanced Telephone Interconnect feature. Fortinet FortiGate 100D supports 650+ Mbps of firewall traffic or 120 simultaneous SIP sessions. It provides four onboard 10/100/1000 interfaces.

To install this hardware, see “Installing a Firewall in ASTRO 25 Systems” in the *Fortinet Firewall Feature Guide*. The *Fortinet Firewall Feature Guide* also includes port assignments for the telephony firewall devices.

Telephony firewalls are not used for systems with the ISSI 8000/CSSI 8000 architecture.

NOTICE: If an intersystem firewall in the zone where Enhanced Telephone Interconnect is present, that ISG 1000 firewall can also serve as the telephony firewall.

3.4.2 RNI-DMZ Firewall Installation

When the Key Management Facility (KMF) is used to centrally manage encryption keys on the Telephone Media Gateway (TMG), the Enhanced Telephone Interconnect (ETI) feature requires a Radio Network Infrastructure (RNI)-Demilitarized Zone (DMZ) firewall.

- If the RNI-DMZ firewall does not exist in the system, install and configure it using the “Firewalls Common Installation Process for ASTRO 25 Systems” in the *Fortinet Firewall Feature Guide*.
- If the RNI-DMZ firewall already exists in the system and is configured for the ASTRO® 25 systems release that includes ETI, its configuration already supports the ETI feature.

3.4.3 Zone Core Protection Firewall Installation

If Zone Core Protection (ZCP) is present on the ASTRO® 25 system where Enhanced Telephone Interconnect (ETI) components are being installed, load new configurations provided by Motorola for the ZCP firewalls, using the procedure in “Loading/Restoring a Firewall Configuration Locally Using TFTP” in the *Fortinet Firewall Feature Guide*.

Information on the ZCP firewalls is located in the *Zone Core Protection Infrastructure Feature Guide*.

Chapter 4

Enhanced Telephone Interconnect Configuration

This chapter details configuration procedures relating to Enhanced Telephone Interconnect.

4.1 Telephone Media Gateway Configuration Overview

This section describes the configuration needed to bring a Telephone Media Gateway (TMG) into service in an Enhanced Telephone Interconnect subsystem.

4.1.1 Configuring the Telephone Media Gateway

As with the installation of this feature, the configuration of the Telephone Media Gateway (TMG) has dependencies. Follow a specific sequence of events when configuring the TMG. This process defines this configuration process.

Process:

1. Discover and configure the TMG in the Unified Network Configurator Wizard (UNCW). See Discovering the Telephone Media Gateway Devices with the UNC on page 78.
2. If your system operates in Time Division Multiple Access (TDMA), set the TDMA interconnect mode. See Establishing the TDMA Interconnect Mode on page 105.
3. Assign a Key Management Facility (KMF) for centralized key management in the UNCW. See Telephone Media Gateway KMF Assignment on page 105.
4. Load keys onto the TMG with the Key Variable Loader. See Loading Encryption Keys on page 105.

4.1.2 Telephone Media Gateway Network Management Configuration

Perform network management of the Telephone Media Gateway (TMG) using the Unified Network Configurator (UNC), Unified Event Manager (UEM), and the Configuration/Service Software (CSS) application. Much of the device configuration is performed in the initial installation of the TMG and is covered in Chapter Enhanced Telephone Interconnect Installation on page 62.

4.1.2.1 Telephone Media Gateway Configuration in the UNC

Enabling Enhanced Telephone Interconnect in the ASTRO® 25 system includes the discovery and configuration of the KMF, if desired, and the Telephone Media Gateways (TMGs) using the Unified Network Configuration Wizard (UNCW) before the configuration is published to the Provisioning Manager. Also, see the *Unified Network Configurator User guide* .

4.1.2.1.1 Establishing the TDMA Interconnect Mode

When and where to use:
The ASTRO® 25 radio system supports and Phase 2 Time Division Multiple Access (TDMA). Set the Telephone Media Gateway (TMG) interconnect Mode in the Unified Network Configurator Wizard (UNCW). This procedure describes how to set the TDMA interconnect mode.

Procedure:

1. Launch the UNCW from the network management client by logging in with the administrative username and password.

   The UNCW appears.

2. From the list of available wizards on the left side, select the **Zone Configuration** link under **Zone Level Configuration**.

   The right side of the window is updated with the **Zone Configuration** form.

3. Select the **AEB Switch** and **ISS Configuration** tab.

   The **AEB Switch** and **ISS Configuration** fields appear.

4. In the **TDMA Interconnect Mode** field, click **Phase 2 TDMA** to set the TDMA mode.
5. Choose **Submit** to save the change in the UNCW.

   The TDMA interconnect mode is established.

6. Publish the infrastructure data to the Provisioning Manager.
7. Approve the remedy job generated after submitting changes from the UNCW.

4.1.2.1.2 Encryption Capability Configuration

This section covers procedures related to assigning a Key Management Facility (KMF) to a Telephone Media Gateway (TMG) key loading, and upgrading algorithms on the TMG.

NOTICE: Procedures from this section are only necessary if the TMG is used for encrypted calls.

4.1.2.1.3 Telephone Media Gateway KMF Assignment

When the Telephone Media Gateway (TMG) audio is encrypted, a Key Management Facility (KMF) is assigned to the TMG in the Unified Network Configurator Wizard (UNCW). Adhere to these rules:

- In the Zone Configuration Wizard, the **TMG OTEK Capable** parameter on the AEB Switch and **ISS Configuration** tab has to be set to **true**.
- All TMGs in one zone must have the same KMF ID.

For details, see the procedure “Assigning a KMF ID to a TMG” in the *Unified Network Configurator User guide*.

4.1.2.1.4 Loading Encryption Keys

The Telephone Media Gateway (TMG) supports Key Variable Loader (KVL) loading of keys and Over-the-Ethernet-Key Management (OTEK) using the Key Management Facility (KMF). Follow this procedure to load keys from the KVL to the TMG. See the *Key Management Facility User Guide* for centralized key management procedures.

NOTICE: This procedure is performed after the Software Download (SWDL) because if the Motorola Advanced Crypto Engines (MACE) is updated during SWDL, the keys are erased.

Procedure:

1. Connect the KVL to the Voice Processor Module (VPM) using the KVL cable. Ensure that the KVL is powered.
2. Verify that the green KVL LED on the VPM is illuminated.
3. Use the KVL to load the keys into the TMG. See the loading instructions in the guide specific to your KVL model:
   - *KVL 3000 Key Variable Loader User Guide*
   - *KVL 3000 Plus Users Guide*
   - *KVL 4000 Key Variable Loader User Guide*
4. Disconnect the KVL from the TMG.

4.1.2.1.5 TMG Algorithm Upgrade with the KVL

Follow the instructions in the Key Variable Loader (KVL) manual specific to your model to update the algorithms on the Telephone Media Gateway (TMG). See:

- *KVL 4000 Key Variable Loader User Guide*
- *KVL 3000 Plus Users Guide*
- *KVL 3000 Key Variable Loader User Guide*

CAUTION: When new algorithms are being loaded from the KVL to the TMG, all call processing is disrupted, including clear calls. Also, the TMG resets after the algorithm is programmed.

4.1.2.1.6 Radio User Interconnect Profile in the Provisioning Manager

Security group and other interconnect parameters are set for the subscriber radios using the Provisioning Manager after the keys are loaded on the Telephone Media Gateway (TMG). The zone controller uses the Exclusion Class ID field to screen restricted digits. See Interconnect Subsystem Configuration in the Provisioning Manager on page 108 and “Radio Interconnect Profile” in the *Provisioning Manager User guide* for more information.

4.2 PRNM Interconnect Subsystem Configuration

The Enhanced Telephone Interconnect subsystem relies on discovery and configuration in the Private Radio Network Management (PRNM) suite of products. The following software applications are used to manage the ASTRO® 25 radio system.

Subscriber radio information is beyond the scope of this document. See the documentation specific to the radios active in your system.

4.2.1 Enabling Telephone Interconnect on the ASTRO 25 System in the UNCW Process

This task provides the Unified Network Configurator Wizard (UNCW) configuration process for establishing Enhanced Telephone Interconnect (ETI) in the ASTRO® 25 system.

When and where to use:
Use this process to enable telephone interconnect in the UNCW for use in an ASTRO® 25 system.

NOTICE: See the *Unified Network Configurator User guide* for the procedures involved in "Enabling Telephone Interconnect on the ASTRO 25 System Using the UNCW Process."

Process:

1. If encryption is being used for interconnect calls, create the Key Management Facility (KMF) in the Unified Network Configurator Wizard (UNCW).
2. Discover the Telephone Media Gateways (TMGs) by selecting Master Site as the discovery type.
3. In the Zone Configuration Wizard, set the **Contains Interconnect Sub-System** to **Yes** in the **AEB Switch and ISS Configuration** tab.
4. Set the Interconnect Sub-System (ISS) parameters.

   NOTICE: See the *UNC Wizard Online Help* for parameter descriptions.

5. Publish the infrastructure data to the Provisioning Manager.
6. Approve the remedy job generated after submitting changes from the UNCW.

4.2.1.1 Configuring Interconnect Calls in the UNCW

While "Enabling Telephone Interconnect on the ASTRO 25 System Using the UNCW Process" describes the process for enabling the Enhanced Telephone Interconnect (ETI) feature, more interconnect and Telephone Media Gateway (TMG) hardware parameters can be set in the Unified Network Configurator Wizard (UNCW).

When and where to use: Use this procedure to configure the system level configuration parameters associated with telephone interconnect in the ASTRO® 25 system. See the *UNC Wizard Online Help* for descriptions of the configuration parameters.

Procedure:

1. If the TMG is encrypted, add a Key Management Facility (KMF) by selecting the **Key Management Facility** option under **System Level Configuration** in the navigation tree and assign the TMGs (up to 20 per zone) to a KMF.
2. Set the interconnect resource values by selecting **Level of Service** option under **System Level Configuration** in the navigation tree.
3. Verify TMGs in the system or delete a TMG by selecting the **TMG Configuration** option under **Zone Level Configuration** in the navigation tree.
4. Set the Interconnect Sub-System (ISS) configuration, interconnect timers, and key management settings for the TMGs by selecting the **AEB Switch and ISS Configuration** tab for the appropriate **Zone ID** under **Zone Level Configuration** in the navigation tree.

   NOTICE: A 0 in the TMG KMF ID field on this screen indicates the TMG is not key managed.

5. Configure any disallowed dialing patterns.
6. Publish the infrastructure data to the **Provisioning Manager**.
7. Approve the remedy job generated after submitting changes from the UNCW.

4.2.1.2 Configuring Disallowed Dialing Patterns

This procedure describes how to add dialing restrictions. Once the restrictions are added using this procedure, the values can be deleted by selecting the Delete radio button next to the numbers and submitting the change through this same wizard.

When and where to use:
Use this procedure to block any numbers that you do not want ASTRO® 25 subscribers to be able to dial.

Procedure:

1. Launch the Unified Network Configurator Wizard (UNCW) from the network management client by logging in with the administrative username and password.
2. From the list of available wizards on the left side, select the **Exclusion Class Configuration** link under **Zone Level Configuration**.

   The right side of the window is updated with the **Exclusion Class Configuration** form.
3. Select the appropriate **Zone ID** and **Exclusion Class ID** from the drop down lists to configure the patterns.

   NOTICE: Each zone has 15 Exclusion Class IDs.

   The wizard to Add the Disallowed Patterns appears.
4. Click **Add Row** to add the disallowed patterns.

   NOTICE: Each Exclusion Class can have up to 16 disallowed patterns.
5. Type the barred numbers (use numeric digits 0-9 and up to 15 characters in length) and press **Submit**.

   A `Configuration updates successful` confirmation message appears.
6. Publish the infrastructure data to the Provisioning Manager.
7. Approve the remedy job generated after submitting changes from the UNCW.

4.2.2 Interconnect Subsystem Configuration in the Provisioning Manager

The process for setting up the Enhanced Telephone Interconnect (ETI) subsystem in the Provisioning Manager involves creating the following objects:

- Interconnect Subsystem
- Radio Interconnect Profile (this includes both radio users and radio objects)
- Default radio access permissions
- Dispatch console or AIS (for the AMBE+2 noise suppression algorithm)
- Zone

NOTICE: Delete an Interconnect Subsystem record only if the Radio User and Radio User Interconnect Profile do not contain any references to this record. In cases where interconnect references exist, remove them first to delete the Interconnect Subsystem record.

Add these objects by creating a record for each in the Provisioning Manager. See Chapter 4 in the *Provisioning Manager User guide* or the online help.

Ensure that the Direct Inward Dialing (DID) configuration in the Unified Network Configurator (UNC) is synchronized from the Provisioning Manager. For details, see the “Publish Infrastructure Data Wizard” section in the *Unified Network Configurator User guide*.

4.3 Configuring the NEC UNIVERGE 3C System

This process provides the configuration process for the NEC UNIVERGE 3C system.

The NEC UNIVERGE 3C application is administered using the NEC 3C Administrator utility. Unless otherwise indicated, the default values of the various components of the NEC UNIVERGE 3C application can be used.

Process:

1. Launch **3C Administrator**. See step 1 in Creating Mapping Lists for Non-DID Calls on page 110 or Creating Mapping Lists for DID Calls on page 111.
2. Configure the Mapping List settings on the **General** tab. SeeCreating Mapping Lists for Non-DID Calls on page 110 or Creating Mapping Lists for DID Calls on page 111.
3. Configure dialing plan settings on the **Number Plan** tab. See Numbering Plans on page 112.
4. If American English is not the native language for users within your system, record a new Auto Attendant greeting. See Replacing the American English Greeting on page 115.
5. Configure the calling capabilities outside of the ASTRO® 25 system (also known as Telephony area). See Telephony Area Modification on page 115.
6. If your system Enhanced Telephone Interconnect (ETI) configuration includes an NEC BranchHub media gateway, set up the NEC BranchHub media gateway with Configuring the BranchHub Media Gateway on page 118.
7. If your system ETI configuration includes an NEC COHub media gateway, set up the NEC COHub media gateway with Configuring the COHub Media Gateway on page 119.
8. Create a zone controller SIP trunk for use with third-party media gateways with Zone Controller NEC SIP Trunk on page 121.
9. View the UNIVERGE 3C license file. See Reading the License File on page 125.
10. Install the Motorola-certified Windows OS updates with the *MOTOPATCH for Windows* media on the IP Private Branch eXchange (PBX) server.

    NOTICE: The MOTOPATCH requirement does not apply to the K core or Express Trunking configurations except if your organization purchased Security Update Service (SUS). MOTOPATCH media is available for deployment in your system. SUS for K core, but not Express Trunking configurations.
11. Save a copy of the UNIVERGE 3C system database by backing up the IP PBX server with Backing Up the UNIVERGE 3C System Database on page 138 and automate the backups with Scheduling Automatic Database Backup on page 139.

4.3.1 UNIVERGE 3C Administrator Settings

This section describes how to configure the settings on the following tabs in the 3C Administrator application:

- General
- Number Plan
- Trunks

4.3.1.1 General System Settings

The General System Settings in the 3C Administrator include:

- Creating map files that can be translated into actual subscriber IDs within the ASTRO® 25 system.
- Establishing a Direct Inward Dialing (DID) mapping list, optional
- Creating number plans for non-DID numbers (also called dialing plans).
- Auto attendant greeting and schedule
- Telephony area

4.3.1.1.1 Mapping List Creation

The Zone Controller (ZC) recognizes that the digits included in the Session Initiation Protocol (SIP) invite message represent an actual subscriber ID by examining the first three digits. If the first three digits are 210, the ZC recognizes the digit string represents an actual subscriber number. Because the largest subscriber ID for the ASTRO® 25 system is 16777212 (0xFFFFFC in hex), and accommodates every possible eight digit subscriber number, two map file entries are required. If the first three digits are 215, the ZC recognizes the digit string represents a Direct Inward Dialing (DID) call, and the digit string must be translated into an actual subscriber ID.

When setting up mapping lists, use `?` as the wildcard if a digit might be present and `X` as the wildcard when a digit is required.

Choose one of the procedures below to create a mapping list.

- Perform Creating Mapping Lists for Non-DID Calls on page 110 if you are not using Direct Inward Dialing (DID).
- Perform Creating Mapping Lists for DID Calls on page 111 if you are using Direct Inward Dialing (DID).

4.3.1.1.2 Creating Mapping Lists for Non-DID Calls

Perform this procedure if you are not using Direct Inward Dialing (DID).

Procedure:

1. From **Start**, select **All Programs** → **3C Administrator**.

   The 3C Administrator utility launches.

2. In the **3C Administrator** main window, under **System** - **Motorola Astro25** on the **General** tab, expand **Mapping Lists**.

   The tree displays **Mapping List** options in the hierarchy.

3 Select **Address Mapping**. Right-click **Add**.

  The **Mappings** window opens.

4 Enter a reference name for the new mapping file (for example, Motorola Mapping).

5 In the **Mappings** window, click **Add** and enter:

  a Under **Type**, select **Operator** from the pull-down menu.

  b Enter the number `0` followed by seven `?` for an 8-digit number.

  c Click **Define Rule** and enter the following information in the **Dial** fields on a line-by-line basis:

  d **Fixed** in the first pull-down list.

  e Enter the digits `210`.

  f In the second line, select **All** in the first pull-down list.

  g Click **OK** to save your changes.

6 Repeat step 5 for the digits `1` through `9` .

  A total of 10 entries are made.

7 Click **OK** to save your data.

8 Click **Media Servers** tab and click **Add** to add the entry in the list.

9 Click **OK**.

  The **Properties for Address Mapping Lists** window closes.

4.3.1.1.3
Creating Mapping Lists for DID Calls

Perform this procedure if you are using Direct Inward Dialing (DID).

Procedure:

1 From **Start**, select **All Programs** → **3C Administrator**.

  The **3C Administrator** utility launches.

2 In the **3C Administrator** main window, under **System - Motorola Astro25** on the **General** tab and expand **Mapping Lists**.

  The tree displays **Mapping List** options in the hierarchy.

3 Select **DID Mapping**, and right-click **Add**.

  The **Mappings** window opens.

4 Enter a reference name for the new mapping file (for example, Motorola DID Mapping).

5 Click **Add** in the **Mappings** window and enter the following by clicking in the fields:

  a Under **Type**, select **Tie Line** from the pull-down menu.

  b Enter the number `0` followed by enough `X` characters to represent the total number of digits forwarded by the Central Office (CO). For example, if CO forwards two digits, the entry is `0X`. But if the CO forwards four digits, the entry is `0XXX`.

  c Click **Define Rule** and enter the following information in the **Dial** fields on a line-by-line basis:

  d **Fixed** in the first pull-down list.

  e Enter the digits `215` followed by as many `0` characters as required to create a eight-digit number. For example, if two digits forwarded by the Central Office, then the **Fixed Digit** field must contain `215000`. If four digits are forwarded by the CO, then the **Fixed Digi**t field must contain `2150`.

f In the second line, select **All** in the first pull-down list.

g Click **OK** to save your changes.

6 Repeat step 5 for the digits `1` through `9`.

A total of 10 entries are made.

7 Click **OK** to save your data.

4.3.1.1.4
Numbering Plans

Numbering plans, or dialing plans, must be configured so that the UNIVERGE 3C application derives valid dialed numbers, extensions, and tie trunk numbering. Creating a Number Range for Mapped Non-DID Numbers on page 112 describes how to create the range for non-Direct Inward Dialing (DID) numbers.

The numbering plan assigns special functions, as required. For example, you can define:

- Extension 500 as the Auto Attendant extension.
- Extensions added as an outside service number when using Automatic Route Selection (ARS) for routing calls (that is, Define “9” as a primary “Outside Service’ number).

The numbering plan can assign number ranges for Mobile Subscriber IDs, as well as special features for a digit (that is, define 9 as an outside service.

The number ranges in the plan may include the following:

- Eight-digit mapped number ranges for non-DID and DID number ranges.
- A three-digit value for the extension created for the Auto Attendant feature.
- A three-digit value for the pseudo-outside service number as needed for ARS functionality.

The number range to create for DID numbers uses the values created under the Number Map field on the General tab. Creating a Number Range for Mapped DID Numbers on page 113 describes how to create the number range for DID subscribers.

NOTICE: All ranges must be added using a prefix of 215 for DID.

Creating the Auto Attendant Extension on page 113 provides information on creating the Auto Attendant extension that the server requires.

To make the Auto Attendant functional, configure the Auto Attendant Prompt Day Greeting and Auto Attendant Schedule using Setting the Auto Attendant Greeting and Schedule on page 114.

NEC ships the Non-DID Auto Attendant Greeting using a pre-recorded .wav file using American English language, which says, “Please enter a radio ID followed by the # or hash sign.” If installing the UNIVERGE 3C system in a country that does not use the English language, you can customize the greeting by using Replacing the American English Greeting on page 115.

4.3.1.1.5
Creating a Number Range for Mapped Non-DID Numbers

This procedure describes how to create the range for non-Direct Inward Dialing (DID) numbers.

Procedure:

1 In the **3C Administrator** main window, under **System - Motorola Astro25** navigate to the **Number Plan** tab.

2. Right-click **Add** → **Tie Number**.
3. Create a number range starting with `210` followed by eight `"?"`. This creates a number range from 21000000000 through 21099999999.
4. Specify the Session Initiation Protocol (SIP) trunk created for the Zone Controller.
5. Enter `Non-DID Number Range` as the **Number Plan** name.
6. Click **Apply**. Click **OK** to save the changes.

   The created tie line number range displays on the **Number Plan** tab.
7. Right-click the new number range and select **View Properties**.
8. Verify the **Allow transfers from the Auto Attendant** box is checked.
9. Click **OK** to close the window.

4.3.1.1.6

Creating a Number Range for Mapped DID Numbers

The number range to create for Direct Inward Dialing (DID) numbers uses the values created under the Number Map field on the 3C Administrator **General** tab. This procedure describes how to create the number range for DID subscribers.

NOTICE: All ranges must be added using a prefix of 215 for DID.

Procedure:

1. In the **3C Administrator** main window, under **System - Motorola Astro25** navigate to the **Number Plan** tab.
2. Right-click **Add** → **Tie Number**.
3. Create a number range starting with `215` followed by five `"?"`. This entry creates a number range from 21500000 through 21599999.
4. Specify the SIP trunk created for the zone controller.
5. Enter `DID Number Range` as the **Number Plan** name.
6. Click **Apply**. Click **OK** to save the changes.

   The created tie line number range displays on the **Number Plan** tab.
7. Right-click the new number range. Select **View Properties**.
8. Verify the **Allow transfers from the Auto Attendant** box is **not** selected.
9. Click **OK** to close the window.

4.3.1.1.7

Creating the Auto Attendant Extension

This procedure provides information on creating the Auto Attendant extension that the server requires.

Procedure:

1. In the **3C Administrator** main window, under **System - Motorola Astro25** navigate to the **Number Plan** tab.
2. Right-click **Add** → **Add Sphericall VM Address**.
3. Enter the following values:
   - **Number** = Enter a valid extension (500 recommended)

- **Name** = Auto Attendant
- **Type** = Auto Attendant

4 Click **Add** next to the **Ports** area of the dialog box.

5 Expand **Media Server** to show all available ports (48 total).

6 Click **port 1**, scroll to the bottom of the entries, then press SHIFT and click the last entry to highlight all entries.

All ports appear selected with the highlight.

7 Click **OK** to add all ports.

8 Click **Apply**. Click **OK** to save the changes.

4.3.1.1.8 Setting the Auto Attendant Greeting and Schedule

To make the Auto Attendant functional, the Auto Attendant Prompt Day Greeting and Auto Attendant Schedule must be configured using this procedure.

Procedure:

1 In the **3C Administrator** main window, under **System - Motorola Astro25**, expand **Media Servers (Sphericall) Auto Attendant Prompts** on the **General** tab.

2 Right-click **Day Greeting**. Choose **View Properties**.

The **Properties for Auto Attendant Prompt Day Greeting** dialog box appears.

3 Enter the following values:

- **Name** = Day Greeting
- **Timeout (T.O.)** = 20 seconds (recommended)
- Key definitions as follows:
- Key = T.O., Action = Hang Up, and Parameter = 0
- Keys 0 through 9 (listed 1 per line), Action = Blind Transfer, and Parameter = Any number
- Key = *, Action = Go To, and Parameter = 0000
- Key = #, Action = Blind Transfer, and Parameter = Any number

4 When complete, click **OK** to save the changes.

5 Expand **Media Servers (Sphericall) Auto Attendant Schedule** and verify that a **Default Media Servers (Sphericall) Auto Attendant Schedule** appears. If so, proceed to step 6. If not, right-click **Add** to create one.

6 Right-click **Default**. Choose **View Properties**.

7 Enter the following values to set the **Default** schedule:

- **Schedule Name** = Default
- Schedule Entries:
- **Weekday** = Monday
- **Start Time** = 8:00 AM
- **Prompt** = 0000 Day Greeting

8 Delete all other schedule entries (leaving only the default you created in step 7).

9 Click **OK** to save the default schedule.

4.3.1.1.9 Replacing the American English Greeting

The Non-Direct Inward Dialing (DID) Auto Attendant Greeting is a pre-recorded `.wav` file using American English language, which says “Please Enter a Radio ID followed by the # or hash sign.” by default. If installing the Sphericall system in a country that does not use the English language, customize the greeting by using this procedure.

Prerequisites: Obtain the following items before starting this procedure:

- Audio recording software and a microphone to create a `.wav` file.
- A person with a clear speaking voice to participate in the recording.

Procedure:

1. Record the Radio ID message in the local language in a `.wav` file.
2. Name the new file `p_radio_id.wav`.
3. Copy `p_radio_id.wav` to directory `c:/Program Files(x86)/Sphere/Media Server/AA` and the *Motorola Database Backup* DVD.
4. Rename the prior greeting `AAPrompt0000.wav` to `AAPrompt0000.wav.save`.
5. Replace the default Auto Attendant greeting `.wav` file (`c:/Program Files(x86)/Sphere/Media Server/AA/AAPrompt0000.wav.save`) with the custom Motorola greeting wav file (`p_radio_id.wav`) by renaming the new AA prompt file `AAPrompt0000.wav`.

The new greeting is active.

4.3.1.1.10 Automatic Route Selection Call Routing

The Automatic Route Selection (ARS) utility can be used to route calls out particular trunks based on the number dialed by the mobile subscriber. The ARS utility can be set up to block all calls to particular number, as required. Activating Automated Route Selection on page 117 describes how to enable ARS.

Outside Pseudo-Service numbers determine what defined trunk port on which a call is routed. The ARS utility uses number lists created to contain dialed digit strings, which are exemptions to the “All numbers” list. For example, this feature is useful for calls to a specific exchange that you want to route out on a particular trunk.

4.3.1.1.11 Telephony Area Modification

The UNIVERGE 3C system derives its calling capabilities to the outside from the Telephony area. This area is where the type of calling is specified (that is, 1 + 10-digit numbers). Several templates are provided that contain interoperable fields that automatically provide common and default settings.

A default Telephony Area is created when the 3C Administrator application is installed on the Unified Communications Manager server. This default telephony area has the fields populated with settings consistent with the North American numbering plan. Create a telephony area when a particular site installation requires many different field settings.

The following sections give an overview of the various Telephony Area tabs and fields that can be modified. Detailed topic-specific help can be obtained by clicking **Help** in each screen.

NOTICE: This document provides procedures to configure Localization Settings for North America. For other countries, consult NEC *Book 2: Install and Configure the UNIVERGE System - Appendix B: International System Information for Localization Settings outside of North America*.

The **General** tab provides the system administrator with several fields, such as defining the Country Code, Area Code, and softswitch number where the Sphericall application resides. Local Area Codes and dialing characteristics of specific Number Ranges can be modified.

The fields under the **Automatic Route Selection** tab determine how to best route an outside call (mobile to land) based on the number dialed. An example would be an instance where a system has two phone lines, one to a local service provider and one to a preferred long distance carrier. Local numbers are routed out the local service provider trunk while long distance calls are steered to the long distance provider trunk.

4.3.1.1.12

Adding Restricted Numbers to the Number Range Lists

A number range list is first created under the **Number Range List** screen under the Sphericall Administrator **General** tab (not under the **Telephony Area** tab). By clicking **Add**, the number range list can be specified, then a previously created Outside Service can be specified to route the call as described in this procedure. A Restricted Numbers Number Range List prevents radio subscribers from accessing telephony service that is not part of daily job requirement (1-900 calls, international calls, and so forth.). If not a restricted number, the calls use the All Numbers Number Range List, which allows all calls.

Procedure:

1. Right-click **Number Range Lists**. Click **Add**.
2. Enter `Restricted Numbers` in the **Name** field.
3. Click **Add** to enter each restricted number.
4. Click **OK** to save the changes.

4.3.1.1.13

Configuring Automatic Route Selection for Restricted and Non-Restricted Calls

You must configure Automatic Route Selection (ARS) for both restricted and non-restricted calls. If a called number is not on the restricted list, the call is processed.

This procedure describes how to configure ARS for both call types.

Procedure:

1. In the **3C Administrator** main window, under **System - Motorola Astro25**, select **Telephony** Areas.
2. Right-click **Default Area**. Choose **View Properties**.
3. Click the **Automatic Route Selection** tab.
4. Click **Add**. Select **Restricted Numbers** from the pull-down list on the right in the **Number Range Lists** column.
5. Select **809** from the pull-down list on the right in the **Primary Outside Service** column.
6. Select **none** from the pull-down list on the right in the **Secondary Outside Service** column.
7. Click **Add**. Select **All Numbers** from the pull-down list on the right in the **Number Range Lists** column.
8. Select **808** from the pull-down list on the right in the **Primary Outside Service** column.
9. Select **none** from the pull-down list on the right in the **Secondary Outside Service** column.

10 Click **OK** to save the changes.

4.3.1.1.14
Configuring Dialing Rule Overrides

The fields under the **Dialing Rule Overrides** tab determine how the Sphericall system manipulates the dialed numbers in a created Number Range list. For example, if a mobile subscriber dials a number that requires a leading 1 added, then a Dial Rule Override can be specified. Numbers within the All Numbers list are simply routed as is. This procedure describes how to configure the overrides.

The **Telephony Area Dialing Rules** tab specifies how dialing and Caller ID rules are specified. Do not change these fields unless necessary. More details are available by pressing **Help**.

NOTICE: Caller ID presented to the Public Switched Telephone Network (PSTN) does not represent the actual calling mobile ID.

Procedure:

1 In the **3C Administrator** main window, under **System - Motorola Astro25**, select **Telephony Areas**.

2 Right-click on **Default Area**. Choose **View Properties**.

3 Click the **Dialing Rule Overrides** tab.

4 Click **Add**. Set the **Number Range List and Dial Rule Override** values.

5 Click **OK** to save the changes.

4.3.1.1.15
Activating Automated Route Selection

This procedure describes how to enable the Automated Route Selection (ARS) feature to set dialing restrictions (for example, call barring) within the system.

Procedure:

1 In the **3C Administrator** main window, right-click **System - Motorola Astro25**. Choose **View Properties**.

2 Choose **Enable ARS** to activate the ARS feature.

3 Click **OK**.

The ARS settings configured in the **Telephony Area** tab are active.

4.3.1.1.16
Trunk Configuration

Configuration or modification of any Public Switched Telephone Network (PSTN) and Session Initiation Protocol (SIP) trunks associated with the Sphericall system is done under the **Trunks** tab.

Devices under the **Trunks** tab are automatically assigned as hubs when the device checks in or when a SIP endpoint registers with the UNIVERGE 3C application. PSTN trunks (BranchHub media gateway or COHub media gateway) appear when the particular media gateway checks in with the Sphericall application. SIP trunks are manually added.

Three types of SIP trunk are used in the system. The SIP trunk can be used to:

1 Connect the zone controller

2 Restrict dialed digits from the subscribers on the ASTRO® 25 system (also called a *soft trunk* or an *inactive trunk*).

3 Connect to an external SIP connection

Configuration of the zone controller SIP trunk is described in Zone Controller NEC SIP Trunk on page 121.

NOTICE: Consult Chapter 7 in the NEC *Book 4: Integrate UNIVERGE 3C Partner Technologies* manual for information on how to configure the SIP trunk from the Unified Communications Manager to the external IP Network SIP endpoint for the Enhanced Telephone Interconnect with telephony firewall configuration.

4.3.1.2

Media Gateway Configuration

When the NEC BranchHub or COHub media gateways are connected to the network and powered up, they attempt to initialize with the Media Gateway Controller (MGC), which is part of the Sphericall application. After the media gateway checks in with the MGC, it downloads configuration data from the Sphericall application.

NOTICE: This document provides procedures to configure the IP Private Branch eXchange (PBX) media gateways for most common installations. See Chapter 2 of *Install and Configure the UNIVERGE 3C System* manual for information on specific settings as required.
Set the IP addresses of the IP PBX media gateways before configuring the IP PBX media gateways.

4.3.1.2.1

Configuring the BranchHub Media Gateway

When and where to use:
When the BranchHub media gateway first powers up, it sends out a multicast message in an attempt to find a Media Gateway Controller (MGC). The MGC is part of the Sphericall application. After the BranchHub media gateway finds the MGC, it requests configuration information. Because the IP address is statically assigned, the media gateway does not use Dynamic Host Configuration Protocol (DHCP) to obtain one.

This procedure describes the final configuration process for the BranchHub media gateway using the 3C Administrator utility.

Procedure:

1. From **Start**, select **All Programs** → **3C Administrator**.

   The Sphericall Administration utility launches.

2. In the **3C Administrator** main window, click the **Trunks** tab.
3. Expand the **Hub**. Right-click the **Port** being configured. Choose **View Properties**.
4. On the **General** tab, configure the following for each port being placed into service:
   - Name
   - Hardware ID
   - Max Duration = 21600
   - Telephony Area = Default Area
   - Zone = Motorola Astro25 Development 1
   - Select the check boxes for:
   - Template = Analog
   - In Service
   - Maintenance Testing
   - Allow Emergency Calls from non-Emergency Group Stations

5 On the **Channels** tab, set the following:

- Channel number
- In Service = checked
- Signaling Mode = Loop Start
- Outward Calls Allowed = checked for mobile-to-land calls
- Call Offering = After 2 rings or Immediate
- Reliable Disconnect = checked
- Disconnect on CP Tone = unchecked
- Dial Tone Timeout = 3
- Dial without Dial Tone = checked
- Variant = US/Mexico Deaf...

NOTICE: If the channel you are configuring should allow outward calls (mobile-to-land calls), check **Outward Calls Allowed**.

6 On the **Default Routing** tab, enter the extension for the Auto Attendant from the Number Plan on the **General** tab.

NOTICE:
The Auto Attendant extension must already be created. Numbering Plans on page 112 describes how to create a numbering plan.

The **Address Type** field may display `Sphericall VM` instead of `Auto Attendant` for the Auto Attendant extension.

7 For ports being configured for outside dialing (mobile-to-land calls), on the **Outward Routing** tab, add any Numbers or Outside Dialing Rules. Click **Add Outside Service** and add the outside service number (808) from the Number Plan created on the General tab.

NOTICE:
The number 808 must be created and specified for Outside Service or the mobile-to-land calls fail. This number is used by Automatic Route Selection (ARS) to route all valid mobile-to-land calls. See Telephony Area Modification on page 115.

Any outside dialing rules added are specified in the **Outside Dialing Rules** field. For example, a leading 9 is prefixed in front of the dialed digit string with all digits in the digit string to be sent to the Public Switched Telephone Network (PSTN). So, if the mobile dialed 5552368, then the digit string 95552368 is sent to the PSTN.

8 Click **Apply**. Click **OK** to save the changes, then reset the BranchHub media gateway by left clicking then right-clicking the BranchHub icon and selecting **Restart**.

4.3.1.2.2
Configuring the COHub Media Gateway

When and where to use:
When the COHub media gateway first powers up, it sends out a multicast message in an attempt to find a Media Gateway Controller (MGC). The MGC is part of the Sphericall application. When the IP Private Branch eXchange (PBX) media gateway finds the MGC, it requests configuration information. Because the IP address is statically assigned, the media gateway does not use Dynamic Host Configuration Protocol (DHCP) to obtain one.

This procedure describes how to configure a general T1 CAS trunk. See the *NEC Install and Configure the UNIVERGE 3C System* and *NEC COHub Installation Manual* documentation for ISDN, which varies depending on the country of installation.

Procedure:

1. From **Start**, select **All Programs** → **3C Administrator**.

   The **3C Administration** utility launches.

2. In the **3C Administration** main window, click the **Trunks** tab.
3. Right-click any **Hub** in bold text. Click **Accept**.
4. Expand the **Hub**. Right-click the **Port** being configured. Choose **View Properties**.
5. On the **General** tab, configure the following for each port being placed into service:
   - Name
   - Hardware ID
   - Max Duration = 21600
   - Telephony Area = Default Area
   - Outbound Hunt Area = Descending
   - Zone = Motorola Astro25 Development 1
   - Select the check boxes for:
   - The initialization settings vary depending on the type of services being secured from the PSTN. You must consult with the service provider to formalize the actual settings used in the various pull-down lists on this dialog box.
   - In Service
   - Maintenance Testing
   - Allow Emergency Calls from non-Emergency Group Stations
6. On the **Channels** tab, set the following parameters:
   - Channel number
   - In Service = checked
   - Signaling Mode = Ground Start
   - Outward Calls Allowed = checked for mobile-to-land calls
   - Call Offering = After 2 rings or Immediate
   - Reliable Disconnect = checked
   - Disconnect on CP Tone = checked

   NOTICE: For individual channels providing DID operation, the **Signaling Mode** field should be set to **E and M** with the **Outward Calls Allowed** field not checked. **Call Offering** can be set to **Immediate** for the Auto Attendant to answer immediately. The Auto Attendant feature is not used for DID.

7. On the **Inward Routing** tab, provide information for any channels set for **E and M**. The **Inward Routing** boxes must be checked, while the **Inward Digits** must show the total number of digits passed by the serving switch, and you must add the Motorola DID Mapping table created earlier.

   NOTICE: You can test a digit string by putting a test number in the **Input DID** field and clicking **Test**.

8. On the **Default Routing** tab, add the extension for the Auto Attendant from the **Number Plan** on the **General** tab. Then all inbound (land to mobile) calls are sent to the Autonomous Access (AA) feature to collect DTMF digits representing the mobile subscriber being called.

   NOTICE: The Auto Attendant extension must already be created. See Creating the Auto Attendant Extension on page 113.

9. On the **Outward Routing** tab, add any Numbers or Outside Dialing Rules. Click **Add Outside Service** and add the outside service settings. If you want to add any Outside Dialing Rules, such as digits are to be added to the dialed digit string passed to the Telco service provider, add the rules in the **Outside Dialing Rules** area. You must specify the **Address Type** as **PSTN** in this rule or outside dialing does not work.

10. Click **Apply**. Click **OK** to save the changes. Reset the COHub media gateway by left then right-clicking the COHub icon and selecting **Restart**.

4.3.1.2.3 Zone Controller NEC SIP Trunk

In Enhanced Telephone Interconnect (ETI) subsystems that use a non-NEC IP Private Branch eXchange (PBX) media gateway, see the manufacturer media gateway documentation for installation and configuration information. When the Zone Controller (ZC) registers, the NEC UNIVERGE 3C system automatically creates a hub/trunk. Delete the generated trunk before adding in a new trunk with the agent defined. Follow Creating the Zone Controller SIP Trunk User Agent on page 121 and Creating and Configuring a ZC SIP Trunk on page 123 to create a ZC SIP trunk. Reading the License File on page 125 describes how to read the UNIVERGE 3C license file.

4.3.1.2.4 Creating the Zone Controller SIP Trunk User Agent

This procedure provides the initial setup of the Session Initiation Protocol (SIP) User Agent.

NOTICE: Third-party media gateways use a SIP trunk between the NEC UNIVERGE 3C IP PBX server and the third-party media gateway, and creating the trunk is similar to creating the ZC - NEC SIP trunk described here. Consult the NEC *Book 4: Integrate UNIVERGE 3C Partner Technologies*, Chapter 7 SIP Trunking for information on how to configure the SIP trunk from the Unified Communication Manager to the external IP Network SIP endpoint for the Enhanced Telephone Interconnect with telephony firewall configuration.

Procedure:

1. In the **3C Administration** main window, right-click the **System - Motorola Astro25** on the **General** tab. Choose **View Properties**.

   NOTICE: The SIP User Agent Profile must be created for SIP messaging to be enabled between the IP Private Branch eXchange (PBX) server and the Zone Controller (ZC).

   The **System Properties** dialog box appears.

2. Click the **SIP** tab.

   The existing SIP User Agent Profiles appear.

3. Click **Add**.

4. Create an entry for **ASTRO25 - ZC** with the following parameters:
   - Version = All
   - Endpoint = Trunk
   - Agent Description = ZC SIP Trunk

⚠ **CAUTION:** The entry name is case sensitive and a space must be present before and after the hyphen for the SIP trunk to process traffic.

The Default check mark does not show for the new profile because this is a custom SIP User Agent.

5. Click **OK**.
6. To access a pull-down menu, click the **ASTRO25 - ZC** entry and set the **User Agent** parameters to each of the following values by right-clicking in the value column.

   'From' header source = Original CLID

   'P-Asserted _dentity' header source = Original CLID

   'P-Asserted Identity' pass through = Unsupported

   talk Event (Notify Request) based 3PCC = Unsupported

   to-tag (SUBSCRIBE Request) In New Subscription = Disallowed

   Anonymous Calling = Unsupported

   Auto Switch to TCP = Supported

   CSTA Content Type = Unsupported

   CSTA Event Tag = Unsupported

   Call Recording Notification = Disabled

   Click-to-Dial = Ring Caller's Phone First

   Click-to-Conference = Unsupported

   Convert Firmware = Not applicable

   Desktop Audio Switching Supported = Unsupported

   Desktop Video = Unsupported

   Drop call on 400 Re-INVITE response = unsupported

   Drop call on 486 Re-INVITE response = unsupported

   Drop call on 488 Re-INVITE response = unsupported

   Enable Distinctive Ringing = Disabled

   Endpoint Created By = Call Manager

   Extended Presense States = Unsupported

   Extension to DID mapping = Diabled

   Find Terminal Method = Default

   Hardware Address = Unavailable

   INVITE Request URI Source = Outbound Contact-URI

   INVITE Without SDP = Unsupported

   MWI NOTIFY Request = Unsupported

   MWI SUBSCRIBE Request Unsupported

   Media Server Max Packetization (ms) = 20 ms

   OPTIONS Request = Unsupported

   Populate Caller from PAI = Unsupported

   REFER Based 3PCC = Unsupported

   REFER Based Transfer = Supported

Re-INVITE with Held SDP = Holds Call and Provides MoH

Receiving MoH = Supported

Reliable Provisional Response = Unsupported

Remote Reboot = Unsupported

Retry After Value Sent in SIP Response (sec) = 300sec

Send Forwarding Information = Disabled

Send Non-Primary Number = Disabled

Send Transferring Information = Disabled

Session Timer = Unsupported

Session Timer Refresher = Call Manager

Timer C = Unsupported

Video = Unsupported

xpidf + xml support for Presence = Unsupported

7 Click **OK** to set the values.

The **User Agent Profile ZC SIP Trunk** dialog box closes.

8 Click **Apply** to save the new **SIP User Agent** settings.

NOTICE: Steps 1 through 8 scan be skipped in the future once the **ASTRO25 - ZC** entry is saved in the database.

4.3.1.2.5

Creating and Configuring a ZC SIP Trunk

This procedure describes how to configure the Zone Controller (ZC) Session Initiation Protocol (SIP) trunk. The SIP trunk capacity is determined by the number of trunks purchased with the license file. The **Capacity** fields set in this procedure are:

- Total Capacity: total number of simultaneous calls the SIP trunk can support.
- Inbound Capacity: total number of inbound calls to accept.
- Outbound Capacity: total number of outbound calls to accept.

When setting these fields, consider:

- Guaranteed Outbound Calls = Total Capacity - Inbound Calls
- Guaranteed Inbound Calls = Total Capacity - Outbound Calls

Set the values as follows:

Total Capacity = `10`

Outbound = `7`

Inbound = `8`

results in the following result:

- A guarantee of three inbound calls with a maximum of eight
- A guarantee two outbound calls with a maximum of seven
- Five (three plus two) slots can be either inbound or outbound

NOTICE: Read the number of available licenses (see Reading the License File on page 125) and divide the total number of licenses by two. Devote one-half of the licenses to the ZC SIP trunk, and the other half for other outside trunk resources. Use this formula unless it is necessary to make the Total Capacity, Outbound Capacity, and Inbound Capacity values the same.

IMPORTANT: The ZC SIP trunk is automatically created when the ZC sends a SIP Register message to the Unified Communication Manager. If a SIP Register message is not sent, disconnect the Unified Communication Manager from the network by unplugging the Ethernet cable for a minute then re-connecting the cable. Then, the system should send a SIP Register message from the ZC to the Unified Communication Manager. If the SIP trunk is still not created, press F5 to refresh the screen.

Because Caller ID is not supported for ASTRO® 25 system, you are disabling this feature when configuring the ZC SIP trunk.

Procedure:

1 In the **3C Administrator** main window, choose the **Trunks** tab.

  The available trunks display in the window.

2 Expand the **ZC SIP** trunk object.

3 Right-click **Port 1**. Select **View Properties**.

4 On the **General** tab, verify the **In Service** box is checked and that the total capacity is consistent with the value in the license file. See Reading the License File on page 125.

5 Enter values for the **Inbound Capacity**, **Outbound Capacity**, and the **Total Capacity** fields based on the information provided before this procedure.

  CAUTION: If no values are entered in these fields, the UNIVERGE 3C system does not work.

  NOTICE: The maximum number of supported simultaneous calls is 120. However, your license file must support the intended capacity.

6 Highlight any information in the **Outbound Caller ID** field on the **General** tab, click **Remove**, then **Apply**.

  NOTICE: The Private Branch eXchange (PBX) phone number in the Telephony Area is used to populate any subsequent SIP messages. A default digit string is automatically created when the UNIVERGE 3C application is installed. This default digit string can also be changed to a local directory number, but it is not necessary for the system to operate.

  The system disables the Caller ID feature and saves the other settings on the **General** tab.

7 On the **Authorization** tab, perform the following actions:

  - Check the **Use Authorization** check box.
  - Enter the **Account** and **Password** for the PBX User account for SIP authentication. These credentials must match those set up in the zone controller.
  - In the **Realm** field, enter the domain name the **Unified Communications Manager** server is a part of.
  - From the **Type** pull-down menu, choose **MD5**.
  - From the **Authorization Type** pull-down menu, choose **To Respond/To Challenge**.

  NOTICE: See “Changing the IP PBX Server User Name and Changing the IP PBX Server User Password” in the *Zone Controller Feature guide*.

8 On the **Outward Routing** tab, enter the tie lines created earlier for the mapped number ranges.

9 Click **Apply**. Click **OK** to save the changes.

4.3.1.2.6 Reading the License File

This procedure describes how to read the UNIVERGE 3C license file.

CAUTION: DO NOT attempt to directly read the encrypted XML license file using an editor. Any changes made, intentional or not, corrupt the file and shut down the UNIVERGE 3C application even if the changes are removed.

Procedure:

1 In the **3C Administrator** main window, select the **Tools** menu.

2 Select **View License Summary**.

3 Verify the number of trunks is consistent with what was ordered from NEC.

4.3.1.2.7 Changing the Computer Name

When and where to use:
The computer name of the **Unified Communications Manager** must match the computer name of the user. Perform this procedure to change the computer name.

NOTICE: If UNIVERGE 3C software is not installed (for example, in the event of a disaster recovery), do not perform steps 1 and 14 through 18.

Procedure:

1 From **Start**, select **Services** → **Sphericall Services** → **Sphericall TFTP Services**, and set each service to manual startup.

2 Click the **Server Manager** icon in the lower-left corner of the system tool tray. Choose **Change System Properties**.

3 Click **Change** to rename the computer. The full computer name is ***`<name.domain name>`***. For example, a full computer name is `MySystemComputer.MyDomainName`.

The **Computer Name/Domain Changes** window appears.

4 Enter the prefix (for example, MySystemComputer) in the **Computer Description** field.

5 Select **Workgroup** and set the workgroup field.

6 Click **More** and enter the computer name suffix (for example, zone6).

7 Verify that **Change Primary DNS Suffix when Domain Membership Changes** is not selected. The suffix of the full computer name is required so that DNS works properly.

8 Click **OK**.

9 Enter in the AD Domain administrator user name and password.

10 Click **OK**.

A **You must restart your computer to apply these changes** screen appears.

11 Click **OK**.

12 Close the **System Properties** window.

A **You must restart your computer to apply these changes** screen appears.

13 Click **Restart Now**.

The new computer name is active on the next login.

14 Change the **DBServer Registry Key** after the Unified Communication Manager restarts using the following commands:

a Press the **Windows icon** key + **R** to open the **Run** dialog box. Type `regedit`.

b Select `HKEY_LOCAL_MACHINE Software`, `Wow6423`, `Sphere`, `DBServer, 1.0`.

c Select **Server Name** and enter the computer name without the .<zonezone number>.(for example, Z006IPPBX01.zone6 is Z006IPPBX01).

d Select **Software**, **Wow6423**, **Sphere**, **Admin**, then repeat substep 14.3.

The registry key for the server is changed to reflect the new computer name.

15 From **Start**, select **Services** → **Sphericall Services** → **Sphericall TFTP Services**, and set each service back to automatic startup.

16 Click **3C Administration**.

The **3C Administration** window opens to the **General** tab.

17 Click **Media Gateway Controllers** and delete the old instance of the computer name.

18 Click **Media Servers** and delete the old instance of the computer name.

4.3.1.2.8
Log On Banner Modification

For information on how to change the IP Private Branch eXchange (PBX) server default log on banner to one specifically suited for your organization, see the procedure “Changing Log On Banners Through a Domain Controller” in the *Windows Supplemental Configuration Setup guide*.

4.3.1.2.9
NEC System Password Modification

The following table provides guidance on where to locate information on changing passwords in the NEC UNIVERGE 3C system.

Table 10: Changing NEC System Passwords

Type of Password	Procedure
Domain account passwords	To change domain account passwords, see “Resetting User Passwords in Active Directory” in the *Authentication Services Feature guide*.
Local administrator account password	To change the local password on the IP Private Branch eXchange (PBX) server: 1 Log on to the IP PBX server as the local administrator. 2 Press CTRL + ALT + DELETE and select **Change Password**. 3 Enter and verify the new password, then click **OK**.
IP PBX media gateway password	See Configuring the IP PBX Media Gateway Addresses and Password on page 95.
PBX user password (used for Session Ini-	To change the PBX user password:

Type of Password	Procedure
tiation Protocol (SIP) link authentication)	1 In the 3C Administrator main window, right-click the **System - Motorola Astro25** on the **General** tab and choose **View Properties**. **NOTICE:** The SIP User Agent Profile must be created for SIP messaging to be enabled between the IP PBX server and the Zone Controller (ZC). 2 Expand the **SIP** trunk object. 3 Right-click **Port 1**. Select **View Properties**. 4 On the **Authorization** tab, enter the **Account** and Password. These credentials must match to what is set up in the zone controller. See Chapter 6 of the *Zone Controller Feature guide* for details on changing the IP PBX server user name and password. 5 Click **Apply**. Click **OK** to save the changes.

4.3.1.3

Voice Announcement Configuration

If a land-to-mobile call attempt fails during the initial call set up stage, the NEC UNIVERGE 3C application offers the option to play a voice announcement. The announcement played depends on the specific error condition detected by the system.

The announcements consist of *.wav files that correlate with the specific 4XX SIP error messages sent to the UNIVERGE 3C application by the zone controller based on the error detected. In addition to the announcements included with the UNIVERGE 3C application, you can create custom announcement audio files using commercial recording software. This allows for announcements in different languages not included with the UNIVERGE 3C application.

4.3.1.3.1

SIP Error Response Codes (4XX and 5XX codes)

For a non- Direct Inward Dial (DID) land-to-mobile call, the landline user overdials a subscriber ID through Dual Tone Multi-Frequency (DTMF) after being prompted to do so by the Auto Attendant feature. For DID calls, the serving switch sends the pre-determined number of digits to the UNIVERGE 3C application without Auto Attendant intervention. This results in a SIP Invite sent to the zone controller from the UNIVERGE 3C application. If the ZC determines a condition exists and the call cannot be completed it sends an error response code back to the UNIVERGE 3C application, which triggers the particular voice announcement informing the land line user the call cannot be completed.

The following SIP error codes determine the reason for the call failure.

400

Bad Request. The SIP Invite sent to the zone controller has a syntax error, usually because the Mapping List has bad information such as a leading 210 (non-DID) or 215 (DID) in front of the digit string is not present in the SIP Header Field.

403

Forbidden. The target subscriber is either not authorized for interconnect or is presently at a SmartX (3600) site.

404

Not Found. The target subscriber is not in either the non-DID or DID database.

480
Temporarily Not Available. The target subscriber is not registered on the system, does not answer within the ring time, or denies an answer request.

486
Busy Here. The target subscriber is currently involved in another interconnect call or Telephone Media Gateway (TMG) resources are temporarily unavailable.

488
Not Acceptable Here. The SIP Invite sent to the zone controller does not have Session Description Protocol (SDP) in the message body or an unsupported codec type has been specified.

503
Service Unavailable. A serious error condition has occurred and the zone controller has determined that interconnect service in general is unavailable. This error may be due to multiple conditions.

4.3.1.3.2 Enabling the Enhanced Telephone Interconnect Voice Announcement Feature

The following process provides details on enabling the voice announcements in the event of a call setup failure in an ASTRO® 25 system.

When and where to use: Use this process to enable Music On Hold and voice announcements after the IP PBX server with UNIVERGE 3C v8.5 software is installed in an ASTRO® 25 system.

Process:

1. Enable Music On Hold (MOH). See Enabling Music On Hold on page 128.
2. Enable voice announcements. See Enabling Voice Announcements on page 129.
3. Add any customized voice announcements to the system.
4. Verify that the audio recordings play by making land-to-mobile test calls under a failure condition.

4.3.1.3.2.1 Enabling Music On Hold

Music On Hold (MOH) enables recorded music to fill the silence heard by telephone callers who are waiting to continue a call.

When and where to use: Use this procedure to enable Music On Hold (MOH). This feature must be enabled before enabling the voice announcements on your ASTRO® 25 system.

Procedure:

1. Launch **3C Administrator**.
2. Click **General** and expand the **Explorer** tree.
3. Click **Music On Hold**.
4. Right-click **Media Server MOH** to select **Properties**.

   The **Properties** window opens.
5. Click **Servers** and verify that the media server is specified. If not, click **Add** and select the media server specified under the **Media Server Explorer** tree element.
6. Click **Zones** and verify the zone name matches the name under the **Zones Explorer** tree element at the bottom of the tree.
7. Select **MOH Enabled**.

8. Click **OK** to save and close the **MOH Properties** window.

The music plays when a call is placed on hold with the Enhanced Telephone Interconnect feature in an ASTRO® 25 system. You can now enable voice announcements.

4.3.1.3.2.2 Enabling Voice Announcements

Voice announcement are pre-recorded messages saved as `*.wav` files set to play for callers under certain conditions.

When and where to use: Use this procedure to activate voice announcements on your ASTRO® 25 system.

Procedure:

1. Launch **3C Administrator**.
2. Click **General** and expand the **Explorer** tree.
3. Right-click **System** to select **Properties**.

   The **System Properties** window opens.
4. Click **Call Behavior**.
5. In the **Failed Call Announcement Behavior** group box, select **Enable Failed Call Announcement**.

   The **Failed Call Announcement Behavior** window opens.
6. Verify that the fields are populated with the 4XX and 5XX messages, the message types are set to SIP and a correlating `*.wav` file appears.
7. If necessary, modify the fields. Click **OK**.
8. In Windows, navigate to the following directory: `C:\Program Files(x86)\Sphere\Media Server\Sysvox\en`

   NOTICE: The country specified in the Telephony area determines which Sysvox directory subfolder that UNIVERGE 3C uses. For example, selecting the France template initiates the …`\Sysvox\fr` subdirectory for the files specified in the Failed Call Announcement Behavior window.
9. Verify the same `*.wav` file name appears in this folder and that the name matches what appears in the **3C Administrator** application. File names are case-sensitive.

The voice announcements are available for use with the Enhanced Telephone Interconnect feature in an ASTRO® 25 system.

4.3.1.3.2.3 Customizing Voice Announcements

You can create custom voice announcements instead of using the default files supplied with the UNIVERGE 3C application with any commercially available recording application that creates `*.wav` files. The new recording file must match the file name specified in the Failed Call Announcement Behavior window and duplicate files with the exact same name cannot be present.

Prerequisites: Obtain the following items:

- Any audio recording software capable of saving a `.wav` file
- Voice talent
- Recording script

When and where to use: Use this procedure to add a customized voice announcement to your ASTRO® 25 system.

Procedure:

1. Create the audio recording script seek approval by your legal department and management.
2. Using audio recording software, record the new announcement.
3. Save the file with a `.wav` extension.
4. In **3C Administrator**, click **General** and expand the **Explorer** tree.
5. Right-click **System** to select **Properties**.

   The **System Properties** window opens.
6. Click **Call Behavior**.
7. In the **Failed Call Announcement Behavior** group box, select **Enable Failed Call Announcement**.

   The **Failed Call Announcement Behavior** window opens.
8. Verify that the fields are populated with the 4XX and 5XX messages, the message types are set to SIP and a correlating `*.wav` file appears.
9. Modify the fields where you want to add the new `.wav` file and click **OK**.
10. In Windows, navigate to the following directory: `C:\Program Files(x86)\Sphere\Media Server\Sysvox\en`

    NOTICE: The country specified in the Telephony area determines which Sysvox directory subfolder that UNIVERGE 3C uses. For example, selecting the France template initiates the …`\Sysvox\fr` subdirectory for the files specified in the Failed Call Announcement Behavior window.
11. Copy the same `*.wav` file in this folder and ensure that the name matches what appears in the **3C Administrator** application. File names are case-sensitive.

The customized recordings are available for use with the Enhanced Telephone Interconnect feature in an ASTRO® 25 system.

4.3.1.4 MOTOPATCH Updates on the IP PBX Server

The *MOTOPATCH for Windows (OS)* CD contains a Motorola-certified release of OS updates for Windows devices within the ASTRO® 25 radio system. The software media contains a `readme.txt` file with installation instructions to follow.

NOTICE: The MOTOPATCH requirement does not apply to the K core or Express Trunking configurations except if your organization purchased Security Update Service (SUS). Then MOTOPATCH media is available for deployment in your system. SUS is available for K core, but not Express Trunking configurations.

Chapter 5

Enhanced Telephone Interconnect Optimization

This chapter contains optimization procedures and recommended settings relating to Enhanced Telephone Interconnect.

5.1 Optimizing Access to Interconnect Services

Radios must be properly programmed to make and receive enhanced telephone interconnect calls.

Telephone interconnect services are intensive users of system time. Each call requires a single channel to be dedicated for the duration of the call, and enhanced telephone calls typically last longer than talkgroup calls. Because of this intense use, and because of direct toll costs, you need the ability to limit the use of this feature.

5.1.1 Interconnect through Radio and User Configuration Optimization

Radios can be configured through the Customer Programming Software (CPS) so that they can receive enhanced telephone interconnect calls, but not initiate them. Radios can also be programmed with specific call lists (telephone numbers) and configured to prevent users from calling non-programmed phone numbers. Individual radio users may be configured with maximum monthly call times through the Radio User object in the Provisioning Manager.

5.1.2 Individual Interconnect Profiles

Each radio user is assigned an Interconnect Profile ID (a Provisioning Manager object). These profiles are created in the Provisioning Manager and assigned to radio users. Your system may have various different individual interconnect profiles available for assignment to radio users. Among other settings, the individual interconnect profiles specify a Priority Level.

Telephone interconnect calls can be assigned as priority level 2 through level 10, depending on individual requirements. The priority level for interconnect calls is separate from the priority level assigned to dispatch calls (a user could have different priorities for interconnect and dispatch). Level 2 is the highest assignable priority while level 10 is the default priority setting. The system uses priority levels to determine the assignment of system resources during busy periods. Ten levels of priority (1 through 10) are available. The highest priority, level 1, is reserved for emergency calls.

5.1.3 Interconnect through Infrastructure Configuration Optimization

In addition to individual radio programming, the infrastructure can be configured to limit telephone interconnect services.

Sites or channels can be configured to limit interconnect calls through the Shared Services feature.

5.1.4 Interconnect Control through the Shared Service Algorithm

The Shared Service feature is a sophisticated method of balancing telephone interconnect capability with dispatch traffic. There are two types of shared service are available.

Table-driven Shared Service

A standard feature that enables the system manager to specify the maximum number and duration of interconnect calls, which are allowed at any given time for each site using the Level of Service (LOS) object in the Unified Network Configurator Wizard (UNCW). A number of LOSs can be configured with different settings for maximum numbers and maximum duration of calls. These levels of service can then be assigned individually for two-hour time blocks throughout the day in the Shared Service object of the UNC Wizard. Each site is configured with its own table.

Dynamic Shared Service (DSS)

An optional feature that expands the table-driven shared service functionality. DSS provides an automatic adjustment to the configured table-driven shared service tables according to the current system loading. DSS allows you to create more flexible telephone interconnect usage patterns, which can be saved as different LOSs. These dynamic levels of service can then be assigned individually for two-hour time blocks throughout the day in the Shared Service object of the UNCW. Each site is configured with its own table.

5.1.5 Limit Interconnect Time at the Zone Level

Interconnect can also be limited by the Maximum Interconnect Call Duration setting for the zone object.

5.2 Dynamic Shared Service Algorithm

Dynamic Shared Service (DSS) is an optional feature that expands the table-driven shared service functionality. Dynamic shared service provides an automatic adjustment to the configured table-driven shared service tables according to current system loading. DSS allows you to create more flexible telephone interconnect usage patterns, which can be saved as different Levels of Service (LOS). These dynamic levels of service can then be assigned individually for two-hour time blocks throughout the day in the Shared Service object of the UNC Wizard. Each site is configured with its own table.

Chapter 6

Enhanced Telephone Interconnect Operation

This chapter details tasks to perform after the Enhanced Telephone Interconnect is installed and operational on your system.

6.1 Telephone Media Gateway Operation

This section provides common procedures for an installed and fully configured Telephone Media Gateway.

6.1.1 Turning on the Telephone Media Gateway

The Telephone Media Gateway (TMG) does not have an on/off switch. The device is activated by supplying power. Perform this procedure to power up the TMG and verify that it is working.

See Telephone Media Gateway LEDs on page 159 for descriptions of the LEDs on the TMG.

Procedure:

1. Connect the power supply 12V output line cord to the rear panel connector on the TMG.
2. Connect the opposite end of the power line cord to the AC power source.
3. Verify that the power LED is on.

6.1.2 Turning off the Telephone Media Gateway

Perform this procedure to turn off the Telephone Media Gateway (TMG).

Procedure:

1. Disconnect the power line cord from the AC source.
2. Disconnect the power supply 12V output cable TMG chassis.

6.1.3 Rebooting the Telephone Media Gateway by Power Cycling the Hardware

This procedure reboots the Telephone Media Gateway (TMG) hardware by power-cycling.

Procedure:

1. Trace the power line cord from the round power port on the left side of the device to the power source.
2. Disconnect the cable from the AC power source.

   The TMG is off.

3 Verify the Power LED on back of the device is not lit.

4 Reconnect the power line cord to the AC source and verify the power LED is on.

The Power LED is green when reboot is complete.

6.1.4 Rebooting the Telephone Media Gateway in the CSS

An alternative method to powering down the hardware, is to reset the Telephone Media Gateway (TMG) using the Configuration/Service Software (CSS) as described in this procedure.

Procedure:

1 Launch the Configuration/Service Software (CSS) application using a serial connection (as described in Chapter Enhanced Telephone Interconnect Installation on page 62).

NOTICE: If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the **Username**, **Password**, and **Elevated Privileges Password** fields, as they cannot be left blank.

2 Select **Tools** → **Set IP Address and Box Number**.

The **Set IP Address and Box Number** dialog box appears populated with the IP address for the TMG.

3 Click **Reset**.

4 Click **OK** in the confirmation box to proceed with the reset.

The TMG restarts.

5 Proceed to Changing SNMPv3 Configuration and User Credentials on the Telephone Media Gateway on page 73 to reconfigure the SNMPv3 credentials.

6.1.5 Rebooting the Telephone Media Gateway in the UEM

The Unified Event Manager (UEM) also provides an option for resetting the Telephone Media Gateway (TMG).

Procedure:

1 Launch the **Unified Event Manager**.

2 From the **Network Database** link, right-click the **Telephone Media Gateway** device.

3 Choose **Command**.

4 Select the entity associated with the device.

5 Choose **Reset**. Click **Apply**.

The cursor changes into an hour glass when the process is initiated and it changes to normal when the process is completed.

6.1.6 Telephone Media Gateway Logon

The Telephone Media Gateway has a default service account, and your system administrator has those credentials. Change the default credentials when the device is installed. Set the appropriate IP address, login, and password the first time you connect to the device, which is described in Chapter Enhanced Telephone Interconnect Installation on page 62.

6.1.7 Telephone Media Gateway Accounts Administration

You can set up a local password for the Telephone Media Gateway (TMG) using Configuration/Service Software (CSS) as described in Setting the Telephone Media Gateway Local Password Configuration on page 70.

Obtain the required user credentials information (security level, authentication passphrase, and encryption passphrase) to configure the site devices before proceeding with changing or resetting a password.

The user credentials information includes both the current and new credentials. Without the current credentials, you are not able to access the device and cannot change the user credentials. Changing to the incorrect user credentials may lead to not being able to access the TMG from the Network Managers for the site devices or for the site devices to send alarms for fault management.

Table 11: Telephone Media Gateway Accounts on page 135 provides the user accounts and the network management application that can be used to set or change them.

NOTICE: Contact your system administrator for a list of all user accounts and passwords for your system.

Table 11: Telephone Media Gateway Accounts

Type of Account	Description and Network Management Application Used
Local service account*	This account is used for setting IP addresses and to configure the TMG device locally if it cannot connect to the rest of the system (for example, site link failure). Two privilege levels are available. The higher privilege allows for setting IPs and resetting the TMG. Credentials can be set or changed through Configuration/Service Software (CSS) (serial connection).
Master admin account	Required for the configuration, fault management, and other SNMPv3 communications with the Unified Network Configurator (UNC), Unified Event Manager (UEM), and CSS (Ethernet connection). Security is enabled by default.
Inform A account	Required for SNMPv3 inform event messages to UNC and UEM from devices (Ethernet connection).
Inform B account	Required for SNMPv3 inform event messages to UNC and UEM from devices (Ethernet connection).
CSS account	Used by CSS.
SNMPv3 user admin account	Used to administer the SNMPv3 Users (UEM). No other User Account is allowed to change the User Credentials.
* This account is not stored in the UNC, so changes are not backed up in the system.	

6.1.8 Telephone Media Gateway Back Up

When you install and configure a Telephone Media Gateway using the Configuration/Service Software application, save the settings to an archive file. This file can be retrieved to restore a previous configuration. See the *CSS Online Help* for more information.

6.1.9

Telephone Media Gateway Status

The operational status of the Enhanced Telephone Interconnect subsystem can be viewed using the network manager (Unified Network Configurator) and the fault manager (Unified Event Manager).

6.1.9.1

ETI Status in the UEM

The following Enhanced Telephone Interconnect (ETI) subsystem information is reported by the Unified Event Manager (UEM):

- Telephone Media Gateway: a Device Managed Resource (DMR) that includes the Telephone Media Gateway (TMG) Zone Controller (ZC) Link and TMG status.
- Motorola Interconnect System: a Logical Managed Resource (LMR) and includes the ZC TMG Link and ZC IP Private Branch eXchange (PBX) Link status.

6.1.9.2

Viewing Status in the UNC

The EMC Smarts™ Network Configuration Manager application contains auditing functionality. Standards and tests are created to ensure that the device configurations meet the ASTRO® 25 radio system operational rules. As part of the Unified Network Configurator Wizard (UNCW) functionality, the tests are run to determine any devices that are not compliant. In such cases, remedy jobs are automatically created to resolve the issues. You must schedule these remedy jobs manually.

This procedure describes how to verify if the Telephone Media Gateway (TMG) is compliant.

The UNC Operation chapter of the*Unified Network Configurator User guide* also describes how to generate an audit report and make devices compliant.

Procedure:

1 Log in to the EMC Smarts™ Network Configuration Manager application.

   NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

   The **EMC Smarts Network Configuration Manager** main window appears.

2 In the navigation pane of the main UNC window, expand **Networks** and select the **Astro 25 Radio Network**.

3 Double-click **Devices**.

   The diagram of devices appears in the right pane.

4 Change to a table view by clicking the **Table** icon in the right pane upper menu.

   The list of devices is populated in a table.

5 Click the **status** column to sort devices by their status.

6 Scroll down to see TMG compliance status.

6.1.10

Telephone Media Gateway Removal

When a Telephone Media Gateway (TMG) is removed from an ASTRO® 25 system, remove any Key Management Facility (KMF) association first. Also, use the Unified Network Configurator Wizard (UNCW), not EMC Smarts™ Network Configuration Manager/VoyenceControl, in the Unified Network

Configurator network management application to delete a TMG. See the *Unified Network Configurator User guide* for more information.

6.2 NEC UNIVERGE 3C System Use

This section explores the basic operation of the NEC UNIVERGE 3C hardware.

6.2.1 Launching the NEC UNIVERGE 3C System

When and where to use:
This procedure describes the initialization of the NEC UNIVERGE 3C system.

Procedure:

1. Power on the computer that has the NEC UNIVERGE 3C application installed.

   The NEC UNIVERGE 3C application automatically launches and the supporting services are started.

2. Double-click the **Primary Service** icon on the desktop to verify the Sphericall supporting services are running.
3. When used, power on the IP Private Branch eXchange (PBX) media gateways and verify the LEDs are operational.

   System discovery begins as the media gateways search for the Media Gateway Controller (MGC), which is part of the UNIVERGE 3C application.

4. When the MGC is found, the media gateways automatically begin downloading configuration information.

   The media gateways then sit in an idle state waiting for instructions from the MGC.

5. Verify that the IP PBX media gateways are in the idle state on the screen.

   The device scrolls the name of the IP PBX media gateway and the number of available ports when idle.

6.2.2 NEC UNIVERGE 3C Hardware Operation

See the NEC documentation for details on the operation of the equipment, including display messages, LEDs, and so forth.

6.2.3 UNIVERGE 3C System Database Back Up

After the system is configured, perform a database backup of the configured IP Private Branch eXchange (PBX) server to save the UNIVERGE 3C configuration to DVD. Create a backup at the following intervals:

- Monthly - create a full backup of the UNIVERGE 3C database to DVD. Label and store in a secure area.
- After modifying the database - create a backup of the UNIVERGE 3C database after any significant changes are made.

6.2.3.1 Backing Up the UNIVERGE 3C System Database

This procedure describes the backup routine. This operation requires a formatted DVD-R on which to save the backup copy. If you need to format the media, see Formatting a DVD-R on Windows Server 2008 R2 on page 138.

Procedure:

1. Log on to the **Unified Communication Manager** using the administrator account.
2. Stop the dbserver process in the Sphericall processes window on the Unified Communications Manager.
3. Right-click **System Properties** to select **View Properties**.
4. On the **Database** tab, choose **Enable Database Replication**. Click **OK**.

   Force replication copies the database from the primary UCM to all secondary UCMs.
5. On the main menu, select **Tools** → **Force Replication**

   This action creates a database backup file (`PBX.mdb.backup`).
6. Insert the DVD-R media into the computers **DVD** read/write drive.

   The system recognizes the **E:** drive.
7. Copy the `C:\Program Files (x86)\Sphere\Backup` directory to the DVD by clicking the directory and dragging it to the DVD drive.

   NOTICE: This directory contains a copy of the active database, which cannot be copied directly if the application is executing.
8. Copy the `p_radio_id.wav` file to the DVD by clicking on the file and dragging it to the DVD drive.

   The configuration is saved to DVD.

6.2.3.2 Formatting a DVD-R on Windows Server 2008 R2

This procedure describes how to format the DVD-R media that you can use to back up the UNIVERGE 3C system database.

Procedure:

1. Insert the blank media into DVD drive on the IP Private Branch eXchange (PBX) server.
2. From **Start**, right-click **Computer** and select **Manage**.

   NOTICE: You may be required to enter the domain account login and password.
3. In the left pane, expand **Storage**.
4. Select **Disk Management**.
5. In the center pane, right-click **E:** drive and select **Format**.
6. Type the system name in the **Volume** label field and uncheck the **Perform quick format** check box.
7. Click **OK**.

   A warning message appears.

8 Click **OK**.

   The system formats the disk.

9 Verify that the LED on the DVD drive is not lit, then close the **Service Manager** window.

10 From **Start**, right-click **Computer** and select **Open**.

11 Verify that the E: drive shows a disk with the system name you provided.

   The disk is ready for a system backup.

6.2.3.3 Scheduling Automatic Database Backup

You can also set up automatic database backups to run at specific time intervals. This backup is required if any updates are made to the configuration of the Unified Communications Manager. Use this procedure to schedule the automatic database backup.

Procedure:

1 Click **3C Administrator**.

2 Right-click **System**.

   The **System Properties** window opens.

3 Select the **Perform daily maintenance at** check box.

4 Set the time using the pull-down menu.

   The database backup is scheduled to create the `PBX.mdb.backup` file at the selected time. Only one copy of the file is created and the existing database backup file is overwritten. Also, the file must be manually copied to secure media (for example, DVD, network resource server).

5 Optionally, copy the default Auto Attendant greeting `.wav` file at `c:/Program Files(x86)/Sphere/Media Server/AA/p_radio_id.wav` to the secure media.

6.2.3.4 Restoring the UNIVERGE 3C 7.1 System Database

Use this procedure to restore a UNIVERGE 3C 7.1 system database configuration from a backed-up DVD. This procedure is for systems running the UNIVERGE 3C 7.1 software only. If you have the current 8.5.2.3 software on the IP PBX server, see Restoring the UNIVERGE 3C 8.5.2.3 System Database on page 140.

⚠ **CAUTION:** Because the UNIVERGE 3C service must be stopped to restore the database, perform this procedure when the system is least used.

Procedure:

1 Place the DVD with the backed up `pbx.mdb.backup` file in the DVD read/write drive.

2 Stop the dbserver process in the **Sphericall processes** window on the Unified Communications Manager.

3 Right-click the `E:\pbx.mdb.backup` file and select **Copy**.

   The backup data is copied to the clipboard.

4 Navigate to `C:\Program Files (x86)\Sphere\data` folder.

5 Paste the file in the `C:\Program Files (x86)\Sphere\data` folder and rename the file `pbx.mdb`.

6. From **Start**, select **Administrative Tools** → **Services**.
7. Right-click **Sphericall** and **Sphericall TFTP**. Select **Stop** to stop the services.
8. After the **Sphericall** services stop, right-click the `pbx.mdb` file in the `C:\Program Files (x86)\Sphere\data folder` and rename it as `pbx.mdb.bak`.
9. Right-click the `pbx.mdb.backup` file and rename it as `pbx.mdb`.
10. Right-click the services **Sphericall** and **Sphericall TFTP**. Select **Start** to start the services.
11. After the service successfully re-starts, open the **Sphericall Console** window and verify the services have started.

    Sphericall Service appears in the **Service (Local)** list of applications.
12. Close the **Services** window.

6.2.3.5
Restoring the UNIVERGE 3C 8.5.2.3 System Database

Use this procedure to restore a configuration from a backed-up DVD. This procedure is for systems running the UNIVERGE 3C 8.5.2.3 software.

Prerequisites: Ensure that you have the following items:

- A DVD with a recent backup of the system database (`pbx.mdb.backup`)
- An operational Primary UCM and a secondary UCM rebuilt and in a functioning network

When and where to use:

⚠ **CAUTION:** Because the UNIVERGE 3C service must be stopped to restore the database, perform this procedure when the system is least used.

The following procedure assists you in recovering essential files from a disaster recovery storage server location to a new build of the 3C system. Once the system database is restored, restore both the cfg or the calls database.

Procedure:

1. Navigate to `C:\Program Files (x86)\Sphere\data` folder.
2. Paste the backed-up file in the `C:\Program Files (x86)\Sphere\data` folder and rename the file `pbx.mdb`.
3. From **Start**, select **Administrative Tools** → **Services**.
4. Right-click **Sphericall** and **Sphericall TFTP**. Select **Stop** to stop the services.
5. After the **Sphericall** services stop, copy the entire `Sphere\backup` folder from the backup storage device to the live 3C system `Sphere\backup` folder.
6. Open a command window.
7. Enter: `cd Sphere\data`
8. Enter: `restorecfgdb`
9. Enter: `restorecallsdb`***<day>***
10. Start the Windows Sphericall services.
11. Ensure that you are on the Primary UCM, then follow the procedure to force the database replication to Secondary UCMs. See Backing Up the UNIVERGE 3C System Database on page 138.

Chapter 7

Enhanced Telephone Interconnect Maintenance

This chapter describes periodic maintenance procedures relating to the Enhanced Telephone Interconnect feature.

7.1 Enhanced Telephone Interconnect Hardware Maintenance

Aside from the Telephone Media Gateway (TMG) routine battery replacement (Replacing the TMG Battery on page 141), no serviceable parts in the Enhanced Telephone Interconnect subsystem require maintenance or calibration. Exterior cleaning of the TMG, NEC Sphericall system components, and telephony firewall using a clean, lint-free cloth or soft brush is sufficient.

7.1.1 Replacing the TMG Battery

When and where to use:
A 3 V coin cell battery on the Telephone Media Gateway (TMG) Motorola Advanced Crypto Engines (MACE) digital circuitry requires periodic replacement.

Table 12: Battery Replacement Time

The following table lists the recommended time table for replacing the MACE coin cell battery.

Hardware State	Replacing Time
Installed in the system	Every two years
Stored	Once a year

This procedure describes how to replace the battery.

Procedure:

1. Unplug the TMG power line cord from the AC source.
2. Disconnect all power and data/control connections to and from the TMG.
3. Dismount the hardware from the equipment rack.
4. Remove the cover screws and the chassis cover from the TMG.
5. Unpack the replacement battery.
6. Lift up an exposed edge of the battery until it “pops” out of the holder and put the old battery aside.

   NOTICE: When replacing the battery, ensure that its wider side is at the top.

7. Place the new battery carefully on top of the holder and with a slight rocking action, push it downward into the holder.

   The battery clicks into place.

8. Reinstall and secure the TMG chassis cover.
9. Reconnect all data/control and power connections to the TMG.
10. Reconnect the power supply 12 V cable.
11. Reconnect the power line cord to an AC source.
12. Verify the LEDs status and restore the proper operation of the TMG within the system.
13. Properly dispose of the old (Lithium) battery.
14. If you are using encryption, restore the encryption keys on the TMG using the Key Management Facility (KMF) or Key Variable Loader (KVL).

7.2 TMG Software Maintenance

No patches are available for the Telephone Media Gateway. If the software needs to be altered, new software is transferred and installed on the software as a system update.

Motorola-certified updates to the Windows 2008 Server software running on the IP Private Branch eXchange (PBX) server are performed through MOTOPATCH for Windows (OS) updates. A `readme.txt` file is provided with that software to provide installation instructions.

NOTICE: The MOTOPATCH requirement does not apply to the K core or Express Trunking configurations except if your organization purchased Security Update Service (SUS). Then MOTOPATCH media is available for deployment in your system. SUS is available for K core, but not Express Trunking configurations.

Chapter 8

Enhanced Telephone Interconnect Troubleshooting

This chapter provides fault management and troubleshooting information relating to Enhanced Telephone Interconnect.

8.1 Enhanced Telephone Interconnect Failures

A Telephone Interconnect Device (TID) interfaces an ASTRO® 25 system to the Public Switched Telephone Network (PSTN). This connection provides a means of making mobile-to-land telephone calls and land-to-mobile calls, where the mobile is an ASTRO® 25 subscriber radio. The TID must be colocated with the zone controller in each zone. Each zone can contain a single TID.

The following paths are required for Enhanced Telephone Interconnect (ETI):

- Control Link Path: Each TID is interfaced through the LAN switch to the zone controller.
- Audio Path: Audio connections between the TID and the ASTRO® 25 system take place through the Telephone Media Gateway (TMG).
- Telephone Line Connectivity: A TID can be configured to support loop start, Direct Inward Dial (DID), or DS1 trunks.

Failure of a telephone interconnect device in a multiple zone system may be transparent to the user if other TID devices are in the system. If only one TID device exists in the system (single or multiple zone), only telephone call capability is affected. All other voice dispatch functions continue to operate.

If no interconnect-capable channels are available, interconnect calls cannot be placed. Channels may be unavailable because they are busy, interconnect incapable (interconnect capability turned off), or they have failed. Interconnect calls are busied if all interconnect channels are busy. Interconnect calls are rejected if only interconnect incapable channels are available or if all interconnect capable channels have failed.

Interconnect calls are rejected if no TMG resources are available.

Regardless of the infrastructure, user limitations, or channel availability, Customer Programming Software (CPS) programming of the subscriber radio can prevent interconnect calls from being attempted.

If shared service dictates that an interconnect call is busied, the call is busied, regardless of whether an interconnect-capable channel is available at the site.

Interconnect calls are rejected if the TID has reached its Telephone Line Connectivity limit.

8.2 Troubleshooting Tools

This section provides information on the troubleshooting tools used for the Enhanced Telephone Interconnect system.

8.2.1

Unified Event Manager

The Unified Event Manager (UEM) is the fault management application for ASTRO® 25 systems. The UEM provides a centralized view of the operational status of the system by displaying intuitive, graphical representations (subsystem topology maps) of the system.

The UEM can manage the following elements for the Enhanced Telephone Interconnect (ETI) feature:

- High level element Interconnect Subsystem
- Telephone Media Gateway (TMG) communication status

The Zone Controller (ZC) and the TMG report the operational status of the interconnect subsystem to the UEM. For additional information on the UEM, see the *Unified Event Manager User guide*.

NOTICE: The NEC Sphericall components are not managed by the UEM.

The UEM can also be used to perform diagnostic activities on the TMG. You can send enable, disable, and rest requests. The following table provides status events and troubleshooting scenarios for the TMG.

Table 13: UEM Troubleshooting Scenarios for the TMG

Problem	State/Reason Code	Troubleshooting Actions
TMG State is not Enabled	Disabled/User Requested	Enable the TMG from the UEM.
	Critical Malfunction/No ZC IP address	• Check the configuration of the Box ID, Zone number, and Domain Name Services (DNS), using Configuration/ Service Software (CSS) or Unified Network Configurator (UNC). • Verify that DNS is up.
	Minor Malfunction/Lack of Keys	Perform key configuration, using Key Management Facility (KMF) or Key Variable Loader (KVL).
	Minor Malfunction/Duplicate Key	Check the key configuration, using KVL or KMF.
	Minor Malfunction/Battery Low	Replace the battery. See Replacing the TMG Battery on page 141.
ZC link is down	TMG Box State is not Enabled/No Reason	See actions listed above.
	TMG Box State is Enabled/No Reason	• Check the configuration of Zone ID and Box ID. • Check that the ZC configuration of TMGs matches the TMG configuration.

Table 14: UEM Troubleshooting Scenarios for the ETI Feature

The following table describes some additional actions to take when troubleshooting the ETI feature with the UEM.

UEM Status	Troubleshooting Actions
Interconnect Subsystem down	• Verify that the ZC Private Branch eXchange (PBX) link is up. • Verify that a ZC TMG link is up.
ZC ISS IP PBX link Critical Alarm	• Verify that the ZC has been configured with the Interconnect Subsystem • Verify that a proper URI and domain name has been provisioned ZC and IP PBX server. • Verify that DNS is up.
ZC TMG link Critical Alarm	• Verify that the ZC configuration of TMGs matches the TMG configuration. • Verify that DNS is up.

8.2.2

ZoneWatch Raw Display

Troubleshooting the Enhanced Telephone Interconnect (ETI) system can be performed by viewing the real-time events in the ZoneWatch raw display while you are trying to perform a particular action (such as an enhanced telephone interconnect call). This capture of interconnect call information is enabled in the Provisioning Manager. When you try using the service, the raw display in ZoneWatch typically shows a sequence of events for acknowledging the call request and servicing the call.

Table 15: ZoneWatch Troubleshooting Scenarios

The following table provides event scenarios using the ZoneWatch application for troubleshooting.

Event	Troubleshooting Action
Land-to-Mobile or Mobile-to-Land call cannot be completed due to authentication failure	Verify the Zone Controller (ZC) and IP Private Branch eXchange (PBX) server is provisioned with the same IP PBX server username and password
An individual interconnect attempt is rejected.	• Examine the call reject reason in ZoneWatch. • For configuration related reject reasons, Radio User Record Call Capabilities and/or Radio User Interconnect profile setting in the Provisioning Manager may have to be updated. • For secure capability related rejects, the Radio User Secure setting in the Provisioning Manager may have to be updated. Check the secure key configuration in Telephone Media Gateway (TMG) and the subscriber radio. • For Land-to-Mobile Direct Inward Dialing (DID) call related rejects, the Radio User Interconnect Settings in Provisioning Manager may have to be updated.

Event	Troubleshooting Action
Land-to-Mobile call fails and there is no call reject logged in ZoneWatch	Check the IP PBX server configuration to verify that the IP PBX server sends a Session Initiation Protocol (SIP) INVITE for the call.
End of call TMG Failure	Occur whenever a secure call fails. When encryption fails, perform the following actions: • Verify keys are loaded correctly using the Key Management Facility (KMF) or Key Variable Loader (KVL). This may require loading appropriate algorithms first. • Verify Provisioning Manager and Radio configuration - Common Key References (CKRs) must match. - Keys in the subscriber radio and TMG must match.

8.2.3
Enhanced Telephone Interconnect Call Events

An enhanced telephone interconnect call can be initiated by a subscriber or by a landline phone. The following example shows the typical events displayed in the raw display or an Air Time Information Access (ATIA) log file when a subscriber initiates a telephone interconnect call. The subscriber selects to make a phone call, selects the phone number to dial, and presses the Push-to-Talk (PTT) switch. The zone controller receives the call request and the following event messages appears:

```
Radio Status Traffic - Proceeding Ack Sent
```

```
Call Activity Update Extended - Start of New Call
```

The infrastructure dials the landline phone number and the following event message is displayed. The landline phone begins to ring.

```
Call Activity Update Extended - Start of New Call
```

When the subscriber radio user answers the call, the following message is displayed, and the voice transaction begins:

```
Call Activity Update - Call State Change
```

When the landline user answers the call, the following message is displayed, and the voice transaction begins:

```
Call Activity Update - Call State Change
```

The landline user, subscriber, or infrastructure eventually terminates the call and the following event appears:

```
End of Call - ZC End of Call
```

The following table describes each of the event messages that may be displayed during an interconnect call (in the proper sequence). Each of the individual event messages includes a long list of details about the event. It also lists some of the more significant fields that may be helpful when analyzing messages for telephone interconnect call problems.

Table 16: Telephone Interconnect Call Raw Display Messages

Message	Event Description	Significant Fields
`Radio Status Traffic - Proceeding Ack Sent`	The subscriber has dialed the landline phone number and has pressed the PTT switch. The system is responding to the call request from the subscriber.	Radio ID, Site, Zone, Controlling Zone Information
`Call Activity Update - Start of New Call`	The resources have been set up to start the interconnect call and the landline phone rings. The event message explains the type of call (Digital, Central Mobile to Land Interconnect).	Radio ID, Call #, Call Type (Digital, Central Mobile to Land Interconnect), Active Site/Channel, Resources (Telephone Media Gateway (TMG), Secure Key #, Busy Resources
`Call Activity Update - Call State Change`	The landline user has picked up the phone. The infrastructure transitions from ringing to an active voice call.	Transition (Ring to Active), Call #, Call Type (Digital, Central Mobile to Land Interconnect), Radio ID, Active Site/Channel, Resources (TMG), Multicast IP, Secure Key #
`Call Activity Update - Call State Change`	The system transitions from ringing the target subscriber into becoming an active interconnect call. Voice services begin.	Transition Interconnect Ring to Active, Call Type, Call #, Radio ID (caller), Radio ID (target), Site/ Channel, Local/Controlling Zone, Busy Resources, Multicast IP, Secure Key #
`End of Call - ZC End of Call`	The subscriber or landline user has terminated the call. The system can also terminate the call if there are problems or if the subscriber has exceeded monthly interconnect time.	Reason (Phone line termination command received during call), Call #, Controlling/Local Zone IDs
`Flexible Interconnect Call Billing Info`	Upon termination of an enhanced interconnect call, the system issues a packet containing billing information (such as the phone number, duration, and so on) for the call.	Offset to Zone Controller (ZC) Reserved Section, Offset to Call Section, Offset to Interconnect Section, Offset to Phone Number Section, Offset to Security Section, Offset to Alias Section, Call Section Timestamp, Universal Call Number (lower comp), Controlling Zone ID, Duration in Seconds, Subscriber ID, Call Type

8.2.4

NEC UNIVERGE 3C Administration

Basic troubleshooting of the IP Private Branch eXchange (PBX) server and IP PBX media gateways is performed using an application called NEC UNIVERGE 3C, which resides on the NEC Unified Communications Manager server (IP PBX server).

The IP PBX server and IP PBX media gateway components are not managed by the Unified Event Manager (UEM), do not generate SNMP traps, and do not provide dial-in access for troubleshooting. The Windows Remote Desktop feature can be used for troubleshooting the UNIVERGE 3C application.

8.2.4.1 DNS Record Settings for Unified Communication Manager to Zone Controller SIP Trunk Failover

When the ASTRO® 25 system is installed, a script is run to create all Domain Name Services (DNS) records. Enhanced Telephone Interconnect requires two Service (SRV) records, one for each Zone Controller (ZC) in the zone.

The DNS SRV records allow for ZC failover from the active ZC to the standby ZC. This failover is accomplished by routing Session Initiation Protocol (SIP) messages in a round-robin scheme to the active ZCs SIP port. If no response is sent to the Unified Communication Manager, DNS routes the SIP message to the next ZC based on the SRV records.

Verifying SRV Records on the Domain Controller on page 148 provides the means to verify SRV records.

This example is at Zone 7.

Example:

```
_sip._udp.zone7 SRV zc01.zone7
```

```
_sip._udp.zone7 SRV zc02.zone7
```

Also DNS A records are for zc01.zone7 and zc02.zone7.

In this example you would verify SRV records on the following Domain Controller:

```
Z007.DC01.zone7 - Zone 7 DNS (Z007-dns01)
```

8.2.4.2 Verifying SRV Records on the Domain Controller

Procedure:

1. Log on to the Domain Controller ESX server (`10.<zone>.233.121`) using root administrator credentials.
2. Choose **Domain Controller**and log on.
3. From **Start**, select **DNS**.
4. Click the desired zone (example: zone7) in the **Forward Lookup Zones** list.
5. Click **_udp** and verify that there is an SRV record for each ZC.

8.2.4.3 Adding or Deleting UNIVERGE 3C Active Directory User/Group Accounts

When and where to use:
If you cannot start the Unified Communications Manager or the Media Server application does not start, it is probably because the UNIVERGE 3C Active Directory user and group accounts are not being created on the ASTRO® 25 AD Domain Controller for the zone. This procedure describes how to set up the UNIVERGE 3C AD users and accounts.

Procedure:

1. Log on to the Domain Controller ESX server (`10.<zone>.233.121`) using root administrator credentials.

2 Click the **Domain Controller** and login.

3 Select **Active Directory**.

4 If required, add or delete the following accounts under Users:

If…	Then…
If you want to add users,	perform the following actions: **a** Add **Sphere-MS**. **b** Add **Sphere-DB**. **c** Proceed to step 5.
If you want to delete groups,	perform the following actions: **a** Select **Sphericall Admins** and **Sphericall Recording**. **b** Delete the groups. **c** Exit this procedure.

5 Under **Users**, create the **Sphericall Recording** and **Sphericall Admins** group accounts, if required.

6 Add users **Sphere-MS** and **Sphere-DB** to each group.

NOTICE: If the problem persists, verify that the Unified Communications Manager server has been joined to the AD Domain Controller. If not joined, see Joining the Unified Communications Manager Server to the ASTRO 25 Domain on page 98.

8.2.4.4

UNIVERGE 3C System Troubleshooting

Although the Unified Event Manager (UEM) is not used for fault management of the NEC UNIVERGE 3C system, many ways to obtain valuable information while troubleshooting failed interconnect calls are available:

- View system events in the UNIVERGE 3C console
- View system status events in the Windows Event Viewer
- View the scrolling marquees and monitor status LEDs on the front of the IP Private Branch eXchange (PBX) media gateways
- View Media Gateway Controller (MGC) and the IP PBX media gateway log files captures in the UNIVERGE 3C system
- Monitor the SIP trunk capacity
- Modify the dB level to resolve mobile to land call issues
- Install a third-party packet analyzer on the IP PBX server

CAUTION: Third-party packet analyzers can potentially generate large capture files, which if allowed to get large enough, can adversely affect the UNIVERGE 3C application. These analyzers should run only during troubleshooting. Stop the capture then discard the capture files once the issue is resolved to save space.

8.2.4.4.1

UNIVERGE 3C Console for System Status Events

When troubleshooting the UNIVERGE 3C system, as the first step, verify that all seven services are running in the console window. Double-click the **Console** icon on the desktop by clicking on the **Process Control** tab. If all but the Media Server service is running, the most likely a problem is with establishing a connection with the Domain Controller. See Adding or Deleting UNIVERGE 3C Active Directory User/Group Accounts on page 148.

You can also view trace information in the UNIVERGE 3C Console by clicking on the **Trace** tab. This provides a snapshot of UNIVERGE 3C log activities.

8.2.4.4.2 Windows Event Viewer for System Status Events

If you observe UNIVERGE 3C events in the Windows Event Viewer, see *Understanding UNIVERGE 3C Events in Windows Event Viewer* in the NEC UNIVERGE documentation (ships with the product) for interpreting the types of errors logged to Windows Event Viewer.

8.2.4.4.3 Scrolling Marquee Status Display on the IP PBX Media Gateways

Marquee display on left side of NEC BranchHub media gateway and COHub media gateway displays various information regarding the device. When idle, the scrolling display shows the media gateways name and enabled ports. If Awaiting Finder is constantly displayed, either the UNIVERGE 3C application has failed or there is a network connectivity problem.

8.2.4.4.4 LEDs on the IP PBX Media Gateways

When call attempts are placed to the BranchHub media gateway, the correlating LED above the called port flashes in cadence to the application of ringing voltage. If you do not observe this flashing, check that the RJ21X connector on the front of the BranchHub media gateway is in the correct position, firmly seated, and securely fastened using the Velcro strap.

When using the COHub media gateway, verify that the LED next to the RJ–48 connector on the front of the device is green. A yellow LED indicates frame slips and may cause inbound or outbound call attempts to fail. A red LED indicates loss of signal and any call attempt fails.

8.2.4.4.5 Log Files

Log files for the Media Gateway Controller (MGC) or the IP Private Branch eXchange (PBX) Media Gateway provide run-time information. Access these logs at: C:\Program Files (x86)\Sphere \Application Logs\Media Gateway and C:\Program Files (x86)\Sphere\Application Logs\mgc. If NEC is involved in the troubleshooting, they most likely require specific log files. Follow Backing Up the UNIVERGE 3C System Database on page 138 for the steps to copy particular files to a CD or DVD.

8.2.4.4.6 SIP Trunk Capacity

Inbound and outbound capacities for the Session Initiation Protocol (SIP) trunk are required. Call attempts fail with a 488 Not Available Here message when there is no SIP trunk capacity. This message can be viewed using the Wireshark application (see Packet Analyzer Installation on page 151) or by examining the NEC Media Gateway Controller (MGC) application logs.

8.2.4.4.7 NEC UNIVERGE 3C Troubleshooting Documentation

The system ships with NEC documentation available here: `C:\Program Files (x86)\Sphere \Documentation\`. You can also access the manufacturer Web site periodically for updates.

8.2.4.4.8 Modifying the DB Level to Resolve Mobile to Land Call Issues

This procedure describes how to decrease the dB level 1 dB at a time to troubleshoot mobile-to-land calls that are not being sent to the dialed number.

IMPORTANT: Consult with the Motorola Solutions Support Center (SSC) before making any changes to DB levels.

Procedure:

1. From **Start**, select **All Programs** → **3C Administrator**.
2. In the **3C Administrator** main window, click the **Trunks** tab.
3. Expand the **Hub** in bold text that is having the problem.
4. Right-click the port that is having the problem and select **View Properties**.
5. Click the **Settings** tab.
6. Click **Add**.
7. In the **Name** field, click the pull-down menu and select **Trunk Volume in DB**.
8. Decrease the dB value by 1.
9. Click **Apply**. Click **OK** to save the changes.
10. Repeat steps 4, 5, then 8 and 9 until the problem is corrected.

8.2.4.4.9 Packet Analyzer Installation

Wireshark software is an open-source packet analyzer that can be used for troubleshooting the Sphericall system. It is available at http:www.wireshark.org. Run a packet analyzer only during troubleshooting. Stop the capture then discard the capture files once the issue is resolved to save disk space.

8.2.4.5 Call Processing Problems

The recommended method to diagnose call processing problems is to install Wireshark on the Unified Communication Managerserver and capture the Session Initiation Protocol (SIP) call trace. This capture shows you a high-level snapshot of where and when the call is failing and at which device.

Calls do not complete due to a number of reasons including hardware failure, software bugs, or messaging problems (SIP, Public Switched Telephone Network).

If either a Mobile-to-Land or Land-to-Mobile call fails, it is most likely a route issue. If both are down, it is most likely that something a fundamentally wrong with how the NEC application is configured or a hardware failure.

8.2.5 Motorola Solutions Equipment Administration

Fault management and administration of the Motorola Solutions system components is accomplished using the Unified Event Manager (UEM).

8.2.5.1
ETI Troubleshooting in the UEM

This section describes how to troubleshoot Enhanced Telephone Interconnect (ETI) issues using the Unified Event Manager.

8.2.5.1.1
Links and Individual Components Monitoring Using the Unified Event Manager

Use the Unified Event Manager (UEM) to monitor critical links and components in the system. Monitoring may take place remotely from a central operations center. Two types of monitoring include:

- Real-time monitoring of UEM Topology Maps
- Evaluation of UEM Active Alarms View on a regularly scheduled basis

See the *Unified Event Manager User guide* for more information.

8.2.5.1.2
Unified Event Manager Active Alarms View

The Unified Event Manager (UEM) Active Alarms View is useful for troubleshooting because it captures alarms that may occur intermittently or during off-hours. For example, review the Active Alarms View to correlate the reported loss of service with patterns of critical alarms for links and equipment.

When analyzing the Active Alarms View, look for these types of patterns:

- Failures sent with time stamps on or about the same time.
- Failures from equipment attached to particular links, for example, routers, switches, controllers, comparators, and base radios.
- Many devices are capable of sending out events that report both critical and non-critical events. Learn to distinguish between critical and non-critical events.

See the *UEM Online Help* for more information.

8.2.5.2
Using IP PBX Group Objects for Auditing and Security

This procedure describes how to add or delete IP Private Branch eXchange (PBX) group objects.

Procedure:

1. Log on to the Domain Controller ESX server (`10.<zone>.233.121`) using root administrator credentials.
2. Choose **Domain Controller** and login.
3. From the **Start** menu, choose **Run**, then type `gpedit.msc`. Press ENTER.
4. Choose **Telephony Server** → **Computer Configuration** → **Policies**.
5. Choose **Windows Settings** → **Security Settings** → **Local Policies**.
6. Choose **User Rights Assignment** → **Manage Auditing** → **Security Log**.
7. Delete or add the IP PBX groups.

If…	Then…
If you want to add groups,	perform the following actions:

If…	Then…
	a Click **Add User or Group**. **b** Enter `<domain name>/<group>` (`Sphericall Admins` or `Sphericall Recording`).
If you want to delete groups,	perform the following actions: **a** Click **Remove**. **b** Select the group you want to delete.

8 Click **Apply**. Click **OK**.

The modified **Telephony Server** group object is saved.

8.3

Software Download to TMG Troubleshooting

The Unified Network Configurator (UNC) management software provides secure download to the Telephone Media Gateway (TMG) with the Software Download Manager (SWDL). If you are unable to download the software using secure SWDL, you can download in clear mode. See the *Unified Network Configurator User Guide* and *Software Download Manager User guide*s for more information.

8.4

Passwords and SNMPv3 Passphrases

You can enable/disable the password reset mechanism in the Configuration/Service Software (CSS) application. See the *CSS Online Help* “Device Security Configuration - Security Services (Serial)” screen for information. To obtain the keys for resetting either password or SNMPv3 passphrases for the Telephone Media Gateway (TMG), contact Motorola Solutions Support Center.

NOTICE: The default values for the local passwords and SNMPv3 passphrases, as well as the keys for the local password reset procedure, may vary by system release. These items are treated as sensitive information and are provided to the user through secured communication.

Table 17: Local Password and SNMPv3 Passphrase Troubleshooting

Scenario	SNMPv3 Passphrase Known	Local Password Known	To Reset SNMPv3 Passphrase	To Reset Local Log on Password
User is locked out of local login, but knows SNMPv3 passphrases.	✓	X	See the *CSS Online Help* “SNMPv3 User Configuration”.	See the *CSS Online Help* “Resetting Device Passwords.”
User knows local login, but not the SNMPv3 passphrases.	X	✓	See the *CSS Online Help* “Reset SNMPv3 Configuration (Serial)”.	See the *CSS Online Help* “Device Security Configuration – Security Services (Serial)”
User knows both passphrases and local service password.	✓	✓	See the *CSS Online Help* “SNMPv3 User Configuration”.	See the *CSS Online Help* “Device Security Configuration – Security Services (Serial)”

Scenario	SNMPv3 Passphrase Known	Local Password Known	To Reset SNMPv3 Passphrase	To Reset Local Log on Password
User does not know SNMPv3 passphrase nor service account password.	X	X	Contact Motorola Solutions Support Center.	Contact Motorola Solutions Support Center.

Chapter 9

Enhanced Telephone Interconnect FRU/FRE

This chapter lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) and includes replacement procedures applicable to Enhanced Telephone Interconnect.

9.1 ETI Hardware Replacement

This manual provides installation procedures for the Enhanced Telephone Interconnect (ETI) subsystem components.

See the *Firewall* manual for replacement procedures related to the telephony firewall.

See the appropriate ASTRO® 25 system subscriber radio, Key Variable Loader (KVL), and Key Management Facility (KMF) manuals for specific component repair and replacement procedures.

9.1.1 Replacing the Telephone Media Gateway

This procedure describes how to replace the Telephone Media Gateway (TMG) in the event of a hardware failure.

IMPORTANT:
Before replacing the TMG, pull the configuration and hardware information from the device into the Unified Network Configurator (UNC) by performing the Pull All procedure. For instructions on how to perform a Pull All procedure, see the *Unified Network Configurator User guide*.

This step may not be possible if communication is severed between the TMG and the UNC. If this issue occurs, perform one of the following actions:

- Use the last known good configuration files from the UNC.
- Use files provided by Motorola when your system was commissioned.

Regardless of the source, copy the configuration file to the service computer with 3com® TFTP software enabled.

Contact your system administrator to obtain the following information before performing this procedure:

- IP address for the TMG
- Account usernames and passwords for (types of accounts)

.

Procedure:

1. Disconnect the TMG power supply line cord from an AC source.
2. Disconnect the power supply 12V cable from the rear of the TMG chassis.
3. Remove the existing TMG:
   a. Label and disconnect all communication cabling from the TMG.
   b. Disconnect the ground cable from the rear of the chassis.
   c. Remove the screws securing the TMG to the rack.

   d Pull the TMG out through the front of the rack.

4. Remove the mounting brackets from the existing TMG and install the brackets on the replacement Telephone Media Gateway.
5. Install the replacement TMG:
   - a Install the replacement TMG in the rack and secure it with the screws previously removed.
   - b Secure the ground cable to the ground location on the rear of the chassis.
   - c Attach all communication cabling to the TMG.
6. Proceed with the installation and configuration procedures in this manual to install a new TMG.

9.1.2 IP PBX Server Replacement

Call the Motorola Solutions Support Center for repair and/or replacement instructions at one of the following phone numbers: North America: 1-800-221-7144; International: 302-444-9800.

9.1.3 IP PBX Media Gateway Replacement

To replace the IP Private Branch Exchange Media Gateway, see the following NEC documentation that ships with your system:

- NEC *BranchHub Installation Manual*
- NEC *COHub Installation Manual*

9.2 TMG Component Disposal

The Motorola Solutions Support Center (SSC) provides technical support, Return Material Authorization (RMA) numbers, and confirmations for troubleshooting results. Call the SSC for information about returning faulty equipment or ordering replacement parts. North America: 1-800-221-7144 / International: 302-444-9800.

The Motorola SSC coordinates all repair and replacement of NEC hardware. Call the number above to open a case when troubleshooting hardware failures.

After removing a failed Telephone Media Gateway, ship it to the Motorola Infrastructure Depot Operations (IDO) for further troubleshooting and repair. Return any failed units to the Motorola Solutions IDO at 2214 Galvin Drive, Elgin, IL 60123. The field shop contacts the Motorola SSC to request a replacement or repair, and the Depot ships out a replacement Field Replaceable Entity (FRE). Included in the packaging is paperwork with instructions on how to return the failed unit.

Properly dispose of any replaced Lithium batteries.

⚠ **CAUTION:** Do not attempt to repair or service subcomponents in the Telephone Media Gateway.

9.3
ETI FRU/FRE Parts List

The following table provides the Enhanced Telephone Interconnect (ETI) subsystem Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) parts list.

Table 18: Enhanced Telephone Interconnect Parts List

Kit/Part Number	Description
T7589A	Motorola Telephone Media Gateway (TMG) Voice Processor Module (VPM), includes the external power supply
01009513001	VPM Power Supply FRU (for TMG)
30009351001	DC Cable (connects 12V DC from the power supply to the VPM/TMG)
1575395h01_revD	VPM/TMG Power Supply Tray
42009052001_revB	Power Supply Velcro Fastener (for use with tray)
528585-001-00	Backup Battery (for TMG)
58009256065	DB9F and RJ-45 VPM Programming Adapter (for TMG)
TT05509AA	JITC-compliant IP PBX server, w/3 simultaneous lines. This is a Dell PowerEdge R 610 computer server pre-configured with necessary OS, software, and NEC Sphericall license file in custom domain name.
TT05501AA	Licensing for three additional JITC-compliant simultaneous lines.
TT05502AA	NEC BranchHub Media Gateway analog hub (each has capacity of six analog lines)
TT05503AA	NEC COHub Media Gateway digital hub (each has capacity of 24 T1 or 30 E1 lines)
DDN9590A	Juniper Networks SSG140 (supports up to 30 calls)
DDN9881A	Juniper Networks SSG 520M firewall Field Replaceable Entity (FRE) (supports up to 120 calls)

Cabling information for the TMG is found in Installing the Telephone Media Gateway Requirements on page 62, and cabling information for the NEC Sphericall system is found in Preparing for NEC UNIVERGE 3C System Installation on page 84. Also, various algorithm options are available for the Telephone Media Gateway.

Chapter 10

Enhanced Telephone Interconnect Reference

This chapter contains supplemental reference information relating to Enhanced Telephone Interconnect.

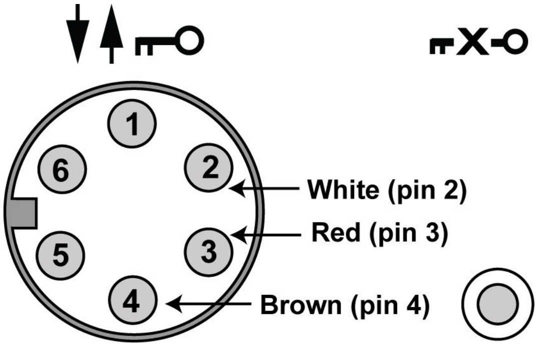
10.1 Telephone Media Gateway Hardware Information

This section provides reference information on the Voice Processor Module hardware used as the Telephone Media Gateway.

10.1.1 Telephone Media Gateway Ports and Connector Diagrams

The following illustration shows the view into the connector of the Key Variable Loader (KVL) port cable at the front panel of the Telephone Media Gateway (TMG). When the KVL is connected, follow the instructions in the user guide for the model of KVL you are using to load encryption keys.

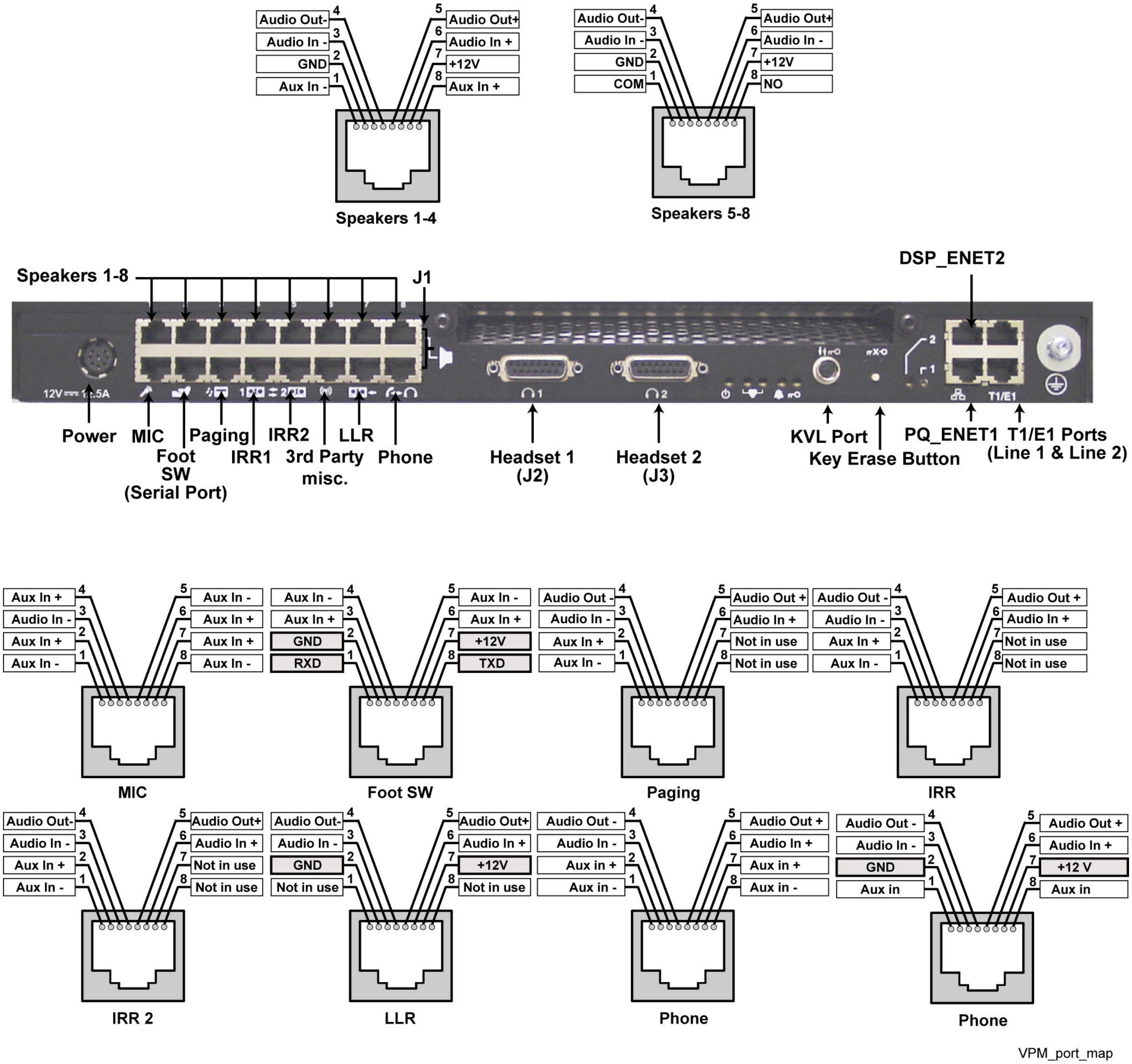
Figure 14: KVL Loader Port and the Key Erase Button



VPM_KVL_loader_port

Because the Voice Processor Module (VPM) hardware is used for other applications within the ASTRO® 25 system, Figure 15: Voice Processor Module Port Mapping on page 159 illustrates the port mapping for the hardware and Telephone Media Gateway on page 23 provides the ports used for the TMG application of the device.

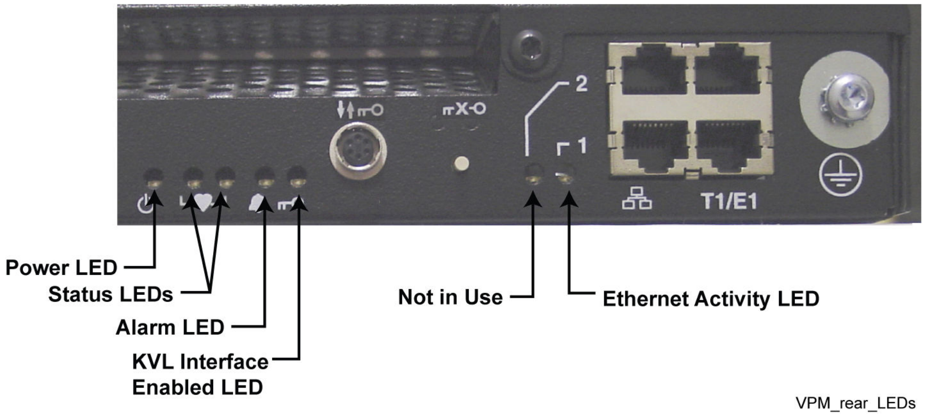
Figure 15: Voice Processor Module Port Mapping



10.1.2 Telephone Media Gateway LEDs

The Telephone Media Gateway (TMG) has five types of LEDs indicating the general conditions for the device and its Ethernet activities.

Figure 16: TMG LEDs



10.1.2.1
TMG Power LED

The Power LED is on (solid green) if the power is supplied to the box from the external power supply.

10.1.2.2
TMG Status LEDS

The following table describes the Voice Processor Module (VPM) Status LEDs.

Table 19: Status Definitions for the Telephone Media Gateway Status LEDs

State	Status LED (Green)	Status LED (Red)	Description
Online	On	Off	Telephone Media Gateway (TMG) is fully functional.
Link Down	Flashing	Off	TMG is functional, but the Zone Controller link is not ready yet or the link cannot be established (possibly because the Ethernet link is unplugged, the Zone ID is not configured, the Domain Name Services (DNS) is not configured or is not reachable, or the Zone Controller is not reachable).
Impaired	On	Flashing	TMG is running, but is impaired (likely because the software update failed).
Failure	Off	On	Fatal failure detected.

10.1.2.3 TMG Security Alarm LED

The Security Alarm LED is on when a major critical hardware failure at Motorola Advanced Crypto Engines (MACE) chips is detected.

10.1.2.4 TMG KVL Interface Enabled LED

The Key Variable Loader (KVL) Interface Enabled LED is on when the Telephone Media Gateway (TMG) is ready to perform key loading.

10.1.2.5 TMG Ethernet Activity LEDs

Two Ethernet Activity LEDs are observable, but only the one marked with **1** is functional. The following table provides the definitions for the Voice Processor Module (VPM) Ethernet Activity LED.

Table 20: TMG Ethernet Activity LEDs

State	Activity LED (Green)	Description
Link Inactive	Off	The link is not established
Link Established	On	The link is established but there is no current activity
Link Active	Flashing	Ethernet activity

10.2 NEC UNIVERGE 3C Hardware Information

See the NEC hardware documentation referenced in Related Information on page 19. Each system ships with the current documentation set pre-loaded.

10.3 SIP Messages between the ZC and IP PBX Server

Table 21: Common SIP Messages Exchanged between the ZC and the IP PBX Server on page 161 provides common Session Initiation Protocol (SIP) messages between the Zone Controller (ZC) and IP Private Branch eXchange (PBX) server.

Table 21: Common SIP Messages Exchanged between the ZC and the IP PBX Server

SIP Message	Description
SIP REGISTER	Used to establish the ZC and IP PBX link.
SIP OPTIONS	Acts as a link maintenance heart beat mechanism.
SIP INVITE	Used to initiate an interconnect call.
SIP 401 Unauthorized	Indicates an authentication challenge to SIP INVITE for every interconnect call.
SIP 180 Ringing	For subscriber radio initiated calls, this message indicates that landline is ringing. For landline initiated calls, this

SIP Message	Description
	message indicates that the ZC is processing the call request.
SIP 200 OK	Used to establish interconnect call.
SIP BYE	Indicates that subscriber radio or landline has terminated the call.
SIP 4xx (other than SIP 401)	An error message. The call attempt is rejected for various reasons.
SIP 5xx	An error message. The call attempt is rejected for various reasons.
SIP 6xx	An error message. The call attempt is rejected for various reasons.

10.4 NEC UNIVERGE 3C System Initialization Settings

The UNIVERGE 3C system requires the following initialization settings to work correctly in an ASTRO® 25 system.

⚠ **CAUTION:** Use only the IP PBX server initialization settings provided here. Any additional configuration changes may negatively affect functionality.

Table 22: System Initialization Settings

Name	Description	Value Range	Setting
G.711 CODEC only	Used by UNIVERGE 3C endpoints for low latency media streams which minimizes the perception of echo.	True False (default)	`True`
Jitter Buffer Size	Jitter Buffer absorbs variation in packet delivery. Requests from an endpoint the number of jitter buffers to be used when establishing a media stream with another endpoint. For example, when a UNIVERGE 3C endpoint connects to a UNIVERGE 3C Media Server, it uses a jitter buffer size of 3.	0 to 20 2 (default)	`1`
Maximum Call Duration Timer (in minutes)	This setting controls the number of minutes after which call without changes is dropped. Changes in this context are changes to the call state, for example hold/unhold/transfer/media changes. The only exception to this is music on hold, this setting has no effect as	0 (disabled) (default) Max. is 1440 minutes (1 day)	`68`

Name	Description	Value Range	Setting
	long as you are connected to MOH.		
MG Poll Multicast Address Used	Used for Media Gateway Controller (MGC) discovery.	239.193.0.0 to 239.193.0.254 239.193.0.0 (default)	`239.193.0.0`
MG Security > Access via telnet _RDBG remote logging	Specifies whether telnet access to the media gateway is enabled. This setting also enables or disables RDBG remote logging on TCP port 6532.	True - telnet is enabled (default) False - telnet is disabled	`False`
MG Security > Console lock time (sec) after unsuccessful logins	Specifies the length of time, in seconds, the console is locked after unsuccessful login attempts.	0 to 86400 60 (default)	`900`
MG Security > Inactivity time (sec) before console logout	Specifies the length of time, in seconds, the console session may be idle before it is automatically logged out.	60 to 16777215 600 (default)	`60`
MG Security > Minimum lower case characters	Specifies the minimum number of lower case characters in the password.	0 to 27 0 (default)	`5`
MG Security > Minimum numeric characters	Specifies the minimum number of numeric characters in the password.	0 to 27 0 (default)	`1`
MG Security > Minimum password length	Specifies the minimum password length, in characters.	1 to 27 6 (default)	`14`
MG Security > Minimum special characters	Specifies the minimum number of special characters in the password. Special characters are !”%()* +,-./:=>@[]^`{|}~	0 to 27 0 (default)	`1`
MG Security > Minimum upper case characters	Specifies the minimum number of upper case characters in the password.	0 to 27 0 (default)	`1`
MG Security > Unsuccessful logins before console locks	Specifies the number of consecutive unsuccessful login attempts that result in the console being locked.	1 to 255 5 (default)	`3`
Performance monitoring sta-	If enabled, the UNIVERGE 3C applications generate the performance monitoring	Enabled (default) Disabled	`Disabled`

Name	Description	Value Range	Setting
tistics generation	statistics that can be viewed in Performance Monitor.		
Restrict Admin to Servers	Configuration to restrict whether Admin can only be run from a Unified Communications Manager server.	False (default) True (enabled for JITC)	True
RTP receive packet size maximum from UNIVERGE 3C Media Server in milliseconds	Size of the voice packets from the IP PBX server to an endpoint.	80 milliseconds (default) Range: 20 80 milliseconds	20
SecureMG	To enable UNIVERGE 3C applications and media gateways to support TLS/SSL. Currently only supported system-wide. ⚠ **CAUTION:** Setting this value to True prevents correct operation of the Enhanced Telephone Interconnect feature. This setting must be False.	False (default) True (enabled for JITC)	False
SIP > DNS SRV Service Enabled	The DnsSrvServiceEnabled MGC setting specifies whether the MGC performs DNS SRV queries on the SPD/OP. This setting defaults to true. The administrator must change this setting to false if the SPD/OP specifies a host name, if the SPD is not a valid DNS domain name with an SRV record, or if the authoritative DNS server for the SPD does not support SRV queries.	Enabled (default) Disabled	Enabled
SIP > DNS NAPTR Service	The DnsNaptrServiceEnabled MGC setting specifies whether the MGC performs DNS NAPTR queries on the SPD/OP. This setting defaults to true. The administrator may optimize MGC performance by changing this setting to false if the	Enabled (default) Disabled	Disabled

Name	Description	Value Range	Setting
	SPD/OP specifies a host name or if the authoritative DNS server for the SPD does not support NAPTR queries.		
Syslog IP Address	The IP address of the machine where Syslog server is running.	Entry: IP address of the Syslog server IPv4 format only.	`10.zone>.233.249`
Syslog Locking Policy	Configuration to set the Audit logging failure policy.	Ignore (default): Changes are allowed to the DB even when Syslog server is not running. Disallow Changes: Changes are not allowed to the DB even when Syslog server is not running. DB is locked if Syslog server is not running. This setting is required for JITC.	`Ignore`
Syslog Server IP Port	Port used by the Syslog server.	Default: 1468 (standard port) **NOTICE:** This configuration is for TCP communication and must not be blocked by firewall.	`514`

Chapter 11

Enhanced Telephone Interconnect Disaster Recovery

This chapter contains information relating to the disaster recovery process for the Enhanced Telephone Interconnect feature.

11.1 Recovery Sequence for Enhanced Telephone Interconnect Devices

This section details the recovery of the following devices:

- Telephone Media Gateway
- IP Private Branch eXchange (PBX) server
- IP PBX media gateway (optional)
- Telephony firewall (optional)

11.1.1 Recovering the Telephone Media Gateway

Follow this process to replace an entire Telephone Media Gateway (TMG).

Process:

1. Remove the old TMG hardware. See Telephone Media Gateway Removal on page 136. Install the new TMG hardware. See Telephone Media Gateway Installation on page 62.
2. Perform basic device configuration using the serial port. See Provisioning the Telephone Media Gateway Serial Connection Parameters on page 67.
3. Perform basic device configuration using the Ethernet port. See Configuring the Telephone Media Gateway in the CSS (Ethernet Connection) on page 68.
4. Enable secure credentials.
   a. Set the Software Download Manager (SWDL) transfer mode in the Configuration/Service Software (CSS). See Setting the Software Download Manager Transfer Mode on page 70.
   b. Set the local password configuration. See Setting the Telephone Media Gateway Local Password Configuration on page 70.
   c. Set the date and time in CSS. See Setting the Date and Time on the Telephone Media Gateway on page 72.
   d. Set the serial security service. See Setting the Serial Security Services on page 72.
5. Complete the configuration of the Information Assurance (IA) features in the CSS, as follows:
   a. Create, update, or delete an SNMPv3 user. See Adding or Modifying an SNMPv3 User on page 75.
   b. Verify the SNMPv3 credentials. See Verifying an SNMPv3 Connection in the CSS on page 76.

- **c** Configure Domain Name Services (DNS) in the CSS. See “Configuring DNS Using CSS” in the *Authentication Services Feature guide*.
- **d** Configure for Secure SHell (SSH). See “Configuring SSH for RF Site Devices and VPMs Using CSS Overview” in the *Securing Protocols with SSH Feature Guide*manual.
- **e** Configuring the local cache size for the Telephone Media Gateway. See “Setting the Local Cache Size for Centralized Authentication Using CSS” in the *Authentication Services Feature guide*.
- **f** Enable RADIUS authentication in the CSS. See “Configuring RADIUS Sources and Parameters Using CSS” in the *Authentication Services Feature Guide*.
- **g** Enable Centralized Authentication in the CSS. See “Enabling/Disabling Centralized Authentication Using CSS” in the *Authentication Services Feature guide*.
- **h** Optionally, enable Centralized Event Logging in the CSS. See “Enabling/Disabling Centralized Event Logging on Devices Using CSS” in the *Centralized Event Logging Feature guide*.
- **i** Customize the Login Banner using CSS. See Customizing the Login Banner in the CSS on page 77.

NOTICE: You can also see the *CSS Online Help* in the software application to complete these tasks during the device configuration.

6. Connect the TMG to the Gateway Router. See Connecting the Telephone Media Gateway to the Network on page 78.
7. Replace the TMG in the Unified Network Configurator (UNC). See “Replacing a Device” in the *Unified Network Configurator User guide*.
8. Perform a SWDL from the UNC. See Installing Telephone Media Gateway Software on page 78.
9. Set up the TMG. See Configuring the Telephone Media Gateway on page 104.

11.1.2
Recovering the IP PBX Server

When and where to use:
The following process is used only in the event of a disk drive failure when the Windows 2008 Operating System and IP Private Branch eXchange (PBX) application need to be completely reinstalled. If available, use the IP PBX server Redundant Array of Independent Disk (RAID) backup disk to recover the server. Perform this process if the IP PBX server RAID backup disk is not available.

Follow the steps in this process to replace an entire NEC UNIVERGE 3C system.

Process:

1. Load the Dell Operation System (OS) Restoration Disk (backup of the OS) provided with the server into the DVD drive.
2. Run the installation and restoration steps on the installation script.
   - **a** From **Start**, select **Computer** → **Drive** → **E:** → **Setup**.
   - **b** Click **Do not get latest updates for installation**.
   - **c** Choose **Windows Server 2008 R2 Standard (Full Installation)**.
   - **d** Choose **Custom (Advanced) Installation**.
   - **e** Install on the OS on the C: Drive.
   - **f** Enter the product key from the label on the server.

NOTICE: After installation, verify that the proper time zone is selected by choosing **Start** → **Control Panel** → **Clock** → **Language** → **Region** → **Date and Time** to change the time zone.

3 Set the IP address of the IP PBX server. See Configuring the IP Address of the Unified Communications Manager Server on page 97

4 Join the Unified Communications Manager to the ASTRO domain. See Joining the Unified Communications Manager Server to the ASTRO 25 Domain on page 98, which also applies the Windows 2008 Security Group Policy using the Telephony Server Organizational Unit (OU).

5 Enable Remote Desktop for the server. See Configuring Remote Desktop for the Unified Communications Manager on page 99..

6 Enable file sharing. See Sharing the UNIVERGE 3C File System on page 99.

7 Configure the Unified Communications Manager server as a McAfee Anti-Malware client using the ASTRO® 25 system Core Security Management Server application. See “CSMS – Deploying McAfee Client Software to Anti-Malware Clients” in the *Core Security Management Server Feature guide*.

8 Install the NEC UNIVERGE 3C 8.5 software from the two 8.5.2.3 software installation media (base and SP3) using the default settings. Use the following installation wizards:

   a Unified Communications Manager Commissioning including license key from the License Key DVD.

   b Unified Communications Manager System Commissioning. See Commissioning the UNIVERGE 3C Unified Communications Manager on page 100.

9 Perform a UNIVERGE 3C database restoration.

If…	Then…
You have a recent database backup on another network resource or DVD and modifications were made to the UNIVERGE 3C application configuration since the initial deployment of the equipment at your site,	perform the following actions: **a** Obtain the most recent copy of the database. **b** Restore the database using Restoring the UNIVERGE 3C 7.1 System Database on page 139. **c** Restore the custom .wav file using Replacing the American English Greeting on page 115 steps 3 through 5 using the .wav file on the backup DVD.
You have the original backup of the database supplied by Motorola Solutions on DVD at the time of deployment with specific settings for you site (dialing plan, Trunks, Auto Attendant (voice announcement), default domain name, and so forth),	perform the following actions: **a** Obtain the copy of the backup DVD supplied by Motorola Solutions. **b** Restore the database using Restoring the UNIVERGE 3C 7.1 System Database on page 139. **c** Restore the custom .wav file using Replacing the American English Greeting on page 115 steps 3 through 5 using the `.wav` file on the backup DVD.

10 Verify UNIVERGE 3C security settings are applied. See NEC UNIVERGE 3C System Initialization Settings on page 162.

11 Apply the approved Microsoft patches and service update using the MOTOPATCH for Windows OS CD to the Unified Communications Managers.

NOTICE: The MOTOPATCH requirement does not apply to the K core or Express Trunking configurations except if your organization purchased Security Update Service (SUS). Then MOTOPATCH media is available for deployment in your system. SUS is available for K core, but not Express Trunking configurations.

12 Use the Windows Supplemental CD to apply local settings to the application, database, and IP PBX media gateways by performing the following actions. See “Configuration Using the ASTRO 25 System Windows Supplemental CD User Interface” in the *Windows Supplemental Configuration* manual.

a Insert the disk into the IP PBX server DVD drive and double-click the following file: D:\Windows Security Configurations\bin\Windows_Supplemental_GUI

b When the GUI appears, select **Windows Security Configurations**.

c Click **Device Specific Settings**.

d From the **Select a Device** pull-down menu, select **Telephony Server** and choose **Run Scripts**. Follow the instructions.

e When finished, reboot the server. After the server reboots and all UNIVERGE 3C services have started, reboot the IP PBX media gateways by simultaneously pressing both buttons on the side of the marquee display on the front panel of the device until the display goes blank, then release the buttons to begin the restart.

NOTICE: In the Windows Supplemental Configuration GUI, the IP PBX server is called the Telephony Server, as shown in sub-step 12.d.

13 Select the UNIVERGE 3C Console and verify that all UNIVERGE 3C processes are running (no process IDs of 0). See NEC UNIVERGE 3C Application Configuration on page 95.

14 Initiate a mobile-to-landline call with an ASTRO® 25 subscriber radio and verify that the correct number is dialed and audio is exchanged in both directions.

15 Initiate a landline-to-mobile call with an ASTRO® 25 subscriber radio and verify that the correct number is dialed and audio is exchanged in both directions.

11.1.3 Recovering an IP PBX Media Gateway

This procedure describes how to replace a defective NEC BranchHub or COHub media gateway, if one is used in your system.

Process:

1 Record all NEC BranchHub or COHub media gateway data and MAC addresses for reference from the front display panel of the device or using Command Line Interface (CLI) when connected to the IP Private Branch eXchange (PBX) media gateway through a serial connection.

2 Configure the new IP PBX media device to be compatible with the network environment that exists for the UNIVERGE 3C system. This configuration includes assigning the static IP address to the new IP PBX media gateway. See Configuring the IP Address of the Unified Communications Manager Server on page 97.

3 Install the new NEC BranchHub or COHub media gateway and turn on the power.

After the media gateway is powered up, it checks in with the Unified Communications Manager. This action creates a new Network Interface record and new Inside Line records (for a BranchHub media gateway) with the same number of ports, or new Outside Line records with the appropriate number of channels (for a COHub or BranchHUB media gateway).

4 Power down old NEC BranchHub or COHub media gateway.

5 From **Start**, select **All Programs** → **3C Administrator**.

6 Click the appropriate tab based on the NEC BranchHub or COHub media gateway you want to replace. Click the **Trunks** tab.

7 In the **Trunks** tab, expand the folder to view all available **BranchHub** or **COHub** media gateways.

8 Highlight the **BranchHub** or **COHub** media gateway that you want to replace, right-click and select **Replace Hubs**.

The **Replace Hub** dialog box appears.

9 Expand the folder to view the **BranchHub** or **COHub** media gateways available within your system to replace the defective BranchHub or COHub media gateway.

10 Highlight the **BranchHub** or **COHub** media gateway you want to use as the replacement for the defective device.

11 Click **OK**. Click **OK** again.

12 Click the **Trunks** tab to see the newly added BranchHub or COHub media gateway.

13 Expand the folders listed in the file tree to view all available media gateways within your organization UNIVERGE 3C system.

14 Highlight the newly added **BranchHub** or **COHub** media gateway. Right-click and select **Hub Properties**.

The **Properties for Hub** dialog box appears.

15 Verify the accuracy of all records and protocol fields for the device specific to your site.

16 Click **OK**.

Any changes are saved and the **Properties for Hub** dialog box closes.

11.1.4 Recovering the Telephony Firewall

See “Recovering a Firewall in an ASTRO 25 System” in the *Fortinet Firewall Feature Guide* to recover the telephony firewall.

Chapter 12

Enhanced Telephone Interconnect Software Upgrade from 7.1 to 8.5.2.3 SP3

The IP PBX server software must be upgraded on systems running UNIVERGE 3C Server software 7.1. The current release is 8.5.2.3 with Service Pack 3 (SP3).

12.1 Upgrading to UNIVERGE 3C Version 8.5.2.3

Prerequisites: Ensure that you have the following items:

- UNIVERGE 3C 8.5.2.3 Installation Disc 1 of 2 (Part #400997)
- A UNIVERGE 3C v.8.5.2.3 license. Contact NEC to obtain this license if you do not have one.
- The server is currently running the Sphericall application and is joined to the ASTRO domain.
- All programs are closed, such as the **Sphericall Administrator** utility.
- All configuration data, accounts, and passwords are saved.
- There is a current backup of the `C:\Program Files(x86)\Sphere\data\pbx.mdb.backup` file and store it off the server.

When and where to use:
Perform this task if your system is operating UNIVERGE 3C server software 7.1. The installation process is in two parts. First, prerequise software must be installed before installing the UNIVERGE 3C application. All software is included on one DVD, athough the new v8.5 license file is on a separate DVD.

After performing this task, add 8.5.2.3 Service Pack 3, which requires separate installation media. Ensure that you have both DVDs before beginning the upgrade process.

NOTICE: Ensure that the **SRV3CDatabase** and **SRV3cMediaServer** domain user accounts are added to the system before beginning this procedure.

Procedure:

1. Insert UNIVERGE 3C 8.5.2.3 Disc 1 of 2 (Part #400997) in the DVD drive of the IP PBX server.
2. In Windows Explorer, navigate to the DVD drive and double-click `Launch.exe`.

   Unless the User Account Control (UAC) is disabled, a UAC message appears. The software installation begins.

3. Perform one of the following actions:

If…	Then…
If UAC is disabled,	Go to the next step.
If the UAC is not disabled,	Enter the domain account credentials. Press **OK**.

4 Choose **Install Prerequisite Software**.

A warning message appears.

5 Click **OK**.

The prerequisites install on the IP PBX server.

6 Click **Install**.

The prerequisites install on the IP PBX server.

7 Click **Finish**.

8 After the prerequisite software installs, click **Yes** to reboot the server.

The IP PBX server restarts.

9 In Windows Explorer, navigate to the DVD drive and double-click `Launch.exe`.

10 Click **Install Unified Communications Manager** to install the 3C Manager, Desktop, and the Administrator application.

11 Click **Yes, Continue**.

The **3C Installation** window appears.

12 Follow the dialog boxes for upgrading to UNIVERGE 3C 8.5.2.3.

13 When prompted, provide the path to the new UNIVERGE 3C 8.5.2.3 license file.

14 When prompted for the **Automatic Client Update**, select **Yes - Copy the package**. Click **Next**.

15 When the **Windows Security** window appears, select **Install this driver software anyway**. Repeat this step as needed.

16 When prompted to reboot, click **Yes**.

Postrequisites: Proceed with the upgrade with the Service Pack 3 media. See Upgrading to UNIVERGE 3C Version 8.5.2.3 Service Pack 3 on page 172.

12.2 Upgrading to UNIVERGE 3C Version 8.5.2.3 Service Pack 3

This task describes the process for upgrading to service pack 3 after the base software to UNIVERGE 3C software version 7.1 to 8.5.2.3.

When and where to use:
Ensure that you have successfully upgraded from UNIVERGE 3C software version 7.1 to 8.5.2.3 and that you have the UNIVERGE 3C 8.5.2.3 Service Pack 3 Installation Disc 2.

Service Pack 3 is a mandatory software upgrade for the Enhanced Telephone Interconnect feature in an ASTRO® 25 radio system. SQL Server Authentication must not be used in a Joint Interoperability Test Command (JITC) certified installation, so during this procedure you configure the server for Windows Authentication mode only.

Procedure:

1 Once 8.5.2.3 upgrade is complete and the computer restarts, insert the UNIVERGE 3C 8.5.2.3 Service Pack 3 disk, run `setup.exe`, and follow prompts.

2 When the system prompts for confirmation for a momentary interruption, click **Yes**.

3 Reboot the server.

4 At the prompt, run **IP Phone Upgrades** as needed.

5 From the **3C Administration** main window, right-click the **System - Motorola Astro25** on the **General** tab and choose **View Properties**.

6 Click the **SIP** tab.

7 Update the **ZC SIP User Agent** parameter **Invite without SDP** to **Unsupported**.

8 Click **OK** to set the values.

The **User Agent Profile ZC SIP Trunk** dialog box closes.

9 Click **Apply** to save the new **SIP User Agent** settings.

10 If the ETI feature is configured with a telephony firewall, perform the following actions:

a On the desktop, double-click **3C Administrator**.

b In the **3C Administrator** main window, select the **Trunks** tab.

The available trunks display in the window.

c Right-click the trunk connecting IP PBX with external IP network.

d In the context menu that appears, select **View Properties**.

e Note down all values and configuration settings from the following tabs:

- **General**
- **Authorization**
- **Inward Routing**
- **Outward Routing**
- **Emergency Groups**
- **Settings**
- **Caller ID Rules**
- **Mobility**

f Close the **Properties** window by clicking **OK**.

g Click **+** next to the trunk connecting IP PBX with the customer’s external IP network to expand the navigation tree.

h Right-click the port that appears.

i Repeat step step 10 d.

j Note down all values and configuration settings from all tabs.

k Close the **Properties** window by clicking **OK**.

l Right-click the trunk connecting IP PBX with external IP network and press DELETE.

m Wait about 60 seconds and refresh the screen by pressing **F5**.

n If the SIP trunk is not re-discovered automatically, repeat previous step.

o Repeat steps from step 10 c to step 10 d.

p Restore all the previously noted down values and configuration settings.

q Close the **Properties** window by clicking **OK**.

r Repeat steps from step 10 g to step 10 h.

s Repeat step 10 d.

t Repeat steps from step 10 p to step 10 q.

u From the **Start** menu, select **Administrative Tools** → **Services**.

v In the **Services (Local)** section, right-click **Sphericall Service**.

w From the context menu that appears, select **Restart**.

x In the **Services (Local)** section, right-click **Sphericall TFTP**.

y From the context menu that appears, select **Restart**.

The upgrade from UNIVERGE 3C 7.1 to 8.5.2.3 SP3 is complete.