System Release 7.17
ASTRO® 25
INTEGRATED VOICE AND DATA

# Fault Management Reference Guide

NOVEMBER 2016

MN003270A01-A

# 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 particular system, or may be dependent upon the characteristics of a particular 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.

This page intentionally left blank.

# Contact Us

## Motorola Solutions Support Center

The Solutions Support Center (SSC) is the primary Motorola Solutions support contact. Call:

- Before any software reload.
- To confirm troubleshooting results and analysis before removing and replacing a Field Replaceable Unit (FRU) and Field Replaceable Entity (FRE) to repair the system.

| For... | Phone |
|---|---|
| United States Calls | **800-221-7144** |
| International Calls | **302-444-9800** |

## North America Parts Organization

For assistance in ordering replacement parts or identifying a part number, contact the Motorola Solutions Parts organization. Your first response when troubleshooting your system is to call the Motorola Solutions SSC.

| For... | Phone |
|---|---|
| Phone Orders | **800-422-4210** (US and Canada Orders)<br>For help identifying an item or part number, select choice 3 from the menu. |
|  | **302-444-9842** (International Orders)<br>Includes help for identifying an item or part number and for translation as needed. |
| Fax Orders | **800-622-6210** (US and Canada Orders) |

## 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 with the error
- A description of the error

We welcome your feedback on this and other Motorola Solutions manuals. To take a short, confidential survey on Motorola Solutions Customer Documentation, go to docsurvey.motorolasolutions.com or scan the following QR code with your mobile device to access the survey.

This page intentionally left blank.

# Document History

| Version | Description | Date |
|---|---|---|
| MN003270A01-A | Original release of the *Fault Management Reference Guide* | November 2016 |

This page intentionally left blank.

# Contents

**Copyrights.................................................................................................. 3**

**Contact Us.................................................................................................. 5**

**Document History.......................................................................................... 7**

**List of Figures............................................................................................. 15**

**List of Tables.............................................................................................. 17**

**List of Processes.......................................................................................... 19**

**List of Procedures.........................................................................................21**

**About Fault Management – System Perspective.................................................. 23**

What Is Covered In This Manual?............................................................. 23

Helpful Background Information............................................................... 23

Related Information.................................................................................. 23

**Chapter 1: Fault Management Introduction..........................................................25**

1.1 Overview...............................................................................................25

1.2 Obtaining Support...................................................................................25

1.2.1 Necessary Information.......................................................................25

1.2.2 Calling for Service.............................................................................26

1.2.3 Motorola Solutions Radio Rental........................................................ 26

1.2.4 Motorola Solutions Test Equipment Service Center............................... 27

1.3 Returning FRUs and FREs.......................................................................27

1.4 Recommended Test Equipment............................................................... 28

1.4.1 General Radio Workshop Test Equipment........................................... 28

1.4.2 Laptop Computer............................................................................. 30

1.4.3 Networking Test Equipment for Field Shop Use.....................................31

1.4.4 Portable and Mobile Radios.................................................................31

1.5 Routine Maintenance Best Practices...........................................................31

1.5.1 Maintaining Facilities and Structures.................................................. 31

1.5.2 Software Backup...............................................................................31

1.5.2.1 Software Backup Guidelines...........................................................32

1.5.3 Verification of System and Device Operation....................................... 33

1.6 Service Best Practices...............................................................................33

1.6.1 Best Practices Overview......................................................................33

1.6.1.1 Troubleshooting Tips.......................................................................34

1.6.2 Situation Analysis...............................................................................35

1.6.2.1 Situation Analysis Tips....................................................................36

1.6.3 Fault Isolation....................................................................................38

1.6.3.1 Fault Isolation Tips........ 38
1.6.4 Job Completion........ 40
1.6.4.1 Job Completion Tips........ 40
1.7 Problem Assessment Summary........ 41
1.8 General Safety Precautions........ 41
1.8.1 DC Mains Grounding Connections........ 43
1.8.1.1 Disconnect Device – Permanently Connected........ 43
1.8.1.2 Multiple Power Source........ 43
1.8.1.3 Connection to Primary Power........ 43
1.8.1.4 Replaceable Batteries........ 44
1.8.2 Maintenance Requiring Two People........ 44
1.8.3 Equipment Racks........ 44
1.8.3.1 Lifting Equipment Racks Horizontally........ 44
1.8.3.2 Lifting Equipment Racks Vertically........ 44
**Chapter 2: Fault Management Tools........ 47**
2.1 Unified Event Manager........ 47
2.1.1 Resolving System Events in UEM........ 49
2.1.2 Alarm Summary........ 50
2.2 MOSCAD Network Fault Management........ 51
2.2.1 SDM3000 Builder Application........ 51
2.3 Unified Network Configurator........ 52
2.4 Provisioning Manager........ 52
2.5 ZoneWatch........ 52
2.6 ATIA Log Viewer........ 53
2.7 Configuration/Service Software........ 53
2.8 Software Download Manager........ 54
2.9 Configuration Tool For MLC 8000........ 55
2.10 Local Logs and Administration........ 55
2.11 Network and Device Commands........ 56
2.11.1 Ping........ 56
2.11.2 Trace Route........ 57
2.11.3 Pathping........ 57
2.11.4 ARP........ 58
2.11.5 Ipconfig........ 58
2.11.6 Netstat........ 58
2.11.7 Nslookup........ 58
2.11.8 Telnet........ 58
2.11.9 SSH........ 59
**Chapter 3: Fault Management – System and Device Level........ 61**

3.1 Overview....61
3.2 Suggested System Monitoring....61
3.2.1 Isolating Faults in the Unified Event Manager....62
3.2.2 Viewing Alarms and Events Using the Unified Event Manager....63
3.3 System-Level Reliability....63
3.3.1 Multiple System Components....64
3.3.1.1 Dynamic System Resilience....64
3.3.1.2 Control Channel Backup....64
3.3.1.3 Multiple Remote Sites....64
3.3.1.4 Multiple Dispatch Consoles....65
3.3.1.5 Multiple Network Manager PCs....65
3.3.1.6 Router Links....65
3.3.1.7 Redundant Network Transport Components....65
3.3.2 Modes of Operation....66
3.3.2.1 Standard Operating Modes....66
3.4 RF Subsystem Reliability....69
3.4.1 ASTRO 25 Repeater Subsystem....69
3.4.1.1 ASTRO 25 Repeater Site Modes of Operation....69
3.4.2 Simulcast Subsystem....70
3.4.2.1 Simulcast Subsystem Modes of Operation....71
3.4.2.2 Single Transmitter Receiver Voting Subsystem – Modes of Operation....76
3.4.2.3 Simulcast Subsystem Behavior in Failure Scenarios....77
3.4.3 3600 RF Subsystems....80
3.4.3.1 3600 RF Subsystems – Modes of Operation....80
3.4.4 ISSI.1 Network Gateway Site....81
3.4.4.1 ISSI.1 Network Gateway Site – Modes of Operation....81
3.4.5 ISGW....82
3.4.5.1 ISGW – Modes of Operation....82
3.4.6 WAVE 7000 Site....82
3.4.6.1 WAVE 7000 Site Modes of Operation....82
3.4.7 Conventional Sites and Conventional Subsystems....82
3.4.7.1 Conventional Sites and Conventional Subsystems – Modes of Operation....82
3.5 PTP Device Fault Management....83
3.5.1 PTP Device Management – Description....83
3.5.1.1 PTP 800 Link Configurations....83
3.5.1.2 PTP Device Fault Management – Capacity and Capability....84
3.5.2 PTP in ASTRO 25 Architecture....84
3.5.2.1 PTP System Diagrams....84
3.5.2.2 PTP Device Deployment – Site Diagrams....90

3.5.3 PTP Device – Installation and Configuration Considerations.................................. 96
3.5.4 PTP Device Installation............................................................................................97
3.5.5 PTP Device – Operations......................................................................................... 98
3.5.5.1 Access to PTP Device..................................................................................98
3.5.6 PTP Device – Maintenance and Troubleshooting...................................................98
3.5.6.1 PTP Diagnostics and Device Command.................................................... 99
3.5.6.2 PTP Asset Management............................................................................. 99
3.6 Failure Categories.......................................................................................................... 99
3.6.1 Hard Failure............................................................................................................ 99
3.6.1.1 Troubleshooting Hard Failures....................................................................99
3.6.2 Intermittent Failure.................................................................................................102
3.6.2.1 Troubleshooting Intermittent Failures........................................................102
3.6.3 Configuration Failures............................................................................................103
3.6.3.1 Troubleshooting Configuration Problems..................................................103
3.6.4 Miscellaneous Failures.......................................................................................... 104
3.7 Traffic Plane Failures...................................................................................................105
3.7.1 Control Plane Failure............................................................................................ 105
3.7.1.1 Call Processing Failure............................................................................. 105
3.7.1.2 Call Management Failure..........................................................................105
3.7.1.3 Mobility Management Failure....................................................................106
3.7.1.4 InterZone Communications Failure...........................................................106
3.7.2 Audio Plane Failures..............................................................................................106
3.7.2.1 Subscriber Unit Failure..............................................................................106
3.7.2.2 Zone Controller Failure............................................................................. 106
3.7.2.3 SmartX Site Converter Failure.................................................................. 106
3.7.2.4 Voice Processor Module Failure............................................................... 106
3.7.2.5 Telephone Interconnect Device Failure..................................................... 106
3.7.2.6 Other Interconnect Failure Considerations............................................... 107
3.7.3 Data Plane Failures............................................................................................... 107
3.7.3.1 GGSN Failures..........................................................................................107
3.7.3.2 Packet Data Gateway – PDR or RNG Failures.........................................107
3.7.3.3 Border Gateway Failures........................................................................... 108
3.7.4 Network Management Plane.................................................................................108
3.7.4.1 Capacity Lost When Servers Fail..............................................................108
3.7.4.2 Subnet Structure........................................................................................ 110
3.8 Troubleshooting Services with Raw Display/ATIA Events...........................................110
3.8.1 Registration............................................................................................................111
3.8.2 Group Affiliation (Changing Talkgroups)................................................................112
3.8.3 Site Handover........................................................................................................ 112

3.8.4 Deregistration..........113
3.8.5 Group Call..........113
3.8.6 Private Call..........115
3.8.7 Telephone Interconnect Call..........117
**Appendix A: Service Laptop and Software Setup..........121**
A.1 Service Laptop Overview.......... 121
A.1.1 Service Laptop Requirements for CPS..........121
A.1.2 Service Laptop Requirements for RSS and CSS.......... 121
A.1.3 Service Laptop Requirements for SDM3000 Builder..........122
A.1.4 Service Laptop Requirements for Other Software..........122
A.2 Customer Programming Software..........123

This page intentionally left blank.

# List of Figures

Figure 1: Best Practices System Level Troubleshooting Model........ 34
Figure 2: Warning Label on Hot Modules........ 42
Figure 3: Lengths and Angles for Lifting Using the Eyenuts........ 45
Figure 4: Proper Alignment of the Eyenuts........ 46
Figure 5: New Mode of Operation........ 48
Figure 6: UEM Fault Management Diagnostic Flowchart........ 50
Figure 7: Methods for Accessing Local Logs and Administration Environments........ 56
Figure 8: Remote Site-A Put in the Malfunctioned State Because of Availability Number Trigger........ 76
Figure 9: Comparator to Channel Relationship........ 78
Figure 10: Loss of Site Link........ 78
Figure 11: User Disabled Channels........ 79
Figure 12: Loss of Control Channels........ 80
Figure 13: One Hop – T1 Single Link Using PTP........ 85
Figure 14: One Hop – T1 Redundant Link Using PTP........ 85
Figure 15: Two Hop – Ethernet Redundant Link Using PTP........ 86
Figure 16: PTP Ribbon Topology........ 87
Figure 17: PTP Hub and Spoke Topology........ 88
Figure 18: PTP Ribbon Topology – Customer Backhaul Reuse........ 89
Figure 19: PTP Ribbon Topology – Simulcast Backhaul Reuse........ 90
Figure 20: M3 system – T1/E1 Microwave Site Link with PTP........ 91
Figure 21: M1/M2 system – T1/E1 Microwave Site Link with PTP........ 91
Figure 22: M Core System – Microwave Ethernet Site Link with PTP........ 91
Figure 23: L Core System – Microwave Ethernet Site Link with PTP........ 92
Figure 24: ASTRO 25 Repeater Site T1 Microwave Site Link with PTP........ 92
Figure 25: ASTRO 25 Repeater Site Last Hop T1 with PTP........ 92
Figure 26: ASTRO 25 Repeater Site Ethernet Site Link with PTP........ 93
Figure 27: ASTRO 25 Repeater Site Last Hop Ethernet with PTP........ 93
Figure 28: IP Simulcast Prime Site T1 Microwave Site Link with PTP........ 94
Figure 29: IP Simulcast Remote Site Last Hop T1 Microwave Site Link with PTP........ 94
Figure 30: IP Simulcast Prime Site Ethernet Site Link with PTP........ 95
Figure 31: IP Simulcast Remote Site Last Hop Ethernet with PTP........ 95
Figure 32: MCC 7500 T1 with PTP........ 96
Figure 33: MCC 7500 Ethernet with PTP........ 96

This page intentionally left blank.

# List of Tables

Table 1: Equipment List....28
Table 2: General Troubleshooting Tips....34
Table 3: Situation Analysis Tips....36
Table 4: Fault Isolation Tips....39
Table 5: Job Completion Tips....41
Table 6: Ping Responses....57
Table 7: System Monitoring....61
Table 8: Devices That Impact Traffic Planes....105
Table 9: Lost System Capacity Due to Server Failure....108
Table 10: Registration – Raw Display Messages....111
Table 11: Group Affiliation – Raw Display Messages....112
Table 12: Site Handover – Raw Display Messages....113
Table 13: Deregistration – Raw Display Messages....113
Table 14: Group Call – Raw Display Messages....114
Table 15: Private Call – Raw Display Messages....116
Table 16: Telephone Interconnect Call – Raw Display Messages....118

This page intentionally left blank.

# List of Processes

PTP Device Installation ........................................................................................................................ 97

This page intentionally left blank.

# List of Procedures

Situation Analysis .................... 35
Fault Isolation .................... 38
Job Completion ....................40
Isolating Faults in the Unified Event Manager .................... 62
Hard Failure Isolation Approach .................... 100
Example of Hard Failure Isolation .................... 101

This page intentionally left blank.

# About Fault Management – System Perspective

This manual provides an introduction to system-level fault management. Included sections are a comprehensive introduction to the tools used for troubleshooting, and system-level troubleshooting.

## What Is Covered In This Manual?

This manual contains the following chapters:

- Fault Management Introduction on page 25, provides an overview of fault management from the system perspective.
- Fault Management Tools on page 47, provides the information about the tools used when solving problems at the system level.
- Fault Management – System and Device Level on page 61, provides the information and procedures to use when solving problems at the system level.

## Helpful Background Information

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

## Related Information

Refer to the following documents for associated information about the radio system.

**NOTICE:** Also see the manuals or online help for other software applications described in this manual.

| Related Information | Purpose |
|---|---|
| *Standards and Guidelines for Communication Sites* | Provides standards and guidelines that should be followed when setting up a Motorola communications site. Also known as the R56 manual.<br>This manual may be purchased on CD **9880384V83** 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. |
| *Unified Event Manager* manual and online help | Covers the use of Unified Event Manager (UEM), the application that provides reliable fault management services for devices in the ASTRO® 25 IV&D radio system. |
| *MOSCAD Network Fault Management* manual (and user guides/online help for software applications | Provides information required to install, configure, manage and use the MOSCAD® Network Fault Management (NFM), an optional ASTRO® 25 IV&D solution that provides tools to configure, monitor and control auxiliary system devices (such as tower |

| Related Information | Purpose |
|---|---|
| described in this manual) | lights, power, and environmental equipment) in communication sites. |

Chapter 1

# Fault Management Introduction

This chapter provides a high-level description of Fault Management and the function it serves on your system.

## 1.1 Overview

Most ASTRO® 25 systems use different types of equipment located various sites spread over a large geographic area. Other systems may be more centrally located, but understanding what fault management tools are available and how they operate will allow you to quickly identify the source and nature of a problem within the system.

System component modularity supports efficient fault management activities by supporting the quick replacement of Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) if necessary.

Motorola Solutions advanced manufacturing techniques and methodologies require the support equipment to be Advanced Test Equipment (ATE) based to provide Motorola Solutions depot service centers with the ability to repair defective boards if necessary.

## 1.2 Obtaining Support

Motorola Solutions recommends that you coordinate any repair activity through the Motorola Solution Support Center (SSC) to ensure that any problem is rectified in a timely fashion and that all warranty requirements are met.

Check your contract for specific warranty or extended warranty information for service by a Motorola service center. Motorola can provide technical support services throughout the life-cycle of a system. Along with other considerations, the subsequent sections describe information you should provide when you call Motorola Solutions service personnel and the addresses and telephone numbers of various Motorola Solutions service centers.

### 1.2.1 Necessary Information

Collect the following information before you call Motorola Solutions support staff:

- Location of the system
- Date the system was put into service
- Software/firmware versions used in the following:
  - ASTRO® 25 repeaters
  - Routers
  - Master site and RF site switches
  - Zone controllers
  - Network Management applications
  - Radio Control Management
  - Telephone Interconnect Device (TID)
  - Comparator

  - Servers
  - Software version of the Configuration/Service Software (CSS) used to program the equipment listed
  - Configuration Tool For MLC 8000
  - If available, MOSCAD NFM devices (GMCs, GWSs)
  - If available, SDM3000 Network Translators, SDM3000 RTUs
  - If available, FSA devices (AMCs, ALCs)
- Serial number of each device
- Symptom/observation of the problem:
  - When did it first appear?
  - Can it be reproduced?
  - What is the step-by-step procedure to cause it?
  - Do other circumstances contribute to the problem? For example, changes in weather or other conditions?
- Maintenance actions taken before the problem occurred:
  - Upgrade of software or equipment
  - Changed configuration – hardware and/or software
  - Reloaded software – from the backup or from a CD-ROM, its version and date
  - Device and System Logs (see individual device documentation for methods to collect such logs)

## 1.2.2 Calling for Service

After collecting the required information and writing a detailed problem report, contact one of the support centers. They can help with the problem. You can also obtain a Return Material Authorization (RMA) number for faulty FRUs and FREs from them. The following centers are available:

- Motorola Solution Support Center (SSC): see Contact Us on page 5.
- Motorola Radio Support Center:
  - Phone (800) 227-6772
  - Fax (800) 318-0281

**NOTICE:** The Motorola Radio Support Center repairs mobile and portable radios, and related RF equipment.

The North America Parts Organization is your source for manuals, replacement parts, and assemblies. For the telephone numbers, see Contact Us on page 5.

The address for the United States, Canada, Central America, and South America is:

Motorola Solutions, Inc. North America Parts Organization
2200 Galvin Drive
Elgin, IL 60123, USA

## 1.2.3 Motorola Solutions Radio Rental

Motorola Radio Rental group rents Motorola Solutions radios, mobiles, base stations, repeaters, and accessories.

The address for the United States, Canada, Central America, and South America is:

Motorola Radio Rental
1307 E. Algonquin Road
Schaumburg, IL 60196, USA

The telephone numbers are:

- (888)-736-8567 (domestic)
- (888)-615-2057 (fax)
- (800)-268-3395 (Canada only)

### 1.2.4 Motorola Solutions Test Equipment Service Center

The Motorola Test Equipment Service Center provides:

- Test equipment support
- Technical support
- Repair services
- Software support and upgrades
- Module exchange program
- Pre-scheduled calibrations
- Reconditioned equipment sales
- Equipment rentals

The Service Center telephone numbers are:

- (800)-323-6967
- Fax: (847)-783-2800

## 1.3 Returning FRUs and FREs

Return faulty FRUs or FREs to Motorola Solutions for repair. When you return a board or assembly for service, follow these best practices:

- Always use a static grounding wrist strap to handle any assembly containing CMOS devices.

  **IMPORTANT:**
  Many replacement FRUs are shipped without software installed.

  Your new FRU cannot be brought into service if the installed firmware has not been removed.
- Place any assembly containing CMOS devices in a static-proof bag or container for shipment.
- Obtain a Return Authorization (RA) number from the Motorola Solution Support Center (SSC) or Radio Support Center.
- Include the warranty, model, kit numbers, and serial numbers on the job ticket, as necessary. If the warranty is out of date, you must have a Purchase Order.
- Print the return address clearly in block letters.
- Provide a phone number where your repair technician can be reached.
- Include the name of the contact person for return.
- Pack the assembly tightly and securely, preferably in its original shipping container.

## 1.4 Recommended Test Equipment

This section contains information on the test equipment for maintaining and troubleshooting your system.

### 1.4.1 General Radio Workshop Test Equipment

Table 1: Equipment List on page 28 lists the general types of test equipment necessary for maintaining and troubleshooting your system. You can purchase equipment with Motorola Solutions part numbers from the Motorola North America Parts Organization.

Table 1: Equipment List

| Description | Motorola Part Number |
|---|---|
| **General Equipment** | |
| 150 MHz 4 Channel Digital Storage Oscilloscope | R1612B |
| Transmission Test Set (TIMS Set), Test Tablet and TIMS Module | R1683A |
| Aeroflex 3920 Service Monitor | R3920A and R2075A (P25) and R2076A (P25 Trunking) |
| 50 Ohm Terminated Load | T1013A |
| Antenna Tester 806–960 MHz | R1419A |
| Antenna Tester 80–520 MHz | RRDN6671A |
| Laptop Computer: see Laptop Computer on page 30. | |
| Punch Block Impact Tool | 66-80388A39 |
| MODAPT – RJ45 Breakout device | 8183069X01 |
| Remote RJ11/RJ-45 Cable tester, maximum length 365.7 m (1200 ft) | R1414A |
| PC Cable Tester (RG58, 59, 62, BNC, RJ45, RJ11, DB-9, DB15, DB25, Centronics 36 pin) | R1415A |
| Amprobe Instruments GP-1 Earth Tester | R1542A |
| AEMC Instruments 3731 Clamp-On Ground Resistance Tester – (http://www.aemc.com/products/index.asp) | See website |
| **Networking Tools for Field Shop Use** | |
| T1 or E1 Test Set | |
| **Equipment Specific to ASTRO-TAC® 9600 Comparators** | |
| Configuration/Service Software (CSS) | DLN6455A |
| CSS Programming Cable if Ethernet is not used | 3080369E31 |
| **Equipment Specific to GCP 8000 Site Controller** | |
| Configuration/Service Software (CSS) | DLN6455A |
| **Microwave Test Equipment** | |

*Table continued…*

| Description | Motorola Part Number |
|---|---|
| Agilent E4407B 9 kHz to 26.5 GHz Spectrum Analyzer | R1732A |
| Agilent E4418B Power Meter | |
| Agilent 8481D Power Sensor | |
| Agilent 8481H Power Sensor | |
| Agilent OmniBer 717 Performance Analyzer | |
| **Equipment Specific to ASTRO® Spectras** | |
| Radio Service Software (RSS) | RNV4184P |
| ASTRO® Spectra Programming Cable | 3080369B73 |
| RIB (Standard Radio Interface Box/battery powered) | RLN4008E |
| Smart RIB (same as RLN4008E, but includes Flash capability for upgrading software in radio user units; however, this unit is AC powered only) | RLN1015D |
| **Equipment Specific to ASTRO® Spectra Plus** | |
| CPS (Configuration Programming Software) | RVN4185D |
| ASTRO® Spectra Mobile Plus programming cable and RIB. There are many different options. See Service Brief SM-MO-0101 at Motorola Online: http://businessonline.motorolasolutions.comhttp://motonline.mot.com | |
| **Equipment Specific to ASTRO® Sabers** | |
| Radio Service Software (RSS) | RNV4184P |
| ASTRO® Saber Programming Cable | RKN4046A |
| RIB (Standard Radio Interface Box/battery powered) | RLN4008E |
| Smart RIB (same as RLN4008E, but includes Flash capability for upgrading software in radio user units; however, this unit is AC powered only) | RLN1015D |
| **Equipment Specific to XTS3000s** | |
| Radio Service Software (RSS) | RNV4184PK |
| XTS3000 Programming Cable | RKN4035D |
| RIB (Standard Radio Interface Box/battery powered) | RLN4008E |
| Smart RIB (same as RLN4008E, but includes Flash capability for upgrading software in radio user units; however, this unit is AC powered only) | RLN1015D |
| **Equipment Specific to XTS5000s** | |
| CPS (Configuration Programming Software) | RNV4184P |
| XTS5000 Programming Cable | RKN4105A (USB)<br>RKN4106B (RS232) |
| **Service Aids and Test Equipment for the GTR 8000** | |
| GTR 8000 Configuration/Service Software (CSS) | DLN6455K |
| GTR 8000 RS-232 programming cable (same as for QUANTAR® stations) | 3080369E31 |

*Table continued…*

| Description | Motorola Part Number |
|---|---|
| TDMA Mobile Emulator (Requires 390XOPT200 and 390XOPT201 and 390XOPT220) — Aeroflex option for the 3920 service monitor | 390XOPT245 |
| TDMA Test Suite (Requires 390XOPT200 and 390XOPT201) — Aeroflex option for the 3920 service monitor | 390XOPT220 |
| TDMA Advanced Test Suite - Combines 390XOPT220 & 245 (Requires 390XOPT200 and 390XOPT201) — Aeroflex option for the 3920 service monitor | 390XOPT262 |
| **Service Monitor HPD Options** | |
| HPD Testing Option — Aeroflex option for the 3920 service monitor | R2091A<br>390XOPT300 |
| HPD Advanced Analysis Package — Aeroflex option for the 3920 service monitor | R2092A<br>390XOPT301 |
| HPD Testing Suite (Incl. R2091A/R2092A) — Aeroflex option for the 3920 service monitor | R2093A 3900 HPD Test Suite |
| **Equipment Specific to MLC 8000 Comparators** | |
| MLC 8000 Configuration Tool with Analog Display and Control | |
| Rohde&Schwartz NRT-Z14 Directional Power Sensor 25-1000 GHZ 0.1-120W Recommended for all uses. Average reading power meter for use when a service monitor is not available. | |
| Digital Multimeter (DMM) | |
| RJ45–to-RJ45 one-to-one cable | FKN8695A |
| DB9 to RJ45 Adaptor | |
| ESD field service kit | |
| **Equipment specific to SDM3000 Network Translators (SNTs) and SDM3000 RTUs** | |
| SDM3000 Builder | F5597 |

## 1.4.2 Laptop Computer

A laptop computer is a valuable tool for most troubleshooting. You can use it to obtain information about the functioning of system components and the transport architecture between sites.

Primary uses of your laptop include:

- Quick checking of component status and configuration, and reconfiguration where required.
- Saving hard and soft copies of all configuration information for a system.
- Configuring and servicing base radios with the CSS application.

  **NOTICE:** CSS is not used to program radios. CPS is used for that function.

- Running remote diagnostics when the system is equipped with a dialup modem, or through a T1/E1 cable connection.

For more details about the laptop, see Service Laptop and Software Setup on page 121.

### 1.4.3 Networking Test Equipment for Field Shop Use

The following networking test equipment is required for testing the LAN/WAN devices and their associated links:

- Handheld T1/E1 test set
- Serialtest Software with ComProbe
- SerialBERT opt

### 1.4.4 Portable and Mobile Radios

Portable and mobile units, if programmed correctly and included and configured correctly in the database, may be effective in gathering troubleshooting information.

- As a valid radio user, you may be able to duplicate the problem being reported and/or talk with other users who have experienced the problem.
- Depending on the nature of the problem, it may be useful to place a call to a specific site to isolate the cause of the problem.

## 1.5 Routine Maintenance Best Practices

You can avoid many system problems through routine maintenance. Performing maintenance tasks on a regular basis allows you to become familiar with normal system operation. It helps you spot anomalies before they become problems. Monitoring system health lets you repair failing devices before they cause operation problems.

Motorola Solutions designed your system with redundancy and fault tolerance to lessen the chance of a failure degrading the system operation. Repairing a failed or failing device helps maintain redundancy and fault tolerance.

### 1.5.1 Maintaining Facilities and Structures

Maintaining the facilities and structures that contain your system hardware is important. The structures keep the electrical subsystems out of the weather. They also provide a stable and secure platform for their operation. Motorola Solutions provides specifications for the construction of the facilities that you must maintain to ensure long system life.

See *Standards and Guidelines for Communication Sites* (6881089E50), also known as the *R56* manual, for specific information.

### 1.5.2 Software Backup

This section discusses the reasons for software backup, and general guidelines for backup.

Software controls your system on many levels, from the device firmware to the system-level software that controls and maintains:

- User data
- System configuration data
- System and device health

Specific software backup procedures are covered in the individual device-level manuals. For system-wide backups and disaster recovery procedures using the Backup and Restore Server (BAR), see the *Backup and Restore Services* manual. The following devices also use software backup procedures:

- Network Management servers, described in the *Private Network Management Servers* manual
- Zone controller, described in the *Zone Controller* manual
- InfoVista, described in the *InfoVista* manual
- Routers (all), described in the *Unified Network Configurator* manual
- LAN switches (all), described in the *Unified Network Configurator* manual

If system software applications do not contain correct, up-to-date radio user data, users can encounter problems when they attempt to communicate. If the system does not contain correct device status data, the system does not allocate resources properly. Therefore, it is essential to back up your system data (for example, radio CSS data) as well as your device data, on a regular basis.

Your organization should develop and maintain a system for data backup. In many organizations, the system administration team is responsible for developing the backup process and performing backups. However, as a service manager it is your responsibility to verify that the backups are performed as specified in your plan. That way, in case of a failure, you can reconstruct the operational system more easily.

### 1.5.2.1 Software Backup Guidelines

The following list provides general guidelines for backing up software and databases on your system:

- Institute and document a backup program. There are disasters specific to certain regions (such as tornadoes or earthquakes) that may require other storage considerations. Rebuilding a damaged site is much easier when valid configuration data is available for reload.
- Perform a backup any time a maintenance action may affect system data or configuration. This enables you to restore properly configured software and data if you find a problem later.
- Schedule backups at times that affect the fewest users.
- Use more than one backup CD for each device, preferably enough to provide incremental backups and at least one historical backup. For example, use a different backup CD for each month/configuration change, and a backup CD to provide a four-month historical archive.

  **NOTICE:** It is recommended to use Sony or Memorex CD-RW media for storing backups. Do not reuse the CD more than 50 times for storing backups.
- Make two copies of each backup:
  - One for off-site storage
  - One for on-site access
- Store backup CDs to ensure that the data is archived in a way that provides a history of system changes. This practice is helpful if a configuration change causes a problem in system operation.
- Clearly identify the backup CDs with an identifying code such as the specific date or event for which they were made.
- Consistently and accurately log the backup CDs by their identifying code and the specific backup usage. This practice is necessary for system recovery in case they are required for reloading the data or system.
- Store one set of backup CDs off-site or in a fireproof vault to protect them in case the site suffers damage. Store the other set of backup CDs on-site in a fireproof vault.

## 1.5.3 Verification of System and Device Operation

The Unified Event Manager (UEM) is a fault management application designed for the following critical fault management functions:

- Discovering devices
- Reporting faults
- Detecting and reporting the loss of communication and synchronization
- Ability to fault manage PTP (Point-to-Point) Wireless Ethernet Bridge devices (optional)

For additional information on UEM operation, see the *Unified Event Manager* manual.

Check the Unified Event Manager periodically throughout each shift to see the current state of system functionality. See the *Unified Event Manager Online Help* or the *Unified Event Manager* manual for techniques that allow you to set your viewing and display preferences.

Periodic reviews of the system's operational status and individual device health are important from a maintenance viewpoint. Understanding your system allows you to prioritize alarms and plan system maintenance more accurately. For instance, if a device experiences sporadic loss of a link, there is a need to investigate and correct the problem, even though system capabilities may be unaffected. Knowing that the problem exists, but does not affect system operation, allows you to schedule its repair for a convenient time, without unnecessarily engaging the staff.

The network fault management application is a useful tool in assessing system health. Review the alarms, faults, and device statuses reported to the fault manager throughout each shift to ensure that devices and links are operating normally.

If InfoVista is purchased, critical device reports are generated periodically to check for trends or symptoms of possible problems that may influence the system.

# 1.6 Service Best Practices

This section provides an overview of a logical approach to troubleshooting system-level problems.

## 1.6.1 Best Practices Overview

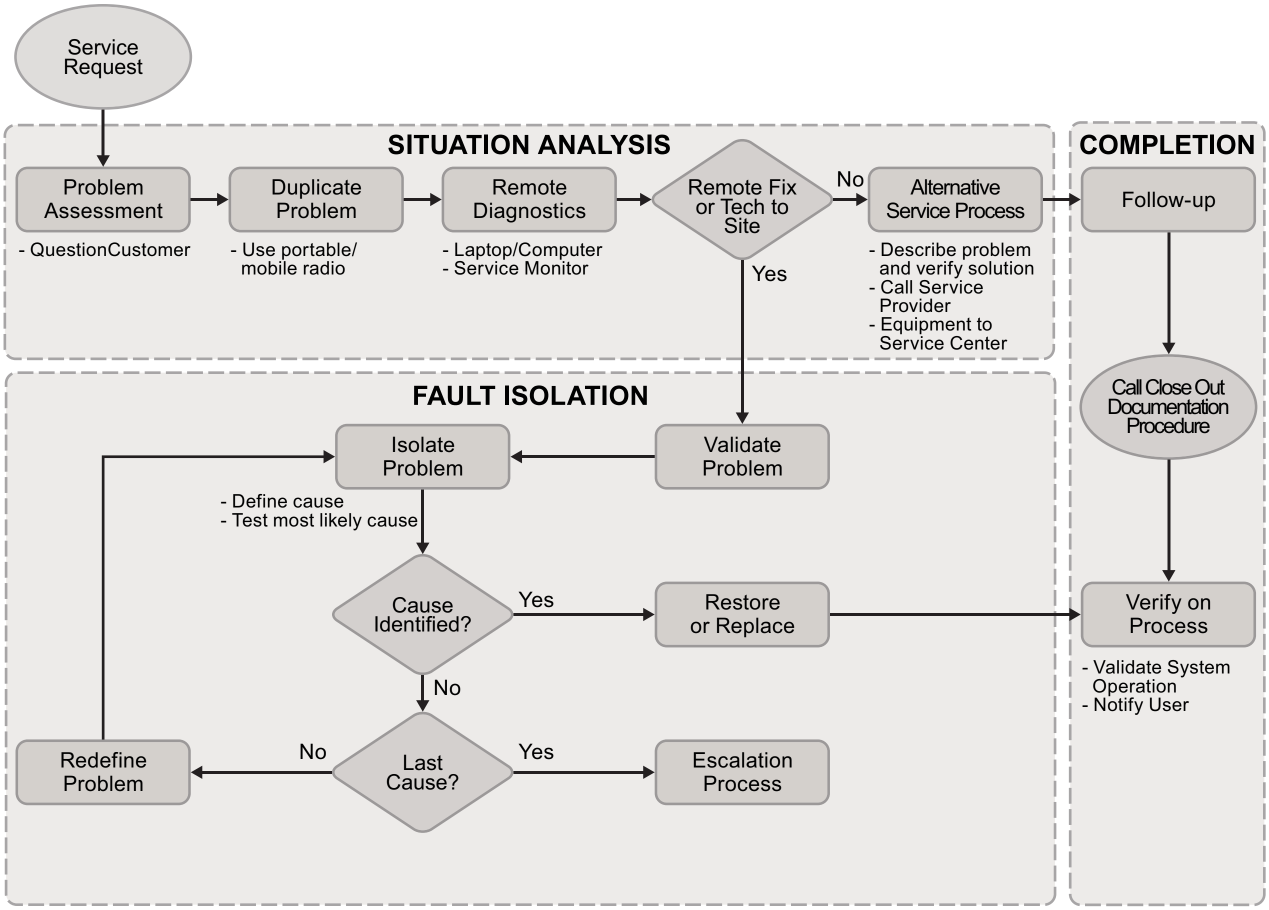
The Best Practices System Level Troubleshooting Model has a situation analysis, fault isolation/ location, and a completion phase. The model is shown in Figure 1: Best Practices System Level Troubleshooting Model on page 34 and can be summarized as follows:

- **Fault isolation** section in which the problem, symptom, or fault is validated, where possible, and the problem is isolated to one or more FRUs. The fault isolation phase depends heavily on the outcome of the situation analysis phase, plus a further use of system tools and techniques, and troubleshooting aids.
- **Completion** section which varies from shop to shop. However, it usually includes verification that the problem has been solved and that all customers are satisfied with the results.

**NOTICE:** The Troubleshooting Model:

- Is intended as one approach
- Is based on the assumption that you understand the system
- Provides a framework for approaching problems

**Figure 1: Best Practices System Level Troubleshooting Model**



### 1.6.1.1
## Troubleshooting Tips

Table 2: General Troubleshooting Tips

| Tip | Description |
|---|---|
| Educate your customers and let them educate you. | Let your customers help you in diagnosing the problem.<br>• If appropriate, ask them what they think might be the cause.<br>• If they are causing the problem, educate them on what to do to avoid the problem. |
| Make sure that someone in your service organization has a backup copy of the latest system database. | Establish routine backup and archive procedures tailored to your system. |
| The larger the system, the more time you may need to spend learning it and identifying the potential problems or causes before attempting a solution. | Have inexperienced technicians learn the system by performing preventive maintenance. |

*Table continued…*

| Tip | Description |
|---|---|
| Understand the system. | • For wide area systems, you need a basic understanding of digital telecommunications and networking concepts (for example, T1 and Ethernet).<br>• Understand the system configuration. If a system is complex, break it down into a usable block diagram. Understand how the individual devices work together.<br>• Keep up to date on product service bulletins. |
| Avoid assumptions. | • Do not draw conclusions.<br>• Consider all reasonable possibilities. |
| Keep authorized staff informed. | • Keep the dispatcher informed for efficient routing of service calls.<br>• Keep end-user customers informed.<br>• If problem resolution is a longer term process, keep customers advised of your progress. |

1.6.2
## Situation Analysis

The Best Practices situation analysis lists several steps, as illustrated in Figure 1: Best Practices System Level Troubleshooting Model on page 34.

**Procedure:**

1 Assess the problem.

| If… | Then… |
|---|---|
| **You learned about the problem from a Radio User call** | **a** Interview the user to verify the exact nature of the problem. Try to determine information such as the radio IDs of the involved radios, any talkgroups that were involved, as well as any sites or channels. Also attempt to determine the time of the call and the OmniLink call ID.<br>**b** Continue with step 2. |
| **You learned about the problem from an alarm** | Continue with step 2. |

2 Try to duplicate the problem.

| If… | Then… |
|---|---|
| **You know the source of the problem** | Continue with Fault Isolation on page 38. |
| **You do not know the source of the problem** | Continue with step 3. |

3 Use the Unified Event Manager, MOSCAD Network Fault Management, CSS, or other applications to diagnose the problem; verify the Provisioning Manager if the problem is isolated to a particular radio or talkgroup. If InfoVista has been purchased, check reports for critical transport devices to determine further causes of the particular problem.

| If… | Then… |
|---|---|
| **You know the source of the problem** | Continue with Fault Isolation on page 38. |
| **You do not know the source of the problem** | Continue with step 4. |

**4** Send someone to the site to diagnose the problem.

| If… | Then… |
|---|---|
| **You know the source of the problem** | Continue with Fault Isolation on page 38. |
| **You do not know the source of the problem** | Continue with step 5. |

**5** Escalate the problem. Call Motorola Solution Support Center (SSC) at this point for help.

1.6.2.1
## Situation Analysis Tips

The situation analysis tips are as follows:

- All fault isolation begins with a thorough understanding of the problem:
  - **Be sure that you understand what your radio users mean.** For example, the comment “I am having a receive problem” may either mean “I am having a hard time hearing some transmissions” or “radio users are not receiving me”. Talk to the user to find out what is really wrong so that you do not go off in the wrong direction. Rephrase what you hear, and ask the question in another way: “You mean you do not hear all of the traffic?”
  - **Try and duplicate the problem.** For example, you might be able to use your portable or mobile unit to duplicate such problems as dropouts, distortion, and the inability to access a feature. Your portable may also help you quickly establish whether a site is in wide or site trunking, and eliminate other parts of the system as “probably OK”.
  - **Use remote diagnostic tools** (such as analog remote access or web browser tools) if you cannot duplicate the problem.

    In some cases, for example when tower lights are out, power is down, or in the case when transport architecture problems occur, you may have to use alternative processes.
- The assumptions you make during the situation analysis portion of the call influence the rest of the troubleshooting process. If your initial assumptions are accurate, you can isolate and fix the problem quickly. Conversely, if your assumptions are inaccurate, you may miss something important or make it difficult to solve the problem. Because these initial assumptions are important, do not jump to conclusions about the cause of the problem. While front-end analysis sometimes seems a waste of time, using all of the tools and aids at your disposal pays large dividends.
- Finally, the situation analysis section is a systematic and logical set of steps for tackling a problem. Motorola Solutions experience shows that a systematic approach is the best practice for solving system problems.

Table 3: Situation Analysis Tips

| Tip | Description |
|---|---|
| Get as much information as possible from customers to identify the cause of the problem. | • Talk with the person who is most familiar with the system.<br>• Verify what customers said, so that you can eliminate incorrect information and avoid wasted effort.<br>• Ask the question in a different way to see if you get the same answer. |

*Table continued…*

| Tip | Description |
|---|---|
| If multiple customers (or users) are affected, monitor all channels. | Eliminate channels with no problems. If many customers are having the same problem, it is typically at the central site. Sometimes an intermittent problem is really a continuous problem affecting only one or two channels. |
| Try to identify where and when a problem occurred. | • Ask these questions:<br>- How many people experienced the problem?<br>- How many people are currently working?<br>- Can you do a roll call? The dispatcher calls and listens to all radios. This enables you to listen to radios in all locations. You can then speak directly to people having the problem.<br>- Where were you when the problem occurred?<br>• Do not predetermine the cause of a complaint. Keep an open mind for other possible causes.<br>• Try to contact the user directly to clarify the problem. For example, the comment “I am having a receive problem” might really mean, “People are having trouble receiving me”. |
| Identify the bad site in a multi-site system. | • Use system diagnostics tools to lead you to the problem site.<br>• Analyze the customers’ input to see if a particular geographic area is affected. |
| Perform checks to locate the problem. | • Check diagnostics.<br>• Check for alarms.<br>• Review equipment history.<br>• Isolate to a geographic area.<br>• Identify which area the problem is in:<br>- Identify the sites, which could affect an area<br>- Visit remote sites<br>• Use portables to monitor site channels, activity, and interconnect.<br>Constantly use radios to monitor the system when in-transit, so you can determine what the system is doing. |
| Use available equipment, software, and techniques. | Use the following whenever possible:<br>• Portable radio (with all system functions). Use it to listen to system while driving to site to identify and verify the problem<br>• Laptop Computer<br>• Remote terminal emulation, Unified Event Manager, CSS, MOSCAD NFM, and ZoneWatch<br>• Local Diagnostics – Inspect LEDs and cables, command line commands<br>• History of system database problems<br>• System documentation/information |

*Table continued…*

| Tip | Description |
|---|---|
| Determine if external situations may have caused the problem. | Ask these questions:<br>• Was there a power surge or lightning strike in the area?<br>• Did a storm front pass through?<br>• Are there any new radio structures in the area? |

1.6.3
## Fault Isolation

**Procedure:**

1. Validate the problem at the site, or in the subsystem.
2. Isolate the problem to a particular Field Replaceable Unit (FRU) or Field Replaceable Entity (FRE).
    1. Define the cause of the problem.
    2. Test the most likely causes. A particular problem or alarm could be due to several different causes. You may have to evaluate several different causes for any given problem.

| If… | Then… |
|---|---|
| **you identified the cause of the problem** | make the necessary fix. This may require:<br>• Reloading software or database(s), or<br>• Replacing a FRU or a FRE.<br>Continue with Job Completion on page 40. |
| **you did not identify the cause of the problem, but there are other possibilities to test** | Continue repeating step 2 until you either:<br>• successfully identify the cause of the problem and can continue with Job Completion on page 40, or<br>• run out of possible causes to test. If you run out of possible causes, continue with step 3. |

3. If you are unable to isolate the problem and you have no more possible causes to test, you must escalate the process. The escalation process you follow may be unique to your network. In most cases, however, it involves more skilled technicians, either from Motorola Solutions or Motorola Solutions-approved contractors. The technicians repeat this process until a primary cause of the problem is identified. When the primary cause of the problem is identified and fixed, continue with Job Completion on page 40.

1.6.3.1
### Fault Isolation Tips

Remember these points when you perform the fault isolation and location process:

- No matter how sure you are that the information gathered in the Situation Analysis step is correct; verify it at the site or subsystem.
- Sometimes the verification process involves sending a technician to the site to plug in to the equipment (such as repeaters or a site controller). Do it to verify information or to gain detailed information you might not be able to obtain remotely in your system.
- On-site visual inspections can yield information that is unavailable online:

  - Visual inspection may show evidence of things like mechanical damage, rodents, or electrical burn marks.
  - Visual inspection includes checking the LEDs on the equipment. Look to see if the LEDs are lit, flashing, or steady. Check the color of the LEDs. What do the indicators tell you about each object?
- If the first tested “cause” turns out not to be the problem, you may have to check one or more additional causes.
- Know when to call for help. Sometimes you do not find the problem, and redefining the problem does not get you any further. In such cases, call a group leader, service manager, a more experienced technician, or the Motorola Solution Support Center (SSC).
- Remember not to get stuck in a loop – use the process of elimination to determine what is working, then concentrate on what is not.

Table 4: Fault Isolation Tips

| Tip | Description |
|---|---|
| Be prepared. Have a plan before taking any action. | • Know what to consider when replicating a problem.<br>• Replicate and experience the problem.<br>• Ask yourself, “What can make it happen?”<br>• When resetting equipment, collect all diagnostics/messages so you do not lose valuable data.<br>• As a last resort, if you cannot identify the cause of the problem, do a complete optimization of the entire system.<br>• On large systems distributed over a wide area, it may be helpful to go out in pairs.<br>• Verify that your test equipment is calibrated and working properly.<br>• Make sure that you have the proper tools to do the job. |
| Use system diagrams. | • Keep up-to-date block diagrams on hand.<br>• Use the elimination process. |
| Do not assume that any previous system condition/alignment did not change. | Verify whether system parameters have changed. |
| Verify what is not the problem. | • Identify what is **not** causing a problem by using the process of elimination.<br>• Test for the most probable cause first. |
| “Divide and conquer”. | Break the system down into smaller, more manageable blocks (subsystems). |
| Know your system. | • Consult appropriate technical documentation.<br>• Consult appropriate end-user system documentation.<br>• Know how to check and monitor each subsystem/component.<br>• Know how to determine if a subsystem/component is working. |

*Table continued…*

| Tip | Description |
|---|---|
| | • Know how to isolate problems to the subsystem/component.<br>• Look at a subsystem/component, then look at other subsystems/components it interacts with. |
| Always recheck your test results. | • What you do can affect other aspects of the system.<br>• If you get questionable results, recheck your test procedures. |
| Use visual inspection techniques. | • Determine which LEDs are illuminated.<br>• Determine their color, state, and meaning.<br>• Ensure that all boards in a card cage are seated properly. |

1.6.4
## Job Completion

The final element in the Best Practices model is job completion. Once again, it depends on your specific shop or your organization's procedures. If you use an alternative service process, follow up and make certain that the problem has been solved. Also, make sure that your customers are satisfied, and that all paperwork is completed.

The following steps show an example of a job completion process.

**Procedure:**

1. Verify that the problem has been solved or corrected.

   **NOTICE:** If you need to use an outside source (such as a Motorola Solutions technician or a third-party repair facility), you may need to follow up with that source to confirm that they have finished making repairs.

   | If… | Then… |
   |---|---|
   | **the problem is solved or corrected** | • notify the stakeholders who are responsible for the system.<br>• continue with step 2. |
   | **the problem is not solved or corrected** | • retrace and repeat the Fault Isolation Process. In some cases you may need to repeat the Situation Analysis Process because your initial diagnosis of the cause of the problem was incorrect.<br>• if you cannot solve or correct the problem after repeated attempts, escalate the problem. |

2. Document the nature of the problem, the ultimate cause of the problem, and the repairs or configuration changes that corrected the problem.
3. Close out the Service Request call according to your organization's standard operating procedure.

1.6.4.1
### Job Completion Tips

The job completion tips listed in Table 5: Job Completion Tips on page 41 emphasize the importance of maintaining system documentation. It involves configurations, site logs, and other related information, especially when changes or upgrades are made to fix problems or improve system capabilities.

Table 5: Job Completion Tips

| Tip | Description |
|---|---|
| Update records and configuration documents. | • Develop your own system documentation and flowcharts for each system you are responsible for.<br>• Maintain and enforce standards for consistency. Keep copies of system documentation in the trucks, at the site, in the shop.<br>• Set up a problem, procedures, and a maintenance database.<br>• Maintain a site log. |
| Maintain a site log. | • Log all equipment readings.<br>• Document all problems and all changes at each site.<br>• If the problem is intermittent, leave a note in the site log because the same technician may not always be the one to return to the next call. |
| Verify that the customer's problem has been resolved. | Notify your customers of the fix and have them verify proper system operation, then re-verify yourself. |

## 1.7 Problem Assessment Summary

The following list summarizes an approach to Problem Assessment:

- The easiest and most basic check of the system is to use the Unified Event Manager to check system health. If unresolved changes of state are noted, correct them at the earliest. It is a basic step for all problem solving.
- Resources are critical in all trunked systems. It applies especially to a system in which the lack of resources can easily prevent a particular call type from being completed.
- Resources must be available and correctly configured.
- Some radio user complaints are normal in all complex telecommunication systems.
- The level of expertise among users varies, which can potentially cause complaints.

## 1.8 General Safety Precautions

⚠ **CAUTION:** Compliance with Federal Communications Commission (FCC) guidelines for human exposure to Electromagnetic Energy (EME) at Transmitter Antenna sites generally requires that Personnel working at a site shall be aware of the potential for exposure to EME and can exercise control of exposure by appropriate means, such as adhering to warning sign instructions, using standard operating procedures (work practices), wearing personal protective equipment, or limiting the duration of exposure. For more details and specific guidelines, see Appendix A of *Standards and Guidelines for Communications Sites* (6881089E50).

Observe the following general safety precautions during all phases of operation, service, and repair of the equipment described in this manual. Follow safety precautions necessary for the safe operation of all equipment. See the appropriate section of the product service manual for additional safety information. Because of the danger of introducing additional hazards, do not install substitute parts or perform any unauthorized equipment modifications.

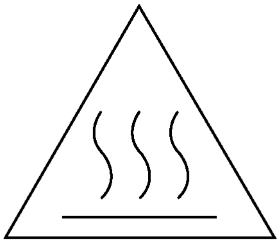
**NOTICE:** The installation process requires preparation and knowledge of the site before the installation begins. Review installation procedures and precautions in *Standards and Guidelines for Communications Sites* (6881089E50), before performing any site or component installation.

Always follow all applicable safety procedures, such as Occupational Safety and Health Administration (OSHA) requirements, National Electrical Code (NEC) requirements, local code requirements, safe working practices, and good judgment. General safety precautions include the following:

- Read and follow all warning notices and instructions marked on the product or included in this manual before installing, servicing, or operating the equipment. Retain these safety instructions for future reference.
- If you are troubleshooting the equipment while power is on, be aware of the live circuits.
- Do not operate the radio transmitters unless all RF connectors are secure and all connectors are properly terminated.
- Ground all equipment in accordance with *Standards and Guidelines for Communications Sites* (6881089E50), and specified installation instructions for safe operation.
- Slots and openings in the cabinet are provided for ventilation. Do not block or cover openings that protect the devices from overheating.
- Only a qualified technician familiar with similar electronic equipment should service the equipment.
- Some equipment components can become hot during operation. Turn off all power to the equipment and wait until sufficiently cool before touching.
- Maintain emergency first aid kits at the site.
- Have personnel call in with their travel routes to help ensure their safety while traveling between remote sites.
- Institute a communications routine during certain higher risk procedures. have an on-site technician continually update management or safety personnel of the progress so that help can be dispatched if needed.
- Never store combustible materials in or near equipment racks. The combination of combustible material, heat, and electrical energy increases the fire safety hazard.
- Equipment shall be installed in site to meet the requirements of a “restricted access location”, per UL60950-1, which is defined as follows: “Access can only be gained by service persons or by a user who has been warned about the possible burn hazard on equipment metal housing. Access to the equipment is through the use of a tool or lock and key, or other means of security, and is controlled by the authority responsible for the location”.

**WARNING:** Burn hazard. The metal housing of the product may become extremely hot. Use caution when working around the equipment.

**Figure 2: Warning Label on Hot Modules**



**CAUTION:**

Ground all antenna transmission line shields in compliance with Motorola R56 requirements.

Protect all antenna transmission lines by transient suppression devices in compliance with Motorola R56 requirements.

DC input voltage shall be no higher than 60 VDC. This maximum voltage shall include consideration of the battery charging “float voltage” associated with the intended supply system, regardless of the marked power rating of the equipment. Failure to follow this guideline may result in electric shock.

**WARNING:** RF energy burn hazard. Disconnect power in the cabinet to prevent injury while disconnecting and connecting antennas.

**IMPORTANT:** Use Motorola Solutions trained personnel to service all equipment.

1.8.1
## DC Mains Grounding Connections

**CAUTION:** This equipment is designed to permit the connection of the grounded conductor of the DC supply circuit to the grounding conductor at the equipment. If this connection is made, meet all of the following conditions:

- Place the equipment in the same immediate area (such as, adjacent cabinets) as any other equipment that has a connection between the grounded conductor of the same DC supply circuit and the grounding conductor, and also the point of grounding of the DC system. Ground the DC system elsewhere.
- Connect this equipment directly to
  - The DC supply system grounding electrode conductor
  - A bonding jumper from a grounding terminal bar
  - A bonding jumper from a grounding terminal bar
  - A bus in which the DC supply system grounding electrode conductor is connected
- Place the DC supply source within the same premises as the equipment.

  **NOTICE:** Switching or disconnecting devices must not be in the grounded circuit conductor between the DC source and the point of connection of the grounding electrode conductor.

1.8.1.1
### Disconnect Device – Permanently Connected

Incorporate a readily accessible disconnect device (circuit breaker or switch) in the building installation wiring.

1.8.1.2
### Multiple Power Source

This product has multiple power sources. If service requires the power source to be removed, disconnect all input (AC and DC) to completely remove power from the equipment before servicing it.

1.8.1.3
### Connection to Primary Power

For supply connections, use wires suitable for at least 167 °F (75 °C.)

### 1.8.1.4 Replaceable Batteries

**DANGER:** Risk of explosion if you replace the battery with an incorrect type. Dispose of the used batteries according to the instructions.

## 1.8.2 Maintenance Requiring Two People

Identify maintenance actions that require two people to perform the repair. Two people are required when:

- A repair has the risk of injury that would require one person to perform first aid or call for emergency support. An example would be work around high voltage sources. If an accident occurs to the first person, a second person may be required to remove power and call for emergency aid.
- Use the National Institute of Occupational Safety and Health (NIOSH) lifting equation to determine whether a one or two person lift is required when removing or replacing a system component in its rack. The NIOSH equation is found in the *NIOSH Publication* (Pages 94 to 110).

## 1.8.3 Equipment Racks

Do not lift equipment racks without the use of lifting equipment unless sufficient personnel are available to ensure that regulations covering health and safety are not breached. Motorola Solutions recommends the use of an appropriate powered mechanical lifting apparatus for moving and lifting the equipment racks. In addition to these points, refer to and comply with any local regulations that govern the use of lifting equipment.

**WARNING:** Crush hazard could result in death, personal injury, or equipment damage. Equipment racks can weigh up to 360 kg (800 lb). Follow the instructions in this section for proper lifting procedures.

### 1.8.3.1 Lifting Equipment Racks Horizontally

In some cases, equipment racks are shipped in horizontal position. Use the appropriate lifting apparatus to lift the racks upright. Comply with all applicable health and safety regulations, and any other regulations applicable to lifting heavy equipment.

**WARNING:**

- Do not use the eyenuts mounted on the top of the rack to lift the rack upright from a horizontal position. The eyenuts are not designed to lift horizontally and, if used improperly, could fail resulting in damage to equipment or injury to personnel.
- Crush hazard: could result in death, personal injury, or equipment damage.

### 1.8.3.2 Lifting Equipment Racks Vertically

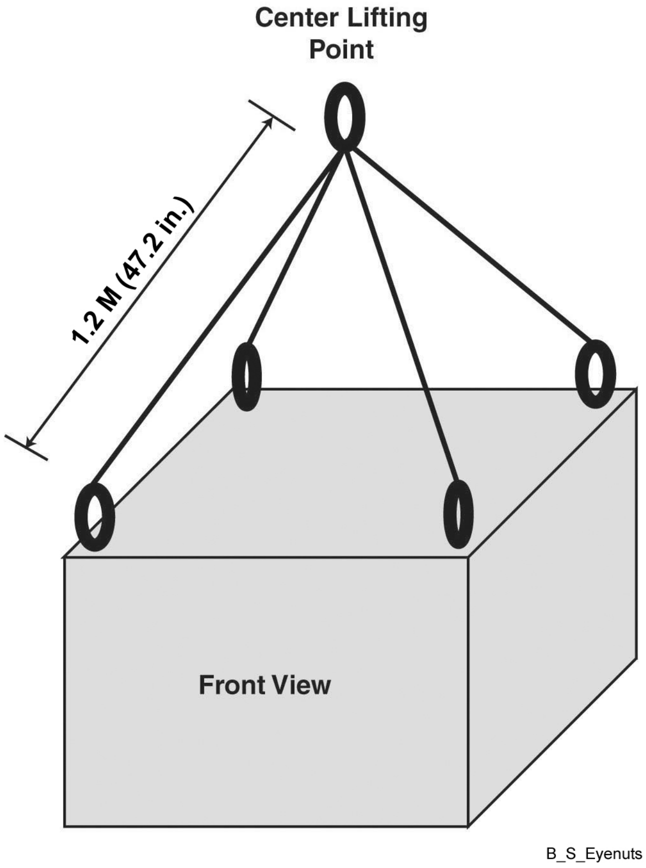
Some equipment racks have four M10 eyenuts mounted in the top of the rack. Use these eyenuts to lift the equipment rack vertically. Before using these eyenuts, visually check them and the rack hardware for any damage that may have occurred during shipping.

**WARNING:** If damage is apparent, do not use the eyenuts. Contact Motorola Solutions for replacements.

Use all four eyenuts when lifting the equipment rack. The minimum distance from each eyenut to the lifting point must be 1.2 m (47.2 in.) Using shorter length than specified could cause the eyenuts to fail.

Figure 3: Lengths and Angles for Lifting Using the Eyenuts on page 45 shows the minimum lengths and proper lifting angles using the eyenuts.

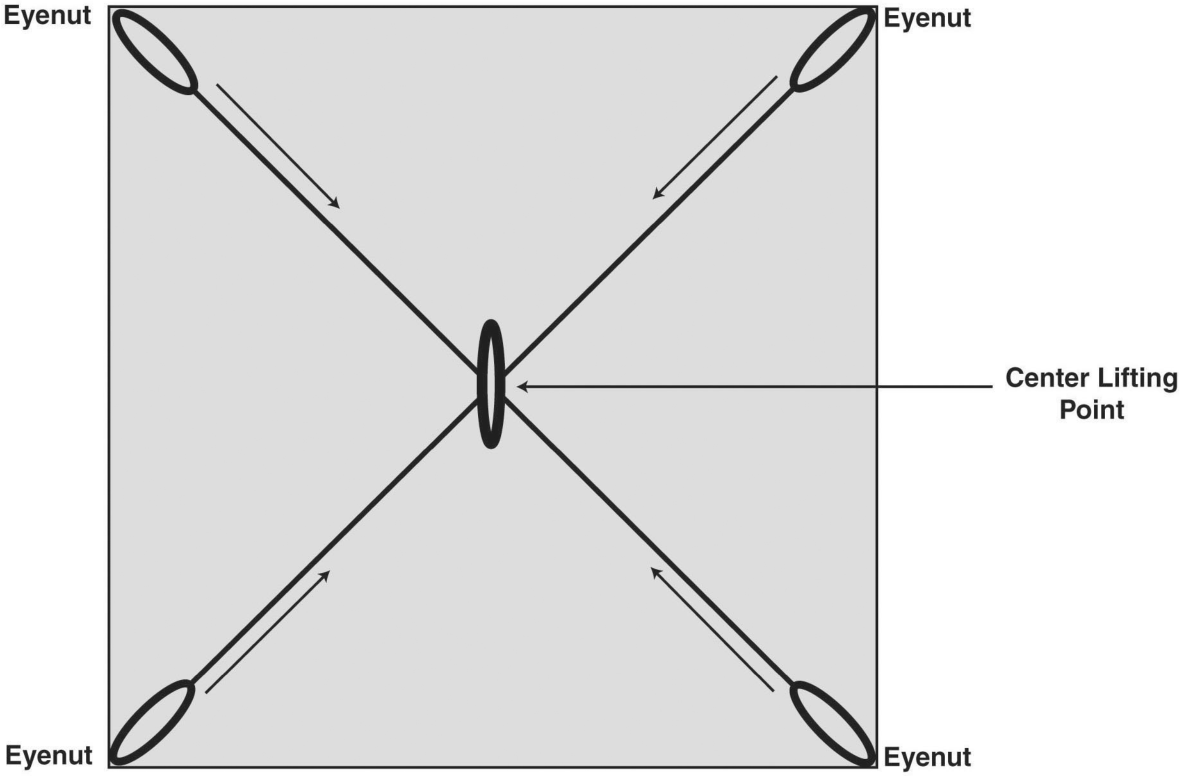
**Figure 3: Lengths and Angles for Lifting Using the Eyenuts**



If eyenuts are removed or become loose, install them properly before lifting the equipment rack. Tighten the eyenuts and bolt assembly by hand. Correct eyenut tightness and alignment are crucial to ensure that the eyenut assembly performs to its intended lifting capacity. Align the eyenuts to point towards the center lifting point of the cabinet and tightened to between 90 and 120 in-lbs torque.

Figure 4: Proper Alignment of the Eyenuts on page 46 shows the proper alignment of the eyenuts.

**Figure 4: Proper Alignment of the Eyenuts**



Chapter 2

# Fault Management Tools

This chapter covers the list of applications that are available for troubleshooting and servicing equipment in the system.

## 2.1 Unified Event Manager

The Unified Event Manager (UEM) is a fault management application designed for critical fault management functions.

These functions include:

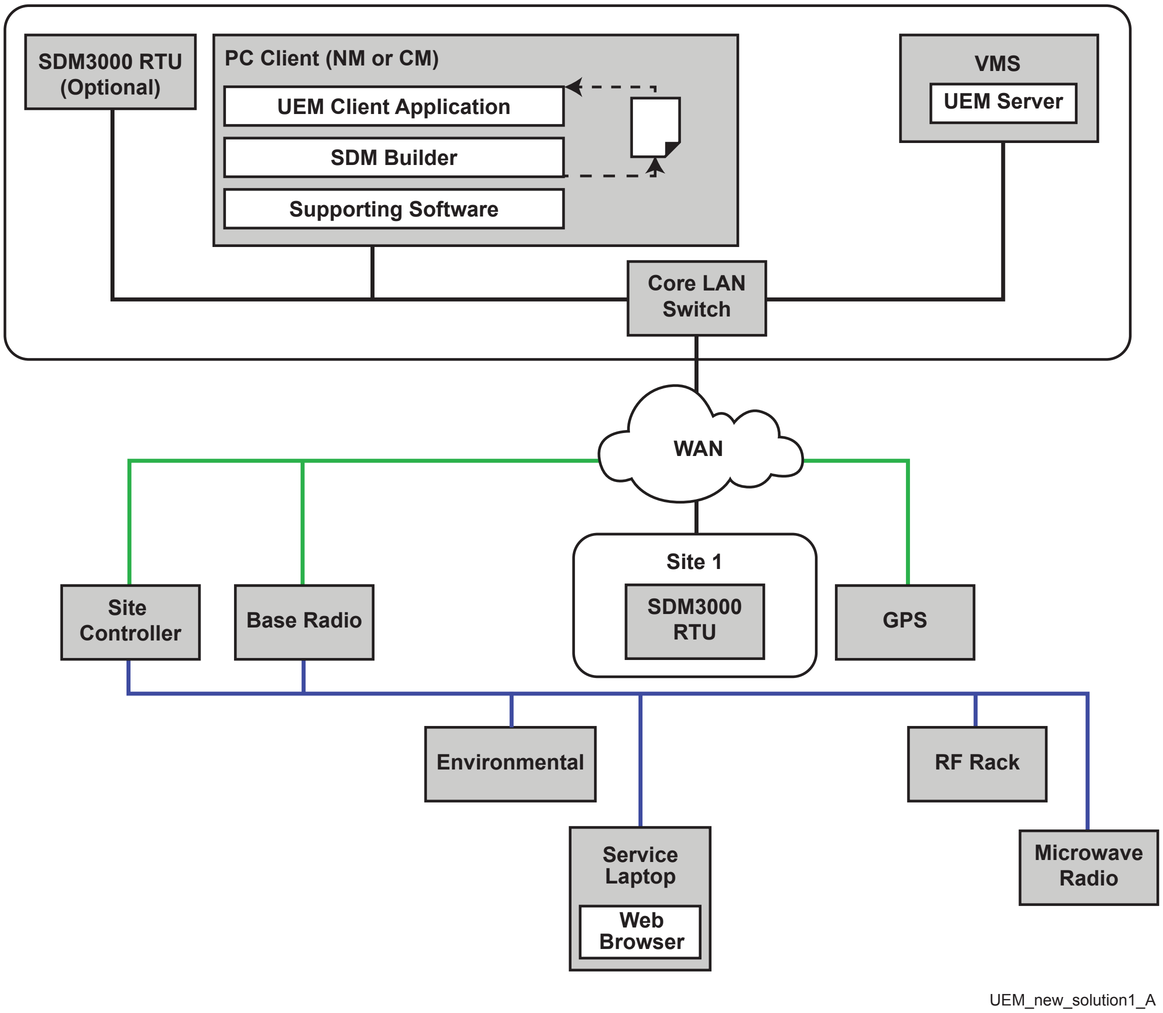
- Processing fault notifications (SNMP traps or informs) sent by network elements
- Detecting and reporting the loss of communication with managed devices (Supervision)
- Ensuring that the reported status is current (Synchronization)
- Discovering a single device or all devices within a subsystem
- Troubleshooting faults
- Sending commands to network elements
- Ability to manage PTP (Point-to-Point) Wireless Ethernet Bridge devices (optional)

UEM has the ability to manage various devices through an SDM Remote Terminal Unit (RTU), and can be established as the main fault manager and aggregate all health information from the system. Depending on the features available with your system, UEM can provide an integrated and more centralized fault management solution with enhanced views and optional integrated support as a replacement of the MOSCAD Graphical Management Computer (GMC) and Graphical Workstation (GWS). See the *Unified Event Manager* manual for details.

- If MOSCAD NFM solution is present in the system, UEM is designed to replace MOSCAD GMC and provide enhanced Centralized Fault Management Solution
- If MOSCAD NFM solution is not present in the system, UEM can be enhanced with MOSCAD RTU components to provide additional information and capabilities.

The following diagram shows fault management solution resulting from the merge of UEM and MOSCAD NFM into a single solution based on UEM. The integrated UEM provides functionality similar to the GMC, and processes the data which was previously managed by MOSCAD GMC.

**Figure 5: New Mode of Operation**



Duplicated fault management is removed on manager level. The information received directly from Network Elements has priority over information received from the RTU. Additional information provided by the RTU is added.

## UEM Enhancements

UEM enhancements, depending on your system, may include the following:

- The map set for UEM can be extended to include the maps similar to GMC maps found in the MOSCAD solution, and can include the system map, the microwave radios map, and the zone map (showing sites in the zone).
- The Site views for viewing the status of the site infrastructure. The content depends on the site type and a list of discovered and managed elements within the site. The information is organized in the following groups:

  **Service**
  Showing services status in the site.

  **Environmental**
  Showing status of Analog Inputs / Digital Inputs and Digital Outputs.

  **Equipment**
  Showing a list of Network Elements grouped by the type.

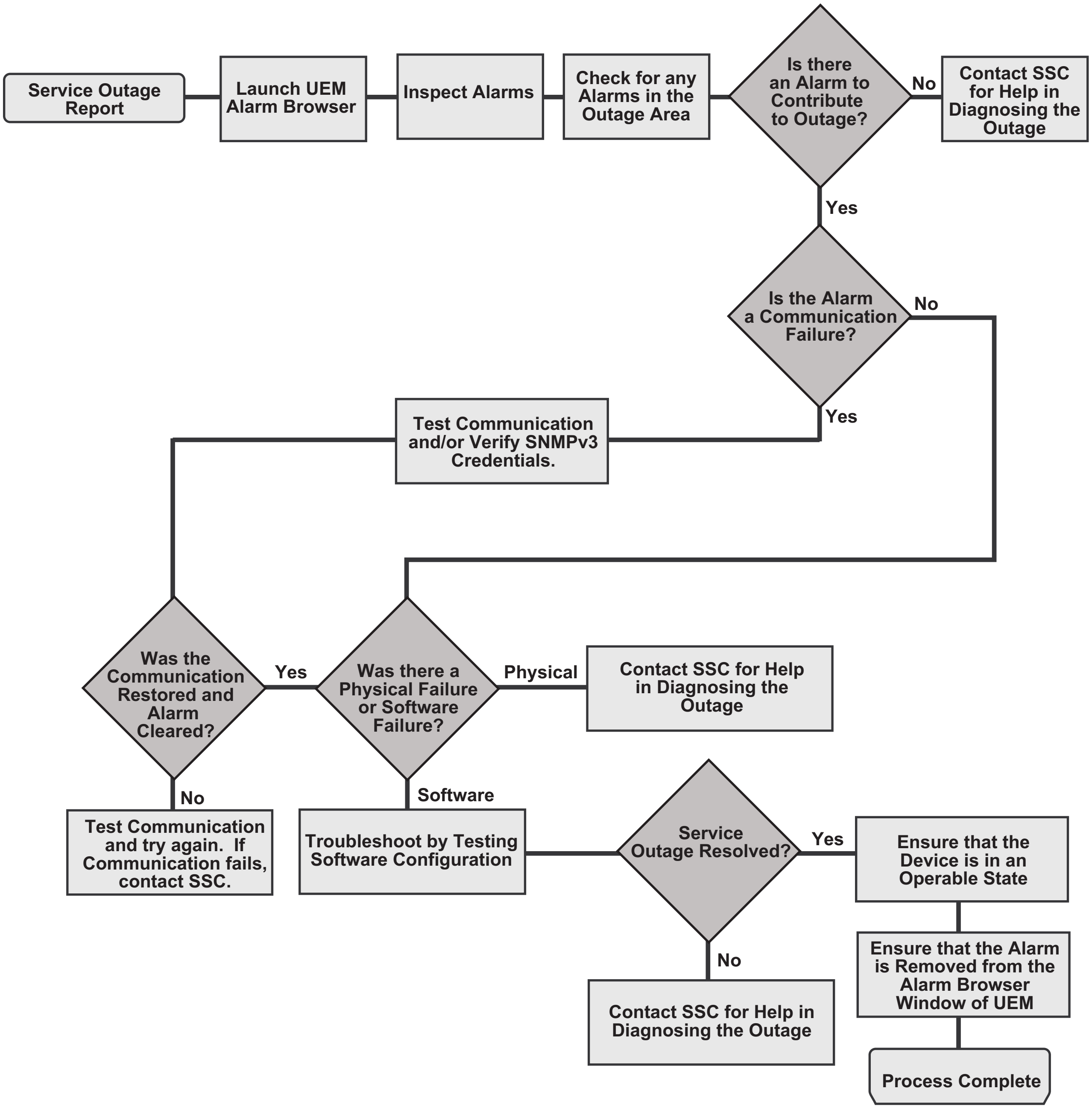
- The Network Element used to display the status of the Managed Resources:
  - Description of the network element and its overall state
  - List of managed resources and their states and values grouped by type and hierarchy
  - Commands (controls) that are possible for a given Network Element
  - Overall status of the associated Network Elements (for example, redundant site controllers)
- Views of Sites, Views of Network Elements managed by UEM, including SDM RTU-associated devices previously managed by the GMC.
- Support for alarm/event report generation with sorting and filtering capabilities, acknowledging / un-acknowledging alarms.
- Creation of optional free-form text for Network Elements managed by UEM, and when an alarm is generated that contain information input by the user.
- Support for reporting and access to information on Analog/Digital Inputs, Digital Outputs, and information on states and events for numerous managed devices.
- The capability to open UEM sessions for other zones in the system from the system map perspective.

## 2.1.1 Resolving System Events in UEM

To resolve a service outage in an ASTRO® 25 system, use the following flowchart.

For more information about using UEM, see the *Unified Event Manager* manual.

**Figure 6: UEM Fault Management Diagnostic Flowchart**


Service Outage Report
Launch UEM Alarm Browser
Inspect Alarms
Check for any Alarms in the Outage Area
Is there an Alarm to Contribute to Outage?
No
Contact SSC for Help in Diagnosing the Outage
Yes
Is the Alarm a Communication Failure?
No
Yes
Test Communication and/or Verify SNMPv3 Credentials.
Was the Communication Restored and Alarm Cleared?
Yes
Was there a Physical Failure or Software Failure?
Physical
Contact SSC for Help in Diagnosing the Outage
No
Test Communication and try again. If Communication fails, contact SSC.
Software
Troubleshoot by Testing Software Configuration
Service Outage Resolved?
Yes
Ensure that the Device is in an Operable State
Ensure that the Alarm is Removed from the Alarm Browser Window of UEM
Process Complete
No
Contact SSC for Help in Diagnosing the Outage

UEM_Fault_Mgmt_Diagnostic_Flow_A

2.1.2
## Alarm Summary

The term *alarm summary* in the Network Management context describes the various levels of alarms within a computer network. Alarms across a network are commonly related to:

- Systems that have failed
- Connectivity issues
- Devices malfunctioning
- Threat assessment reports

## 2.2 MOSCAD Network Fault Management

**NOTICE:** The Unified Event Manager (UEM) provides an integrated and more centralized fault management solution with enhanced views and optional integrated support for various devices managed by MOSCAD NFM, as an alternative replacement of the MOSCAD Graphical Management Computer (GMC) and Graphical Workstation (GWS). See the *Unified Event Manager* manual for details. Transition from Unified Event Manager and MOSCAD Network Fault Management to a centralized and integrated management solution is described in *UEM/GMC Transition Guide*.

The SDM3000 Builder software is used to plan and configure the SDM3000 RTUs and SDM3000 Network Translators in ASTRO® 25 sites. It is a Microsoft Windows-based software application that facilitates easy planning of your zones and sites. Based on information you enter in the SDM3000 Builder screens, the software calculates intersite and intrasite dependencies, such as defining the number, order and connections of the CPU and I/Os in the SDM3000 unit, while taking into consideration your equipment and needs.

The user builds the system level configuration (project) and installs it in the SDM3000 unit. The project is organized in a hierarchical structure of zones and sites. For each site, devices, objects, and MOSCAD equipment are defined. For each item in the project hierarchy, identifiers and characteristics are defined and configured.

The MOSCAD Network Fault Management (NFM) system is used to monitor data about your system and to issue control commands such as turning tower lights on and off, starting backup generators, and turning base stations on and off. MOSCAD NFM is used in fault monitoring to report on the status of many third-party, non-Motorola devices such as power and security devices, microwave radios, and environmental alarms for doors, control tower lights, and other equipment.

MOSCAD NFM Remote Terminal Units (RTUs) are used to monitor network devices and report their status through the MOSCAD GMC Element Manager. MOSCAD NFM displays the MOSCAD NFM alarm information from network elements (devices) supported by MOSCAD NFM RTUs.

**NOTICE:** The MOSCAD NFM SDM3000 RTU can be used to route fault management traffic between the Aviat Eclipse microwave device (formerly Harris Stratex) and the Unified Event Manager server application (UEM) and between the Aviat Eclipse and the MOSCAD NFM GMC. See the *MOSCAD Network Fault Management Feature Guide* manual for details.

MOSCAD NFM systems utilize two methods to obtain data:

- **Polling (interrogation)** – The MOSCAD NFM GMC communicates with the legacy MOSCAD IP Gateway or SDM3000 Network Translator. The legacy MOSCAD IP Gateway or SDM3000 Network Translator communicates with SDM3000 RTUs in the system, asking for all data or for the data that has changed since the last poll. The SDM3000 RTU responds with an “Ack” and the “message” (data).
- **Report by Exception (messaging or Change of State)** – If an input of the SDM3000 RTU changes, the RTU automatically transmits the change to the managing device: MOSCAD NFM GMC, or UEM.

### 2.2.1 SDM3000 Builder Application

The SDM3000 Builder software is used to plan and configure the SDM3000 RTUs and SDM3000 Network Translators in ASTRO® 25 sites. It is a Microsoft Windows-based software application that facilitates easy planning of your zones and sites. Based on information you enter in the SDM3000 Builder screens, the software calculates intersite and intrasite dependencies, such as defining the number, order and connections of the CPU and I/Os in the SDM3000 unit, while taking into consideration your equipment and needs.

The user builds the system level configuration (project) and installs it in the SDM3000 unit. The project is organized in a hierarchical structure of zones and sites. For each site, devices, objects, and MOSCAD equipment are defined. For each item in the project hierarchy, identifiers and characteristics are defined and configured.

**NOTICE:** In integrated and centralized fault management solution, the SDM builder application is used to configure SDM RTUs and the configuration must be loaded into UEM to allow UEM to manage SCADA-components through RTU.

## 2.3 Unified Network Configurator

The Unified Network Configurator (UNC) is an advanced network configuration tool that provides controlled and validated configuration management of system devices, including routers, switches, terminal servers, base radios, site controllers, and comparators. UNC has features that are useful for fault management, including the following:

- **Distribution monitoring** – Indicates the status of configuration changes, whether the change is in progress, completed, pending, or failed.
- **Change logging** – Maintains an audit trail of various user interactions with the configuration system to assist in diagnosing issues.
- **Configuration versioning** – Constantly tracks versions for changes, provides the ability to query configuration changes, and compare versions.
- **Rollback to previous version** – Enables device configuration changes and reinstates a previous version at the click of a button.

The UNC can manage (update the OS, display configurations, etc.) the backhaul switches used to support fault management of the PTP (Point-to-Point) Wireless Ethernet Bridge devices (optional) resided within the PTP subnet (Refer to the *Unified Network Configurator* manual for additional information). Note, however, that the PTP devices are not managed by the UNC.

Additionally, the MLC 8000 devices are not managed by UNC.

## 2.4 Provisioning Manager

The Provisioning Manager is an ASTRO® 25 system application that enables centralized provisioning of ASTRO® 25 system with various system-level, user-level, and device-level configuration required for proper system operation. It also provides features that are useful for fault management, including:

- Change logging – maintains an audit trail of all user interactions with the configuration system to assist in diagnosing issues.
- Provisioning status – provides at-a-glance indicators that show the current provisioning state on the **Home** and **Update Manager** pages.

## 2.5 ZoneWatch

The ZoneWatch application allows you to monitor site and channel activity within the zone. Grid windows display the condition of the sites and channels, and show any activities as they take place. Raw Air Traffic Information Access (ATIA) traffic can also be displayed to view different call processing messages and status updates that are taking place in the zone.

ZoneWatch can be configured with a variety of different profiles to define the watch windows by setting up custom profiles. A variety of different data filters can also be set through application to filter the types of information that ZoneWatch monitors.

Detailed information for ZoneWatch can be found in the *ZoneWatch Online Help*.

## 2.6 ATIA Log Viewer

The ATIA Log Viewer application displays Air Traffic Information Access (ATIA) log files that have been archived in the zone. ATIA messages are recorded and archived daily for all the call processing activities and other site events in the zone. The ATIA Log Viewer allows you to select a daily log file and view activities that took place in the system. Archived log files stored on the ATR server can be accessed through the ATIA Log Viewer application.

**NOTICE:** The ATR server application keeps the logs for 30 days, provided that the total amount of data stored does not exceed 4 GB.

ATIA messages include the date, time, and description of the event that occurred (such as, a subscriber registration, call request, or site handover).

For sites which are capable of working in Dynamic Dual Mode (DDM), ATIA indicates the type of subscribers (FDMA or TDMA-capable) that registers with the system and it also indicates the capability of a console (FDMA, 2-slot TDMA, 2-slot TDMA and FDMA) that registers with the system.

When the talkgroup is configured as Dynamic, ATIA indicates the type of call (FDMA or TDMA). If not, the Zone Controller uses configured values from the UCS server application to set the type of talkgroup.

For details about the ATIA Log Viewer refer to the *ATIA Log Viewer* manual.

## 2.7 Configuration/Service Software

The Configuration/Service Software (CSS) is a Windows-based application installed on the computer used to perform configuration, status reporting, and servicing tasks for infrastructure devices in the system. The CSS application allows a service technician to:

- Configure operating parameters for Voice Processor Module (VPM)-based devices and RF site devices.
- Retrieve status and operational information from a device.
- Perform alignment procedures for the infrastructure devices that can use the CSS.
- Set the IP address for specified devices, which requires a local serial connection.
- Perform most device configuration and servicing tasks either through a serial connection to the device or over the LAN.

CSS can access each device over the local LAN, or individually through the Ethernet service port. The DB-9 serial port connection is used to set the IP addresses for devices. CSS also can be used to view status information, equalize batteries, and check internal logs of the devices.

Configuration/Service Software (CSS) provides screens for configuring and testing remote site devices. CSS supports GTR 8000 Base Radios, GCP 8000 Site Controllers, the GCM 8000 Comparator, STR 3000 base station radios, and ASTRO® 25 repeaters.

CSS supports the configuration and service features, many of which are used to check configuration settings or to run certain tests on equipment. Detailed information for all the CSS features is available in the CSS online help. Also see manuals for particular devices configured with the CSS and the *Trunked IP Simulcast Subsystem Remote Site* manual for specific information on configuring your remote site equipment with CSS and using the CSS as a tool to aid in troubleshooting. CSS provides features that are useful for fault management, which include:

- Set IP Address/Box Number – Through a direct connection to the device serial service port, CSS can set the IP address, the physical address, the network mask, and the box number for the device.
- Read Configuration From Device – CSS can read the configuration parameters for a supported device through either an Ethernet connection or over the network. Changes can be made to the configuration or the configuration can be saved as an archive file to a disk.
- Write Configuration To Device – CSS can write configuration parameters to a supported device.

  **NOTICE:** Devices can also be configured through the Unified Network Configurator (UNC). If both the CSS and UNC were used, the latest of the configurations applies.
- NTP Definition Screen – A primary and secondary NTP source can be defined for the device.
- Status Panel Screen – Hardware and operational status information can be viewed for the device.
- Status Report Screen – Event logs can be viewed to show alarms, changes in device state, and other events. Engineering logs can be obtained as text files and sent to Motorola Solutions for analysis.
- Test and Measurement Screen – For base radio equipment and comparators, ASTRO® 25 pattern tests, BER tests, and RSSI tests can be run for some of the supported devices.
- Metering Screen – Reflected power and voltage standing wave ratio (VSWR) levels can be displayed for base radios.
- Version Screen – This screen shows the hardware and software versions for the device and its components.
- Alignment Screen – For simulcast equipment, this screen is used for aligning equipment in the transmission path. The screen is also used to align the oscillator for the comparators and Site Repeaters.
- Channel Window – For site controllers, this screen shows all the configured channels for the site. Channel status can be viewed and channels can be enabled or disabled.

## 2.8 Software Download Manager

Software Download Manager (SWDL) transfers and installs new firmware in site components including base radios, site controllers, comparators, and Reference Distribution Modules (RDMs).

**NOTICE:** For detailed information on uploading firmware to the devices, see the *Software Download Manager* manual.

SWDL allows you to perform the following actions:

- Download software to site devices.
- Download software to one device (such as one base radio) that has been disconnected from the radio network.
- Update the software on newly added channels or subsites.
- Determine software and hardware versions on target devices.
- Purge (delete) a software version from selected target devices.
- Obtain device IP information.
- Query the site controller for the number of channels and/or subsites in the system.
- Audit a session using historical information recorded by SWDL.

To download software to an ASTRO® 25 system, perform one of the following actions:

- Software download to the entire site (centralized software download).

- Software download to one device that has been disconnected from the radio network (single device software download).

**NOTICE:** Conventional devices are supported only in the single device mode.

For more information see *Software Download Manager* manual.

## 2.9 Configuration Tool For MLC 8000

The MLC 8000 Configuration Tool is used to define Channel Clusters and to configure both the MLC 8000 Subsite Link Converters (also referred to within the configuration tool as AGUs) and the MLC 8000 Analog Comparators (also referred to within the configuration tool as VGUs).

In an analog ASTRO® 25 system, the MLC 8000 Configuration Tool is used to configure the MLC 8000 Subsite Link Converters and the MLC 8000 Analog Comparators.

In a digital ASTRO® 25 system, the MLC 8000 Configuration Tool is used to configure only the MLC 8000 Subsite Link Converters because the GCM 8000 Digital Comparators are configured in the Configuration/Service Software (CSS).

In a mixed mode system, the MLC 8000 Configuration Tool is used to configure both the MLC 8000 Subsite Link Converters and the MLC 8000 Analog Comparators, and the CSS is used to configure the GCM 8000 Digital Comparators.

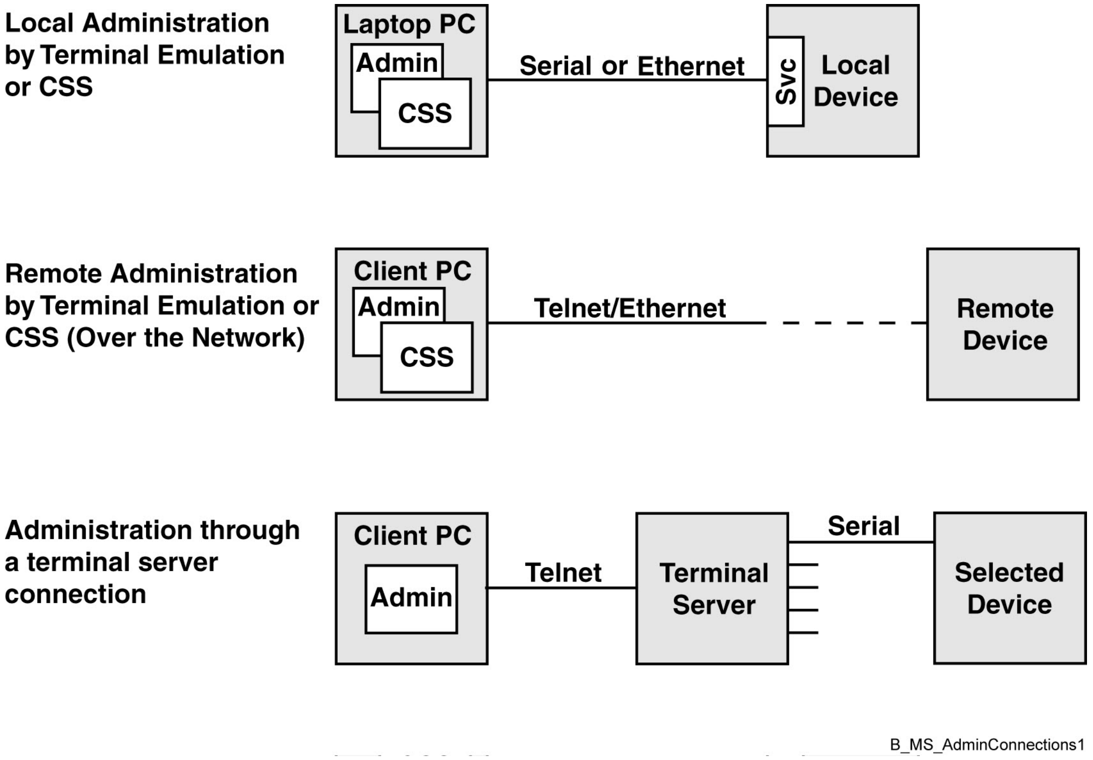
## 2.10 Local Logs and Administration

Many of the devices in the ASTRO® 25 radio network maintain local alarm logs. If a problem has been isolated to a particular device, the local alarm log can reveal additional information about faults and activities that may not have been reported to the Unified Event Manager or other fault reporting analysis tools. Sometimes the local logs include more detailed information that is not polled or accessible by other fault management tools, and in the event of a lost connection, some of the SNMP traps may never get reported to the UEM.

For some components, like comparators, the alarm logs can be viewed through CSS. For other components, like the channel bank, alarm and status information can be gathered through a direct connection through a terminal emulation application. Alarm logs and administrative information can also be accessed for some devices over the network by using a telnet connection to the terminal server or directly to the device's IP address and logging into the administrative environment.

Figure 7: Methods for Accessing Local Logs and Administration Environments on page 56 shows the methods that are used for accessing local log information and device administration environments. A telnet session can be started on a client PC or laptop PC by using terminal emulation software, or by selecting **Run** from the Windows Start menu (for Windows 7 press the Windows key + R) and typing `telnet <ipaddress>`. If using a laptop running the Microsoft Windows operating system, use a third-party application such as PuTTY for this functionality.

**Figure 7: Methods for Accessing Local Logs and Administration Environments**



Menu-driven administration environments can be accessed for devices like the zone controller and network management servers to perform backups, check the system or component status, change the Network Time Protocol (NTP) source, enable or disable the device, and manage redundancy. Other devices, such as the terminal server, channel bank, and routers, also have either menu-driven environments or command line interfaces for setting up basic configuration settings, backing up data, or checking the system status.

For example, the zone controller administration menu provides a selection for viewing the system status along with several other menu item selections to provide fault management information for the system.

## 2.11
## Network and Device Commands

Many device and network commands can be used to determine the status of different ports, links, routes, and devices in the network. Brief descriptions of a few of the commands are given in the following sections. Some commands may include additional flags and options beyond those listed in this manual, and some of the commands may only work in certain operating systems. When working through a client PC, you can run many of these commands through terminal emulation software, or by selecting the Run command from the Windows Start menu and typing `cmd` to open a Windows Command window.

### 2.11.1
### Ping

The `ping` command can be used to verify the connection between two devices in the system and check for any packet loss or loss of connectivity along the overall path. The ping command sends a series of Internet Control Message Protocol (ICMP) echo request packets to a specified device. Replies are then returned back to the originating device. They indicate that the remote device is present and communicating at the IP level. If you are experiencing a network connectivity problem, consider running ping commands from a client PC in the NM subnet at the Master site. Available ping responses are shown in Table 6: Ping Responses on page 57.

**NOTICE:** Factory configuration of gateways, router and firewalls may block ping and traceroute commands and responses due to information assurance requirements. Ping and traceroute commands from PC clients in the NM subnet and responses to hosts in this subnet are always allowed. More details on ping operation can be found in the “Access Control Lists Overview” section of the *Service Access Architecture* manual.

Table 6: Ping Responses

| Response | Description |
|---|---|
| Destination host unreachable | The path to the destination device cannot be found. The furthest reachable point reports the information back to the ping sender. Examine the routing information between the local and remote devices. Check the local network interface, default gateway, and any suspected links, routers, or switches. |
| Request timed out | The destination device did not receive the ping message within the designated time period. The destination device may be configured with the wrong IP address, powered down or disconnected. An intermediate device or link may also be down, or a router or switch may be configured improperly. If some replies are received along with some timeout messages, the network may be congested. |
| Unknown host | The destination name cannot be resolved, or there is a problem with the host name configuration. |
| TTL expired in transit | The ping command did not find the specified host. A circular routing situation has occurred. There may be a problem with the routing wiring or configuration. |

## 2.11.2 Trace Route

The `tracert` command traces the route to a specified remote device and reports statistics for each intermediate device along the path. The command can be used to verify the path to the device, ensure that all devices and links are operational, and verify that the latency between devices in the path are within reasonable limits. Troubled devices or links on the path can be pointed out by lengthy hop times or failures to respond. Using a copy of your system's IP plan, you can verify the paths used between the equipment, check whether primary or secondary routers are in use, and verify that all the IP addresses are correct according to the plan. Some devices running other operating systems may use other similar commands such as `trace-route` or `trace route` (two words).

## 2.11.3 Pathping

`Pathping` is a route-tracing command, which combines the features of the `ping` and `tracert` commands. The `Pathping` command sends packets to each router on its way to a specified destination and computes packet loss statistics for each router in the path. The `Pathping` command can be used to recognize and pinpoint any particular routers or links on the path that may be responsible for heavy packet loss.

## 2.11.4 ARP

The Address Resolution Protocol (`arp`) command reports the physical MAC addresses of any locally connected devices. IP packets include a source MAC address and destination MAC address, which determine how the packets are routed through the network. An incorrect IP-to-physical address match can result in routing problems.

If you want to view the physical address of a device that is not reported in the list, first ping the device, then run the `arp` command again. The device should then be shown in the list.

## 2.11.5 Ipconfig

The `ipconfig` command shows detailed configuration and network connection information for Windows-based equipment such as client PCs, console PCs, Graphical Master Computer (GMC), Graphical Workstation (GWS), or laptop PC being used to troubleshoot the network. Unix/Linux operating systems use the comparable command `ifconfig`.

## 2.11.6 Netstat

The `netstat` command shows all the active TCP, UDP, and ICMP connections for the device, along with the current status of each connection. The netstat command can report the connections that are established with the device. Using the `netstat-a` command, you can view all the listening connections.

You can also view the Ethernet statistics, including the bytes, discards, and errors sent and received.

## 2.11.7 Nslookup

The `nslookup` command can be used to look up the IP addresses of the default server and other device IP addresses that are recorded in the DNS database. This command can be used to verify the DNS entries and to gather IP addresses of devices by their host name (such as atr01.zone1 for the Air Traffic Router in zone 1, or rp3.tlan2.zone1 for the TLAN2 port on core router 1 in zone 1). The command can be helpful if you want to run other administration commands but only know the host name of the particular device.

The `nslookup` command first shows the default DNS server, then provides a prompt for looking up other host names in the network.

## 2.11.8 Telnet

Telnet is used to connect with remote devices over the network such as the terminal server and other administrative interfaces. The `telnet` command can also be used to verify that the application layer is working between devices (while ping and trace route commands test the network layer). A `telnet` session can be started with a terminal emulation software, or by selecting the Run command from the Windows Start menu and typing `telnet <ipaddress>`. If using a laptop running the Microsoft Vista operating system, use a third-party application such as PuTTY for this functionality.

Windows Vista and Windows 7 do not have the built in telnet functionality.

If your system implements information assurance features, refer to the appropriate information assurance manual for more information on the use of protocols.

## 2.11.9 SSH

SSH is used to connect with remote devices over the network such as the terminal server and other administrative interfaces. Unlike telnet, SSH does this using an encrypted connection. The SSH command can also be used to verify that the application layer is working between devices (while ping and trace route commands test the network layer). An SSH session can be started with a third-party application such as PuTTY or by invoking the `ssh` command from a Unix or Linux command line.

If your system implements information assurance features, refer to the appropriate information assurance manual for more information.

This page intentionally left blank.

Chapter 3

# Fault Management – System and Device Level

This chapter provides fault management and troubleshooting information relating to Fault Management.

## 3.1 Overview

A failure in the system does not influence all radio system users in the same way. Some users may be able to continue communicating with no interruption while others may not be able to communicate at all. Since the system does not rely on a single RF source or audio or control data path, the system can work around certain failures. Also, what may appear to a user as device failure may actually be a configuration issue. The isolation and diagnosis of failures in a dynamic, computer-based system like ASTRO® 25 is made easier with the Unified Event Manager (UEM).

The UEM allows you to troubleshoot and isolate problem areas. Since the system and its components are a synthesis of hardware and software, it is important to have a means of differentiating between faulty hardware and other system issues.

## 3.2 Suggested System Monitoring

Table 7: System Monitoring on page 61 contains the basic processes that you should follow as part of system monitoring and fault isolation.

Table 7: System Monitoring

| Action to take | Frequency |
|---|---|
| Review critical system functions in the Unified Event Manager (UEM) Map view. Verify that:<br>• All sites are in Wide Area mode<br>• All zones are in InterZone trunking<br>• A control path exists between the zone controller and sites<br>• A control path exists between zone controllers (in multizone systems) | • At the beginning of your shift<br>• Periodically throughout your shift |
| Review logged alarms in the UEM Alarm view. | Daily |
| Monitor activities within each zone through the Dynamic Reports application. Check for high reject counts or other unusual site activity statistics. | Daily |
| Monitor system-wide statistics through the Historical Reports application. Check for any anomalies including high busy counts, unusually high or low volumes of certain calls or services, and surges of traffic within particular talkgroups. | Monthly, or as needed |

*Table continued…*

| Action to take | Frequency |
|---|---|
| Monitor the performance of network transport equipment by generating reports through InfoVista, if available. Check for any prolonged overloading of critical network transport equipment. | Daily |
| Use ZoneWatch to monitor the general status and activities for all of the sites. Verify that radio users are utilizing the sites, check for any site or channel failures, and observe any unusual raw ATIA messages. | • At the beginning of your shift<br>• Periodically throughout your shift |
| Review PTP device alarms and events in UEM (optional) | As necessary |

3.2.1
## Isolating Faults in the Unified Event Manager

**When and where to use:**
The Unified Event Manager (UEM) alarms browser captures alarms that may occur intermittently or during off-hours. This makes it useful for troubleshooting. For example, you can review the Alarms Browser to correlate reported loss of service with known link outages due to weather. The UEM application features a generic SMTP-based interface that can be configured to send notifications to a destination in the Customer Enterprise Network (CEN). This destination is typically a customer-owned application such as a simple e-mail server that accepts SMTP messages and may allow for further management of notifications such as scheduling.

**NOTICE:** For detailed information on using the Unified Event Manager to monitor your system, refer to the *Unified Event Manager* manual.

**Procedure:**

1. At the beginning of each shift, and throughout the day, analyze the UEM Alarms view. Look for these types of patterns:
   - Traps sent with time stamps on or about the same time.
   - Traps from related equipment.
   - Cards in the same device.
   - Equipment that is part of the same subsystem.
   - Critical and non-critical events. Many devices are capable of sending out traps that report both critical and non-critical events.

   **NOTICE:** Refer to the *Unified Event Manager* manual for details on interpreting traps that you see in the Alarms Browser. Refer to System Release Notes and Product Service Bulletins (PSBs) for current information on traps, and other information that may affect system operation.

   | If… | Then… |
   |---|---|
   | **The system is behaving normally** | Take no further action at this time. Repeat step 1 at intervals throughout the shift. |
   | **The system is generating critical alarms** | Continue with step 2. |

2. Isolate the alarm from the UEM: Use the equipments LED indicators and Configuration/Service Software (CSS). If you are in the same location as some of the malfunctioning equipment, you can use the LEDs on the components to help isolate the alarm. Refer to the remaining chapters of this manual for more details.

| If… | Then… |
|---|---|
| **The system can isolate the fault** | Take corrective action as soon as possible. The system may function with no noticeable loss of service. However, further failures may result in the loss of service. |
| **The system cannot isolate the fault** | Escalate the problem. |

## 3.2.2 Viewing Alarms and Events Using the Unified Event Manager

To correctly categorize a system fault, do not troubleshoot the system. Troubleshooting is done using the UEM which provides the status from the system or zone level down to the device. For a system-level fault-management view, open the UEM application from one or more zones simultaneously on a client. The UEM provides many ways of viewing your fault data.

In the UEM, a user can view a state change of an object or a subnet using the following views: Alarms, Network Events, Network Database or Maps. Alarm severity colors are viewed using the Alarms view. This View provides functionality status at a glance. For more information on using the UEM views, refer to the “UEM Operation” chapter of the *Unified Event Manager* manual.

The Alarms Browser presents the current state of a given components. It allows you to identify problem areas and the component's intermittent failure. After recognizing the problem the user can acknowledge the alarm(s) to easily organize and manage the problems.

The Alarm Summary is used to display the count of the total number of alarms organized by categories and/or severities. Each severity is represented in a single cell or graph, depending on the presentation that is selected. Three different presentations of the alarm summary are available:

- Table view
- Bar graph view
- Pie chart view

The Event Browser presents the logged history of a given component's status. The Alarms and Events Browsers provide you with the ability to filter out events/alarms, allowing to focus on the ones important for you.

For detailed information on using the UEM application, refer to the *Unified Event Manager* manual.

## 3.3 System-Level Reliability

As a very wide area system with potentially thousands of users operating under disaster conditions, ASTRO® 25 reliability capabilities are critical to the effectiveness and the value of the system. Layers of protection are provided at a subsystem/component level.

An ASTRO® 25 system has several system-level reliability features. These features fall into two groups:

- **Multiple System Components** – Multiple system components operate in a redundant mode (operation is switched to the second component in the event of a failure) or in an active parallel mode (in the event of a failure, operation continues but with reduced capacity). See Multiple System Components on page 64.
- **Modes of Operation** include standard and user-initiated system operating modes. See Modes of Operation on page 66.

## 3.3.1 Multiple System Components

This section contains the information on the use of multiple system components of a similar type (such as sites or network equipment) on the ASTRO® 25 system for reliability purposes.

### 3.3.1.1 Dynamic System Resilience

Dynamic System Resilience (DSR) is part of a continually evolving ASTRO® 25 core. Dynamic System Resilience feature adds a geographically separate backup for the master site. DSR creates an always available network that is not affected by equipment failure or catastrophic failure. The failure of any element within the system is taken up by a redundant counterpart of that element, with minimal disruption to the radio users.

With Dynamic System Resilience, full system functionality is automatically maintained without operator intervention. Manual switchover capability is provided for system testing and maintenance. Dynamic System Resilience is supported in multi-zone capable master site configurations. Geographic redundancy can be achieved efficiently as site equipment can be shared within a multi-zone system.

For more information on the Dynamic System Resilience feature, see the *Dynamic System Resilience* manual.

### 3.3.1.2 Control Channel Backup

The network manager is able to configure up to four channels at each site as “control channel capable”. Additionally, you can assign a preference level to each channel that is capable of being a control channel. The preference levels range from one (most preferred) to four (least preferred).

- If a channel is set at preference level “one”, the site controller assigns this channel to be the control channel, and tries to maintain this channel as the control channel.
- If a channel is set at preference level “four”, the site controller assigns this channel to be the control channel only if all other channels at the site with higher preference levels cannot fill the control channel role.

If the main control channel fails, and if there is at least one in-service channel capable of providing the control channel, the site controller assigns a new control channel for the site.

The assignment is based on the preference levels set for the different channels; the site controller assigns the control channel to the channel with the highest preference level. If there is more than one control capable channel, then the new control channel is assigned based on preference level and channel usage. If there are no control capable channels in service, then the site is no longer capable of supporting trunking operations. The new control channel is assigned less than one second after the main control channel failure.

### 3.3.1.3 Multiple Remote Sites

A system is normally configured with multiple remote sites. Often, these sites provide large areas of overlapping RF coverage for subscriber units. It is especially true for the following:

- Mobile subscriber units in a system that provide portable subscriber coverage.
- Systems designed to provide primarily portable coverage.
- Systems where fault management of PTP devices and other equipment is employed (optional).

Therefore, in the event of the loss of service from a single remote site, it may still be possible to obtain service from a different remote site in one of many other locations. Additionally, remote sites can be considered within the RF design to provide coverage reliability at important locations.

### 3.3.1.4
### Multiple Dispatch Consoles

A system is normally equipped with multiple dispatch consoles, which can be located at a single dispatch site or distributed across multiple dispatch sites. A system with multiple dispatch sites provides system reliability against failures that affect the whole site (for example, major catastrophes or complete power failure at the site). Equipping each dispatch site with multiple dispatch consoles provides protection against the failure of a single dispatch console and results in service still being available at the site, but to a reduced number of dispatchers.

### 3.3.1.5
### Multiple Network Manager PCs

A system is normally equipped with multiple Network Management PCs, which can be located at a single Network Management site or distributed across multiple Network Management sites. A system with multiple Network Management sites provides system reliability against failures that affect the whole site (for example, major catastrophes or complete power failure at the site). Equipping each Network Management site with multiple Network Manager PCs provides protection against failure of a single user terminal and results in service still being available at the site, but to a reduced number of Network Manager users.

### 3.3.1.6
### Router Links

The Motorola Cooperative WAN Routing (CWR) solution allows core and exit routers to interface directly with site and InterZone links through a simple, reliable, and passive relay panel. The core and exit routers are configured in pairs to provide path redundancy for audio and control packets. With CWR, the routers work to control an external relay panel to switch a group of 12 non-redundant T1/E1 links between the two routers. One router is always considered as the “Active” router and the other router is considered as the “Inactive” router. Each router is provisioned with two 12-port T1/E1 modules, providing up to 24 T1/E1 link terminations per router pair.

CWR interfaces the master site in one zone to Radio Frequency (RF) sites, dispatch sites, system Network Management, and other zones.

Systems that implement the Flexible Site and InterZone Links feature may or may not include a CWR panel. In these systems, a pair of core backhaul switches are used to connect to the customer Ethernet backbone to ensure network redundancy.

### 3.3.1.7
### Redundant Network Transport Components

The gateway routers provide the Control Rendezvous Point (RP) function for zone controller RF Site Control Paths (ZC-RF SCPs) that service each site. The gateway routers also provide the RP function for InterZone Control Paths (IZCPs) that service each zone. Depending on the configuration, there are one or two gateway routers in a master site. In the Single Zone Redundant i Multizone Capable configurations, the failure of one gateway router does not take RF sites out of the wide area trunking mode. However, when the master site is configured as Single Zone Non-Redundant, the failure of a gateway router results in the site going into the failsoft mode.

Provided the master site is configured as Single Zone Redundant or Multizone Capable, each RF site interfaces to two core routers through the CWR at the master site. This allows the system to stay in wide area trunking mode when a single core router fails. This rule does not apply, when the master site is configured as Single Zone Non-Redundant, with only one core router.

Redundancy for InterZone communications is supported through the exit routers. If the master site is configured as Single Zone Redundant or Multizone Capable, each master site has two exit routers that interface to other zones through the CWR relay panel at each master site. This allows the system to maintain InterZone connectivity when a single exit router failure occurs. This rule does not apply, when the master site is configured as Single Zone Non-Redundant, with only one exit router.

**NOTICE:** Provided the master site is configured as Single Zone Redundant or Multizone Capable, the failure of an exit router temporarily takes a zone out of InterZone trunking with other zones, until the network can converge to the remaining exit router. This convergence takes approximately 10–20 seconds in an ASTRO® 25 multizone system.

In an ASTRO® 25 system, voice, voice control, and NM traffic flow over the same physical bandwidth between the master sites. Traffic is sent as IP into the CWR, with T1s connecting CWR relay panels between zones. Exit routers prioritize voice and voice control over other system traffic. Due to the nature of how routing works between zones, only one exit router in each zone carries InterZone traffic between zones at a time.

Systems with the Dynamic System Resilience feature implemented are considerably less vulnerable to connection problems resulting in the system switching to one of the fallback modes. The extra resilience provided by the Dynamic System Resilience feature allows them to remain in InterZone trunking even in the event of a serious malfunction or a natural disaster. For more information on the Dynamic System resilience feature, see the *Dynamic System Resilience* manual.

## 3.3.2 Modes of Operation

The ASTRO® 25 communication system functions in various operating modes. Standard operating modes identify system operating modes not typically induced by user intervention. Fault states are reported to the Unified Event Manager (UEM) application by the site controller.

The system attempts to maintain the highest trunking mode available (InterZone, zone-level, wide area, site trunking, then failsoft). The ZoneWatch channel grid display shows faults against sites and channels to aid in troubleshooting.

User-initiated operating modes are system operating modes induced by intentional user intervention. Through the use of UEM diagnostic commands, an operator can force the system (such as site, channel or zone) into a lesser operating mode if needed. While usually not desirable, this user intervention may be useful for testing or training users to operate in the unlikely event of partial radio system failure.

**NOTICE:** User-initiated operating modes identify system operating modes typically induced by intentional user intervention. Site Test command resets an ASTRO® 25 repeater site. Using this command causes any subscriber that was locked to the site to scan for other sites in the system.

### 3.3.2.1 Standard Operating Modes

The following are standard operating modes:

- InterZone trunking – InterZone trunking is an operating mode applicable to multizone systems. When the system is in an InterZone trunking mode, the system functions to provide zone to zone communication and typically wide area trunking services for the participating zones. See InterZone Trunking on page 67.
- Wide area trunking – Wide area trunking is an operating mode applicable to multizone or single zone systems. When a system is in wide area trunking, it functions to provide trunking communication services to most, if not all, of the sites in a zone. A system can be in wide area

trunking mode without being in the InterZone Trunking mode or operation. See Wide Area Trunking on page 68.

- Site trunking – Site trunking is an operating mode applicable to multizone or single zone systems. When in Site trunking, a site functions as a standalone trunking system and is under the control of the site or subsystem controller. See Site Trunking on page 68.
- Site Failsoft – Site Failsoft is an operating mode applicable to multizone or single zone systems. When in Site Failsoft, a site functions without the use of a site controller and therefore trunking services are not provided. Base stations and repeaters function only as repeaters. Base radios function only in conventional mode. See Site Failsoft Operation on page 69.
- Local Failsoft within a Trunked IP Simulcast Subsite (remote site) – Local Failsoft is an operating mode applicable to multizone or single zone systems. When the Trunked IP Simulcast Remote Site is in Local Failsoft, the configured base radio operates in a conventional mode through in-cabinet repeat of audio.

**NOTICE:** The Site Failsoft operating mode is considered primarily a standard operating mode because communication resources may function in Site Failsoft mode under conditions not initiated by user intervention. However, the Site Failsoft operating mode can also be user initiated from the diagnostics capability of the Unified Event Manager (UEM).

### 3.3.2.1.1 InterZone Trunking

InterZone trunking is the state of one zone relative to another zone. InterZone trunking means that the two zones involved have:

- An operational InterZone Control Path (IZCP) between the two zones.
- At least one core router in service in each zone.
- Group home zone mapping tables in both zones.

**NOTICE:** Individual unit ID mapping tables are not required for a zone to be able to enter InterZone trunking. However, they are required for individual services to work (for example, private calls).

**IMPORTANT:** InterZone trunking modes do not apply to single zone systems. However, it is important for a single zone system operator to enter a home zone map in the User Configuration Server with all group and radio IDs mapped to Zone 1 as their home zone. To understand system failure and recovery scenarios, it is important to understand home zone relationships with InterZone trunking.

If the zone controller can send messages and receive replies from the other zones, one of the implications is that the following are functional:

- At least one port in the zone controller
- A gateway router
- The LAN switch
- An exit router
- The physical links between the master sites

If any one of the criteria listed for InterZone trunking are not met, the two zones are in a “no InterZone trunking” state with respect to each other.

**NOTICE:** The Unified Event Manager (UEM) application can place zones into a “zone isolated” state. In this state, the isolated zone does not enter InterZone trunking with respect to all other zones in the system.

In an ASTRO® 25 system, the RF sites and subsystems, console operator positions, and telephone interconnect devices do not need to be available for InterZone trunking to exist between two given zones.

### 3.3.2.1.2 Wide Area Trunking

In wide area trunking mode, remote sites receive call processing instructions from the master site zone controller and a radio subscriber registered at a site can communicate with any other radio subscribers in the system. The basic criteria for wide area trunking include an active RF site control path between zone controller and site, an enabled audio gateway router (rendezvous point) in the zone, a control channel, and a voice channel at a site.

If the zone controller can send commands and receive replies from the sites, one of the implications is that minimally the following are functional:

- At least one port in the zone controller
- A gateway router
- The LAN switch
- A core router
- Cooperative WAN Routing
- The site gateway
- The physical link between the master site and the remote site
- PTP radio devices

### 3.3.2.1.3 Site Trunking

Site trunking is a feature which enables each remote site to act as a standalone trunking system, in case communication with the zone controller is lost. The default mode of operation in site trunking is handling dispatch calls with the two priority levels of emergency and normal. Subscriber access control defaults to all individuals and talkgroups allowed. Secure calls at the site are allowed, because all repeaters are ASTRO® 25 capable. The console cannot access calls at a site in site trunking.

The link with the zone controller can be lost if any of the following hardware fails:

- Zone controller
- Zone controller switchover

  **NOTICE:** Loss of a zone controller and subsequent switchover results in the temporary loss of wide area trunking.

- Both core routers
- Both gateway routers
- Both exit routers
- Cooperative WAN Routing
- The LAN switch
- Digital cross-connect switch (if installed)
- site gateway (or both redundant site gateways, if installed)
- Channel bank (if mutual aid is supported at the site)
- SmartX Site Converter
- PTP radio devices

If either of the following conditions occur, the remote site can also enter site trunking mode:

- Communication with the zone controller is lost for a period greater than 3 seconds.
- The network manager has manually directed the remote site into site trunking.

### 3.3.2.1.4 Site Failsoft Operation

If the system is designed properly, many components would have to fail before a site would go into the failsoft mode. Failsoft operation is the last mode that provides communications through repeaters.

The number of repeaters accessible for radio use depends on:

- Whether the subscriber radios are programmed for failsoft
- How they are programmed to operate in failsoft mode

## 3.4 RF Subsystem Reliability

ASTRO® 25 sites and subsystems have several operational states. These states are independent of whether the site or subsystem is part of a single or a multizone system. Four possible modes exist for a given RF site or subsystem in relation to the zone it is in:

- Wide area trunking operation under control of a zone controller
- Site or subsystem trunking under control of the site or subsystem controller
- Site or subsystem Failsoft operation
- Site or subsystem off

This section discusses the unique characteristics of the following types of RF subsystems and sites that can be installed in an ASTRO® 25 system:

- ASTRO® 25 repeater subsystem
- Simulcast Subsystem
- IP Simulcast Geographically Redundant Prime Site
- 3600 RF Subsystem
- ISSI.1 Network Gateway Site
- PS LTE PTT Gateway Site
- Conventional Sites and Conventional Subsystems

### 3.4.1 ASTRO 25 Repeater Subsystem

An ASTRO® 25 repeater site requires a minimum of two ASTRO® 25 repeaters. When two are installed, one assumes the role of the control channel, while the other acts as the site voice channel. The pool of potential control channels and voice channels increases as ASTRO® 25 repeaters are added to a site, thus providing greater fault tolerance. The subsystem includes two site controllers. If the current site controller fails, the standby site controller assumes that control and the site continues to operate in wide area trunking mode. For more information on ASTRO® 25 repeater subsystem see *ASTRO 25 Repeater Site – Infrastructure* manual.

### 3.4.1.1 ASTRO 25 Repeater Site Modes of Operation

The following are the operational modes for an ASTRO® 25 repeater site:

**Wide Area Trunking**

An ASTRO® 25 repeater site can remain in wide-area trunking if the following resources are available:

- One voice channel
- One control channel
- A site controller
- Connectivity through the Ethernet switch or switches
- A site router/gateway
- A physical link between the subsystem and the Master Site/Zone Core
- A logical path between the site router/gateway and the Master Site/Zone Core IP equipment

**Site Trunking**

Site trunking operation takes place when no physical or logical link is between the site routers/gateways and the Master Site/Zone Core. It can also be initiated from the diagnostic capability in the Unified Event Manager (UEM). If a site controller switchover occurs while the site is in the site trunking state, all active calls at the site are transmission trunked.

**Site Failsoft**

Site Failsoft mode of operation at an ASTRO® 25 repeater site takes place only when both site controllers fail, the Ethernet switch fails (or both fail in a dual-switch configuration), no base radios are operational control channel capable, or all voice channels are inoperative. Site Failsoft can also be initiated from the diagnostic capability in the UEM. When an ASTRO® 25 Repeater Site enters Site Failsoft, the channels configured for Failsoft operation begin using their "In-cabinet Repeat" mode. Subscriber radios configured for Failsoft operation can only place calls to other subscriber radios on the same Failsoft channel.

**Site Off**

Site Off is an operational mode that can be initiated from the diagnostic capability in the UEM. In this state, the subsystem is not available to the subscriber radios.

**NOTICE:** Site Failsoft is only supported in FDMA mode.

If a site controller switchover occurs while the subsystem is in wide-area trunking state, all active voice calls at the site continue without any interruption in service. No "in progress" voice calls are lost on a site controller switchover. This stability is possible because the active voice call states and databases of the active and standby site controllers are synchronized.

If one site controller fails, the other maintains the system in wide-area trunking. If the site is in site trunking mode, however, the site controller manages all site functions and call processing.

For ASTRO® 25 repeater sites using dual site routers/gateways, a Master Site/Zone Core interface link failure or a site router/gateway failure has no effect on wide-area operations because the remaining site router/gateway maintains the links. With a single router configuration, however, the subsystem enters site trunking mode if a Master Site/Zone Core interface link failure or a site router/gateway failure occurs.

## 3.4.2 Simulcast Subsystem

In the Unified Network Configurator (UNC), simulcast subsystems and Single Transmitter Receiver Voting (STRV) subsystems are known as multisite subsystems. These multisite subsystems consist of a prime site and up to 15 remote sites. From the master site, the multisite subsystem is considered one site. However, a multisite subsystem operates differently from an ASTRO® 25 repeater site in some of the operational modes. See *Trunked IP Simulcast Subsystem — Infrastructure* manual.

**NOTICE:** The information in this section is applicable to both circuit-based simulcast systems or IP-based simulcast systems.

### 3.4.2.1 Simulcast Subsystem Modes of Operation

Many of the modes of operation available in a Simulcast Subsystem are similar in name to the modes of operation available in an ASTRO® 25 Repeater Site. But there are operational differences between an ASTRO® 25 Repeater Site and a Simulcast (Multi-Site) Subsystem. These differences and some similarities are described in the following sections.

**NOTICE:** Simulcast subsystem with Receive only subsites and Single Transmitter, Receiver Voting (STRV) subsystems, are both types of Multi-Site subsystems and have the same modes of operation as a simulcast subsystem.

The operational modes for both circuit-based and IP-based simulcast subsystems include the following:

- Wide-area trunking
- Site Trunking
- Site Failsoft: Site (Subsystem) Failsoft and Local Failsoft
- Local Failsoft at remote site
- Site Off

**Simulcast Channels States of Operation**

The operational modes for both circuit-based and IP simulcast subsystems include the following:

- Enabled
- Malfunctioned
- Impaired
- User Disabled
- Unconfigured state

**Simulcast Subsites States of Operation**

The operational modes for both circuit-based and IP simulcast subsites include the following:

- Enabled
- Malfunctioned
- User Ignored
- Unconfigured

**Simulcast Subsystem Resource Voting**

Resource Voting impacts the criteria to enter, or not to enter failsoft. For details, see Simulcast Subsystem – Resource Voting on page 75.

#### 3.4.2.1.1 Simulcast Subsystem Wide Area Trunking Mode

Both circuit-based and IP simulcast subsystems remain in wide-area trunking as long as the following resources are available and functioning properly:

- The site control path (transport link, zone controller, gateway router, LAN switches, and core router at the Master Site/Zone Core)
- One site router/gateway
- One prime site controller

- One site switch
- At least one voice channel and associated comparator
- At least one control channel
- The resource Voting rules given in section Simulcast Subsystem – Resource Voting on page 75 dictate that the sub-system should NOT enter failsoft mode.

**NOTICE:** The site control path includes any transport link between the subsystem and Master Site/Zone Core, zone controller, gateway router, WAN and LAN switch, and core router equipment.A functioning site control path results from good communications between the prime site controller and the zone controller.

**NOTICE:** For an IP simulcast subsystem, with a redundant configuration, the LAN maintains wide-area trunking performance if a single switch fails. In a geographically redundant configuration, an outage could occur briefly before restoration of wide-area trunking.

## 3.4.2.1.2 Simulcast Subsystem Site Trunking Mode

When a simulcast subsystem loses the site control path due to a failure in the transport link or site control path equipment, and the subsystem enters site subsystem trunking mode. The subsystem continues to provide trunked voting/simulcast operations. In site trunking mode, subscriber radios can continue to communicate with members of their talkgroup registered at the site subsystem.

**NOTICE:** Communication outside the subsystem, communication with console operators, and centralized telephone interconnect are not available when the subsystem is in site trunking mode.
Any subsite designated as an essential subsite must have the required resources to provide trunking services. For details, see the description of an essential subsite in Simulcast Subsystem – Resource Voting on page 75.

## 3.4.2.1.3 Simulcast Subsystem Failsoft Mode

There are two types of Failsoft available depending on the type of site/subsystem:

- Site Subsystem Failsoft is available for both Circuit-based and IP-based Simulcast subsystems.
- Local Failsoft is only available for IP Simulcast Subsites which are part of M1, M2, M3, or L core system configurations. Local Failsoft is a configurable item on each base radio.

**NOTICE:** An ISR site enters an in-cabinet repeat mode for failsoft. A Simulcast or STRV type system enter sub-system wide failsoft with repeat happening through comparator voting.

**Site Subsystem Failsoft**

can be used when a major failure such as the loss of all Site Controllers at an ASTRO® 25 Repeater Site or a Simulcast Subsystem Prime Site occurs. When this type of major failure occurs, the subsystem can no longer maintain a control channel for use by the subscriber radios operating within the site/subsystem. When this happens, the subscriber radios try to locate another control channel at another repeater site or simulcast subsystem. If the subscriber radios cannot locate another control channel on which to operate and if the following conditions are met, the subscriber radios operate in Site Failsoft:

- One or more channels within the site/subsystem have been configured for Site Failsoft.
- The subscriber radios are configured for Failsoft operation.

With these conditions met, the subscriber radio enter a two-way conventional mode of operation on a given Failsoft channel. While in Failsoft, subscriber radio is limited to communicating only with other subscriber radio on the same Failsoft channel. The channel transmits a beep tone used for Failsoft to notify the radio user that the subscriber radio is operating on a Failsoft channel.

**NOTICE:** Failsoft call traffic is still being voted and simulcasted by the available channel resources.

The subscriber radios can be configured for the following modes of Failsoft operations:

- Failsoft by last known control channel – all talkgroups at a site/subsystem use the last known control channel transmit/receive frequency pair in a conventional mode
- Failsoft by Personality – subscriber radio uses a predefined channel transmit/receive frequency pair in a conventional mode for all talkgroups configured under a given personality in the subscriber radio.
- Failsoft by Talkgroup – subscriber radio uses a predefined channel transmit/receive frequency pair in a conventional mode for a specific talkgroup
- Failsoft Disabled – subscriber radio displays an “Out of Range” indication and no site-based RF communications are possible

Subscriber radios automatically exit Failsoft operation when a control channel is detected and the subscriber radio has synchronized with the site/subsystem.

**Local Failsoft** can be used when a critical failure occurs involving the IP Simulcast Prime Site, or the links between the IP Simulcast Primary Site and an IP Simulcast Subsite are not functioning. Critical failures can be caused by either of the following:

- The comparators at the Simulcast Prime Site are inoperable
- An IP Simulcast Subsite has lost its links to the comparators at the IP Simulcast Prime Site

Under this type of failure, and if one or more of the Multi-Site Base Radio (MsBR) at a subsite have been configured for Local Failsoft, the MsBR enters Local Failsoft mode based on its configuration. MsBRs configured for Local Failsoft transmit a special Failsoft message indicating Local Failsoft.

The timing of the Local Failsoft alarm tone is different than the Site Failsoft beep tone, so that the radio user is able to distinguish between Local Failsoft and Site (subsystem) Failsoft.

The base radio automatically exits Local Failsoft operation, after detecting that the link to the comparator has been reestablished, or when the Local Failsoft configuration has been disabled on the base radios. The subscriber radios automatically exit Failsoft operation when a control channel is detected and subscriber radio has synchronized with the control channel.

**NOTICE:** Any channels frequencies in use for Local Failsoft must be disabled at all other subsites, while Local Failsoft base radios are transmitting to avoid RF interference between the base radios at the different subsites. Use caution when configuring MsBRs for Local Failsoft. As the MsBR in Local Failsoft mode key locally on a simulcast frequency, destructive interference occurs on the same channel if other sub-sites of the simulcast sub-system transmit on the channel and are within the RF coverage range of the MsBR.

### 3.4.2.1.4
## Simulcast Subsystem Site Off Mode

Site Off is a mode of operation initiated from the diagnostics capability of the Unified Event Manager (UEM). In this state, the subsystem is not available to the subscriber radios. Site Off de-keys the control channel, making it unavailable for subscriber radios to lock to.

Within the operational boundaries of the subsystem states, the remote sites may be found in one of the four states:

- Enabled
- Malfunctioned
- User ignored
- Unconfigured (unused)

### 3.4.2.1.5 Simulcast Channel States of Operation

IP Simulcast subsystem channels may be in any of the following states:

- Enabled
- Malfunctioned
- Impaired
- User Disabled
- Unconfigured state

**Enabled State**
When a channel is in the Enabled state, the channel is eligible for assignment in the Multi-Site subsystem.

**Malfunctioned State**
When a channel is in the Malfunctioned state, a resource fault somewhere on the channel has caused the channel to be marked as unusable for call processing. Testing may still be done on the channel. The channel is not precluded from being a Failsoft channel.

**Impaired State**
When a channel is in the Impaired state, a resource fault has occurred somewhere on the channel, but the resource in the malfunctioned state is located in a Malfunctioned or User Ignored subsite. The channel is still used for call processing, but reduced system coverage may result.

**User Disabled State**
When a channel is in the User Disabled state, the user has requested that the channel is not to be used for call processing. User Disabled channels may be tested, and may be used for Failsoft channels.

**Unconfigured State**
If a channel number is unused, the channel is reported to be in the Unconfigured state.

### 3.4.2.1.6 Simulcast Subsystem Subsite States

Each subsite may be in one of the following states:

- Enabled
- Malfunctioned
- User Ignored
- Unconfigured

**Enabled State**
When the subsite is in the Enabled state, the subsite operates as a fully functional part of the Simulcast or STRV subsystem.

**Malfunctioned State**
When individual resource faults degrade the capabilities of the subsite below a defined threshold, the system places the subsite in the Malfunctioned state. When a subsite is in the Malfunctioned state, the system disregards the state of the individual resources at the subsite so that they do not affect the channel states in the rest of the subsystem. The subsite continues to participate in the operation of the subsystem where it cans.

**User Ignored State**
When the user does not want the state of the individual resources at a subsite to affect the channel states in the rest of the subsystem, the user may request to put the subsite in the User Ignored state. Operationally, the User Ignored state is equivalent to the Malfunctioned state.

**Unconfigured State**

If a subsite number is unused, the subsite is reported to be in the Unconfigured state.

### 3.4.2.1.7 Simulcast Subsystem – Resource Voting

When a simulcast subsystem experiences malfunctions, the use of resource voting is the method the simulcast subsystem uses to maximize the number of channels and subsites available for use.

The simulcast subsystem implements “resource voting” to manage the simulcast subsystem resources (channels). The resource voting algorithm collects resource capabilities for the simulcast subsystem and either enables or disables resources based on the current capabilities in the subsystem. Having multiple subsites becomes an asset instead of a liability since the subsites can be removed from the resource voting pool when they are experiencing significant difficulties. The simulcast subsystem degrades gracefully to provide a continuum of available services.

Each simulcast subsite (remote site) is assigned an availability number. The availability number is a parameter that the customer can configure via Unified Network Configurator (UNC) or Configuration/ Service Software (CSS). It specifies the percentage of subsite channels that must experience malfunctions before the subsite is removed from service (placed in the malfunctioned state). Since subsite channel malfunctions affect the status of the channel across the entire IP simulcast subsystem, it is important to have a mechanism that prevents significant problems at a single remote site from bringing down the entire subsystem.

The availability number can have a value from 1 to 100. The default value is 50. For example, for a 10-channel subsystem, a subsite with an availability number of 50 is put in the malfunctioned state if 5 subsite channels at that subsite are in a failed state.

The availability number 100 has special meaning. A subsite with an availability number of 100 is called an essential subsite. Customers assign an availability number of 100 to subsites that provide critical RF coverage. Critical subsites need to be on the air at all costs, even if it means that the entire IP simulcast subsystem is in Failsoft mode. Essential subsites are in the failed state if all of their subsite channels are unavailable (for example, from a link failure). However, if the essential subsite is capable of supporting a wide area Failsoft channel, then the rest of the simulcast subsystem channels follow the capability of the essential subsite’s channels.

A subsite can be put in the malfunctioned state even if its availability threshold is not reached. If all non-essential subsite’s control channels experience malfunctions, then the subsite is put in the malfunctioned state, so that the rest of the IP simulcast subsystem can establish a control channel. If channels 1-4 at a non-essential subsite malfunction, the subsite is put in the malfunctioned state even though its availability number is 50 or higher.

Once a subsite is in the malfunctioned state, all IP simulcast subsystem channels that are out of service due to problems at the subsite in the failed state are returned to service. The subsite in the malfunctioned state is included in all call activity; it participates to the best of its ability. The IP simulcast subsystem channels that are returned to service are in the impaired state; the channels are in use, but not all channel’s resources are functioning properly.

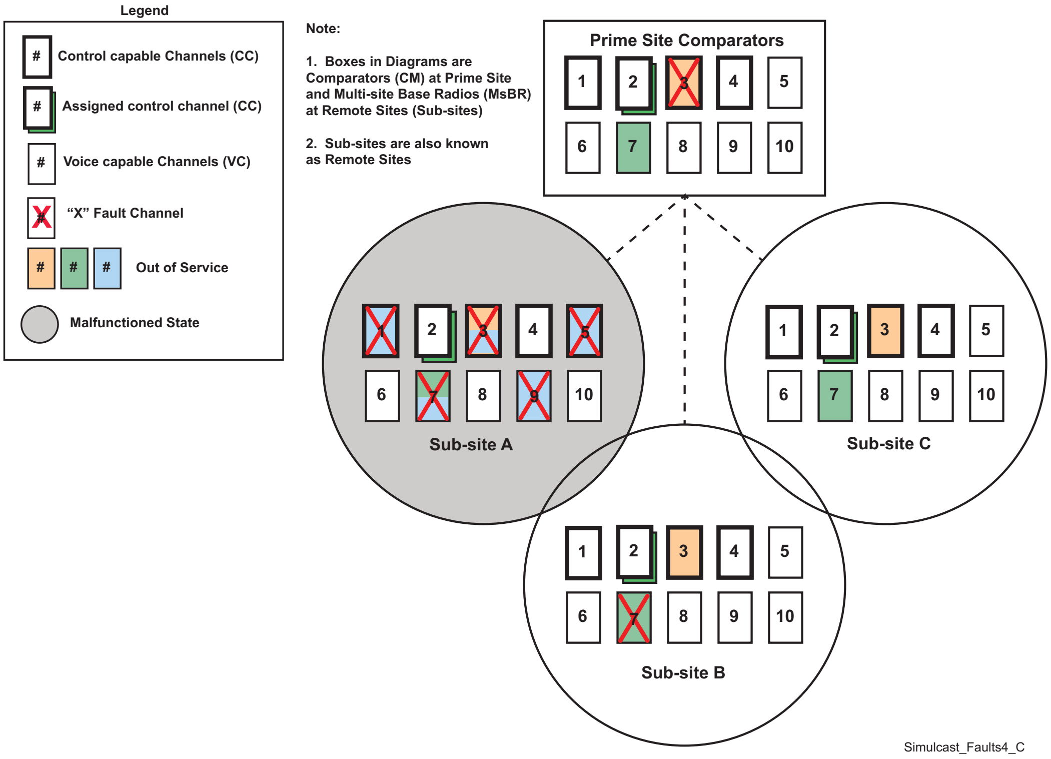
The computation of the percentage of subsite channels in the malfunctioned state is based on the number of channels that are programmed to be traffic capable, minus the number of channels that are user disabled. Channels that are unconfigured are ignored in this calculation: MSC = (CM/(CT-CD))x100.

- MSC is the percentage of Malfunctioned Subsite Channels (channels in the malfunctioned state)
- CM is the number of traffic channels at the Simulcast or STRV remote site which are in the malfunctioned state
- CT is the total number of traffic channels
- CD is the number of user disabled traffic channels

Aside from user-disabled channels, the determination of a state of a subsite is based solely on the state of the equipment at that subsite. Comparator capabilities do not affect the state of the subsites.

In the figure below, the transmitter combiner serving the odd channels of remote site A is in the malfunctioned state. Remote site A is in the malfunctioned state since five of its 10 channels are in the malfunctioned state and the remote site availability number is 50. Channel 3 is still out of service because of the comparator failure, and channel 7 is still out of service due to the channel failure at remote site B. Channels 1, 5, and 9 are in the impaired state. Since the transmitter combiner is causing the channel failures, the impaired channels at remote site A operate normally for the receive side of the channel, but no transmissions originate from remote site A for the impaired channels.

**Figure 8: Remote Site-A Put in the Malfunctioned State Because of Availability Number Trigger**


Legend
# Control capable Channels (CC)
# Assigned control channel (CC)
# Voice capable Channels (VC)
"X" Fault Channel
# # # Out of Service
Malfunctioned State
Note:
1. Boxes in Diagrams are Comparators (CM) at Prime Site and Multi-site Base Radios (MsBR) at Remote Sites (Sub-sites)
2. Sub-sites are also known as Remote Sites
Prime Site Comparators
1 2 3 4 5
6 7 8 9 10
Sub-site A
Sub-site B
Sub-site C
Simulcast_Faults4_C

### 3.4.2.2
## Single Transmitter Receiver Voting Subsystem – Modes of Operation

The operational modes of a single transmitter receiver voting subsystem include the following:

- Wide area trunking
- Site trunking
- Failsoft

### 3.4.2.2.1
## Wide Area Trunking

In wide area trunking, remote sites receive call processing instructions from the master site zone controller. A radio subscriber registered at a site can communicate with any other radio subscribers in the system. The basic criteria for wide area trunking include an active RF site control path between zone controller and site, an enabled audio rendezvous point in the zone, a control channel, and a voice channel at a site.

### 3.4.2.2.2 Site Trunking

When the STRV subsystem loses communication with the master site zone controller, the subsystem continues to trunk its channel resources within its boundaries and is in the site trunking mode.

### 3.4.2.2.3 Failsoft

When the site controllers are not available to provide trunking operations, the subsystem enters a failsoft mode of operation. This also occurs if all control channels are disabled or malfunctioned or if only one channel is enabled. The operating modes of the STRV subsystem are like those for the digital simulcast subsystem.

## 3.4.2.3 Simulcast Subsystem Behavior in Failure Scenarios

This section contains information about system behavior in failure scenarios.

### 3.4.2.3.1 Site Controllers

Redundant site controllers are installed at the prime site to handle trunking control traffic, allocate channel resources in the simulcast subsystem, and manage software downloads to comparators and base radio equipment. During normal operation one Site Controller is active and the other one is inactive. If one site controller fails, the other maintains the system in wide-area trunking. If the simulcast subsystem is in site trunking mode, the site controller manages all site functions and call processing.

**NOTICE:** When redundant routers are installed at the prime site, full redundancy is supported. This is especially important for wide area services that need to remain highly reliable. It also ensures that any loss of a single switch, router, or site controller does not cause a loss of wide area services. If only one router is installed at the prime site, then losing one switch that is connected to the router would cause the multisite subsystem to enter site trunking mode.

See the *GCP 8000 Site Controller* manual for implementation of the Site Controller in a Circuit-Based Simulcast System, IP-Based Simulcast System and IP-Based Simulcast System with Geographic Redundancy.

#### *3.4.2.3.1.1 Split Brain Operation*

The split brain mode applies in IP Simulcast Prime Sites in systems with Geographically Redundant Prime Site feature implemented. If the LAN connection between the two split-prime sites fails, the site controller at the secondary prime site activates due to loss of connectivity with the active site controller at the primary prime site. In addition, the standby comparators also transition to the active state due to loss of heartbeat messaging from the active comparators.

### 3.4.2.3.2 Prime Site Comparators

Each comparator is linked to a channel at each one of the remote sites. In Figure 9: Comparator to Channel Relationship on page 78, comparator 6 is linked to channel 6 at all three subsites. If the comparator fails, channel 6 is removed from service at all subsites.

**Figure 9: Comparator to Channel Relationship**

In an IP Simulcast Prime Site with redundancy, two comparators can be installed for a channel. The two comparators operate in an active/standby configuration for protection against loss of a channel if a single comparator or LAN switch fails.

During split brain operation (see Split Brain Operation on page 77), both comparators for a given channel are active. At that time, the transport network discards any packets received from comparators at the secondary prime site and only forwards packets from comparators at the primary prime site. In specific error cases when traffic between the prime sites is forwarded only in one direction, MsBRs may receive packets from both redundant comparators at the same time.

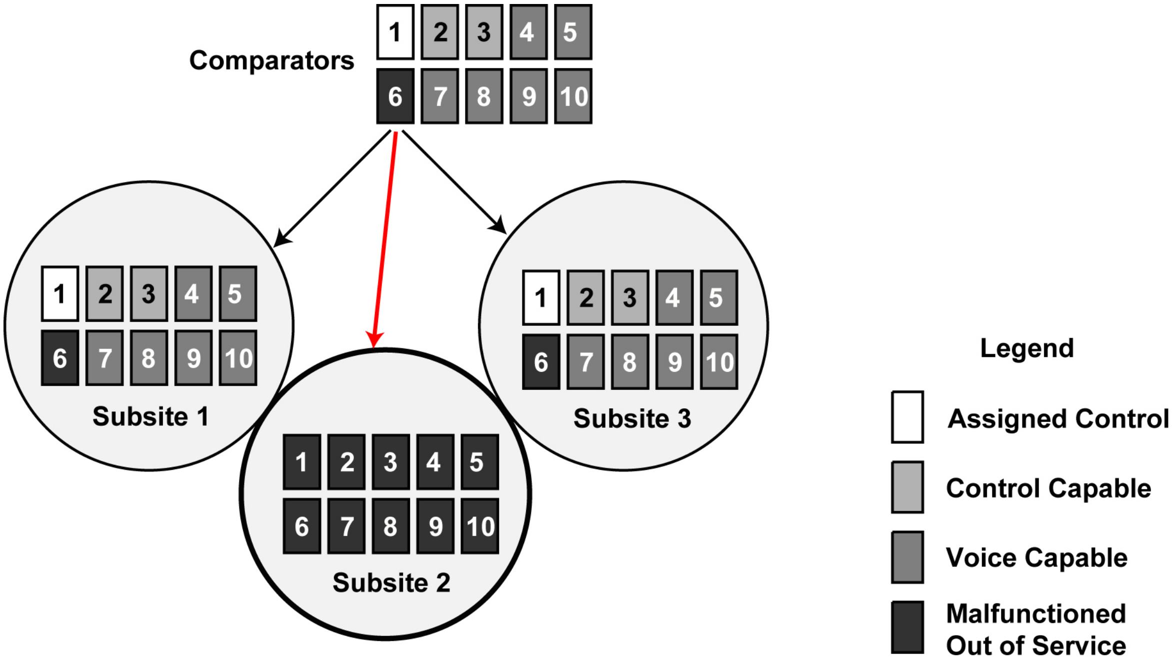
If comparator misconfiguration occurs in a subsystem with Geographically Redundant Prime Sites, faults get reported separately in the primary and the secondary prime site.

### 3.4.2.3.3 Site Links

Loss of the transport media between a subsite and the prime site causes the subsite to be removed from service.

For example, Figure 10: Loss of Site Link on page 78 shows the link between the prime site and Subsite 2 as malfunctioned. This loss removes Subsite 2 from service.

**Figure 10: Loss of Site Link**



B_S_subsystem_TS4

### 3.4.2.3.4 Simulcast Subsystem Channels

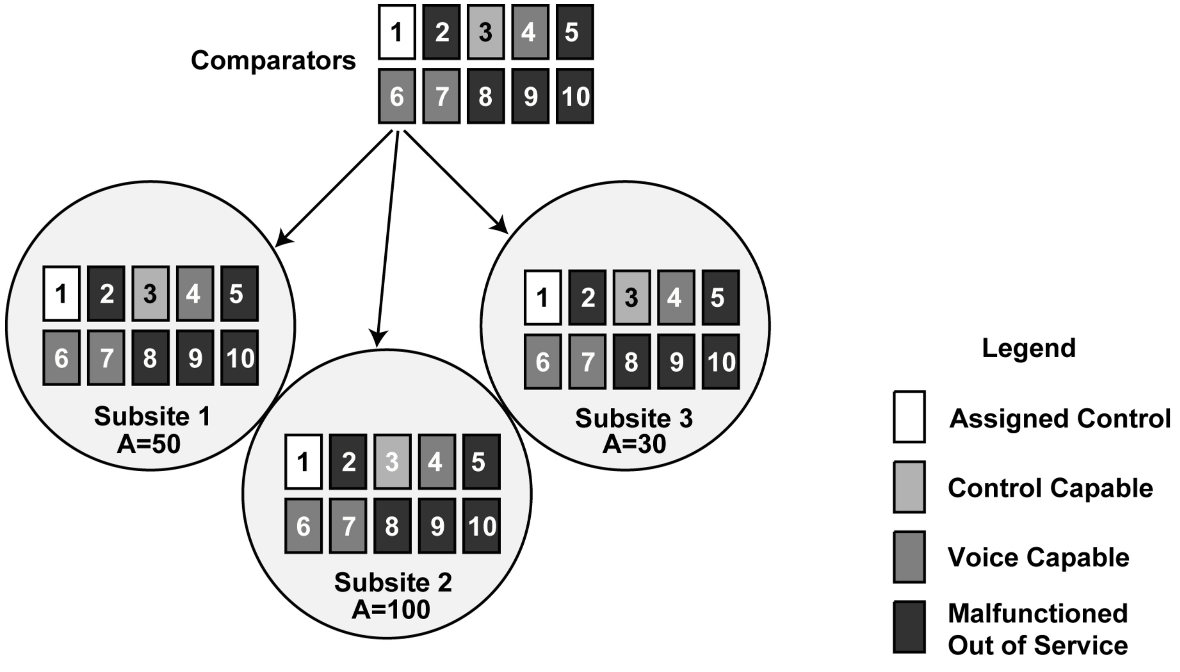
Simulcast subsystem channels may be in the enabled, malfunctioned, impaired, user disabled, or unconfigured (unused) states. The following rules apply when channels malfunction:

- If the percentage of malfunctioned remote site channels is greater than the availability number, the remote site is voted out by the active site controller so that the wide area channels can remain usable.
- The channels in operation with a malfunctioned base radio are displaced.
- Control and voice channel data is still sent to the malfunctioned remote sites.
- If all control channels are disabled because of malfunctions at the remote sites, the site controller chooses a remote site to malfunction to regain a control channel.
- If a nonessential remote site loses all of its control channels, the remote site is voted out by the active site controller.
- User disabled channels are not included in the computation of malfunctioned remote site channels.

Figure 11: User Disabled Channels on page 79 shows the effect of user disabled channels.

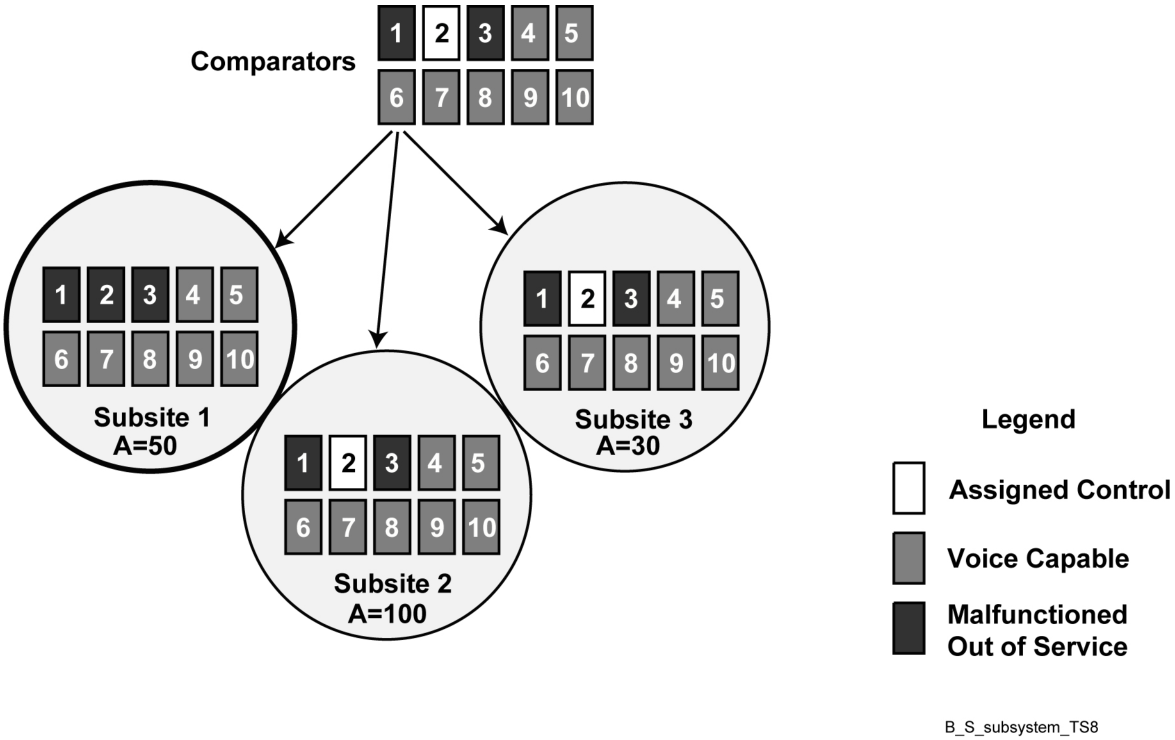
Figure 12: Loss of Control Channels on page 80 shows the effect that losing all control channels has on the subsystem. In this figure, all channels at Subsite 1 that were control channel capable have failed. Since there is no active Control Channel at Subsite 1, it is effectively out of service.

**Figure 11: User Disabled Channels**



B_S_subsystem_TS6

**Figure 12: Loss of Control Channels**



3.4.3

## 3600 RF Subsystems

3600 RF subsystems consist of a single site gateway and a single SmartX site converter which connects to a single existing 3600 RF site or simulcast subsystem.

3.4.3.1

### 3600 RF Subsystems – Modes of Operation

The operational modes of a 3600 RF subsystem include the following:

- Wide area trunking
- Site trunking
- Failsoft
- Site off

3.4.3.1.1

A 3600 RF subsystem remains in wide area trunking as long as the following resources are available and functioning properly:

- The site control path (transport link, zone controller, control router, LAN and WAN switching devices, and core router at the master site)
- One site gateway
- One SmartX site converter
- At least one operational voice channel with wide area capability
- At least one control channel

#### 3.4.3.1.2 3600 RF Subsystems – Site Trunking

When a 3600 RF subsystem loses the site control path (due to a failure in the transport link or site control path equipment) and the subsystem continues to provide trunked operations, the subsystem is in site trunking mode. In site trunking mode, radios can continue to communicate with members of their talkgroup that are also registered at the site. The following resources must be available and functioning properly to support site trunking mode:

- One SmartX site converter
- At least one operational voice channel with wide area capability
- At least one control channel

#### 3.4.3.1.3 3600 RF Subsystems – Failsoft

If the 3600 RF subsystem cannot maintain wide area trunking or site trunking, the subsystem enters the failsoft mode of operation. Failsoft mode occurs when the SmartX site converter is not functioning properly, when all control channels are disabled or malfunction, or when only one channel is enabled. In order for failsoft operation to occur on a channel, the comparator, the link to the remote site, the networking equipment (routers, switches, channel banks, and so on) and the base station on that channel must be operational.

#### 3.4.3.1.4 3600 RF Subsystems – Site off

Site Off is a mode of operation that is initiated from the diagnostics capability of the Unified Event Manager. In this mode, the subsystem is not available to the radios.

### 3.4.4 ISSI.1 Network Gateway Site

The ISSI.1 Network Gateway site consists of the network gateway, site gateway, site switch, and a firewall. It provides wireline interoperability among different P25-compliant networks.

#### 3.4.4.1 ISSI.1 Network Gateway Site – Modes of Operation

The ISSI.1 Network Gateway site can communicate with other ISSI.1 Network Gateway Sites as long as the following conditions are met:

- The ISSI.1 Gateway Module is enabled
- The peer ISSI.1 Network Gateway is enabled

An ISSI.1 Network Gateway site cannot communicate with other ISSI.1 Network Gateway sites, if one of the following happens:

- The ISSI.1 link is down
- One of the devices has experienced a critical malfunction
- The link to Zone Controller is down
- One of the devices has been disabled

## 3.4.5 ISGW

The Intersystem Gateway (ISGW) is a server application residing on a virtual machine. The ISGW supports an Inter-RF Subsystem Interface (ISSI) and a Console Subsystem Interface (CSSI) providing an ASTRO® 25 system with an interconnectivity solution for P25 compatible systems and consoles.

### 3.4.5.1 ISGW – Modes of Operation

For details see *ISSI 8000/CSSI 8000 – Intersystem Gateway* manual.

## 3.4.6 WAVE 7000 Site

The WAVE 7000 site consists of a redundant pair of WAVE 7000 servers, site switches, and site routers. The WAVE 7000 site provides wireline interoperability between an ASTRO® 25 system and a PS LTE system.

### 3.4.6.1 WAVE 7000 Site Modes of Operation

The WAVE 7000 site can provide communication between the ASTRO® 25 system and the PS LTE system as long as the following conditions are met:

- The The WAVE 7000 servers and the Site Relay Module are enabled
- Connectivity to the ASTRO® 25 system exists and is operational

A The WAVE 7000 site cannot provide communication between the ASTRO® 25 system and the PS LTE system sites, if one of the following happens:

- The link to Zone Controller is down
- One of the devices has been disabled

## 3.4.7 Conventional Sites and Conventional Subsystems

Unified Event Mananger (UEM) discovery is supported for a conventional subsystem (Conventional Hub Sites and Conventional Base Radio sites). For this architecture the conventional sites are no longer always colocated with a console site or RF sites with trunking channels.

To support discovery, configuration and fault management of the Conventional Subsystem UNC and UEM use a Conventional Subsystem ID and Conventional Site ID.

The UEM and InfoVista can collect latency, jitter, and dropped packets statistics for the Conventional Subsystem.

For the Conventional Subsystem architecture, auto discovery should be initiated in the Zone where the Base Radio sites reside.

### 3.4.7.1 Conventional Sites and Conventional Subsystems – Modes of Operation

See the *Conventional Operations* manual for details regarding the Modes of Operation for conventional sites and subsystems.

## 3.5
## PTP Device Fault Management

This section provides information on PTP Device Fault Management.

### 3.5.1
### PTP Device Management – Description

Both the PTP 600 and PTP 800 radios (including the PTP 800 IRFU – indoor RF Unit) support fault management functionality across ASTRO® 25 systems. Configuration and performance management for the PTP radios is done via the management application integrated into the radios and accessed via a web browser. Fault management also applies to any Site backhaul switches that are introduced into the backhaul subsystem as part of the feature. For details on managing PTP devices refer to the appropriate PTP User Guide provided by the third-party manufacturer.

The following typical fault management functions are provided for PTP devices:

- Initial discovery of devices
- Notification via event, alarm, and e-mail
- Automatic clearing of alarm
- Synchronization
- Supervision – With supervision fault management functionality, the user is able to determine if the UEM cannot communicate with the site controller due to various reasons, including PTP failure.
- Customer North Bound Interface (NBI) receives all events
- SSC NBI receives all events

Equipment supporting fault management of PTP includes:

- Wireless Bridge PTP radios
- Backhaul Switches
- Transport devices (routers and/or gateways)

The following restrictions for PTP devices are in place:

- Layer 2 backhaul only
- Not supported on DSR systems
- Must have contiguous connectivity to provide mgmt access for the microwave devices
- Maximum of 1024 devices
- The management is done via the PTP management subnet VLAN which is outside the RNI. None of the third-party Microwave devices plug into the LAN of the RNI, only on the WAN side.

#### 3.5.1.1
#### PTP 800 Link Configurations

Each PTP link includes a Compact Modem Unit (CMU) and Radio Frequency Unit (RFU) at the end of each link. The following configuration is available for PTP deployed in the system:

- 1+0 Configuration – a non-redundant link configuration
- 1+1 Configuration – a hot standby, redundant link configuration (available from PTP release 800-03-00 forward, UEM-manageable from 800-04-11 forward)
- 2+0 Configuration – a link configuration using two independent links to provide redundancy

### 3.5.1.2 PTP Device Fault Management – Capacity and Capability

- Maximum of 50 PTP devices per low tier zone (M1, M2)
- Maximum of 10 IP connections for PTP devices at each zone core – you can configure between 1 and the maximum number of available ports
- Maximum of 1000 PTP Devices per high tier zone (M3)
- Maximum of 10 IP connections for PTP devices at each zone core
- Maximum of 10 IP connections for PTP devices are possible at each Simulcast Prime Site or Simulcast Remote Site – you can configure between 1 and the maximum number of connections allowed per switch chassis
- Maximum of 10 IP connections for PTP devices possible at each Conventional-Only site – you can configure between 1 and the maximum number of connections allowed per switch chassis

## 3.5.2 PTP in ASTRO 25 Architecture

You can configure PTP in ASTRO® 25 system in the following ways:

- One Hop – T1 Single Link Using PTP
- One Hop – T1 Redundant Link Using PTP
- Two Hop – Ethernet Redundant Link Using PTP
- PTP Ribbon Topology
- PTP Hub and Spoke Topology
- PTP Ribbon Topology – Customer Backhaul Reuse
- PTP Ribbon Topology – Simulcast Backhaul Reuse

For more details - see PTP manual.

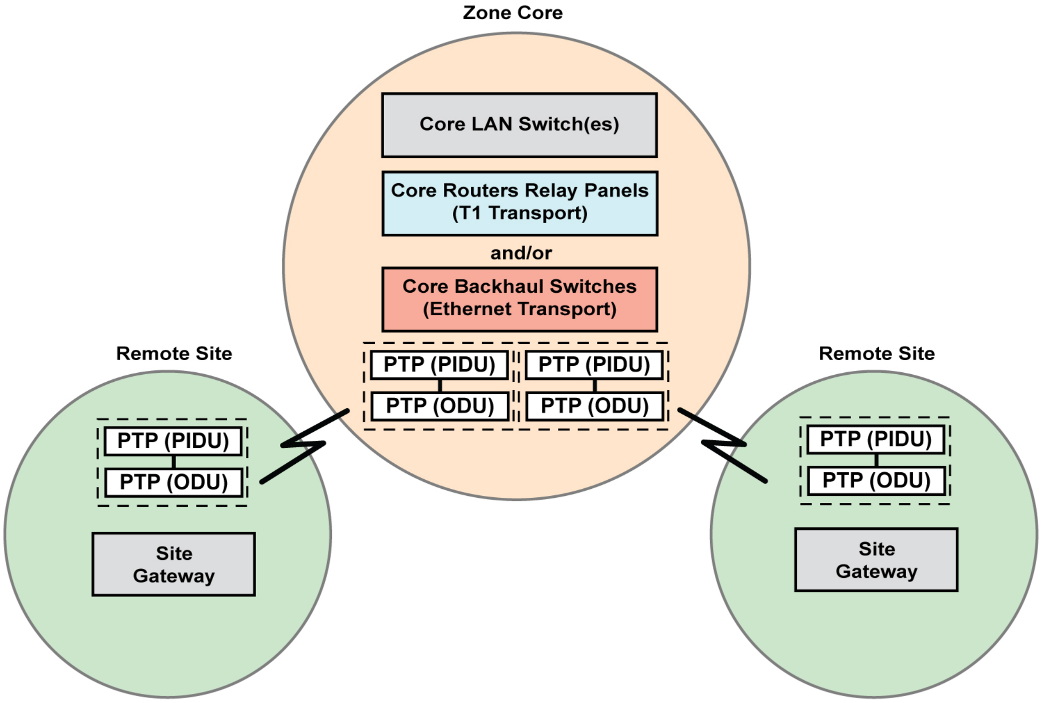
Fault management of PTP devices is supported by various ASTRO® 25 system architectures employing Ethernet backhaul connectivity and either Ethernet or T1 site links. The the diagrams in the following sections show examples of PTP implementation for common ASTRO® 25 system architectures.

**NOTICE:** For PTP implementation other than those shown here, including redundancy, contact your Motorola Solutions or Cambium Networks representative.

### 3.5.2.1 PTP System Diagrams

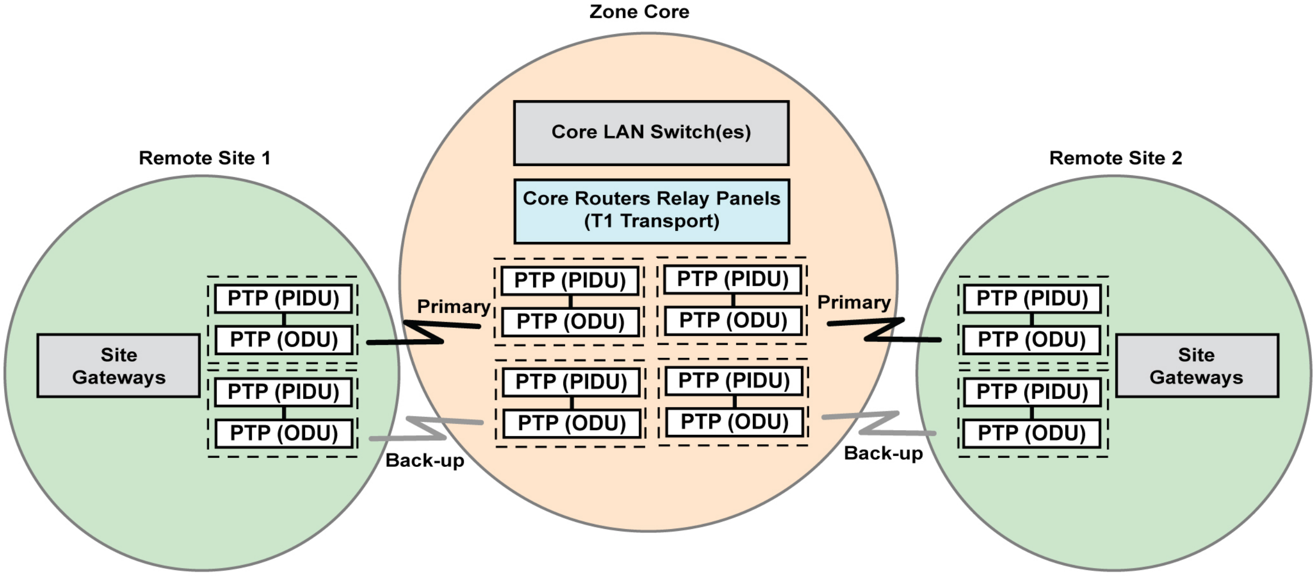
This section shows examples of PTP device deployment in various ASTRO® 25 systems.

**Figure 13: One Hop – T1 Single Link Using PTP**



PTP_1_Hop_single_link_T1_B

**Figure 14: One Hop – T1 Redundant Link Using PTP**



PTP_1_Hop_redun_link_T1_B

**Figure 15: Two Hop – Ethernet Redundant Link Using PTP**

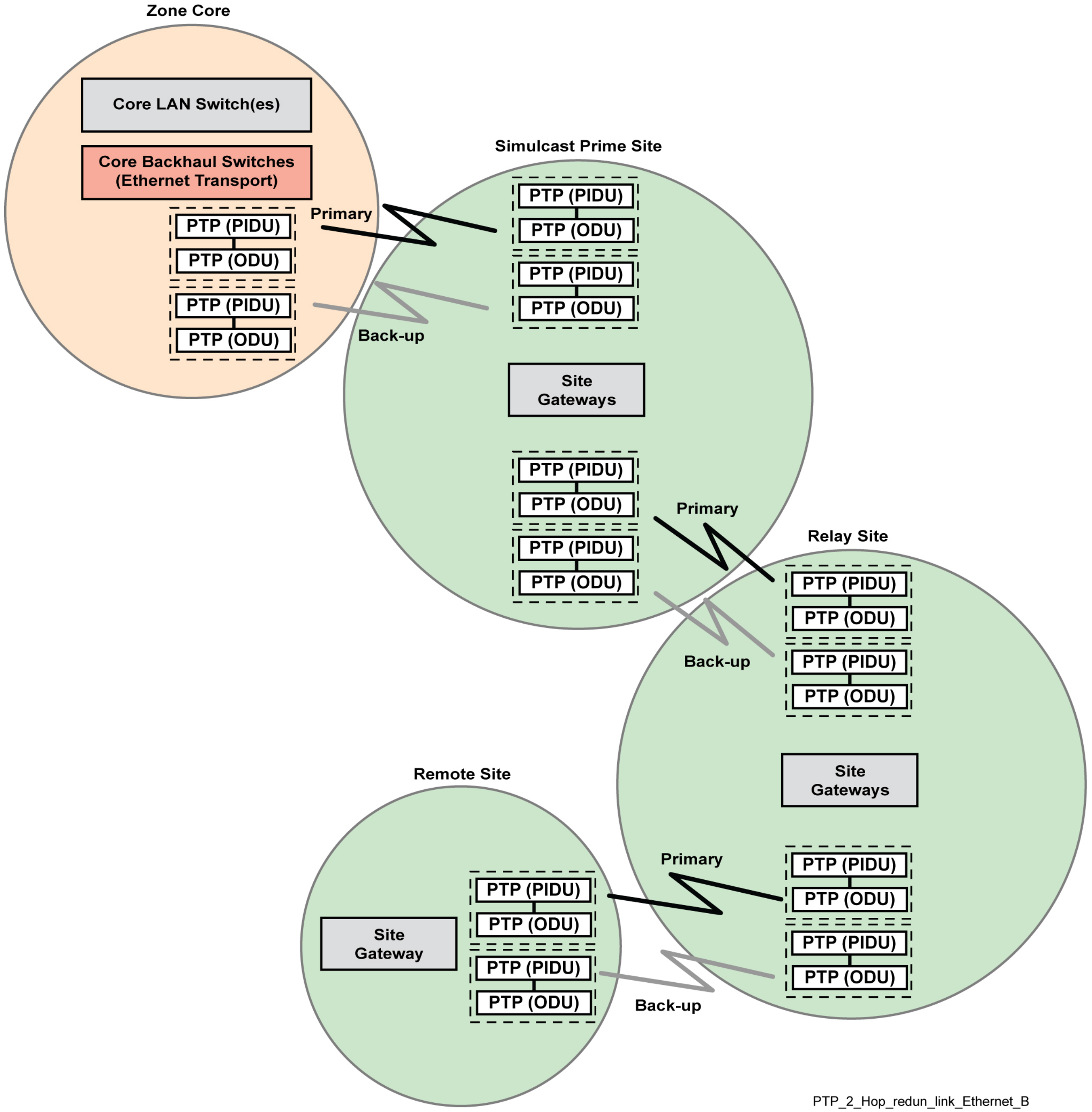
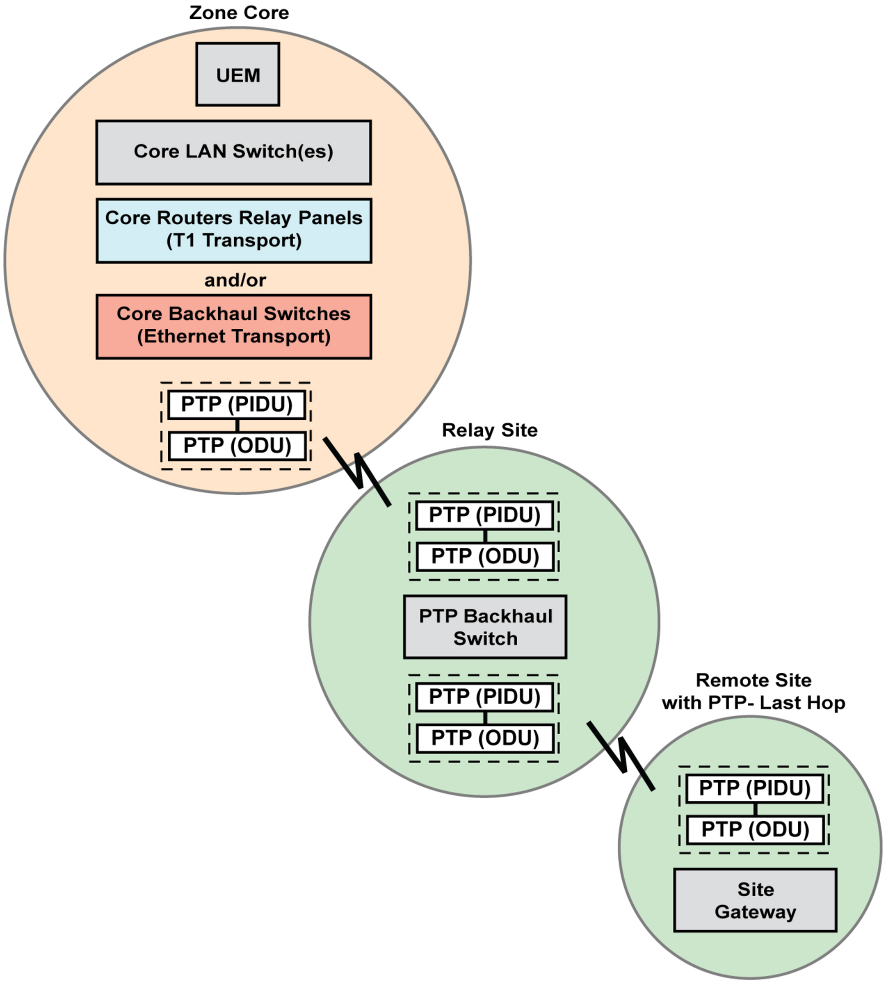


**Figure 16: PTP Ribbon Topology**



PTP_Topology1_B

**Figure 17: PTP Hub and Spoke Topology**

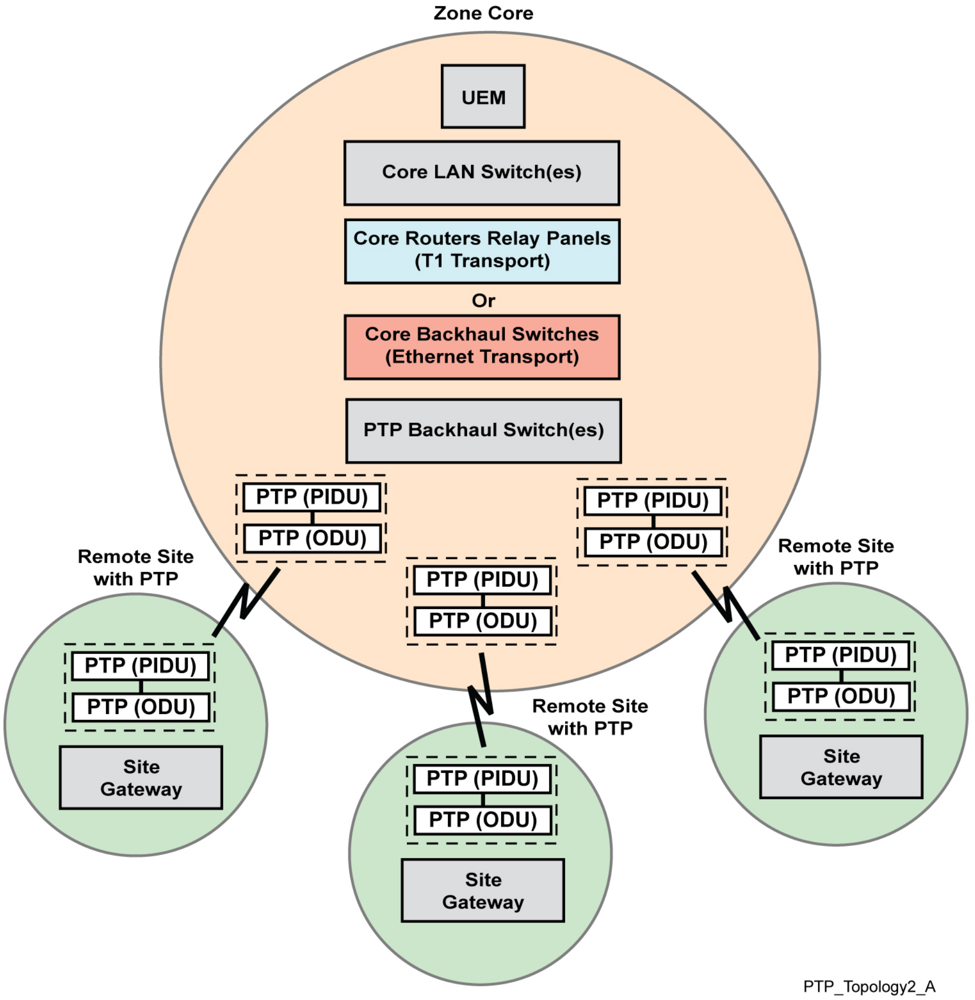
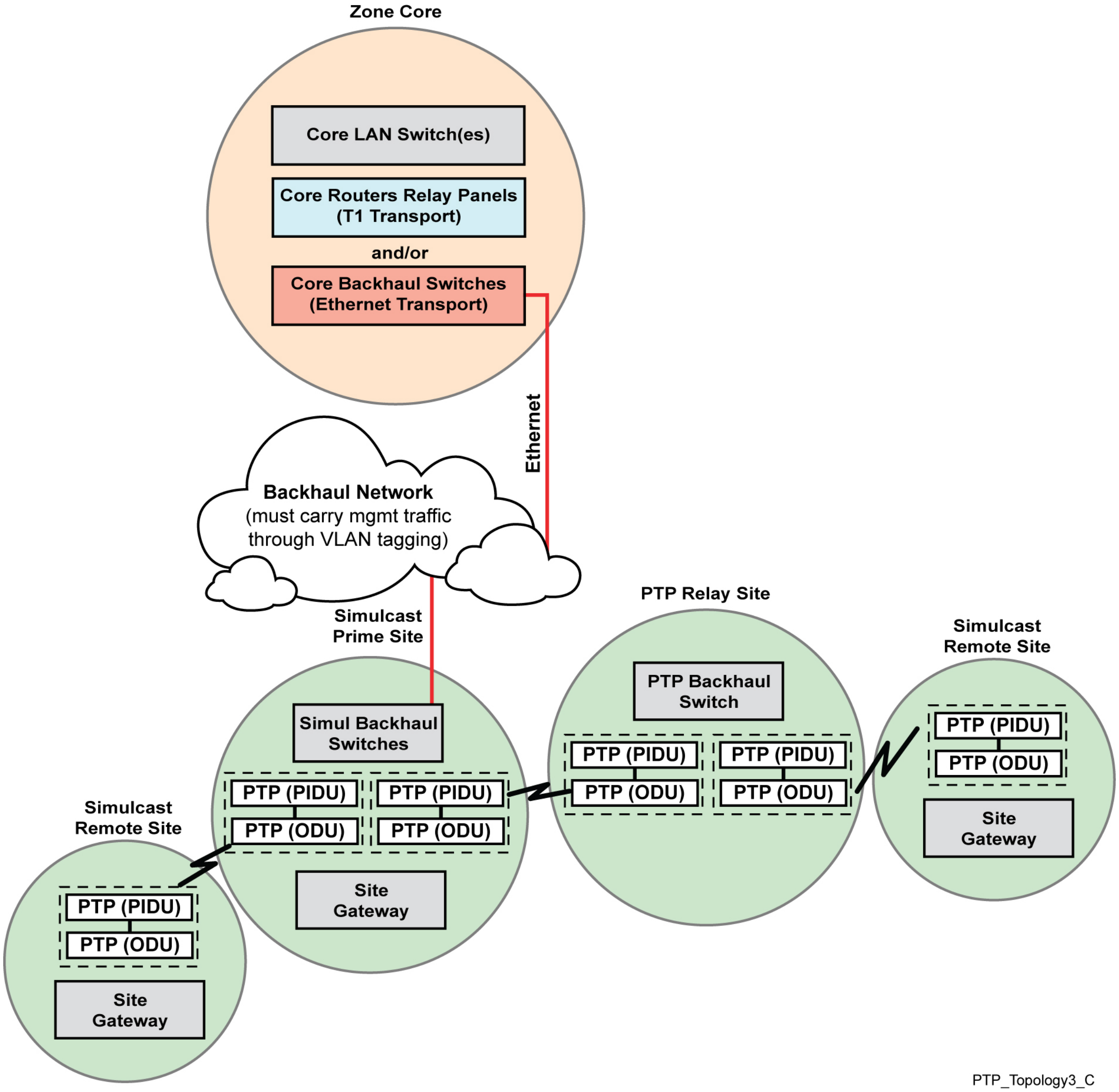
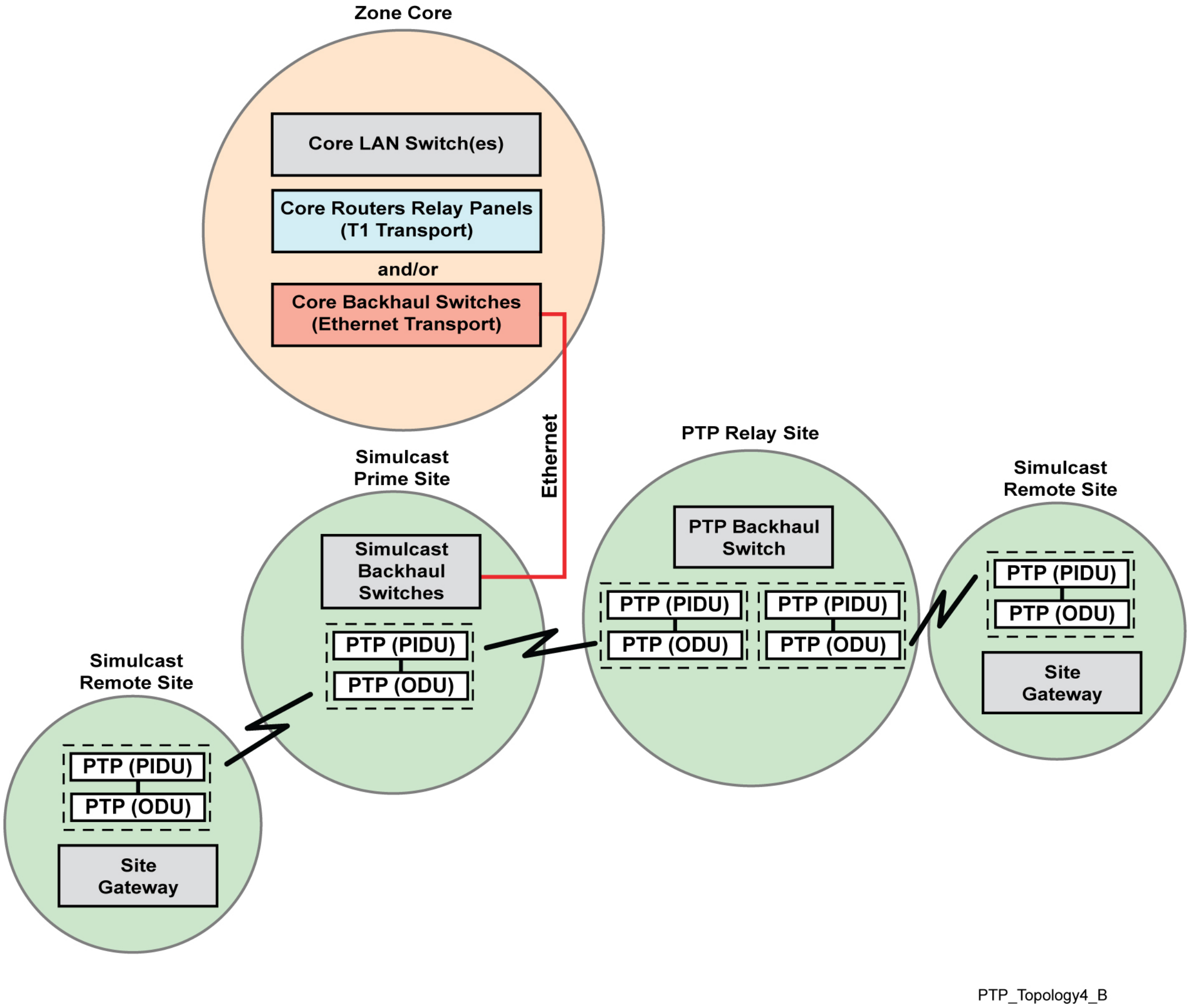


**Figure 18: PTP Ribbon Topology – Customer Backhaul Reuse**



PTP_Topology3_C

**Figure 19: PTP Ribbon Topology – Simulcast Backhaul Reuse**



3.5.2.2

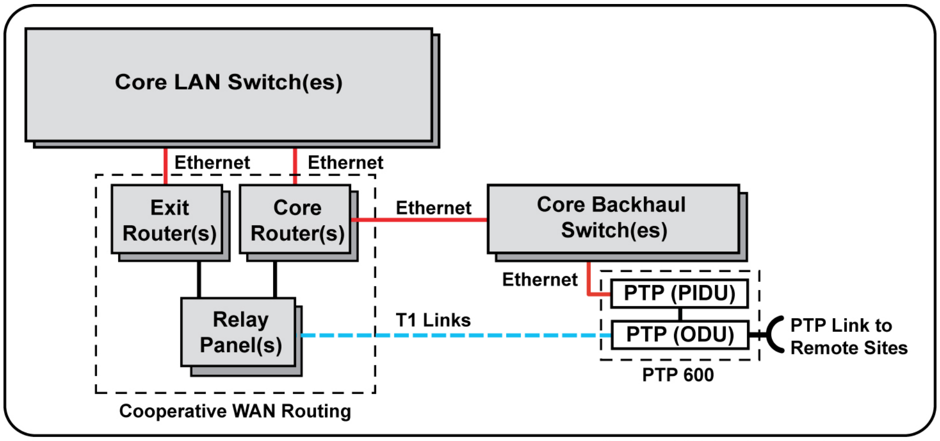
## PTP Device Deployment – Site Diagrams

This section shows examples of PTP device deployment in various sites.

**NOTICE:** One Point-To-Point (PTP) link requires two PTP radios, regardless of whether the link type is T1/E1 or Ethernet.

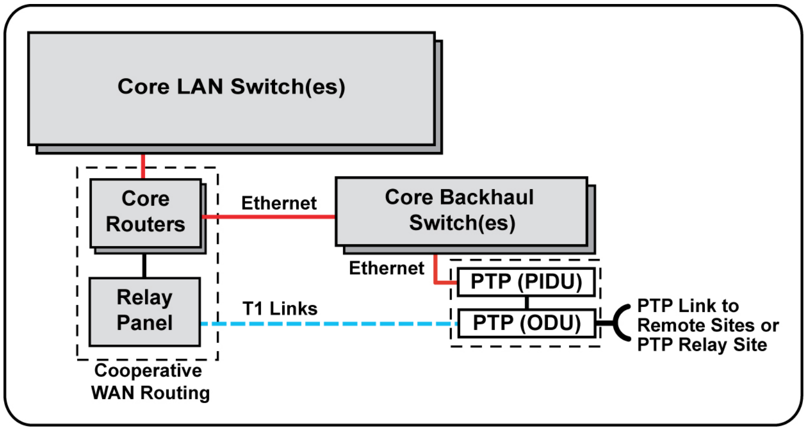
### 3.5.2.2.1 M-Series and L-Series Core with PTP

Figure 20: M3 system – T1/E1 Microwave Site Link with PTP



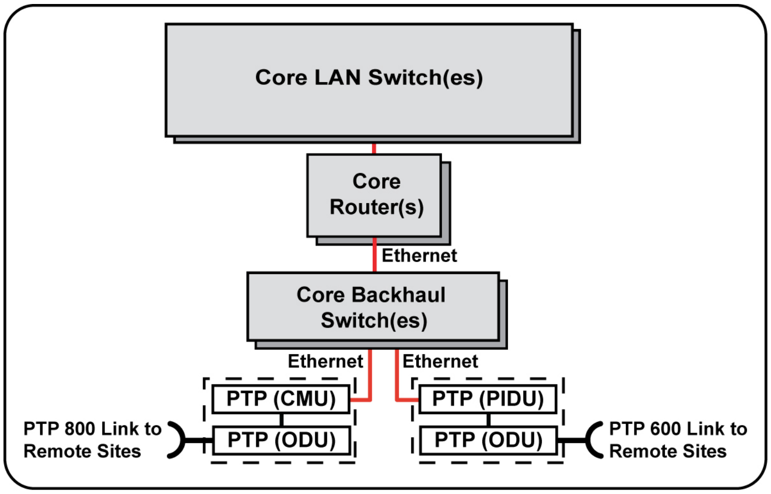
PTP_M3_T1_E1_Microwave_Site_Links_B

Figure 21: M1/M2 system – T1/E1 Microwave Site Link with PTP



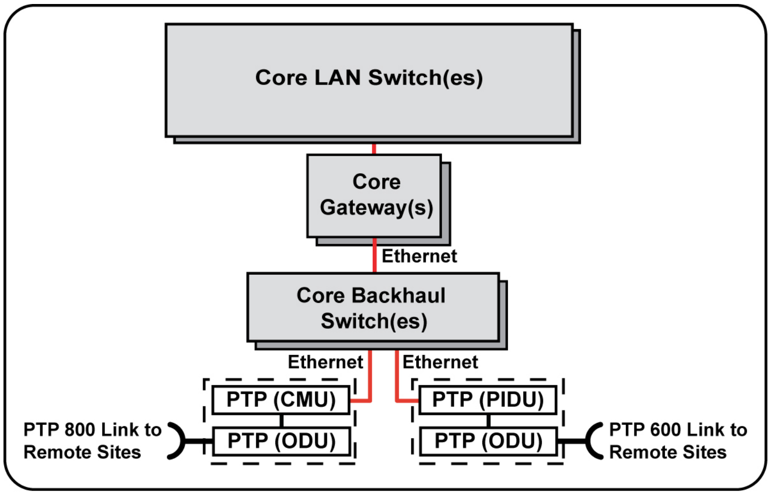
PTP_M1M2_T1_E1_Microwave_Site_Links_B

Figure 22: M Core System – Microwave Ethernet Site Link with PTP



PTP_M1M2M3_Microwave_Ethernet_Site_Links_C

**Figure 23: L Core System – Microwave Ethernet Site Link with PTP**

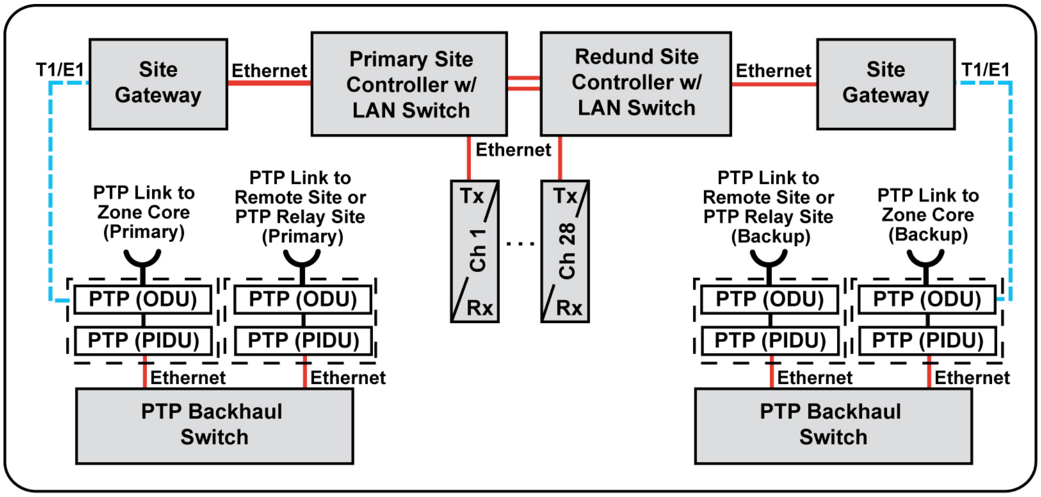


PTP_L1L2_Microwave_Ethernet_Site_Links_C

3.5.2.2.2

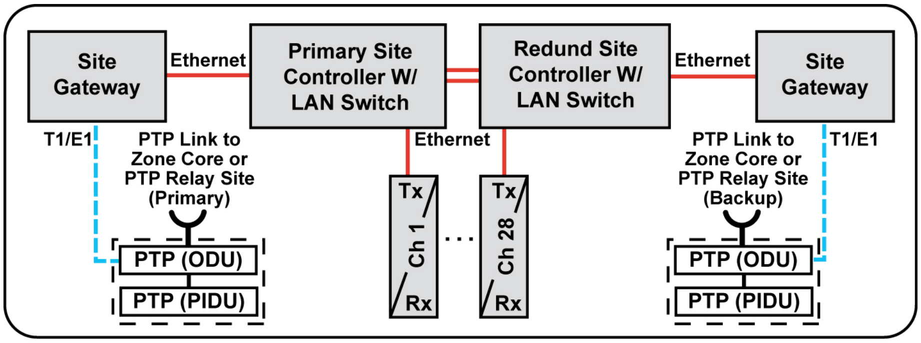
## ASTRO 25 Repeater Site with PTP

**Figure 24: ASTRO 25 Repeater Site T1 Microwave Site Link with PTP**


T1/E1
Site Gateway
Ethernet
Primary Site Controller w/ LAN Switch
Redund Site Controller w/ LAN Switch
Ethernet
Site Gateway
T1/E1
Ethernet
PTP Link to Zone Core (Primary)
PTP Link to Remote Site or PTP Relay Site (Primary)
Tx
Ch 1
Rx
. . .
Tx
Ch 28
Rx
PTP Link to Remote Site or PTP Relay Site (Backup)
PTP Link to Zone Core (Backup)
PTP (ODU)
PTP (PIDU)
PTP (ODU)
PTP (PIDU)
PTP (ODU)
PTP (PIDU)
PTP (ODU)
PTP (PIDU)
Ethernet
Ethernet
Ethernet
Ethernet
PTP Backhaul Switch
PTP Backhaul Switch

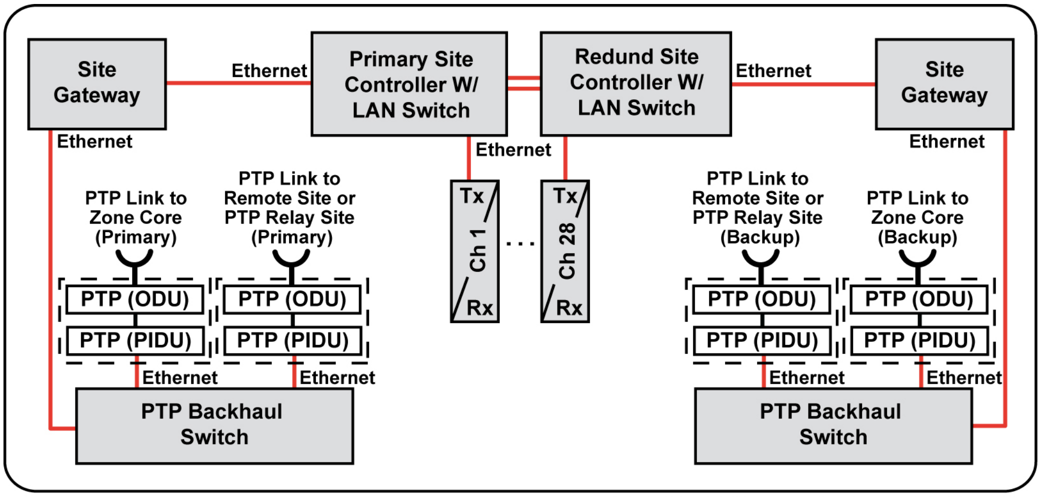
PTP_ASTRO_25_Repeater_Site_T1_Microwave_Site_Links_C

**Figure 25: ASTRO 25 Repeater Site Last Hop T1 with PTP**


Site Gateway
Ethernet
Primary Site Controller W/ LAN Switch
Redund Site Controller W/ LAN Switch
Ethernet
Site Gateway
T1/E1
PTP Link to Zone Core or PTP Relay Site (Primary)
Ethernet
Tx
Ch 1
Rx
. . .
Tx
Ch 28
Rx
PTP Link to Zone Core or PTP Relay Site (Backup)
T1/E1
PTP (ODU)
PTP (PIDU)
PTP (ODU)
PTP (PIDU)

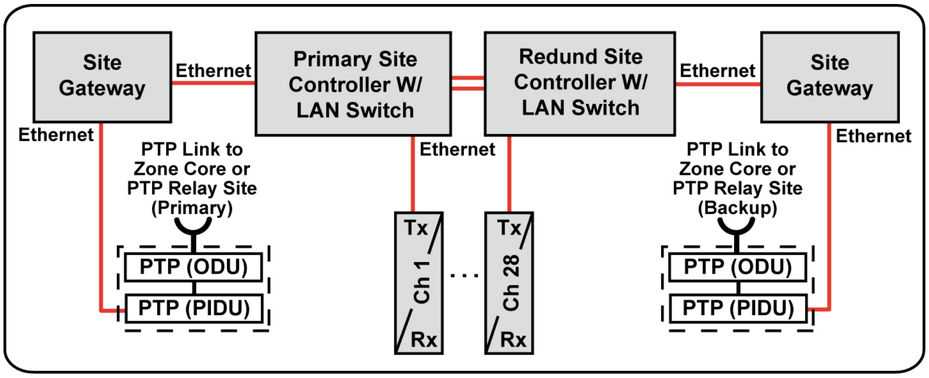
PTP_ASTRO_25_Repeater_Site_Last_Hop_T1_C

**Figure 26: ASTRO 25 Repeater Site Ethernet Site Link with PTP**


Site Gateway
Ethernet
Primary Site Controller W/ LAN Switch
Redund Site Controller W/ LAN Switch
Ethernet
Site Gateway
Ethernet
Ethernet
Ethernet
PTP Link to Zone Core (Primary)
PTP Link to Remote Site or PTP Relay Site (Primary)
Tx
Ch 1
Rx
Tx
Ch 28
Rx
PTP Link to Remote Site or PTP Relay Site (Backup)
PTP Link to Zone Core (Backup)
PTP (ODU)
PTP (PIDU)
PTP (ODU)
PTP (PIDU)
PTP (ODU)
PTP (PIDU)
PTP (ODU)
PTP (PIDU)
Ethernet
Ethernet
Ethernet
Ethernet
PTP Backhaul Switch
PTP Backhaul Switch

PTP_ASTRO_25_Repeater_Site_Ethernet_Site_Links_C

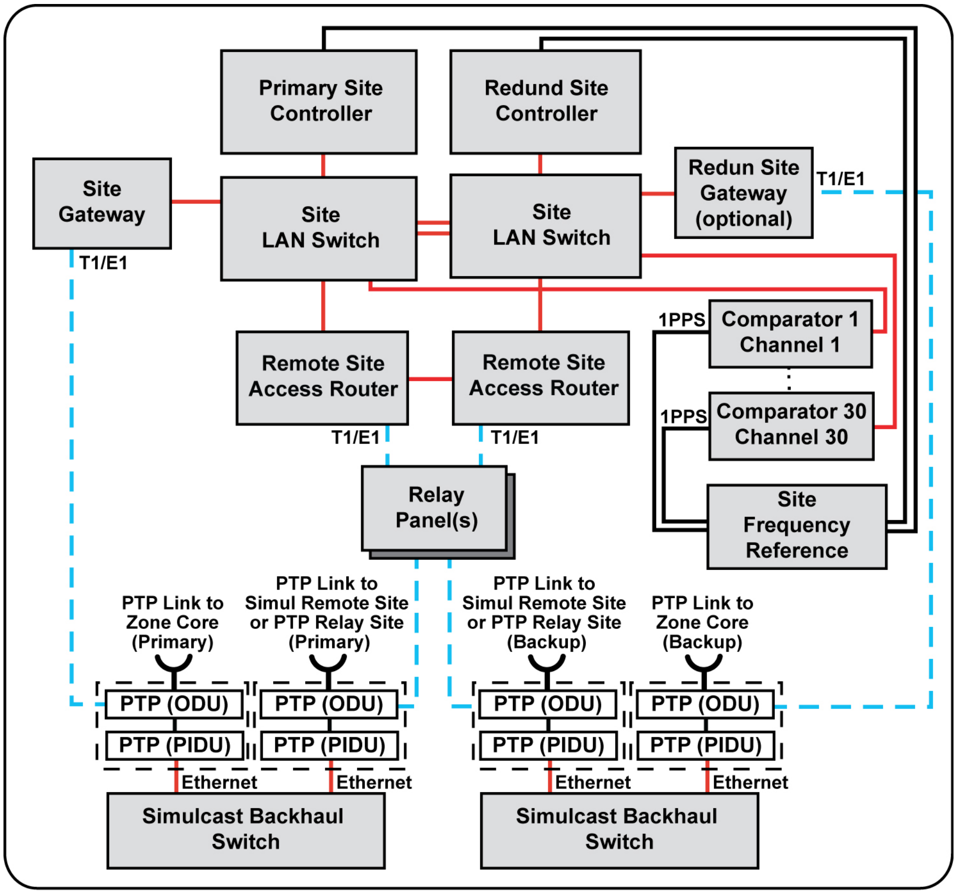
**Figure 27: ASTRO 25 Repeater Site Last Hop Ethernet with PTP**


Site Gateway
Ethernet
Primary Site Controller W/ LAN Switch
Redund Site Controller W/ LAN Switch
Ethernet
Site Gateway
Ethernet
Ethernet
Ethernet
PTP Link to Zone Core or PTP Relay Site (Primary)
Tx
Ch 1
Rx
Tx
Ch 28
Rx
PTP Link to Zone Core or PTP Relay Site (Backup)
PTP (ODU)
PTP (PIDU)
PTP (ODU)
PTP (PIDU)

PTP_ASTRO_25_Repeater_Site_Last_Hop_Ethernet_C

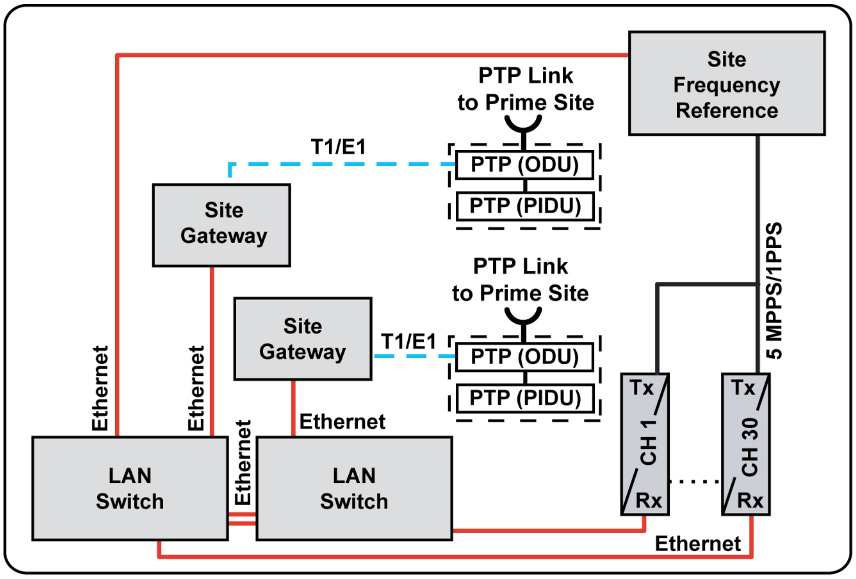
### 3.5.2.2.3
## IP Simulcast Subsystem with PTP

**Figure 28: IP Simulcast Prime Site T1 Microwave Site Link with PTP**



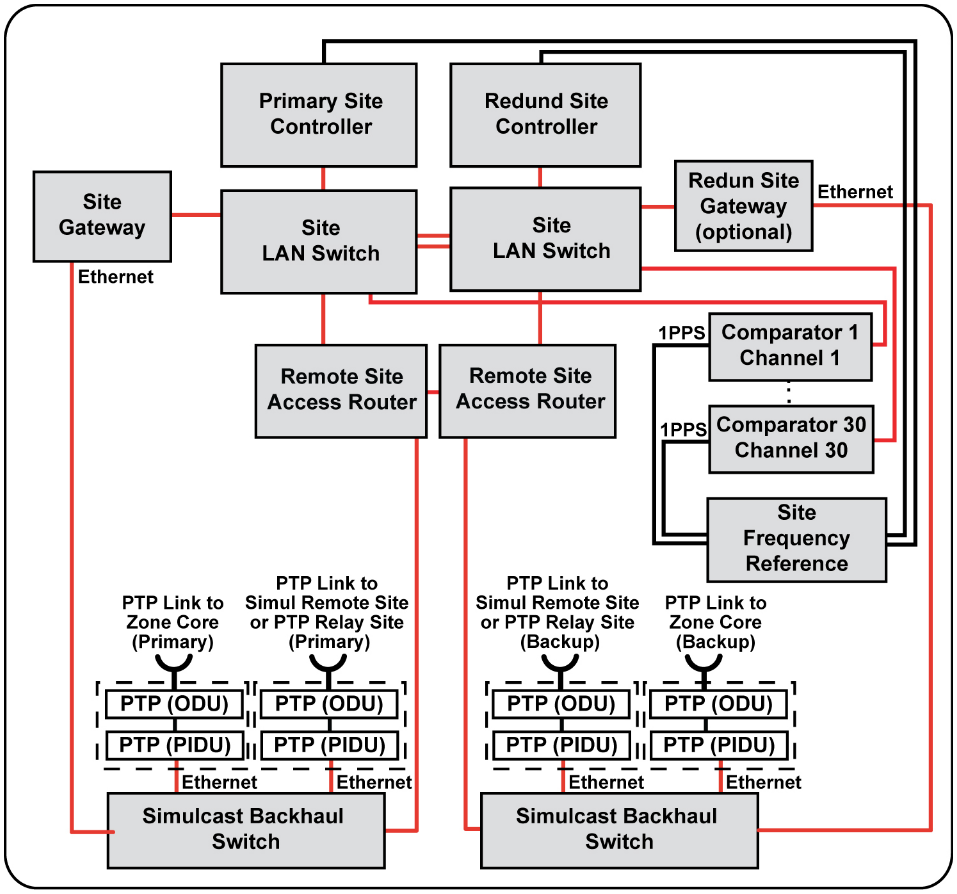
PTP_IP_Simul_Prime_T1_Microwave_Site_Links_C

**Figure 29: IP Simulcast Remote Site Last Hop T1 Microwave Site Link with PTP**



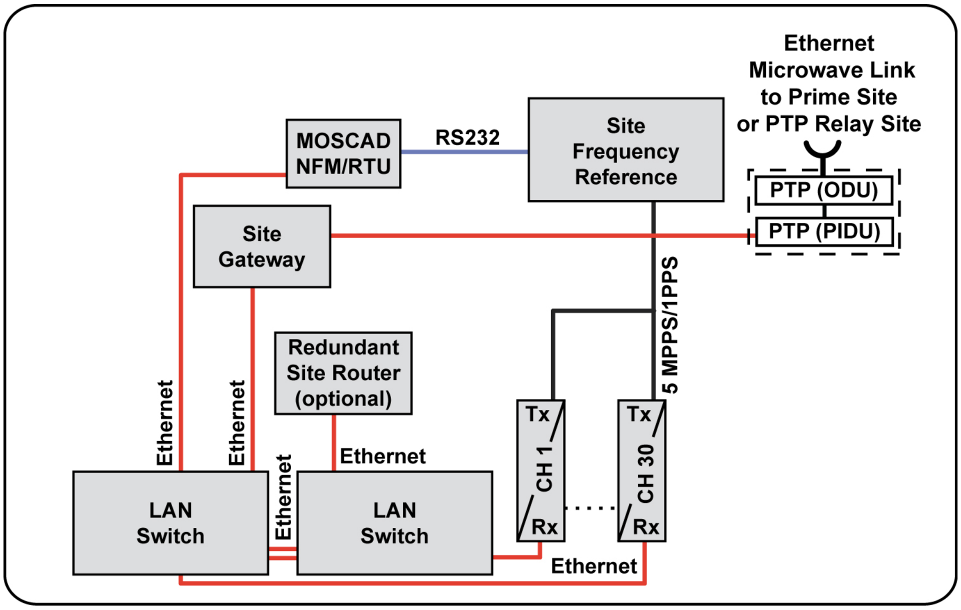
PTP_IP_Simul_Remote_Site_Last_Hop_T1_Microwave_Site_Links_B

**Figure 30: IP Simulcast Prime Site Ethernet Site Link with PTP**


Primary Site Controller
Redund Site Controller
Site Gateway
Site LAN Switch
Site LAN Switch
Redun Site Gateway (optional)
Ethernet
Ethernet
1PPS
Comparator 1 Channel 1
1PPS
Comparator 30 Channel 30
Remote Site Access Router
Remote Site Access Router
Site Frequency Reference
PTP Link to Zone Core (Primary)
PTP Link to Simul Remote Site or PTP Relay Site (Primary)
PTP Link to Simul Remote Site or PTP Relay Site (Backup)
PTP Link to Zone Core (Backup)
PTP (ODU)
PTP (ODU)
PTP (ODU)
PTP (ODU)
PTP (PIDU)
PTP (PIDU)
PTP (PIDU)
PTP (PIDU)
Ethernet
Ethernet
Ethernet
Ethernet
Simulcast Backhaul Switch
Simulcast Backhaul Switch

PTP_IP_Simul_Prime_Site_Ethernet_Site_Links_C

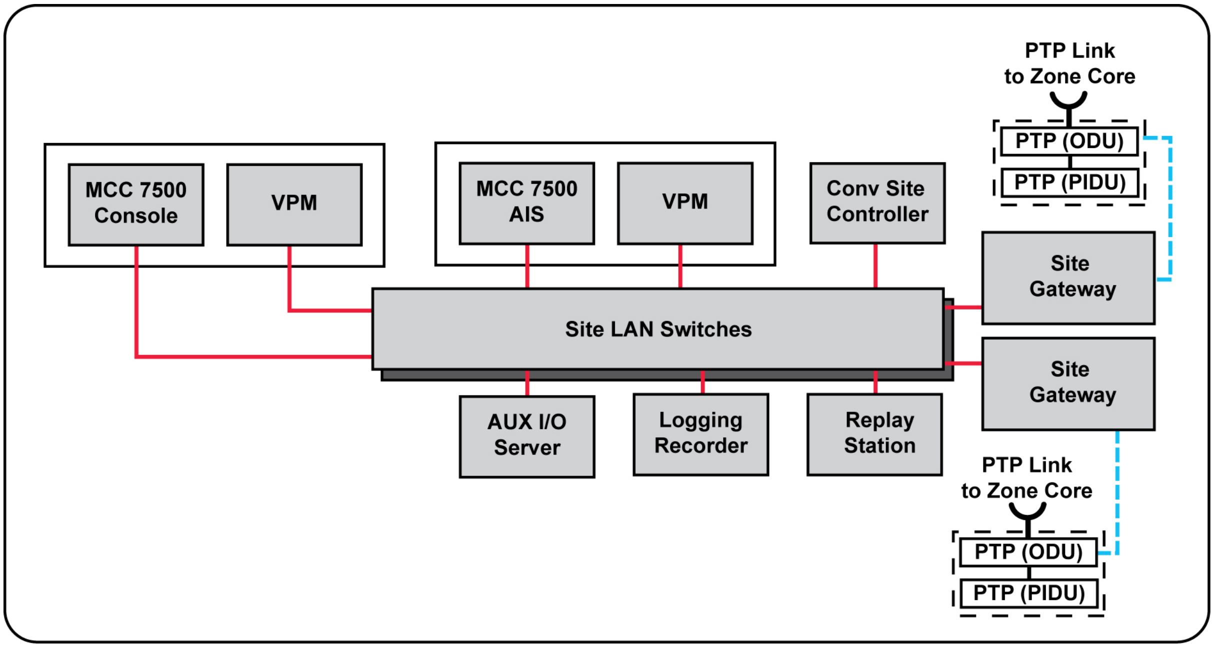
**Figure 31: IP Simulcast Remote Site Last Hop Ethernet with PTP**



PTP_IP_Simul_Remote_Site_Last_Hop_Ethernet_C

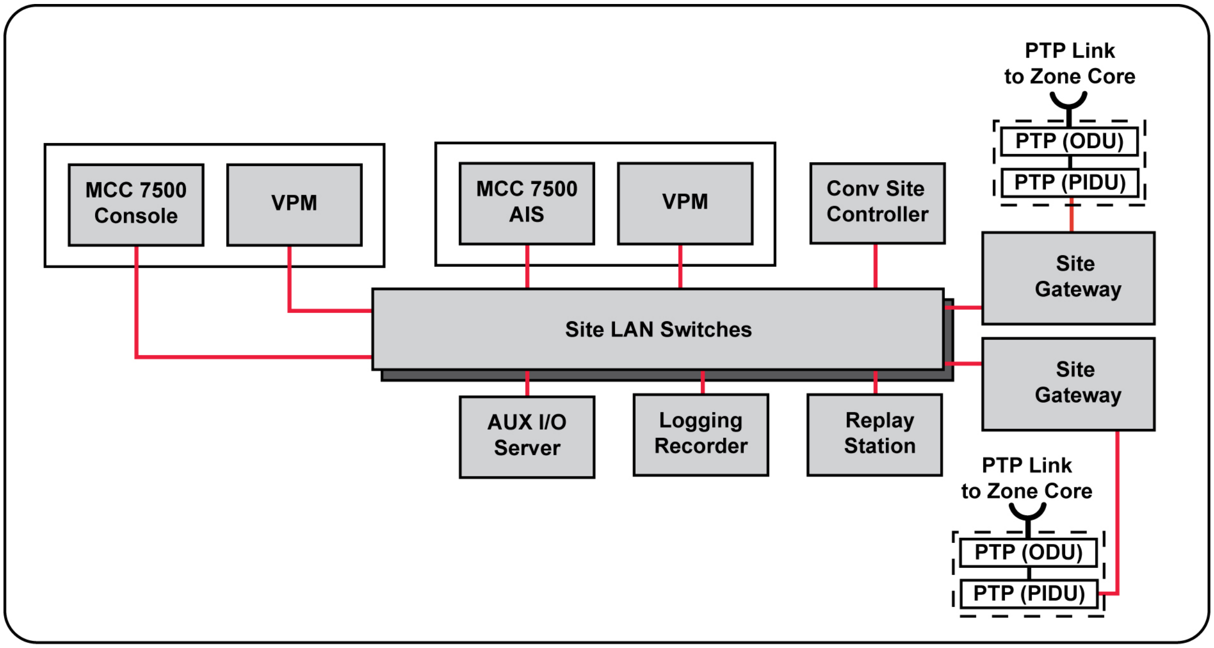
### 3.5.2.2.4
### Dispatch Console Subsystem with PTP

**Figure 32: MCC 7500 T1 with PTP**



PTP_MCC7500_T1_B

**Figure 33: MCC 7500 Ethernet with PTP**



PTP_MCC7500_Ethernet_B

## 3.5.3
## PTP Device – Installation and Configuration Considerations

To setup PTP devices to interface with an ASTRO® 25 system, review the following requirements considerations:

- Review the appropriate PTP User Guide for details regarding basic installation and configuration of PTP devices.
- RADIUS Server Host Configuration Requirement – When interfacing PTP devices to the ASTRO® 25 system, PTP device configuration needs to specify the IP address of a primary and secondary RADIUS server for device authentication. For more details, see the *Authentication Services* manual
- Backhaul Switch – Refer to the *System LAN Switches* manual to interface the PTP and RAD devices to the Site Backhaul Switch
- System Routers and Gateways – Refer to the *S6000 and S2500 Routers* or *GGM 8000 System Gateway* manual for transport device to PTP device interface details
- Descriptive DNS hostnames are assigned to the PTP devices to indicate where these devices are physically located
- Network Time Protocol – When interfacing PTP devices to the ASTRO® 25 system, PTP device configuration needs to specify the IP address of a primary NTP
- Provisioning Manager – Refer to the *Provisioning Manager* manual
- Unified Event Manager – Refer to the *Unified Event Manager* manual
- Other Requirements and Considerations
- PTP products support various redundant and non-redundant link configurations – see your PTP product documentation.
- For installation and details regarding the PTP 800 IRFU – see your PTP product documentation.

3.5.4
## PTP Device Installation

**Prerequisites:**

- Determine which site needs to provide connectivity to another site
- Assign a hostname and an IP address to each PTP radio device
- Obtain configuration files for routers, switches, and firewalls

**Process:**

1. Install and configure PTP radios:
   - For PTP 600 Series Radios, see the “Installation” chapter in the *PTP 600 Series User Guide*
   - For PTP 800 Series Radios, see the “Installation” chapter in the *PTP 800 Series User Guide*
2. Upload new Backup and Restore (BAR) configuration files to the Unified Network Configurator (UNC).
3. Push the configuration files to:
   - Core routers
   - Gateway routers
   - Backhaul switches
   - Firewall (if required)

   See the “Distributing Configurations for Transport Devices with the UNCW” section of the *Unified Network Configurator* manual.
4. Enter the hostname and IP address of each PTP device into DNS using bulk import.
5. Provision the new PTP radios.
   - For PTP 600 Series Radios, see the “Installation” chapter in the *PTP 600 Series User Guide*

- For PTP 800 Series Radios, see the “Installation” chapter in the *PTP 800 Series User Guide*

**6** Discover the PTP radios from the UEM. See the “Discovery Operations” section in the *Unified Event Manager* manual.

**7** Discover the site backhaul switches from UEM.

See the “Discovery Operations” section in the *Unified Event Manager* manual.

**8** Discover the backhaul switches from UNC.

See the “Device Discovery” section of the *Unified Network Configurator* manual.

**9** Perform secure web launching from PTP via UEM.

See the “Point-to-Point Devices Management” section in the *Unified Event Manager* manual.

**10** Perform an Acceptance Test Plan (ATP).

- Verify both audio, data and network management traffic go through successfully between core to each newly expanded site via VLAN.
- Verify wide trunking state for each newly expanded site.

3.5.5
## PTP Device – Operations

The Unified Event Manager (UEM) receives alarms and events associated with the status of PTP devices. The UEM indicates failure status for the site in the **Service Detail View** regardless of whether or not a PTP device is on the same subnet as the Site Controller.

**NOTICE:** If a T1 link is used to connect to a PTP device, the Ethernet port of the far end PTP is not connected. The UEM reports this as an alarm for the device. This alarm needs to be filtered out by the user by using a user-configured UEM alarm filter. For details on creating filters in the UEM, see the *Unified Event Manager* manual.

If possible, create a UEM view to better organize the PTP devices.

If or when a PTP device goes out of services, the subnet that hosts the PTP devices identifies the device in the **Physical Detail View.** You can click on the subnet to determine which of the PTP devices has failed.

3.5.5.1
### Access to PTP Device

Access to a PTP device web page for troubleshooting and diagnostics can be accomplished by using one of the following:

- Use the browser from an Network Management Client and enter the web page info of the PTP device (e.g. http://aaa.bbb.ccc.ddd)
- Use the Unified Event Manager (UEM) GUI: right-click on a PTP device and select **Launch Web Management Application** to launch the Web Application for a PTP device
- Use the UEM GUI: select a PTP device alarm to launch the PTP Web Application for a PTP device

3.5.6
## PTP Device – Maintenance and Troubleshooting

This section describes maintenance and troubleshooting of PTP devices in an ASTRO® 25 system.

### 3.5.6.1 PTP Diagnostics and Device Command

PTP device commands are initiated through the Unified Event Manager (UEM). For more details, refer to the *Unified Event Manager* manual.

For all other maintenance and troubleshooting of PTP devices, refer to the *PTP 600 Series User Guide* or *PTP 800 Series User Guide.*

### 3.5.6.2 PTP Asset Management

In the Unified Event Manager (UEM) it is possible to view the values of specific properties of PTP that describe the versions of software or hardware installed on the device. The data is fetched dynamically, so if any of the displayed values change, the device does not require rediscovery.

See the *Unified Event Manager* manual for details regarding asset management on PTP devices.

## 3.6 Failure Categories

Failures and anomalies can be classified in four general categories:

- Hard failure
- Intermittent failure
- User configuration issues
- Miscellaneous

Correctly classify the source of the problem during troubleshooting, so that the problem can be fixed. An incorrect classification can lead to wasted time and effort.

For example, what appears to be a hardware failure may actually be a user data configuration error. By trying to find a hardware solution, you could waste valuable time and effort that you should be using to find and fix a configuration issue.

### 3.6.1 Hard Failure

A **Hard failure** is a failure that prevents operation to the point that a device or module is rendered nonfunctional. In many cases, Motorola Solutions has designed its devices with the capability of reporting its functional status to the system. This allows a high percentage of device hard failures to be reported reliably to the UEM. Failures in third-party products may be reported using third-party software interfaces (such as Preside or the UNC) or MOSCAD NFM.

Determining most hard failures is relatively straightforward, since reported failures appear in UEM. A high-level object displayed in a color other than green (status OK) indicates a failure of one or more lower-level objects that are part of the high-level object.

### 3.6.1.1 Troubleshooting Hard Failures

A hard failure can be caused by:

- Improper use of the equipment
- A failed component

Finding out that a user was attempting to place calls incorrectly (such as pressing the wrong button or not waiting for a ready signal) is straightforward. User-caused problems usually manifest themselves early, such as when the system is new.

A hard failure means that a device is either inoperable or that a very important function of that device has failed. Depending on the device that has failed, hard failures may or may not have an impact on system operation. Understanding these effects allows intelligent prioritizing of repairs when a failure occurs.

### 3.6.1.1.1
### Hard Failure Isolation Approach

**Procedure:**

1 Review the users problem report. Determine all critical information such as:

- Time of experienced failure
- Location of the user when failure was experienced
- System equipment that was involved with the users call

2 Verify that the user is experienced in the proper use of the radio and has sufficient knowledge of system operation. It may be that the failure is due to an incomplete user training and the improper use of the radio. The user may also have strayed out of the normal operating area.

**NOTICE:** The term *users* includes radio users, console operators, and management users (system maintenance in the zones).

3 Compare the users problem report to other reports you may have received. You are trying to determine if other users have reported the same problem.

| If… | Then… |
|---|---|
| **Many users are reporting the same or similar problems, either:**<br>• **In the same zone or subsystem**<br>• **Within a short period (such as 24 hours or less)** | There is a strong possibility that the problem is in the system. Continue with step 4. |
| **No other users are reporting this problem.** | There is a strong possibility that the problem is in:<br>• The user's radio, or<br>• The users use of the radio. Continue with step 4. |

4 Verify that the system operates correctly with the users equipment. This might entail walking the user through the call service request and noting system function.

5 Verify that the user is configured correctly. If the user is configured correctly, then verify that the system hardware is working correctly.

| If… | Then… |
|---|---|
| **You suspect a hardware fault** | Verify system function in the UEM. The UEM GUI presents the condition of the system and its components through the color of the displayed object or subnet. If any object is abnormal (not green), then a problem has been logged by the UEM. Verify the state of any abnormal object through the Alarms view. Also, the UEM reports device statistics such |

| If… | Then… |
|---|---|
| | as CPU and memory utilization. Thus, along with verifying the state in Alarms view, the user can check these statistics to identify issues.<br>**NOTICE:** CPU and Memory statistics are not collected and stored automatically. This feature must be enabled for statistics to be collected by the UEM. So, unless collection is enabled before the failure, these statistics are not available for analyzing the hard failure. |
| **You are trying to resolve a users failure report** | Restrict your UEM session to the object in the subsystem that the user was involved with. Double-click to navigate within either the Map or the Network Database view to view all involved objects until you can identify those that have failed. |
| **You are performing a scheduled review of the system** | Navigate through the system objects, noting anything out of the ordinary.<br>**NOTICE:** If desired, you can set specific faults to send an e-mail notification when the UEM detects a critical failure. This ensures that corrective action can begin immediately upon receipt of the failure notification. |
| **UEM does not show any hard failures** | Proceed to “Troubleshooting Intermittent Failures”. |

6 When you have identified the hard failures, prioritize and schedule their repair.

7 When the repairs have been completed, verify system operation.

| If… | Then… |
|---|---|
| **Performs satisfactorily** | The process is complete. |
| **Performs unsatisfactorily** | Return to step 3 and repeat the procedure. You may not have diagnosed the problem correctly, or you may have more than one hard failure within the system. |

3.6.1.1.2

## Example of Hard Failure Isolation

This procedure describes a hypothetical system fault isolation approach in the UEM. This example shows how the UEM can help you identify system faults before they cause system performance problems.

**NOTICE:** For zone or system-level alarms and failures, call the Motorola Solution Support Center (SSC) and notify them of any action you took and the results. SSC issues a Case Number which allows proper tracking of the zone controller's functional history. This is helpful if future problems occur.

In this example, the inclusive new fault indication requires further fault isolation, since not every included fault has its own object. This allows proactive fault isolation before a failure affects a system function.

**Procedure:**

1 Review all trouble reports that appeared during the time period you were not on duty. This provides information about the system from the users' point of view.

2 Log on to the UEM.

3. Verify the current state of the system icon through the Map view. Assume that the system icon is cyan (light blue). This indicates that a problem exists at a lower level.
4. Double-click the system icon to open the UEM **Alarms** view.

   You see that the Zone 2 icon is cyan.
5. Double-click the **Zone 2** Alarm row.

   The alarm details for the zone controller appear.
6. Send a technician to that zone controller so the zone controller may be locally accessed to isolate the fault.

## 3.6.2 Intermittent Failure

An **Intermittent failure** is a temporary failure of a system function. This could be due to temporary changes in conditions, or to the partial failure of a system component.

For example, weather conditions could degrade a microwave link to the point of forcing a site or subsystem into site trunking. Another example would be a construction crew cutting a power cable. In both of these situations, the failure condition corrects itself when the weather clears or the crew reconnects power.

Since these failures are temporary, their effects are not noticed at every occurrence, but their effects can range from minor to critical. It is important to identify, understand, and if possible, correct any intermittent failures. Understanding your system's routine intermittent failures allows you to effectively prioritize repairs and inform system users regarding known problems.

The system provides software tools that store status information. This is important where intermittent problems are concerned, since the record of a transient alarm may be the only indication that a problem has occurred. The UEM Alarms Browser records the system's transitions and states so they can be viewed at any time. The Alarms Browser provides a log of your system's past conditions, allowing you to observe the occurrence of intermittent failures even if normal operation has resumed.

### 3.6.2.1 Troubleshooting Intermittent Failures

Always check the system for hard failures first before checking for intermittent failures. Check the system at the beginning of each shift and periodically throughout the shift. Monitoring system functionality, as logged by the system, is the primary way to get to know how your system operates, what situations are routine, and what situations demand special attention.

#### 3.6.2.1.1 Intermittent Failure Troubleshooting

See the flowchart in Resolving System Events in UEM on page 49 to resolve a service outage in an ASTRO® 25 system. For detailed information on using the UEM, refer to the *Unified Event Manager* manual.

#### 3.6.2.1.2 Example of Intermittent Failure Isolation

See the flowchart in Resolving System Events in UEM on page 49 to resolve a service outage in an ASTRO® 25 system. For detailed information on using the UEM, refer to the *Unified Event Manager* manual.

## 3.6.3 Configuration Failures

Once you have ruled out hardware as the cause of a system problem, address configuration issues. Some problems reported by users may have nothing to do with faulty equipment, but with the way the system, console, or the user's radio is configured. This could manifest itself as too many busies indicating that the system manager should reallocate resources, add channels to a site, or change the capability of a device.

### 3.6.3.1 Troubleshooting Configuration Problems

This section discusses, in general terms, the types of configuration to consider before attempting to troubleshoot your system. From a system troubleshooting perspective, there are three aspects of configuration management, each of which involve different hardware:

- User configuration
- Infrastructure configuration
- Console configuration

#### 3.6.3.1.1 Software Failures

A software problem can appear to be a hard failure. For example, subsystem software may enter a mode of operation that it cannot exit. Once you have determined the program or device that has halted, reset the device running the program to restart proper execution of the software.

#### 3.6.3.1.2 User Configuration

Generally, user configuration problems appear soon after system installation or after configuration changes have been made. If you cannot attribute a user communication problem to either a hard failure or intermittent operation, it may be due to the user's configuration in the system database. It is then necessary to verify the user's correct configuration.

Configuring the system is a detailed and intricate operation. Although many factors are considered during the initial planning of your system, the system may not meet the needs of your users once it is operational. For example:

- Users may roam more than planned
- Members of different talkgroups may interact in ways not predicted
- Users may require infrastructure changes

Large systems like ASTRO® 25 tend to evolve more dynamically than small systems due to the number of sites and subsystems and the number and variety of users.

The Service Manager, and anyone else who maintains, administers, manages, or configures the system or user profiles needs a detailed understanding of how the system is configured.

#### 3.6.3.1.3 UCS Server Application Failure

If the User Configuration Server application (UCS) fails, it prevents the UCS server application database restore/replication process from occurring. This makes the Provisioning Manager application unavailable, which prevents editing subscriber information, creating default subscriber records, modification and viewing of home zone maps, and changes to system-level parameters.

3.6.3.1.4

#### Infrastructure Configuration

Technicians and system managers enter infrastructure configuration information in the Provisioning Manager application and discover the devices in the UNC. The User Database Server and the Unified Network Configurator also store configuration data.

The Unified Network Configurator (UNC) exports infrastructure configuration information to a disk file on the zone controller. If a LAN fails, the zone controller is isolated from the UNC. If that happens, the zone controller can operate in standalone mode, using the information from the exported infrastructure configuration file. However, the zone controller would not have access to user configuration information (handled by the User Configuration Server) and would deal with subscriber service requests, based on default settings.

ASTRO® 25 provides a network management path through the LAN/WAN to each of the remote sites. This path allows the UNC application to perform configuration management of remote site stations directly.

When the UNC transfers configuration information to a remote site over the site network management path, the new information overwrites the existing configuration information in the station. However, the UNC cannot configure all configuration information in a remote station. CSS programming is still required when configuring a remote site station.

Site Management packets use the same physical link to a site as the control information. When the control path needs to use the link, control packets take priority over the management packets.

3.6.3.1.5

#### Zone Database Server Failure

If the Zone Database Server application (ZDS) fails in one zone, the failure results in the following:

3.6.3.1.6

#### Fault Management in Console Sites

For more information on troubleshooting Console site faults, refer to sections related to troubleshooting in the *Console Sites* manual or the *MCC 7100 IP Dispatch Console Setup and User Guide*.

3.6.4

### Miscellaneous Failures

The major equipment in the ASTRO® 25 system contains firmware that performs various tests. They include a power-on self test, ongoing circuit function verification, the verification of control communications, and other self-monitoring functions. However, this testing and verification is limited to major equipment functions. As a result, there may be instances when the system does not report a hardware failure reliably. Additionally, hardware failures may go undetected due to the loss of control data communication. If the system cannot communicate with a site, the system reports the status of that site as “unknown”. Perform traditional hardware troubleshooting to isolate the cause of failure in these cases.

In all instances of failure, whether critical or intermittent, document all actions that led to the errant behavior, as well as all corrective actions taken. Finding and correcting system problems is simplified when detailed trouble reports, including information such as severity and the time and date of the event, have been captured in the UEM.

## 3.7 Traffic Plane Failures

Equipment failures can disrupt the transfer of information across the control, audio, or network management planes. The table below lists the devices and the corresponding traffic planes for each device.

Table 8: Devices That Impact Traffic Planes

| Device | Control Plane | Audio Plane | Data Plane | Network Management Plane |
|---|---|---|---|---|
| Zone Controller | X | | | |
| Console Interface Electronics | | X | | |
| SmartX Site Converter | | X | | |
| Voice Processor Module | | X | | |
| Packet Data Gateway (PDR and RNG) | | | X | |
| GGSN | | | X | |
| border gateway | | | X | |
| User Configuration Server | | | | X |
| Zone Database Server | | | | X |
| Zone Statistics Server | | | | X |
| Air Traffic Router | | | | X |
| UEM server | | | | X |

Compared to regular system configurations, systems with the Dynamic System Resilience feature implemented are considerably less vulnerable to various types of traffic plane failures. For detailed information on the Dynamic System Resilience feature as well as for detailed information on troubleshooting DSR-related failures, see the *Dynamic System Resilience* manual.

### 3.7.1 Control Plane Failure

This section explains the impacts of control plane failures.

#### 3.7.1.1 Call Processing Failure

The zone controller is responsible for call registration, individual call, and group call processing in its zone. A failed zone controller results in the loss of system and zone trunking for that particular zone. All call requests, registration requests, and calls in progress are dropped. The zone also drops out of participation in all InterZone calls.

#### 3.7.1.2 Call Management Failure

The zone controller is responsible for managing sites, telephone interconnect services, and other equipment in the zone to arrange calls. With the zone in site trunking, services such as telephone interconnect and console operations are not available.

### 3.7.1.3 Mobility Management Failure

The zone controller maintains mobility information for its zone including a Visitor Location Register (VLR) of all radio users located in the zone, and a Home Location Register (HLR) of all radio users mapped to the zone. A failed zone controller loses all mobility management information. Site location information for all radio users is maintained at the sites. If any roaming radio users are mapped to another zone, their home zones are not able to track their location until the zone is operating normally again.

### 3.7.1.4 InterZone Communications Failure

The zone controller organizes InterZone communications with other zones by passing control messages and routing audio system-wide. A failed InterZone Control Path ceases InterZone communications. InterZone calls and sharing of mobility information with the failed zone also ceases.

## 3.7.2 Audio Plane Failures

This section contains information on audio plane failures.

### 3.7.2.1 Subscriber Unit Failure

The failure of a subscriber unit results in that unit being unable to communicate. The failure does not affect other radio users in the talkgroup, site, or zone.

### 3.7.2.2 Zone Controller Failure

Wide area audio routing is stopped when a zone controller is lost. Consoles become idle and telephone interconnect services are lost.

### 3.7.2.3 SmartX Site Converter Failure

The SmartX site converter allows for 3600 SmartZone® sites to be connected to the ASTRO® 25 system. If the SmartX site converter fails, communication with the SmartZone® site is lost and the site goes into site trunking mode. Refer to the *SmartX Site Converter* manual for troubleshooting information.

### 3.7.2.4 Voice Processor Module Failure

The failure of a VPM usually results in audio processing becoming unavailable. Refer to the *MCC 7500 Dispatch Console with VPM* manual for troubleshooting information.

### 3.7.2.5 Telephone Interconnect Device Failure

A Telephone Interconnect Device (TID) interfaces an ASTRO® 25 system to the Public Switched Telephone Network (PSTN). This provides a means of making radio-to-landline telephone calls and landline-to-radio calls. 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 telephone interconnect:

- **Control Link Path:** The IP PBX Server (TID) interfaces through the LAN switch to the zone controller.
- **Audio Path:** The audio connections are between the Telephone Media Gateway (TMG) and the IP PBX Media Gateway (for analog, T1/E1) or between the TMG and an external IP network through the Telephony Firewall.
- **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 there are other TIDs in the system. If only one TID exists in the system (single or multiple zone), only telephone call capability is affected, all other voice dispatch functions continue to operate.

### 3.7.2.6 Other Interconnect Failure Considerations

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 because 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 configuration, user limitations, or channel availability, CPS programming of the 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 internal audio path resources are not equal to PBX resources.

## 3.7.3 Data Plane Failures

This section describes the status or condition of the ASTRO® 25 data communication system resulting from failures in components supporting the data plane. In the HA Data configuration, both devices in a redundant pair must fail in order for the following failures to be realized.

### 3.7.3.1 GGSN Failures

The GGSN provides inter-networking between your data network and the Motorola ASTRO® 25 communication system. It also handles IP routing services for end-to-end data messaging. This includes static and dynamic IP addressing, IP fragmentation, and Internet Control Message Protocol (ICMP) error reporting to support troubleshooting activities. With the failure of the GGSN, all IP services, as well as the ability of the system to provide data messaging from your data network to mobile data devices in your system are dropped.

### 3.7.3.2 Packet Data Gateway – PDR or RNG Failures

Failure of the PDR results in the disconnection of the data path between the ASTRO® 25 data communication system and mobile subscriber units (MSUs). Thus, the ability to establish context activation for an MSU is lost.

### 3.7.3.3 Border Gateway Failures

Border gateway failure prevents IP data from being sent to or from the Customer Enterprise Network, but inhibits your ability to send data messages from your data network to MSUs and associated data devices.

## 3.7.4 Network Management Plane

This section contains information on the following failures:

- Capacity Lost When Servers Fail
- Subnet Structure

### 3.7.4.1 Capacity Lost When Servers Fail

ASTRO® 25 servers perform different duties or carry specific data. The impact of a server failure on the rest of the system depends on:

- What server failed
- The status of the system at the time the failure occurred.

The table below illustrates system capacities lost upon the failure of each type of server.

Table 9: Lost System Capacity Due to Server Failure

| Subsystem | Server | Capacity Lost |
|---|---|---|
| Network Management Subsystem | User Configuration Server application | • Prevents the UCS server application database restore/replication process from occurring.<br>• Subscriber information cannot be edited, subscriber records cannot be created, and home zone maps cannot be modified or viewed.<br>• System-level parameters cannot be changed with the Provisioning Manager application. The ability of the system to process call requests and assignments is not affected since zone controllers can utilize the information in their HLR/VLRs to process calls during this type of failure. |
| Network Management Subsystem (Continued) | Unified Network Configuration Server application/Unified Network Configurator Device Server (UNCDS) | • Results in the loss of all Unified Network Configurator (UNC) management capabilities, including the Unified Network Configuration Wizard and VoyenceControl applications. This loss prevents the scheduled distribution of device configurations, as well as the management of operating systems and their credentials.<br>**NOTICE:** The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product. |

*Table continued…*

| Subsystem | Server | Capacity Lost |
|---|---|---|
| Network Management Subsystem (Continued) | Zone Database Server application | • Results in a disruption to the distribution of configuration changes made in the Provisioning Manager to Consoles and CCGWs in a zone. |
| Network Management Subsystem (Continued) | Zone Statistics Server application | • Prevents the viewing of zone-wide historical data and statistics.<br>• Zone-level statistics are no longer available to the System Statistics Server.<br>• The ATR server application buffers 8 hours of data.<br>- If the ZSS server application recovers in this time, no low-level statistical information is lost.<br>- If the ZSS server application recovery takes more than 8 hours, only the data collected during the last 8 hours is available.<br>The ability of the system to process call requests and assignments is not affected since zone controllers can utilize the information in their HLR/VLRs to process calls during this type of failure. |
| Network Management Subsystem (Continued) | Air Traffic Router server application | • The ATIA packet data and zone statistics are no longer available. Devices that depend on the ATIA stream are affected. Zone statistics uploads to the ZSS server application and the SSS server application are interrupted. Consolidation of zone and system statistics is delayed until either the ATR server application recovers, or 8 hours pass.<br>• Affiliation data is unavailable for the zone. Dynamic Reports are unavailable. ATIA Log Viewer is unavailable (cannot access log files). The Affiliation Display application becomes unavailable. ZoneWatch application data becomes unavailable.<br>The ability of the system to process call requests and assignments is not affected since zone controllers can utilize the information in their HLR/VLRs to process calls during this type of failure. |
| Network Management Subsystem (Continued) | UEM Server | • Results in the loss of UEM fault/network management functionality for the zone.<br>Failure of the UEM does not impact the ability of the system to process calls. |
| Call Processing Subsystem | Zone Controller | ASTRO® 25 systems are installed with redundant zone controllers. If the active zone controller fails, all sites in the zone go into site trunking mode until the switch to the redundant zone controller is completed. Fault management is unavailable for devices where fault management information is proxied by the active zone controller. |
| Console Subsystem | CDM/ADM Server | The ability to configure/reconfigure the consoles is lost. Call processing is not affected. |

*Table continued…*

| Subsystem | Server | Capacity Lost |
|---|---|---|
| Telephone Interconnect Subsystem | Telephone Interconnect Server | • Causes the server to end all telephone interconnect calls the server is handling.<br>• Call requests are rejected. |

### 3.7.4.1.1 PC Client Failure

PC Client Workstation failure only results in the loss of use of that workstation. System management applications can still be run on other workstations attached to the system.

### 3.7.4.1.2 Terminal Server Failure

Terminal Server failure results in the loss of Out of Band Management capability. Remote and dial-in connectivity to the system is unavailable. System functionality is not affected.

### 3.7.4.2 Subnet Structure

Understanding the network organization and the IP addressing scheme is important, because all management/configuration and call control information flows over IP-based network paths. Being able to determine the status of the network links through the use of tools such as PING is an important part of your troubleshooting process.

The IP network moves the configuration information between the UCS server application, the ZDS server application, and the zone controllers. The IP network also carries other management information such as, Fault Management, Simple Network Management Protocol (SNMP), statistics, and performance data.

The IP network within each zone connects through the WAN equipment to link all zones together into one large network. The UCS server application, for example, exists in one zone, but interacts with the ZDS server application in each zone. In the same fashion, management users in any zone (with the proper privileges) can connect to any management server in the system from a user terminal in their zones.

Each subsystem is assigned its own subnet. Each remote site also has its own subnet assigned. These subnet assignments determine what IP addresses are assigned to the host devices in each subsystem.

The routers in the system act as gateways between the subnets. Each port on a router is associated with a subnet and is assigned a specific IP address based upon the subnet. Routing tables stored in the routers determine how a packet is routed between ports on the router.

A complete listing of the IP address map associated with a specific system is included in the System Installation Guide that came with your system.

## 3.8 Troubleshooting Services with Raw Display/ATIA Events

Another method for troubleshooting features in the system is to view the real-time events in the ZoneWatch raw display while you are trying to perform a particular action (such as a telephone interconnect call). 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. The following sections show the typical output that would be seen during different types of subscriber activity or call requests.

**NOTICE:** Real-time events are collected and can be inspected with ATIA Log Viewer. If you wish to view ATIA log files, ensure that you have ATIA logging enabled on the Air Traffic Router server application (ATR).

Each call is given a unique call number in the raw display. All events that are logged during the duration of the call are identified by the unique call number, until the call is finally terminated. This allows you to trace through the raw display and follow the events for one particular call (such as, Call # 4). After the call is terminated, another call may then use the call number.

The universal call number is unique within the controlling zone, thus combining it with the Controlling Zone ID uniquely identifies a call across the entire system.

When a call involves multiple zones, then some messages or information can appear only in one of the zones. For example, affiliation information appears only in the zone where the individual is affiliated, and Controlling Zone Update messages appear only in the zone that controls the whole call.

For Radio Control Manager (RCM) commands, there is a command number (such as, Command #24150) which identifies all the events related to a particular command sent from the RCM.

Each significant event during the call is given a sequence number. The first event (such as the start of the call) is noted as sequence #1. Subsequent events in the call are given subsequent sequence numbers. For example:

- the call start event is noted as sequence #1
- another radio keying in to reply to the call is noted as sequence #2
- call termination would then be noted as sequence #3

Each raw display event has a date/time stamp, and events are color-coded. Mobility updates are teal, call activities are black, data activities are violet, system events are red, and emergency events show as white text on red background.

## 3.8.1 Registration

A registration activity typically takes place when a subscriber is turned on or when the subscriber enters the coverage area. In the raw display or ATIA log file, the following two events are typically displayed during the registration:

```
Mobility Update – Unit Registration
Mobility Update – Group Affiliation
```

Table 10: Registration – Raw Display Messages on page 111 describes each of the event messages, which are displayed during the registration. Each event message includes a long list of details about the event, such as the radio ID or the site the event took place in. Table 10: Registration – Raw Display Messages on page 111 lists some of the more significant fields that may be helpful when analyzing messages for registration problems.

Table 10: Registration – Raw Display Messages

| Message | Event Description | Significant Fields |
|---|---|---|
| Mobility Update – Unit Registration | Indicates the registration for the individual radio user. The message includes information about the | Radio ID, Site, Zone, WACN ID, System ID, Mobility Request Result |

*Table continued…*

| Message | Event Description | Significant Fields |
|---|---|---|
| | radio, site, and zone. | |
| Mobility Update – Group Affiliation | Indicates a successful talkgroup affiliation. | Radio ID, Talkgroup, Mobility Request Result |

### 3.8.2 Group Affiliation (Changing Talkgroups)

Group affiliation takes place during the registration and when the talkgroup selector on the subscriber has been changed to another talkgroup. The following event is typically displayed in the raw display or ATIA log file when a subscriber changes talkgroups:

```
Mobility Update – Group Affiliation
```

Table 11: Group Affiliation – Raw Display Messages on page 112 describes the event message displayed after a talkgroup has been changed on the subscriber selector. Table 11: Group Affiliation – Raw Display Messages on page 112 lists some of the more significant fields that may be helpful when analyzing messages for affiliation problems.

Table 11: Group Affiliation – Raw Display Messages

| Message | Event Description | Significant Fields |
|---|---|---|
| Mobility Update – Group Affiliation | Indicates a successful affiliation with the newly selected talkgroup. | Radio ID, Talkgroup ID, Mobility Request Result |

### 3.8.3 Site Handover

A subscriber may change sites when roaming or when a site change has been requested. The following mobility update message is typically seen in the raw display or an ATIA log file when a subscriber affiliates with a different site:

```
Mobility Update – Location Registration
```

Table 12: Site Handover – Raw Display Messages on page 113 describes the event message displayed after a subscriber has affiliated with a new site. Table 12: Site Handover – Raw Display

Messages on page 113 lists some of the more significant fields that may be helpful when analyzing messages for site handover problems.

Table 12: Site Handover – Raw Display Messages

| Message | Event Description | Significant Fields |
|---|---|---|
| Mobility Update – Location Registration | Indicates when a subscriber has affiliated at a new site. | Radio ID, Affiliated Talkgroup ID, Site, Zone, Mobility Response Site# |

### 3.8.4
## Deregistration

A subscriber is deregistered from the system after the unit has been turned off. The following update message is typically seen in the raw display or ATIA log file when a subscriber is deregistered from the system:

```
Mobility Update – Deregistration
```

Table 13: Deregistration – Raw Display Messages on page 113 describes the event message displayed after a subscriber has deregistered. Table 13: Deregistration – Raw Display Messages on page 113 lists some of the more significant fields that may be helpful when analyzing messages for deregistration problems.

Table 13: Deregistration – Raw Display Messages

| Message | Event Description | Significant Fields |
|---|---|---|
| Mobility Update – Deregistration | Indicates when a subscriber has deregistered. | Reason (Deregistered by ISP), Radio ID, Site, Zone, WACN ID, System ID |

### 3.8.5
## Group Call

A group call is initiated when a subscriber presses the push to talk button. The zone controller sets up the infrastructure for the call and grants the permission to start a new call. In the raw display or an ATIA log file, the following sequence of events is typically displayed when a group call is started:

```
Radio Status Traffic – Proceeding Ack Sent
Controlling Zone Update – Start of Call
Call Activity Update – Start of New Call
```

After the initiating subscriber has finished talking and released the push to talk button, other subscribers can reply to the call by pressing their push to talk buttons before the call hang timer expires. The following messages are typically displayed when another subscriber presses the push to talk to reply in the group call:

```
Radio Status Traffic – Proceeding Ack Sent
Controlling Zone Update – PTT-ID Active Control
Call Activity Update – PTT-ID Update Active
```

When none of the subscribers responds by pressing their push to talk button, the hang timer expires and the call terminates. The following messages are displayed when a group call terminates:

```
Controlling Zone Update – End of Call
End of Call – ZC End of Call
```

Table 14: Group Call – Raw Display Messages on page 114 describes each of the event messages which may be displayed during a group call (in the proper sequence). Each of the individual event messages includes a long list of details about the event. Table 14: Group Call – Raw Display Messages on page 114 lists some of the more significant fields that may be helpful when analyzing messages for group call problems.

Table 14: Group Call – Raw Display Messages

| Message | Event Description | Significant Fields |
|---|---|---|
| Radio Status Traffic – Proceeding Ack Sent | The calling subscriber has pressed the push to talk button and the system is responding to the call request from the subscriber. | Radio ID (caller), Talkgroup ID, Site, Zone, Controlling Zone Information |
| Controlling Zone Update – Start of Call | The resources have been set up to start the call. The event message explains the type of call (Digital, Talkgroup). | Controlling Zone ID, Active/Busy, Call Type (Digital, Talkgroup), Call #, Participating Zones, Rendezvous Point (RP) |
| Call Activity Update – Start of New Call | The new call is started and the caller can begin speaking. The event message displays the resources assigned to the call and the multicast IP address. | Radio ID (caller), Talkgroup ID, Call #, Call Type (Digital, Talkgroup), Multicast IP, Secure Key |

*Table continued…*

| Message | Event Description | Significant Fields |
|---|---|---|
| Radio Status Traffic – Proceeding Ack Sent | After the caller has released their PTT button, another subscriber has pressed their PTT button to respond to the call. | Radio ID (new subscriber), Talkgroup ID, Site, Zone, Controlling Zone Information |
| Controlling Zone Update – PTT-ID Active Control | The infrastructure sets up for the new subscriber to transmit to the group. | Controlling Zone ID, Call Type (Digital, Talkgroup), Radio ID, Call #, Participating Zones, Rendezvous Point (RP) |
| Call Activity Update – PTT-ID Update Active | The call activity for the new subscriber begins. | Radio ID, Call #, Call Type (Digital, Talkgroup), Target Talkgroup ID, Zone, Site/Channel, Multicast IP, Secure Key |
| Controlling Zone Update – End of Call | The hang timer has expired and the zone controller releases its resources. The message explains the reason why the call has ended. | Reason (Disconnect complete), Call Type (Digital, Talkgroup), Radio ID, Talkgroup ID, Call #, Participating Zones |
| End of Call – ZC End of Call | The call is ended. | Reason (Disconnect complete), Call # |

## 3.8.6 Private Call

A private call is initiated when a subscriber selects the radio ID of another subscriber and presses the push to talk button. The zone controller sets up the infrastructure for the call and rings the target subscriber. The following events are displayed in the raw display or ATIA log file:

```
Controlling Zone Update – Start Of Call
Call Activity Update – Start of New Call
Radio Status Traffic – Private Call Ring Ack
```

When the target subscriber accepts the private call, the following events are displayed. The call is then established and the two subscribers can communicate.

```
Radio Status Traffic – Ring Update
Controlling Zone Update – Call State Change
Call Activity Update – Call State Change
```

When one of the subscribers terminates the private call, the following messages are displayed to indicate the end of the private call:

```
Radio Status Traffic - Cancel Call Ack
Controlling Zone Update – End Of Call
End of Call – ZC End of Call
```

Table 15: Private Call – Raw Display Messages on page 116 describes each of the event messages that may be displayed during a private call (in the proper sequence). Each of the individual event messages includes a long list of details about the event. Table 15: Private Call – Raw Display Messages on page 116 lists some of the more significant fields that may be helpful when analyzing messages for private call problems.

Table 15: Private Call – Raw Display Messages

| Message | Event Description | Significant Fields |
|---|---|---|
| Controlling Zone Update – Start Of Call | The resources have been set up to start the call. The event message explains the type of call (Individual). | Controlling Zone ID, Active/Busy, Call Type (Individual), Call #, Participating Zones |
| Call Activity Update – Start of New Call | | Radio ID (caller), Call Type (Digital, Private Call), Call #, Radio ID (target), Site/ Channel, Local/ Controlling Zone, Secure Key # |
| Radio Status Traffic – Private Call Ring Ack | The system acknowledges that the subscriber is ready for the call. | Radio ID (target), Radio ID (caller), Site, Local/ Controlling Zone |
| Radio Status Traffic – Ring Update | The target subscriber has accepted the call. | Radio ID (target), Radio ID (caller), Site, Local/ Controlling Zone |
| Controlling Zone Update – Call State Change | The system transitions from ringing the target sub- | Controlling Zone ID, Active/Busy, Call Type (Individual), Call #, |

*Table continued…*

| Message | Event Description | Significant Fields |
|---|---|---|
| | scriber into becoming an active private call. Voice services begin. | Participating Zones |
| Call Activity Update – Call State Change | | Transition (User to User Ring to Global Active, Call Type, Call #, Radio ID (caller), Radio ID (target), Site/Channel, Local/Controlling Zone, Busy Resources, Multicast IP, Secure Key # |
| Radio Status Traffic - Cancel Call Ack | The system acknowledges cancelling the call. | Radio ID (target), Radio ID (caller), Site, Local/ Controlling Zone |
| Controlling Zone Update – End Of Call | A caller terminates the call or the call terminates for some other reason (as listed in the event message). | Reason (Initiator canceled call), Call #, Participating Zones |
| End of Call – ZC End of Call | | Reason (Initiator canceled call), Call #, Controlling/Local Zone |

### 3.8.7
## Telephone Interconnect Call

A 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 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 button. The zone controller receives the call request and the following event messages are displayed:

```
Radio Status Traffic – Proceeding Ack Sent
Controlling Zone Update – Start of Call
Call Activity Update – Start of New Call
```

The infrastructure dials the landline phone number and the landline phone begins to ring.

When the landline user answers the call, the following messages are displayed:

```
Controlling Zone Update – Call State Change
Call Activity Update – Call State Change
```

and the voice transaction begins.

The landline user, subscriber, or infrastructure eventually terminates the call and the following events are displayed:

```
Controlling Zone Update – End Of Call
End of Call – ZC End of Call
```

Table 16: Telephone Interconnect Call – Raw Display Messages on page 118 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. Table 16: Telephone Interconnect Call – Raw Display Messages on page 118 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 push to talk button. The system is responding to the call request from the subscriber. | Radio ID, Site, Zone, Controlling Zone Information |
| Controlling Zone Update – Start of 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). | Controlling Zone ID, Active/Busy, Call Type (Individual), Call #, Participating Zones |
| Call Activity Update – Start of New Call | | Radio ID, Call #, Call Type (Digital, Central Mobile to Land Interconnect), Active Site/Channel, Secure Key #, Busy Resources |
| Controlling Zone Update – Call State Change | The landline user has picked up the phone. The infrastructure transitions from ringing to an active voice call. | Controlling Zone ID, Active/Busy, Call Type (Individual), Call #, Participating Zones |
| Call Activity Update – Call State Change | | Transition (Ring to Active), Call #, Call Type (Digital, Central Mobile to Land Interconnect), Radio ID, Active Site/Channel, Multicast IP, Secure Key # |
| Controlling Zone Update – End Of Call | The subscriber or landline user has terminated the call. The system can also | Reason (Phone line termination command received during call), Call #, Participating Zones |
| End of Call – ZC End of Call | | Reason (Phone line termination command received during call), Call #, Controlling/Local Zone IDs |

| Message | Event Description | Significant Fields |
|---|---|---|
| | terminate the call if there are problems or if the subscriber has exceeded their monthly interconnect time. | |

This page intentionally left blank.

**Appendix A**

# Service Laptop and Software Setup

This appendix provides information on the Service Laptop that may be required for system configuration, maintenance, or troubleshooting. In addition, software is described, and its configuration and download are explained.

## A.1 Service Laptop Overview

You may require a Service Laptop for system configuration, maintenance, or troubleshooting.

The following software applications must be installed on the service laptop:

- Configuration/Service Software (CSS) – Used to create and back up device configurations and troubleshoot RF site and Voice Processor Module (VPM)-based devices, including GTR 8000 Base Radios, GPW 8000 Receivers, GCM 8000 Comparators, GCP 8000 Site Controllers, GPB 8000 Reference Distribution Modules, SmartX Site Converters, and Telephone Media Gateways. It also supports specific existing devices as indicated in CSS online help.
- Software Download Manager (SWDL) – Used to download firmware to the base radios and site controller.
- Customer Programming Software (CPS) – Used to program subscriber radios.

Laptop hardware and OS requirements depend on the software you intend to use. See requirements for specific software. Depending on your system configuration, install the appropriate software on the Service Laptop. Follow the instructions on the installation DVDs for each software application.

- For systems with MOSCAD network fault management: Local configuration and troubleshooting of SDM3000 Network Translator (SNT) and Devices in the SDM3000 Builder application. See the *MOSCAD Network Fault Management Feature Guide* manual.
- For systems with the Unified Event Manager (UEM) network fault manager: the general functionality of UEM is managed using internal license configuration based on license key entries and embedded licensing management. See the *Unified Event Manager* manual.
- For systems with MLC 8000 hardware, see *MLC 8000 Configuration Tool User Guide* manual and online help.

### A.1.1 Service Laptop Requirements for CPS

For Customer Programming Software (CPS) service laptop hardware and OS requirements, see CPS_readme.txt file on the CPS installation DVD or in the program installation directory.

### A.1.2 Service Laptop Requirements for RSS and CSS

The Configuration/Service Software (CSS) is used for the GCM 8000 Comparator, GCP 8000 Site Controller, GTR 8000 Base Radio, GPW 8000 Receiver, and GPB 8000 Reference Distribution Module.

The Radio Service Software (RSS) is used for:

- Programming all versions of codeplugs for the QUANTAR® stations and ASTRO-TAC™ Comparators in 3.x and 4.x conventional and trunked systems.
- Software downloading (starting with version R14.00.00 RSS)

Supported operating systems:

- Windows Server 2012 R2 64-bit for RSS (Software Download and CSS is not supported)
- Windows 10 32-bit and 64-bit

Hardware requirements:

- 1 GHz or higher Pentium grade processor
- 1 GB RAM recommended for Windows Server 2012 R2 64-bit
- 1 GB RAM recommended for Windows 10 32-bit
- 2 GB RAM recommended for Windows 10 64-bit
- 300 MB minimum free space for CSS Typical Installation (including Help Text and Software Download Manager) or 100 MB minimum free space for a Compact Installation
- 300 MB minimum free space for RSS Typical Installation (including Help Text and Software Download Manager) or 100 MB minimum free space (for a Compact Installation)

Peripherals:

- Serial port or a USB with a USB-to-serial converter as a connection device (not currently Motorola Solutions-certified)
- Windows-supported mouse or trackball
- Windows-supported 10Base-T Ethernet port for product communication
- Windows-supported printer port for report printing
- DVD for software installation

### A.1.3
## Service Laptop Requirements for SDM3000 Builder

SDM3000 Builder software is a Windows-based application used to set up and configure the SDM3000 Network Translator and SDM3000 devices. Based on information you enter in the SDM3000 Builder screens, the software calculates inter-site and intra-site dependencies, such as defining the number, order, and connections of the CPU and I/Os in the SDM3000 Network Translator and SDM3000 devices, while considering your equipment and needs.

Supported operating systems:

- Windows Server 2012 R2
- Windows 10 32- and 64-bit

Hardware requirements:

- 512 MB of RAM
- 20 GB of minimum free space

### A.1.4
## Service Laptop Requirements for Other Software

Load the laptop with the following software:

- Remote Desktop Connection or a similar utility
- PuTTY (for Serial, Secure SHell (SSH) and Telnet connections) or a similar utility

- Microsoft Internet Explorer (latest) or Firefox (latest) for Configuration/Service Software (CSS) software
- VMware vSphere client (if any Virtual Management Servers are included in your system configuration)
- VMware PowerCLI
- .NET Framework 4.5
- Powershell 4.0

## A.2 Customer Programming Software

Subscriber radios are configured through Customer Programming Software (CPS). A computer running CPS is directly connected to the universal connection port on the subscriber radio and the codeplug is loaded. The configuration settings in CPS are categorized into different types, such as **Radio-Wide** settings, **Controls**, **Display and Menu** settings, and **Secure** settings. Parameters must be set according to the services the radio uses. CPS is used to configure each radio with a system ID, a unique individual ID for the radio, and as many talkgroup IDs as needed.

For subscriber radio programming details, see your subscriber radio user guide and *Customer Programming Software* online help.

This page intentionally left blank.