MOTOROLA SOLUTIONS

MOTOTRBO™

IP Site Connect and Capacity Plus

MOTOTRBO System Planner

System Release M2024.02

AUGUST 2024

© 2024 Motorola Solutions, Inc. All Rights Reserved.

68007024085-PE

Intellectual Property and Regulatory Notices

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.

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.

License Rights

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 nonexclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Open Source Content

This product may contain Open Source software used under license. Refer to the product installation media for full Open Source Legal Notices and Attribution content.

European Union (EU) and United Kingdom (UK) Waste of Electrical and Electronic Equipment (WEEE) Directive

The European Union's WEEE directive and the UK's WEEE regulation require that products sold into EU countries and the UK must have the crossed-out wheelie bin label on the product (or the package in some cases). As defined by the WEEE directive, this crossed-out wheelie bin label means that customers and end users in EU and UK countries should not dispose of electronic and electrical equipment or accessories in household waste.

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

Disclaimer

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

© 2024 Motorola Solutions, Inc. All Rights Reserved

Contact Us

The Centralized Managed Support Operations (CMSO) is the primary contact for technical support included in your organization's service agreement with Motorola Solutions. To enable faster response time to customer issues, Motorola Solutions provides support from multiple countries around the world.

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

- To confirm troubleshooting results and analysis before taking action

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

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

Comments

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

Provide the following information when reporting a documentation error:

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

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

Document History

Version	Description	Date
68007024085-NK	2.9 system release of the *MOTOTRBO IP Site Connect, Capacity Plus System Planner* manual. ● New in this release: ○ MOTOTRBO Link Mode on page 65 ○ MOTOTRBO Link ○ MOTOTRBO Link Standalone Topology ○ MOTOTRBO Link Hybrid Topology ○ Estimate Loading (for MOTOTRBO Link) on page 406 ○ MOTOTRBO Link Mode on page 571 ○ When Ignore Rx Clear Voice/Packet Data and Fixed Privacy Key Decryption Options are not Enabled on page 184 ● Minor edits to the following topics: ○ Data Gateway Privacy Settings on page 189 ○ Keys and Key Management on page 188 ○ Key Mismatch on page 187 ○ When Ignore Rx Clear Voice/Packet Data and Fixed Privacy Key Decryption Options are not Enabled on page 184 ○ Ignore Rx Clear Voice or Packet Data Option on page 185 ○ User Control Over Privacy on page 184 ○ AES Configuration in MOTOTRBO on page 182 ○ Strength of the Protection Mechanism on page 183 ○ Types of Privacy on page 182 ○ Extended Range Direct Mode on page 342 ○ Configuration in Radio on page 344 ○ Configuration in Repeater on page 344	April 2018
68007024085-NL	2.9.5 system release of the *MOTOTRBO IP Site Connect, Capacity Plus System Planner* manual. This update includes the following changes: ● Added Indoor Location on page 135 and its subsections. ● Updated MOTOTRBO Link Mode on page 65 and its subsections.	August 2018

Version	Description	Date
68007024085-NM	2.10 system release of the *MOTOTRBO IP Site Connect, Capacity Plus System Planner* manual. This update includes the following changes: ● Added Software Update Management on page 275 and its subsections. ● Added Repeater Webserver Functions on page 277 and its subsections. ● Added Broadcast Calls on page 577 and the corresponding procedure. ● Added Unaddressed Calls on page 578 and the corresponding procedure. ● Added Open Voice Channel Mode Calls on page 579 and the corresponding procedures.	March 2019
68007024085-NN	2.10.5 system release of the *MOTOTRBO IP Site Connect, Capacity Plus System Planner* manual. This update includes the following changes: ● Added MOTOTRBO 2-4-1 Feature Overview on page 281 and its subsections. ● Added Radio Features on page 291 and its subsections. ● Updated MOTOTRBO Link Mode on page 65. ● Updated Data Applications and MNIS Deployments on page 499 ● Updated Resetting Login Credentials/Certificate on page 280	July 2019
68007024085-NP	Second release of the 2.10.5*MOTOTRBO IP Site Connect, Capacity Plus System Planner* manual. This update includes the following changes: ● Updated Data Applications and MNIS Deployments on page 499 ● Updated Resetting Login Credentials/Certificate on page 280	August 2019
68007024085-NR	Third release of the 2.10.5*MOTOTRBO IP Site Connect, Capacity Plus System Planner* manual. This update includes the following changes: ● Updated Repeater Diagnostics and Control on page 191 ● Updated System Topology with the MNIS on page 493	November 2019
68007024085-NS	First release of the M2020.01 *MOTOTRBO IP Site Connect, Capacity Plus System Planner* manual. This update includes the following changes: ● IP Repeater Programming on page 201	April 2020

Version	Description	Date
	• Enterprise Wi-Fi Roaming Enhancement on page 252 • Fall Alert on page 292 • Gas Detection Solution in MOTOTRBO	
68007024085-NT	Deleted section for MOTOTRBO Sensor Data. Deleted information on Windows 7 support.	May 2020
68007024085-NU	First release of the M2020.02 *MOTOTRBO IP Site Connect, Capacity Plus System Planner* manual. The following sections were updated: • Bluetooth Barcode Scanner Operation on page 237 • Inband Data Services on page 293 • Configuring Caller Alias in Radio Management on page 294	August 2020
68007024085-NV	First release of the M2021.01 *MOTOTRBO IP Site Connect, Capacity Plus System Planner* manual. The following sections were added: • Gas Detection Solution in MOTOTRBO • CapMax System Configuration • Configuring Gas Detector Data in Radio Management	January 2021
68007024085-NW	First release of the M2021.04 *MOTOTRBO IP Site Connect, Capacity Plus System Planner* manual. The following sections were added: • Capacity Plus Network Configurations on page 582 • Repeater Network Configuration Options in Capacity Plus Single Site and Capacity Plus Multi Site on page 386 • Back-End Network Topologies in Capacity Plus Multi Site on page 447 • Back-End Network Characteristics in Capacity Plus Multi Site on page 447 • Data Applications and MNIS Deployment on Separate PCs on page 500	December 2021
68007024085-NY	The following section was updated: • Capacity Plus Multi Site Mode on page 63	January 2022
68007024085-NZ	The following sections were deleted: • MOTOTRBO Text Messaging Application • Services Provided to a Radio User • Services Provided to a Mobile Client • Services Provided to a Dispatcher • Services Provided by the MOTOTRBO Text Messaging Server Application	November 2022

Version	Description	Date
	• Services Provided by the MOTOTRBO Location Services Application • Multi-Channel Device Driver (MCDD) • Text Messaging Application • Text Messaging Client • Text Messaging Client Computer Specifications • Text Messaging Server • Multi-Channel Configuration • Text Messaging Server Administrative Client • Text Messaging Server Computer Specifications • Location Server Computer Specifications • MOTOTRBO Location Client • Location Client Computer Specifications • Modifying the MotoLocator • Multi-Channel Device Driver (MCDD) and Required Static Routes The following sections were updated: • Control Station Configurations on page 210 • Multi-Channel Configuration on page 227 • Multi-Channel Server-Based Data Applications in DCDM on page 334 • Server Based Data Applications in Repeater Mode on page 350 • Wide Area System with a Centralized Data Application Server on page 362 • RF Isolated Single Site Repeaters on page 542 • Services Provided to a Radio User on page 116 • Security Considerations on page 433 • Management Rules for the Juniper Devices on page 596 • System Module (Router) on page 597 • Security Module on page 599 • System Module (Switch) on page 616 • Adaptation of Configurations Templates for No Tunnels Topology on page 626 • AVPN Configuration Templates on page 638 • Hub-to-Spoke Configuration Templates on page 629 • Firewall Module on page 612 • Resetting Login Credentials/Certificate on page 280	

Version	Description	Date
	• Restricted Access to System Key Authentication on page 104 • Radio Operation with Motorola Solutions Headsets with PTT on page 237 • Radio Operation with Motorola Solutions PTT Only Devices on page 237 • Recommended Bluetooth Devices on page 238 • Avoiding Accidental Connection on page 238 • Considerations for Router with Networked Applications on page 508 • All Call on page 88 • Emergency Alarm and Call on page 100 The following sections were added: • Data Security Between the RM and the Devices on page 294 • Key Management on page 295 • Adding the Pre-shared Key to the Radio Management on page 295 • Securing Devices on page 295	
68007024085-PA	The following sections were updated: • Delay/Latency in IP Site Connect Mode on page 427 • System Topology with the MNIS on page 493 • RDS Logs on page 278 • Data Applications and MNIS Deployment on Separate PCs on page 500 The following section was added: • Performing Repeater Factory Reset on page 296	May 2023
68007024085-PB	The following sections were updated: • MOTOTRBO Network Interface Service Deployments on page 207 • Single Site on page 207 • IP Site Connect on page 208 • Capacity Plus Single Site on page 208 • Capacity Plus Multi Site on page 209 • Control Station Configurations on page 210 • Battery Management Application Deployment on page 214 • Battery Fleet Management Application on page 214 • Remote Battery Management Client on page 215	August 2023

Version	Description	Date
	● Remote Battery Management Proxy on page 216 ● Coexistence with Other Data Applications on page 217 ● Basic Deployments of OTAP Software on page 220 ● MNIS and DDMS Operation Overview on page 490 ● Data Application Interface on page 492 ● Data Applications and MNIS Deployments on page 499	
68007024085-PC	The following section was updated: Accessing the Web-page of the Repeater on page 277	January 2024
68007024085-PD	The following sections were updated: ● Radio Management Computer Specifications on page 565 ● Configuring Caller Alias in Radio Management on page 294 The following section and its subsections were deleted: ● Gas Detection Solution in MOTOTRBO	May 2024
68007024085-PE	The following sections were updated: ● Digital Voting on page 388 ● Digital Voting in IP Site Connect (Wide Area Channels) on page 390 ● Digital Voting in Capacity Plus Single Site on page 392	August 2024

Contents

Intellectual Property and Regulatory Notices....2
Contact Us....3
Document History....4
List of Figures....29
List of Tables....36
List of Processes....40
List of Procedures....41
About MOTOTRBO IP Site Connect, Capacity Plus System Planner....43
Related Information....43
Chapter 1: Introduction....45
1.1 Welcome to MOTOTRBO....45
1.2 Software Version....46
Chapter 2: System Feature Overview....47
2.1 MOTOTRBO Digital Radio Technology....47
2.1.1 Digital Radio Technology Overview....47
2.1.1.1 Analog to Digital Conversion....48
2.1.1.2 Vocoder and Forward Error Correction....48
2.1.1.3 Framing....48
2.1.1.4 Time Division Multiple Access Transmission....48
2.1.1.5 Standards Compliance....49
2.1.2 Spectrum Efficiency Through 2-Slot TDMA....49
2.1.2.1 Frequencies, Channels, and Requirements for Spectrum Efficiency....49
2.1.2.2 Delivering Increased Capacity in Existing 12.5 kHz Channels....49
2.1.2.3 2-Slot TDMA Reducing Infrastructure Equipment....50
2.1.2.4 2-Slot TDMA Enables System Flexibility....51
2.1.2.5 2-Slot TDMA System Planning Considerations....52
2.1.3 Digital Audio Quality and Coverage Performance....53
2.1.3.1 Digital Audio Coverage....53
2.1.3.2 Predicting Digital Audio Coverage....54
2.1.3.3 User Expectations for Digital Audio Performance....55
2.1.3.4 Audio Balancing....56
2.2 Basic System Topologies for Digital and Analog Operations....57
2.2.1 Repeater and Direct Mode Configurations....58
2.2.1.1 Analog Repeater Mode....59

2.2.1.2 Digital Repeater Mode....59
2.2.1.3 Dynamic Mixed Mode....59
2.2.1.4 IP Site Connect Mode....60
2.2.1.5 Capacity Plus Single Site Mode....61
2.2.1.6 Capacity Plus Multi Site Mode....63
2.2.1.7 MOTOTRBO Link Mode....65
2.2.2 MOTOTRBO Supports Analog and Digital Operation....82
2.2.3 MOTOTRBO Channel Access....83
2.2.3.1 Impolite Operation....84
2.2.3.2 Polite to All Operation....84
2.2.3.3 Polite to Own Digital System Operation....85
2.2.3.4 Polite to Other Analog System Operation....85
2.2.3.5 Polite, Impolite or Voice Interrupt In A Call....85
2.2.3.6 Repeater Wake-up Provisioning....86
2.3 Digital Voice Features....86
2.3.1 Group Calls....86
2.3.2 Private Calls....87
2.3.3 All Call....88
2.3.4 DTMF Hot Keypad....88
2.4 Advantage Transmit Interrupt....89
2.4.1 Transmit Interrupt Capable System Upgrade....91
2.5 Digital Signaling Features....92
2.5.1 PTT ID and Aliasing....92
2.5.2 Radio Enable/Disable....92
2.5.2.1 Over-The-Air Signaling Enable/Disable....93
2.5.3 Remote Monitor....93
2.5.4 Radio Check....94
2.5.5 Call Alert....95
2.5.6 Remote Voice Dekey....95
2.6 Digital Emergency....95
2.6.1 Emergency Alarm Only....99
2.6.2 Emergency Alarm and Call....100
2.6.3 Emergency Alarm with Voice to Follow....100
2.6.4 Emergency Voice Interrupt for Emergency Alarm....101
2.6.5 Emergency Voice Interrupt for Emergency Voice....102
2.6.6 Emergency Search Tone....102
2.7 Restricted Access to System....103
2.7.1 Restricted Access to System Key Authentication....104
2.7.2 Radio ID Range Check....105

2.8 Digital Voting....105
2.9 CSBK Data....106
2.9.1 Supported Data Service....106
2.9.2 Impacted Features....106
2.9.3 Improved Third-Party Interfaces....107
2.9.4 Affected System Components....107
2.10 Digital Audio....107
2.11 Confirmed Group Data....108
2.12 MOTOTRBO Integrated Data....109
2.12.1 MOTOTRBO Integrated Data Overview....109
2.12.2 Text Messaging Services....110
2.12.2.1 Built-In Text Messaging Service....111
2.12.2.2 Predictive Text Entry....112
2.12.2.3 ETSI DMR Standard Text Messaging....113
2.12.2.4 ETSI DMR Tier 2 UDP/IP Header Compression....114
2.12.3 Location Services....114
2.12.3.1 Performance Specifications....115
2.12.3.2 Services Provided to a Radio User....116
2.12.3.3 Services Provided to a Location Application....116
2.12.3.4 GPS (GNSS) Revert Channel....117
2.12.3.5 Enhanced GPS (GNSS) Revert Channel....118
2.12.3.6 Data Revert Channel....129
2.12.3.7 Global Navigation Satellite System....129
2.12.3.8 GPIO Triggered Event Driven and Distance Driven Location Update....130
2.12.4 Telemetry Services....130
2.12.4.1 Physical Connection Information....131
2.12.4.2 Telemetry Examples....131
2.12.5 Data Precedence and Data Over Voice Interrupt....131
2.12.6 Enhanced Job Tickets....132
2.12.6.1 Job Tickets Registration....132
2.12.6.2 Common Job Tickets Data Communication....133
2.12.6.3 Common Job Tickets Inbox Folders....134
2.12.6.4 Subscriber Created Job Tickets....134
2.12.6.5 All Job Tickets Deletion....135
2.12.6.6 MNIS Network....135
2.13 Indoor Location....135
2.13.1 iBeacon....136
2.13.2 Indoor Location Operation....136
2.13.3 iBeacon Configuration and Operation Parameters....136

2.13.4 iBeacon Deployment Considerations..... 137
2.13.4.1 iBeacon UUID and Radio Operation Considerations..... 137
2.13.4.2 iBeacon BLE Advertisement Time Interval and Radio Scan Mode Operation Considerations..... 137
2.13.4.3 Radio CPS Configurable Scan Interval On/Off Time Operation Considerations..... 140
2.13.4.4 iBeacon Advertisement Tx Power and iBeacon RF Site Survey Considerations..... 141
2.13.4.5 Other iBeacon Deployment Considerations..... 143
2.13.4.6 Indoor Location Deployment Requirement Checklist..... 144
2.13.5 iBeacon OTA Parameters.....145
2.13.6 Radio Indoor Location Configuration and Operation Parameters.....145
2.13.7 Radio Indoor/Outdoor Location Application Services.....146
2.13.8 Third-Party Location Application Services..... 146
2.13.9 Radio GPS Revert Channel Location Services.....147
2.13.10 Radio Enhanced GPS Revert Channel Location Services.....148
2.13.11 Connect Plus Fast GPS Location Services..... 152
2.14 Scan.....154
2.14.1 Priority Sampling..... 155
2.14.2 Channel Marking..... 155
2.14.3 Scan Considerations..... 156
2.14.3.1 Scanning and Preamble..... 157
2.14.3.2 Channel Scan and Last Landed Channel.....159
2.14.3.3 Scan Members with Similar Receive Parameters..... 159
2.14.3.4 Voice Transmission Reception Improvement While Scanning..... 161
2.14.3.5 Disable Scan Hangtime for Voice Calls.....162
2.14.3.6 Unconfirmed Group Data Scanning..... 162
2.14.4 Transmit Interrupt and Scan.....163
2.15 Site Roaming..... 163
2.15.1 Passive Site Searching..... 165
2.15.2 Active Site Searching..... 167
2.15.3 Roaming Considerations.....168
2.15.3.1 Configuring the Roaming RSSI Threshold..... 168
2.15.3.2 Roam List Configuration.....174
2.15.3.3 Scan or Roam..... 177
2.15.3.4 Beacon Duration and Beacon Interval Settings.....177
2.15.3.5 Emergency Revert, GPS/Data Revert, and Roaming Interactions.....179
2.15.3.6 Performance while Roaming..... 180
2.15.3.7 ARS Registration on Roaming..... 181

2.16 Voice and Data Privacy....181
2.16.1 Types of Privacy....182
2.16.1.1 AES Configuration in MOTOTRBO....182
2.16.2 Strength of the Protection Mechanism....183
2.16.3 Effects of Privacy Protection on Performance....183
2.16.4 User Control Over Privacy....184
2.16.4.1 When Ignore Rx Clear Voice/Packet Data and Fixed Privacy Key Decryption Options are not Enabled....184
2.16.4.2 Ignore Rx Clear Voice or Packet Data Option....185
2.16.4.3 Fixed Privacy Key Decryption Option....185
2.16.5 Privacy Indications to User....187
2.16.6 Key Mismatch....187
2.16.7 Keys and Key Management....188
2.16.8 Multiple Keys in a Basic Privacy System....189
2.16.9 Data Gateway Privacy Settings....189
2.16.10 Protecting One Group’s Message from Another Group....190
2.16.11 Updating the Privacy Type....190
2.17 Real-Time Clock Synchronization....191
2.18 Repeater Diagnostics and Control....191
2.18.1 Connecting Remotely Through the Network....195
2.18.2 Connecting Locally Through the USB....195
2.18.3 Connecting Locally Through GPIO Lines....195
2.18.3.1 RDAC Local Settings Rear Accessory Port CPS Programmable Pins....196
2.18.4 Redundant Repeater Setup....197
2.18.5 Dual Control Considerations....199
2.18.6 Digital Voting Control and Monitor....199
2.18.7 General Considerations When Utilizing the RDAC Application to Set Up the Network Connection....200
2.19 Repeater Diagnostics System Enhancement....201
2.20 IP Repeater Programming....201
2.20.1 System Configuration for IRP Support....202
2.20.2 Configuring IRP in RM....202
2.21 Over-The-Air Battery Management....203
2.21.1 Over-The-Air Battery Management Process....204
2.21.2 Automatic Over-the-Air Battery Data Collection Configuration....205
2.21.3 System Level Optimizations....205
2.21.3.1 Battery Data Refresh Timer....205
2.21.3.2 Radio Hold Off Timer....205
2.21.3.3 Manual Battery Data Read Performance....206

2.21.3.4 Radio Battery Utilization While Charging..... 206
2.21.4 Advanced System Deployments..... 206
2.21.4.1 MOTOTRBO Network Interface Service Deployments.....207
2.21.4.2 Control Station Configurations..... 210
2.21.4.3 Battery Management Application Deployment..... 214
2.21.4.4 Coexistence with Other Data Applications..... 217
2.21.5 Battery Fleet Management Computer Specifications.....218
2.21.5.1 Operating System Requirement..... 218
2.21.5.2 Hardware Minimum Requirement.....218
2.21.5.3 Server Hardware Minimum Requirement..... 218
2.21.5.4 Client or Proxy Hardware Minimum Requirement..... 218
2.22 Over-The-Air Radio Programming..... 219
2.22.1 Basic Deployments of OTAP Software.....220
2.22.1.1 Local Single Channel Configuration..... 220
2.22.1.2 Local Single Channel Configuration with Presence..... 221
2.22.1.3 Remote Client Configuration..... 223
2.22.1.4 Remote Client Configuration with Multiple RM Servers..... 224
2.22.1.5 Remote Device Programmer Configuration..... 225
2.22.1.6 Multi-Channel Configuration.....227
2.22.2 Process Flow for Over-The-Air Programming.....228
2.22.2.1 Essential Communication Parameters Initial Programming..... 228
2.22.2.2 Populating the RM Server with Current Radio Configurations..... 230
2.22.2.3 Modification of the Radio Configurations within the RM Server..... 232
2.22.2.4 Delivering the Modified Radio Configurations to the Radios..... 232
2.22.2.5 Delivered Radio Configurations Switchover..... 233
2.23 Voice Operated Transmission..... 234
2.23.1 Voice Operated Transmission Operation..... 234
2.23.2 Voice Operated Transmission Usage.....234
2.23.2.1 Suspending Voice Operated Transmission..... 234
2.23.2.2 Talk Permit Tone 235
2.23.2.3 Emergency Calls..... 235
2.23.2.4 Transmit Interrupt..... 235
2.24 Lone Worker.....235
2.25 Bluetooth Support..... 235
2.25.1 Bluetooth Pairing and Connection.....236
2.25.1.1 Bluetooth Device Pairing with Display Radios.....236
2.25.1.2 Bluetooth Device Pairing with Non-Display Radios.....236
2.25.2 Bluetooth Headset, PTT and Radio Operation.....237
2.25.2.1 Radio Operation with COTS Headsets.....237

2.25.2.2 Radio Operation with Motorola Solutions Headsets with PTT....237
2.25.2.3 Radio Operation with Motorola Solutions PTT Only Devices....237
2.25.3 Bluetooth Barcode Scanner Operation....237
2.25.4 Bluetooth Personal Area Networking Operation....238
2.25.5 Recommended Bluetooth Devices....238
2.25.6 Avoiding Accidental Connection....238
2.26 One Touch Home Revert Button....239
2.27 Password and Lock Feature....239
2.28 Digital Telephone Patch....239
2.28.1 Phone Call Initiation....240
2.28.1.1 Call Initiation by a Radio User....241
2.28.1.2 Call Initiation by a Phone User....241
2.28.2 Access Priority During Phone Calls....243
2.28.3 Ending Phone Calls....244
2.28.4 Digital Telephone Patch System Configuration....244
2.28.4.1 Phone Patch in Single Site and IP Site Connect Local Area Channels....244
2.28.4.2 Phone Patch in IP Site Connect Wide Area Channels....245
2.28.4.3 Phone Patch in Capacity Plus Single Site....247
2.28.5 Wireline Telephony....247
2.29 Voice Announcement Feature....248
2.30 Wi-Fi Support....249
2.30.1 Wi-Fi Network Name....249
2.30.2 Wi-Fi Security Support....250
2.30.3 Wi-Fi Default Profile....250
2.30.4 Wi-Fi Channel Usage....251
2.30.5 Wi-Fi Network Settings....251
2.30.6 Wi-Fi Network Protocols....251
2.30.7 Wi-Fi Features....251
2.30.7.1 Radio Management in Wi-Fi....251
2.31 Enterprise Wi-Fi Roaming Enhancement....252
2.31.1 Configuring Enterprise Wi-Fi Roaming Enhancement in RM....252
2.32 Certificate Management....253
2.32.1 Certificate Management Feature Overview....253
2.32.2 Certificate Enrollment....253
2.32.3 Certificate Renewal and Rollover....254
2.32.4 Design Considerations....254
2.33 Radio Transmit Inhibit....255
2.34 Radio Response Inhibit....255
2.35 Analog Features....255

2.35.1 Analog Voice Features....256
2.35.2 MDC Analog Signaling Features....256
2.35.3 Quik-Call II Signaling Features....257
2.35.4 Analog Scan Features....257
2.35.5 Analog Repeater Interface....258
2.35.5.1 Analog Repeater Interface Settings....258
2.35.5.2 Configuration Summary Table....263
2.35.5.3 Configuration Considerations....264
2.35.6 Auto-Range Transponder System....273
2.35.7 TX Inhibit Quick Key Override....274
2.35.8 Alert Tone Fixed Volume....274
2.35.9 Alert Tone Auto Reset....275
2.35.10 Emergency Permanent Sticky Revert....275
2.36 Software Update Management....275
2.36.1 Activating SUM License....276
2.37 Repeater Webserver Functions....277
2.37.1 Accessing the Webpage of the Repeater....277
2.37.2 Repeater Alarms....278
2.37.3 RDS Logs....278
2.37.3.1 Downloading SLR Repeater Logs....279
2.37.3.2 Enabling Repeater Logs....280
2.37.4 Control Commands....280
2.37.5 Configuration....280
2.37.6 Resetting Login Credentials/Certificate....280
2.38 MOTOTRBO 2-4-1 Feature Overview....281
2.38.1 MOTOTRBO 2-4-1 Benefits....281
2.38.2 Regulatory Requirements....282
2.38.2.1 Application Process....282
2.38.2.2 Sample Attachment to MOTOTRBO 2-4-1 License Application....282
2.38.2.3 FCC Coordinators....283
2.38.3 MOTOTRBO 2-4-1 Site Configurations....284
2.38.3.1 One Transmit Antenna Site Configuration....284
2.38.3.2 Two Transmit Antenna Site Configuration....285
2.38.4 MOTOTRBO 2-4-1 System Configurations....285
2.38.4.1 Impact to MOTOTRBO System and Network Management....285
2.38.4.2 Recommendation when Using 2-4-1 for Control Channel....285
2.38.4.3 MOTOTRBO System Retrofit with 2-4-1 Channels....285
2.38.5 RF Coverage and Near-Far Interference....286
2.38.5.1 Baseline RF Coverage....286

2.38.5.2 RF Channel Coverage Balance....287
2.38.5.3 Near-Far Interference....287
2.38.5.4 Tools and Techniques Determining the Magnitude of Near-Far Interference....288
2.38.6 Near-Far Interference Mitigation Techniques....288
2.38.6.1 Utilization of the Narrow Filter Option....288
2.38.6.2 Multi-Site Implementation – Voting and Simulcast....288
2.38.6.3 Single Site Implementations....289
2.38.7 MOTOTRBO 2-4-1 Deployment....290
2.38.7.1 Deployment – New Systems....290
2.38.7.2 Deployment – 2-4-1 Retrofit Systems....291
2.38.7.3 Deployment – Transmit Power Verification and Balancing Channels....291
2.39 Radio Features....291
2.39.1 Configuring Channel Lock Feature....291
2.39.2 Configuring Wi-Fi Roaming Feature....292
2.39.3 Configuring Wi-Fi Certificate Feature....292
2.40 Fall Alert....292
2.40.1 Configuring Fall Alert in RM....293
2.41 Inband Data Services....293
2.41.1 Configuring Caller Alias in Radio Management....294
2.42 Data Security Between the RM and the Devices....294
2.42.1 Key Management....295
2.42.2 Adding the Pre-shared Key to the Radio Management....295
2.42.3 Securing Devices....295
2.43 Performing Repeater Factory Reset....296
Chapter 3: System Components and Topologies....297
3.1 System Components....297
3.1.1 Fixed End Components....297
3.1.1.1 Repeater....297
3.1.1.2 MTR3000 Base Station/Repeater....299
3.1.1.3 MTR3000 Satellite Receiver....303
3.1.1.4 SLR 1000 Series Repeater....305
3.1.1.5 SLR 5000 Series Repeater....307
3.1.1.6 SLR 8000 Series Repeater....310
3.1.1.7 Satellite Receiver and Voting Repeater....314
3.1.1.8 Radio Control Station....314
3.1.1.9 MOTOTRBO Network Interface Service....315
3.1.1.10 MC1000, MC2000, MC2500 Console....316
3.1.2 Mobile Components....317
3.1.2.1 MOTOTRBO Portable....318

3.1.2.2 MOTOTRBO Mobile....323
3.1.2.3 MOTOTRBO Device Discovery and Mobility Service....327
3.2 System Topologies....328
3.2.1 Direct Mode/Dual Capacity Direct Mode (DCDM)....328
3.2.1.1 Digital MOTOTRBO Radios in DCDM....329
3.2.1.2 Interoperability between Analog MOTOTRBO Radios and Analog Radios in Direct Mode....337
3.2.1.3 Interoperability Between Digital MOTOTRBO Radios, Mixed Mode MOTOTRBO Radios, and Analog Radios in Direct Mode....338
3.2.1.4 Direct Mode Spectrum Efficiency....339
3.2.2 Dual Capacity Direct Mode....340
3.2.2.1 Timeslot Synchronization....340
3.2.2.2 Channel Timing Leader Preference....340
3.2.2.3 Color Code....341
3.2.2.4 Channel Access Rule....341
3.2.2.5 Scan....341
3.2.2.6 Interoperability and Backward Compatibility....341
3.2.2.7 Revert Features....341
3.2.3 Extended Range Direct Mode....342
3.2.3.1 Extended Range Direct Mode Feature Licensing....344
3.2.3.2 Repeater Emission Designator....344
3.2.3.3 Configuration in Repeater....344
3.2.3.4 Configuration in Radio....344
3.2.3.5 System Configuration Considerations....344
3.2.3.6 Repeater TX/RX Isolation....345
3.2.4 Repeater Mode....345
3.2.4.1 Digital MOTOTRBO Radios in Repeater Mode....346
3.2.4.2 Analog MOTOTRBO Radios in Repeater Mode....359
3.2.5 IP Site Connect Mode....361
3.2.5.1 Topologies of the IP Site Connect System....362
3.2.5.2 Network Topologies for IP Site Connect....366
3.2.5.3 Summary of Features in IP Site Connect Mode....370
3.2.6 Capacity Plus Single Site Mode....371
3.2.6.1 Topologies of Capacity Plus Single Site System....372
3.2.7 Capacity Plus Multi Site Mode....380
3.2.7.1 Topologies of Capacity Plus Multi Site System....381
3.2.7.2 Summary of Features in Capacity Plus Single Site and Capacity Plus Multi Site Modes....385
3.2.7.3 Repeater Network Configuration Options in Capacity Plus Single Site and Capacity Plus Multi Site....386

3.2.8 Digital Voting 388
3.2.8.1 Digital Voting in Digital Conventional Single Site/Local Channels 389
3.2.8.2 Digital Voting in IP Site Connect (Wide Area Channels) 390
3.2.8.3 Digital Voting in Capacity Plus Single Site 392
3.2.8.4 Digital Voting in Capacity Plus Multi Site 393
Chapter 4: System Design Considerations 395
4.1 Overview 395
4.2 Analog-to-Digital Migration Plans 396
4.2.1 Pre-Deployment System Integration 396
4.2.2 Preparation and Migration of Analog to Digital 396
4.2.3 New/Full System Replacement 397
4.3 New Frequency Licensing (Region Specific) 397
4.4 Converting Existing 12.5/25 kHz Licenses 398
4.5 Repeater Continuous Wave Identification (CWID) 399
4.6 Repeater Narrow IF Filter 399
4.7 Digital Repeater Loading 399
4.7.1 Assumptions and Precautions for Digital Repeater Loading 400
4.7.2 Voice and Data Traffic Profile 400
4.7.3 Estimate Loading (for Single Repeater and IP Site Connect) 401
4.7.4 Estimate Loading (for Capacity Plus Single Site) 402
4.7.5 Estimate Loading (for Capacity Plus Multi Site) 405
4.7.6 Estimate Loading (for MOTOTRBO Link) 406
4.7.7 Load Optimization (for Single Repeater and IP Site Connect) 408
4.7.7.1 Distribution of High Usage Users 408
4.7.7.2 Minimize Location Periodic Update Rate 409
4.7.7.3 Data Application Retry Attempts and Intervals 410
4.7.7.4 Optimize Data Application Outbound Message Rate 411
4.7.7.5 GPS Revert and Loading 411
4.7.7.6 Enhanced GPS Revert – Loading and Reliability 414
4.7.8 Load Optimization (for Capacity Plus Single Site and Capacity Plus Multi Site) 418
4.7.8.1 Preference for Using a Frequency 418
4.7.8.2 Improving Channel Capacity by Adjusting Hang Times 419
4.7.8.3 Call Priority 419
4.7.8.4 Call Initiation 420
4.8 Multiple Digital Repeaters in Standalone Mode 420
4.8.1 Overlapping Coverage Area 420
4.8.2 Color Codes in a Digital System 421
4.8.3 Additional Considerations for Color Codes 422
4.9 Multiple Digital Repeaters in IP Site Connect Mode 423

4.9.1 System Capacity in IP Site Connect Mode..... 423
4.9.2 Frequencies and Color Code Considerations..... 424
4.9.3 Considerations for the Back-End Network in IP Site Connect Mode.....424
4.9.3.1 Automatic Reconfiguration..... 426
4.9.3.2 Back-End Network Design in IP Site Connect Mode.....427
4.9.4 Flow of Voice/Data/Control Messages..... 432
4.9.5 Security Considerations..... 433
4.9.6 General Considerations When Setting Up the Network Connection for an IP Site Connect System.....434
4.9.7 Considerations for Shared Use of a Channel.....435
4.9.8 Migration from Single Site Systems..... 436
4.9.9 Migration from an Older IP Site Connect System..... 437
4.10 Multiple Digital Repeaters in Capacity Plus Single Site..... 437
4.10.1 System Capacity in Capacity Plus Single Site..... 437
4.10.2 Frequencies and Color Code Considerations..... 438
4.10.3 Considerations for the Back-End Network in Capacity Plus Single Site..... 438
4.10.4 Behaviors in Presence of Failures..... 439
4.10.5 Adaptive Rest Channel Rotation (ARCR)..... 440
4.10.6 Limiting Interference to Other Systems.....441
4.10.7 Plan for Talkaround Mode..... 441
4.10.8 Ways to Improve Battery Life..... 442
4.10.9 MOTOTRBO Telemetry Connection Details.....442
4.10.10 Considerations for Configuring Combined Firmware Versions..... 442
4.10.11 Upgrading from Capacity Plus Single Site.....442
4.11 Multiple Digital Repeaters in Capacity Plus Multi Site.....443
4.11.1 System Capacity in Capacity Plus Multi Site.....443
4.11.2 Considerations for Frequencies, Color Code, and Interference.....444
4.11.3 Considerations for the Back-End Network in Capacity Plus Multi Site.....445
4.11.3.1 Back-End Network Topologies in Capacity Plus Multi Site..... 447
4.11.3.2 Back-End Network Characteristics in Capacity Plus Multi Site.....447
4.11.3.3 Back-End Network Bandwidth Considerations..... 448
4.11.4 Behaviors in Presence of Failures.....449
4.11.4.1 Failure of the Master.....449
4.11.4.2 Failure of a Site.....450
4.11.4.3 Failure of a Repeater.....450
4.11.4.4 Failure of the LAN Switch..... 450
4.11.4.5 Failure of the Back-End Network or Router.....451
4.11.4.6 Failure of a Revert Repeater..... 451

4.11.5 Automatic Reconfiguration..... 451
4.11.6 Security Considerations.....451
4.11.7 Migration.....452
4.11.7.1 Migrating from IP Site Connect.....452
4.11.7.2 Migrating from Capacity Plus Single Site.....453
4.11.8 Upgrade from Capacity Plus Multi Site.....453
4.12 Digital Voting.....454
4.12.1 Repeater to Receiver Configuration.....454
4.12.2 Enable/Disable Digital Voting.....454
4.12.3 Digital Voting Status.....455
4.12.4 Digital Voting Controls/Configurations.....456
4.13 Digital Telephone Patch (DTP).....457
4.13.1 Enable/Disable Phone Gateway Repeater for Phone Calls.....457
4.13.1.1 Conventional Single Site.....458
4.13.2 Enable/Disable a Radio from Initiating/Receiving Phone Calls.....458
4.13.3 Enable/Disable Pre-Configured Target ID.....459
4.13.4 Phone Channel Configuration.....459
4.13.4.1 One APP Box per Repeater Through 4-wire Interface.....459
4.13.4.2 Single Site.....459
4.13.4.3 IP Site Connect.....460
4.13.4.4 Capacity Plus Single Site.....460
4.13.4.5 Capacity Plus Multi Site.....460
4.13.5 APP Box Configuration.....461
4.13.6 Phone System Configuration.....461
4.13.6.1 Radio Configuration in a Phone System.....462
4.13.6.2 Repeater Configuration in a Phone System.....463
4.13.7 Access/De-access Code Configuration.....463
4.13.7.1 Repeater Configuration.....463
4.13.7.2 Radio Configuration.....464
4.13.8 Dual Tone Multi Frequency (DTMF) Configuration.....464
4.13.9 Ringing Modes.....465
4.13.10 Enable/Disable Manual Dial.....465
4.13.11 Connection of APP Boxes to the Repeater in Capacity Plus Single Site and Capacity Plus Multi Site.....465
4.13.12 PBX Routing Configuration in Capacity Plus Single Site.....465
4.14 Transmit Interrupt System Design Considerations.....466
4.14.1 Interruptible Radios.....466
4.14.2 Voice Interrupt.....466
4.14.3 Emergency Voice Interrupt.....467

4.14.4 Data Over Voice Interrupt....468
4.14.5 Remote Voice Dekey....468
4.15 Restricted Access to System (RAS) Design Considerations....469
4.15.1 RAS Key Authentication....469
4.15.2 Radio ID Range Check....471
4.16 Data Sub-System Design Considerations....471
4.16.1 Computer and IP Network Configurations....471
4.16.1.1 Radio to Mobile Client Network Connectivity....472
4.16.1.2 Radio to Air Interface Network Connectivity....473
4.16.1.3 Application Server to Control Station Network Connectivity....475
4.16.1.4 Control Station Considerations....477
4.16.1.5 Required Static Routes....479
4.16.1.6 Application Server and Dispatcher Network Connectivity....479
4.16.1.7 MOTOTRBO Subject Line Usage....479
4.16.1.8 MOTOTRBO Example System IP Plan....481
4.16.1.9 Application Server Network Connection Considerations....481
4.16.1.10 Reduction in Data Messages (When Radios Power On)....482
4.16.1.11 Optimizing for Data Reliability....483
4.16.1.12 Optimizing for Data Throughput....484
4.16.1.13 Data Revert Channels for Capacity Plus Single Site and Capacity Plus Multi Site....486
4.16.2 Data Application Licensing Considerations....488
4.16.3 Mobile Terminal and Application Server Power Management Considerations....489
4.16.4 MOTOTRBO Telemetry Connection Details....489
4.16.5 MOTOTRBO Network Interface Service (MNIS) and Device Discovery and Mobility Service (DDMS)....489
4.16.5.1 MNIS and DDMS Operation Overview....490
4.16.5.2 System Topology with the MNIS....493
4.16.5.3 Data Applications and MNIS Deployments....499
4.16.5.4 Mobility Management and Individual Data Transmission....501
4.16.5.5 Group Messages....502
4.16.5.6 Data Privacy....503
4.16.5.7 Considerations for Advanced MNIS Configurations....504
4.16.5.8 DDMS Usage by MNIS....505
4.16.5.9 Control Station Migration to MNIS....505
4.16.5.10 Considerations for the IP Network....506
4.16.5.11 MNIS Data Gateway and DDMS Computer Specifications....508
4.17 CSBK Data System Design Considerations....509
4.18 GPIO Triggered Event Driven and Distance Driven Location Update System Design Considerations....510

4.19 Customer Fleetmap Development..... 510
4.19.1 Identify a Functional Fleetmap Design Team 511
4.19.2 Radio Users Identification.....511
4.19.3 Radio Users Organized into Groups..... 512
4.19.3.1 Configuring Groups..... 513
4.19.4 IDs and Aliases Assignments.....514
4.19.4.1 Radio ID Identification..... 514
4.19.4.2 Radio Alias Assignments.....515
4.19.4.3 Group ID Identifications.....516
4.19.4.4 Group Alias Assignments..... 516
4.19.5 Determine Which Channel Operates in Repeater Mode or Direct Mode/Dual Capacity Direct Mode.....517
4.19.6 Supervisor Radios Feature..... 517
4.19.7 Configuring the Private Calls Feature..... 517
4.19.8 Configuring the All Call Feature..... 518
4.19.9 Radio Disable Feature..... 519
4.19.10 Remote Monitor Feature..... 519
4.19.11 Radio Check Feature.....519
4.19.12 Call Alert Feature..... 519
4.19.13 RX Only Feature..... 519
4.19.14 Remote Voice Dekey Feature..... 520
4.19.15 Emergency Handling Configuration..... 520
4.19.15.1 Emergency Handling User Roles..... 520
4.19.15.2 Emergency Handling Strategies.....521
4.19.15.3 Acknowledgement of Supervisors in Emergency..... 523
4.19.15.4 Extended Emergency Call Hang Time..... 523
4.19.15.5 Emergency Revert and GPS/Data Revert Considerations.....523
4.19.16 Channel Access Configuration.....527
4.19.17 Zones and Channel Knob Programming.....528
4.20 Base Station Identifications (BSI) Setting Considerations..... 528
4.21 GPS Revert Considerations (For Single Repeater and IP Site Connect only).....529
4.22 Enhanced GPS Revert Considerations.....530
4.22.1 Single Site Mode..... 531
4.22.2 Capacity Plus Single Site and Capacity Plus Multi Site Modes..... 532
4.22.3 IP Site Connect Mode..... 532
4.22.3.1 Other Considerations..... 533
4.23 Enhanced Channel Access Consideration.....533
4.23.1 Enhanced Channel Access Advantages..... 533
4.23.2 Enhanced Channel Access Limitations.....534

4.24 Failure Preparedness – Direct Mode Fallback (Talkaround)....535
4.25 Failure Preparedness – Uninterrupted Power Supplies (Battery Backup)....535
4.26 Dynamic Mixed Mode System Design Considerations....536
4.26.1 Configuring Considerations for a Dynamic Mixed Mode System....536
4.26.2 Distribution Considerations in a Dynamic Mixed Mode System....538
4.27 Advanced Over-The-Air Radio Programming Configurations....538
4.27.1 MOTOTRBO Network Interface Service (MNIS) Configuration....539
4.27.2 Control Station Configuration....539
4.27.3 Conventional Configurations....540
4.27.3.1 RF Isolated Single Site Repeaters....542
4.27.3.2 Local Channel Support on IP Site Connect....544
4.27.3.3 Dynamic Mixed Mode (DMM)....545
4.27.4 Capacity Plus Single Site Trunking Configurations....546
4.27.4.1 Trunked Control Station Without Presence....546
4.27.4.2 Trunked Control Station with Presence....547
4.27.4.3 Control Stations with Presence and No Data Revert Repeaters....548
4.27.4.4 Control Stations with Presence and Data Revert Repeaters....549
4.27.4.5 MNIS without Presence (DDMS)....549
4.27.4.6 MNIS with Presence and No Data Revert....550
4.27.4.7 MNIS with Presence (DDMS) and Data Revert....551
4.27.5 Capacity Plus Multi Site Trunking Configurations....551
4.27.6 Coexistence with Third-Party Data Applications....553
4.27.6.1 RM and Third-Party Data Application with Control Stations....553
4.27.6.2 RM with MNIS and Third-Party Data Application with Control Stations....554
4.27.6.3 RM and Third-Party Data Application with MNIS....554
4.27.6.4 Passive Presence and ARS Monitor ID Configuration....555
4.28 Over-The-Air Authentication Key Management....557
4.29 Over-The-Air Privacy Key Management....558
4.29.1 Updating the Privacy Keys in the System....558
4.30 Performance of Over-The-Air Programming....559
4.30.1 Time to Complete Over-the-Air Operations....559
4.30.1.1 Size of the Configuration Update....559
4.30.1.2 Number of Radios Being Processed....560
4.30.1.3 System Loading and RF Environment....561
4.30.2 Performance Impact on Other Services....563
4.30.2.1 Voice Access Time During an Over-The-Air Operation....563
4.30.2.2 Voice Downtime During a Switchover....564
4.30.2.3 Data Downtime During a Switchover....565
4.31 Radio Management Computer Specifications....565

4.32 Configurable Timers....566
4.33 MOTOTRBO Link Mode....571
4.33.1 System Capacity in MOTOTRBO Link Mode....571
4.33.2 Frequency Considerations in MOTOTRBO Link Mode....571
4.33.3 Delay in MOTOTRBO Link Mode....572
4.33.4 Repeater Role in a Dedicated Link Backhaul System Configuration....572
4.33.5 GPIO Pin Configurations....574
4.33.6 Repeater Diagnostics and Control Feature Considerations....574
4.33.7 Restricted Access to System Feature Considerations....575
4.33.8 Network Application Interface Wireline Interface Feature Considerations....575
4.33.9 Continuous Wave Identification Considerations....576
4.33.10 Failure of the Terminating Site....576
4.33.11 Failure of the Interim or Origin Site....576
4.33.12 Failure of a LAN Switch....576
4.33.13 Failure of a MOTOTRBO Link Repeater....577
4.34 Broadcast Calls....577
4.34.1 Configuring Broadcast Calls....578
4.35 Unaddressed Calls....578
4.35.1 Configuring Unaddressed Calls....578
4.36 Open Voice Channel Mode Calls....579
4.36.1 Configuring Open Voice Channel Mode Calls in TX Mode....580
4.36.2 Configuring Open Voice Channel Mode Calls in RX Mode....580
Chapter 5: Capacity Plus Network Configurations....582
5.1 Juniper Infrastructure....582
5.1.1 Recommended Network Equipment (Juniper)....582
5.1.2 IP Plan for Capacity Plus Single Site and Capacity Plus Multisite Systems....583
5.1.2.1 CPSS and CPMS Systems LAN Networks....584
5.1.2.2 CPSS and CPMS Systems Site IDs....584
5.1.2.3 CPSS and CPMS Systems IP Plan Summary....585
5.1.2.4 Capacity Plus Single Site Detailed IP Plan....585
5.1.2.5 Capacity Plus Multi Site Detailed IP Plan....588
5.1.3 Network Topologies....593
5.1.3.1 Capacity Plus Single Site Topology....594
5.1.3.2 Capacity Plus Multi Site Topologies....594
5.1.4 Types of Configuration Templates....595
5.1.4.1 Site Router Configurations....595
5.1.4.2 Site Switch Configurations....595
5.1.4.3 Add-On Configuration Files....595
5.1.5 SRX Router Configuration Overview....596

5.1.5.1 Management Rules for the Juniper Devices..... 596
5.1.5.2 System Module (Router)..... 597
5.1.5.3 Security Module.....599
5.1.5.4 Interfaces Module (Router).....606
5.1.5.5 SNMP Module (Router)..... 610
5.1.5.6 Routing-Options and Protocols Modules..... 611
5.1.5.7 Firewall Module..... 612
5.1.5.8 Access Module..... 613
5.1.6 SRX Chassis Cluster Configuration Overview..... 614
5.1.7 EX Switch Configuration Overview..... 615
5.1.7.1 System Module (Switch).....616
5.1.7.2 Interfaces Module (Switch).....618
5.1.7.3 SNMP Module (Switch)..... 619
5.1.7.4 Forwarding Options Module..... 619
5.1.7.5 Switch Options Module.....619
5.1.7.6 Routing Options Module.....620
5.1.7.7 Protocols Module.....620
5.1.7.8 VLANs Module..... 621
5.1.7.9 Juniper EX2300 Switch Port Assignments..... 622
5.1.8 Capacity Plus Single Site Topology Configuration Overview..... 624
5.1.8.1 Capacity Plus Single Site Configuration Templates..... 625
5.1.8.2 Adaptation of the SRX Configuration Templates for Capacity Plus Single Site..625
5.1.9 Capacity Plus Multi Site Configuration Topologies.....626
5.1.9.1 No Tunnels Topology Configuration Overview..... 626
5.1.9.2 Hub-to-Spoke Topology Configuration Overview..... 629
5.1.9.3 Auto VPN Topology Configuration Overview.....637
5.1.9.4 NAT Topology Configuration Overview.....643

Chapter 6: Capacity Plus Single Site and Multi Site Procedures and Maintenance.. 650

6.1 Procedures for Juniper Infrastructure..... 650
6.1.1 Loading Basic Configuration with Device Console Port..... 650
6.1.1.1 Configuration of Juniper EX Switch to Allow IP Network Communication.....651
6.1.1.2 Configuration of Juniper SRX Router to Allow IP Network Communication.....652
6.1.2 Transferring Files to and from Juniper Devices Using SCP Protocol.....653
6.1.3 Transferring Files to and from Juniper Devices with the USB Stick..... 654
6.1.4 Loading the Configuration from a File to the Juniper SRX Router and EX Switch.....655
6.1.5 Upgrading Juniper OS on the EX2300 Switch..... 656
6.1.6 Upgrading Juniper OS on the SRX3xx Router.....657
6.1.7 Preparing SRX345 to Deploy Chassis Cluster.....659
6.1.8 Loading Configuration from a File on SRX Series Chassis Cluster..... 660

6.1.9 Upgrading Juniper OS on SRX Series Chassis Cluster....661
6.1.10 Creating and Modifying Credentials on Juniper EX Switch and SRX Router....663
6.1.11 Modifying SNMP Configuration on Juniper EX Switch and SRX Router....664
6.1.12 Clearing Persistent MAC Addresses Table on Juniper EX Switch....664
6.1.13 Changing the WAN IP Address (Juniper)....665
6.1.14 Saving the Rescue Configuration on Juniper Devices....666
6.1.15 Adjusting WinSCP Configuration for Juniper Devices....666
6.1.16 Generating Certificates for Juniper SRX Devices....667
6.1.17 Reserving IP Address on DHCP Server in SRX3xx Router....674
6.1.18 Enabling the Port Mirroring on Juniper EX Switch....675
6.2 Maintenance and Troubleshooting for Juniper Infrastructure....677
Chapter 7: Sales and Service Support Tools....678
7.1 Purpose of This Section Testing....678
7.2 Applications Overview....678
7.3 Service Equipment....678
7.4 Documentation....680
7.4.1 MOTOTRBO Documentation....680
7.4.2 URL....681
Appendix A: Control Station Installation....682
A.1 Control Stations Configuration Options....682
A.2 Data Bearer Service....682
A.2.1 Unconfirmed Data....683
A.2.2 Confirmed Data....683
A.3 Interference....684
A.3.1 Intermodulation....684
A.3.2 Desense (Blocking)....684
A.4 Control Station Installation Considerations....684
A.4.1 Unconfirmed Data Considerations....685
A.4.2 Confirmed Data Considerations....687
A.4.3 Antenna Separation....688

List of Figures

Figure 1: MOTOTRBO System....45
Figure 2: MOTOTRBO Digital Radio Technology....47
Figure 3: Comparison between Today's Analog and MOTOTRBO....50
Figure 4: Analog 2-Channel System....51
Figure 5: MOTOTRBO 2-Channel System....51
Figure 6: MOTOTRBO 2-Slot TDMA....52
Figure 7: Comparison of Audio Quality versus Signal Strength for Analog and Digital....54
Figure 8: Differences in Analog Coverage....55
Figure 9: Transmit Audio Sensitivity....57
Figure 10: MOTOTRBO Link System: Example 1....67
Figure 11: MOTOTRBO Link System: Example 2....75
Figure 12: MOTOTRBO Link System: Example 3....82
Figure 13: Digital Emergency Flowchart....99
Figure 14: Text Messaging Services....111
Figure 15: Location Services....115
Figure 16: Windowed Data Structure for a Window Size of Six....119
Figure 17: Subscriber Scheduling in a Window Map with 30 Seconds Data Frame....121
Figure 18: Subscriber Scheduling in a Window Map with 7.5-Second Data Frame....122
Figure 19: Indoor Location Operation....136
Figure 20: Beacon Interval of 151ms and Radio Normal Scan Mode Detection Alignment....139
Figure 21: Beacon Interval of 181ms and Radio WiFi Coexistence Mode Detection Alignment....140
Figure 22: Beacon RF Site Survey....142
Figure 23: GPS Revert Channel Location Windows Data Structure for a Window Size of Six....148
Figure 24: Number of Analog Scan List Members....158
Figure 25: Misdirected Response While Scanning....160
Figure 26: Misdirected Response While Scanning....161
Figure 27: Example of Neighboring Sites....164
Figure 28: Roaming Triggered by Roaming RSSI Threshold Value....169
Figure 29: Dense Overlapping Coverage (Urban)....171
Figure 30: Isolated No Overlapping Coverage (Rural)....171
Figure 31: Corridor Coverage....172
Figure 32: Multi-Floor Coverage....173
Figure 33: Two Wide-Area Systems (Each with Two Wide-Area Channels)....175
Figure 34: Local Connection Using GPIO Lines....196
Figure 35: Redundant Repeater Setup....198
Figure 36: Battery Fleet Management Application (BFM) set up....204

Figure 37: BMA Deployment in Single Site with MNIS..... 207
Figure 38: BMA Deployment in IP Site Connect with MNIS..... 208
Figure 39: BMA Deployment in Capacity Plus Single Site with MNIS..... 209
Figure 40: BMA Deployment in Capacity Plus Multi Site with MNIS.....210
Figure 41: BMA Deployment in Single Channel Direct Mode with Control Stations..... 211
Figure 42: BMA Deployment in Multi-Channel Direct Mode with Control Stations..... 211
Figure 43: BMA Deployment in Single Site with Control Stations.....212
Figure 44: BMA Deployment in IP Site Connect with Control Stations.....212
Figure 45: BMA Deployment in Capacity Plus with a Control Station.....213
Figure 46: BMA Deployment in Capacity Plus Multi Site with a Control Station.....213
Figure 47: Simplified BMA Deployment Diagram..... 214
Figure 48: BMA Deployment with Client, Server and Proxy on the Same PC.....214
Figure 49: BMA Deployment with Client Remote from Server and Proxy..... 215
Figure 50: BMA Deployment with Client Remote from Multiple Server and Proxies..... 216
Figure 51: BMA Deployment with Multiple Proxies Remote from Server..... 217
Figure 52: Single Channel Non-Remote RM Configuration Through Control Station.....221
Figure 53: Single Channel Non-Remote RM Application Configuration Through MNIS.....221
Figure 54: Single Channel Non-Remote RM Application with Presence and Control Station..... 222
Figure 55: Single Channel Non-Remote RM Application with Presence and MNIS.....222
Figure 56: Single Channel Non-Remote RM Application with Presence 223
Figure 57: Remote RM Client from RM Server with Control Station.....223
Figure 58: Remote RM Client from RM Server with MNIS..... 223
Figure 59: Remote RM Client with Multiple RM Servers with Control Station..... 224
Figure 60: Remote RM Client with Multiple RM Servers with MNIS.....225
Figure 61: RM Server with Remote Device Programmers and Control Stations.....226
Figure 62: RM Server with Remote RM Device Programmers and MNIS.....227
Figure 63: Multi-Channel Non-Remote RM Application Configuration with Control Stations..... 227
Figure 64: Multi-Channel Non-Remote RM Application Configuration with MNIS.....228
Figure 65: Phone Patch Topology in Single Site Configuration..... 245
Figure 66: Phone Patch Topology in IP Site Connect Local Area Channel Configuration.....245
Figure 67: One APP Box Supporting Two Wide Area Channels in IP Site Connect.....246
Figure 68: Two APP Boxes Supporting Two Wide Area Channels in IP Site Connect.....246
Figure 69: APP Boxes Supporting Wide Area Channels and Local Area Channels in IP Site Connect.....246
Figure 70: Phone Patch Topology in a Capacity Plus Single Site Configuration..... 247
Figure 71: Wireline Telephony with Third-party Telephony Application..... 248
Figure 72: Certificate Enrollment..... 254
Figure 73: Certificate Renewal and Rollover..... 254
Figure 74: DR 3000 Cable Schematic for Zetron Controllers..... 265
Figure 75: Hardware Connections between SLR 5000/SLR 8000 and M827/M807 Controller.....268

Figure 76: CPS Configuration for M827/M807 Controller (1 of 2)....269
Figure 77: CPS Configuration for M827/M807 Controller (2 of 2)....270
Figure 78: Hardware Connections between SLR 5000/SLR 8000 and TSCC03 Channel Controller....271
Figure 79: CPS Configuration for TSCC03 Channel Controller (1 of 2)....272
Figure 80: CPS Configuration for TSCC03 Channel Controller (2 of 2)....273
Figure 81: RDS Log for SLR Repeaters....279
Figure 82: RF Site Configurations for MOTOTRBO 2-4-1 Channels....284
Figure 83: Coverage Area Depends on the Strength of an Interfering Signal....287
Figure 84: Satellite Receiver Connections Within a Voting System....304
Figure 85: SLR 1000 Series Repeater....305
Figure 86: SLR 5000 Series Repeater....308
Figure 87: SLR 8000 Series Repeater....311
Figure 88: MOTOTRBO Network Interface Service....315
Figure 89: MOTOTRBO Portable (Display Model)....319
Figure 90: MOTOTRBO Portable (Non-Display Model)....320
Figure 91: MOTOTRBO Mobile Control Head (Full Display Model)....324
Figure 92: MOTOTRBO Mobile Control Head (Numeric Display Model)....324
Figure 93: MOTOTRBO Radios (in digital mode) In Direct Mode/Dual Capacity Direct Mode....329
Figure 94: MOTOTRBO Radios (in digital mode) Text Messaging In Direct Mode/Dual Capacity Direct Mode....330
Figure 95: MOTOTRBO Radios (in digital mode) Text Messaging In Multiple Direct Mode/Dual Capacity Direct Mode....330
Figure 96: Send Telemetry Command from MOTOTRBO Radio to Another MOTOTRBO Radio to Toggle an Output Pin....331
Figure 97: Send Telemetry Message from MOTOTRBO Radio to Another MOTOTRBO Radio when Input Pin State Changes....331
Figure 98: Send Telemetry Command to Toggle an Output Pin from MOTOTRBO Radio to Another MOTOTRBO Radio when Input Pin State Changes....332
Figure 99: MOTOTRBO Radios In Digital Direct Mode/Dual Capacity Direct Mode with Location Server and Local Location Client....333
Figure 100: MOTOTRBO Radios In Digital Direct Mode with Text Message Server, Location Server and Local Dispatchers....333
Figure 101: MOTOTRBO Radios In Digital Direct Mode/Dual Capacity Direct Mode Server Based Configuration with Remote Dispatchers....334
Figure 102: MOTOTRBO Radios in Two Channel Digital Direct Mode Server-Based Configuration with Remote Dispatchers....335
Figure 103: MOTOTRBO Radios in Two Channel Direct Mode GPS Revert Configuration....336
Figure 104: Legacy Analog Radios and MOTOTRBO Radios (in analog mode) in Direct Mode....338
Figure 105: Legacy Analog and MOTOTRBO Analog and Digital Radios in Direct Mode....339
Figure 106: Direct Mode Channels....339
Figure 107: Dual Capacity Direct Mode Channels....339
Figure 108: Time Division Duplex Repeater....342

Figure 109: MOTOTRBO Digital Radios on MOTOTRBO Two-Slot Digital Repeater..... 347
Figure 110: MOTOTRBO Radios in Digital Two-Slot Digital Repeater Mode with Built-In Text Messaging....348
Figure 111: MOTOTRBO Radios in Digital Two-Slot Digital Repeater Mode with Text Messaging..... 349
Figure 112: MOTOTRBO Radios in Digital Two-Slot Digital Repeater Mode with Telemetry Functions.....349
Figure 113: MOTOTRBO Radios in Digital Two-Slot Digital Repeater Mode with a Server-Based Configuration Using Control Stations.....351
Figure 114: MOTOTRBO Radios in Digital Two-Slot Digital Repeater Mode with a Server-Based Configuration Using Control Stations and Remote Dispatchers..... 352
Figure 115: MOTOTRBO Radios in Digital Two-Slot, Digital Repeater Mode with Text Message Server, Location Server Using Control Stations with Local and Remote Dispatchers..... 353
Figure 116: MOTOTRBO Radios in Two-Slot Digital Repeater Mode with GPS Revert Configuration..... 354
Figure 117: Single Site Conventional System with an Enhanced GPS Revert Channel..... 356
Figure 118: IP Site Connect System with an Enhanced GPS Revert Channel.....357
Figure 119: A Capacity Plus Single Site System with an Enhanced GPS Revert Channel..... 358
Figure 120: MOTOTRBO Analog and Legacy Analog Radios on Legacy Analog Repeater..... 359
Figure 121: MOTOTRBO Analog and Legacy Analog Radios on MOTOTRBO Analog Repeater..... 360
Figure 122: MOTOTRBO Digital Radios on a Two-Slot MOTOTRBO Digital Repeater with Analog Legacy Repeater Support.....361
Figure 123: Wide Area System with Centralized Data Application Server..... 363
Figure 124: Wide and Local Area System with Distributed Data Application Servers..... 364
Figure 125: Multiple Wide Area Systems with Centralized Data Application Server 365
Figure 126: IP Site Connect Devices Connected Through LAN..... 367
Figure 127: IP Site Connect Devices connected through a WAN.....368
Figure 128: IP Site Connect Devices connected through LAN and WAN Network.....370
Figure 129: Capacity Plus Single Site Devices with Local RDAC and no Data Application Server.....373
Figure 130: 2-Channel Capacity Plus Single Site System without Data Application Server.....374
Figure 131: Capacity Plus Single Site Devices with Remote RDAC and no Data Application Server.....375
Figure 132: Capacity Plus Single Site Devices with Data over Trunked Channels..... 376
Figure 133: Two-Channel Capacity Plus Single Site Devices with Data over Trunked Channels..... 376
Figure 134: Capacity Plus Single Site Devices with Data over Revert Channels.....378
Figure 135: Capacity Plus Single Site Devices with a Dispatch Console..... 379
Figure 136: Capacity Plus Multi Site System with Data over Trunked Channels.....382
Figure 137: Capacity Plus Multi Site System with Data over Local Revert Channels..... 384
Figure 138: Capacity Plus Multi Site System with Data over Wide Area Revert Channels..... 385
Figure 139: Digital Voting Topology for Conventional Single Site or IP Site Connect Local Channel.....390
Figure 140: Digital Voting Topology for a Two-Site IP Site Connect System..... 391
Figure 141: Digital Voting Topology for a Capacity Plus Single Site System.....393
Figure 142: Digital Voting Topology for a 2-Site Capacity Plus Multi Site System.....394
Figure 143: Number of Users per Slot versus User Experience.....401
Figure 144: Number of Users Versus Number of Channels for Voice-Only Profile.....403

Figure 145: Number of Users Versus Number of Channels for Mixed Profiles....404
Figure 146: Number of Location Updates versus Number of Data Revert Channels....405
Figure 147: Number of Users per Slot Versus User Experience (One Chain, Three Sites)....407
Figure 148: Number of Users per Slot Versus User Experience (Two Chains, Five Sites Each)....407
Figure 149: Number of Users Versus Location Update Period....410
Figure 150: Channel Loading with GPS Revert Channels....412
Figure 151: Minimum Location Update Period versus Number of Subscribers....414
Figure 152: 1-Minute Update Rate with a 10-second Call per Minute at 75% Loading....415
Figure 153: 4-Minute Update Rate with a 10-second Call per Minute at 75% Loading....416
Figure 154: 1-Minute Update Rate with a 20-second Call per Minute at 75% Loading....416
Figure 155: 1-Minute Update Rate with a 20-second Call per Minute at 45% Loading....417
Figure 156: 1-Minute Update Rate with Different Window Sizes, Loading and Call Duration....418
Figure 157: Multiple Repeaters....420
Figure 158: Multiple Repeaters with Overlap....421
Figure 159: Multiple Repeaters with Overlap and Common Frequencies....421
Figure 160: Multiple Digital Repeaters with Unique Color Codes....422
Figure 161: Color Code with Site Congestion....423
Figure 162: Example of Two IP Site Connect Systems with Overlapping Coverage Areas....424
Figure 163: Required Bandwidth for Two Simple IP Site Connect System Configurations....429
Figure 164: Example System for Calculating Bandwidth Requirements without Secure VPN....430
Figure 165: Required Bandwidth Calculations While Utilizing a Secure Virtual Private Network....432
Figure 166: An Example of Interference at Receive Frequency....435
Figure 167: An Example of Interference at Transmit Frequency....436
Figure 168: Connectivity between the Mobile Client and the MOTOTRBO Radio....472
Figure 169: Air Interface Network Connectivity....475
Figure 170: Application Server to Control Station Network Connectivity....477
Figure 171: Example MOTOTRBO System IP Plan....481
Figure 172: The example shows IPv4 addresses in a Capacity Plus Single Site Configuration with Data Revert....488
Figure 173: MNIS and DDMS Interface Overview....491
Figure 174: Location Application with MNIS and DDMS in a Single Site Digital System....493
Figure 175: Multiple Conventional Systems with MNIS....494
Figure 176: Capacity Plus Single Site System with MNIS Deployed in the Same VLAN as the Repeaters....495
Figure 177: Capacity Plus Single Site System with MNIS Deployed in the separate VLAN....496
Figure 178: Capacity Plus Single Site System with MNIS Deployed Remotely....496
Figure 179: Capacity Plus Multi Site System with MNIS....497
Figure 180: Capacity Plus Multi Site System with Two MNIS....498
Figure 181: Capacity Plus Single Site System with MNIS and Control Stations....499
Figure 182: Application and MNIS Deployed on Separate PCs....501

Figure 183: System with Control Stations Used by a Voice Console and Data Applications..... 506
Figure 184: System with a Control Stations Used by a Voice Console and MNIS Used by Data Applications..... 506
Figure 185: Radio Users Organized into Groups.....513
Figure 186: Radio ID Digits.....515
Figure 187: Example of Mismatched Aliasing.....517
Figure 188: Emergency Alarm and GPS Revert Interaction Diagram..... 524
Figure 189: Emergency Alarm and Call and GPS Interaction Diagram.....525
Figure 190: Emergency Alarm with Voice to Follow and GPS Revert Interaction Diagram.....526
Figure 191: Multi-Channel RM Application with Control Stations in Direct Mode.....540
Figure 192: Multi-Channel RM Application with Control Stations in Single Site Repeater Mode..... 540
Figure 193: Multi-Channel RM Application with Control Stations in IP Site Connect Mode..... 540
Figure 194: Multi-Channel RM Application with MNIS in Single Site or IP Site Connect Mode.....541
Figure 195: RM Application with Control Stations Covering RF Isolated Single Site Repeaters.....542
Figure 196: RM Application with Control Stations Covering RF Isolated Single Site Repeaters Using Remote RM Device Programmers.....543
Figure 197: RM Application with MNIS Covering RF Isolated Single Site Repeaters..... 543
Figure 198: RM Application with Control Stations in IP Site Connect Mode Covering Local Channels with Remote RM Device Programmers.....544
Figure 199: RM Application with MNIS in IP Site Connect Mode Covering Local Channels.....545
Figure 200: RM Application in Dynamic Mixed Mode.....546
Figure 201: RM Application in a Capacity Plus Single Site with no DDMS and Trunked Control Station.....547
Figure 202: RM Application in a Capacity Plus Single Site System with a DDMS and Trunked Control Station.....548
Figure 203: RM Application in a Capacity Plus Single Site System with a DDMS, no Data Revert Channels, and Control Stations.....548
Figure 204: RM Application in a Capacity Plus System with a DDMS, Data Revert Channels, and Control Stations.....549
Figure 205: RM Application in a Capacity Plus Single Site System with an MNIS.....550
Figure 206: RM Application in a Capacity Plus System with an MNIS and a DDMS.....550
Figure 207: RM Application in a Capacity Plus Single Site System with an MNIS, a DDMS, and Data Revert Channels.....551
Figure 208: RM Application with Control Stations in a Capacity Plus Multi Site System with Presence (DDMS) and Wide-Area Data Revert Channels..... 552
Figure 209: RM Application with Control Stations in a Capacity Plus Multi Site System with Presence (DDMS) and Local Area Data Revert Channels..... 552
Figure 210: RM Application with MNIS in a Capacity Plus Multi Site System with Presence and Wide or Local Area Data Revert Channels..... 553
Figure 211: RM Application with Control Stations and Passive Presence Configuration with Third-Party Data Application.....556
Figure 212: RM Application with Control Stations and Passive Presence Configuration with Third-Party Data Application on a Capacity Plus Single Site Data Revert Configuration.....556

Figure 213: RM Application with MNIS and Passive Presence Configuration with Third-Party Data Application on a Capacity Plus Single Site Data Revert Configuration..... 557
Figure 214: Time to Deliver a Number of Address Book Entries to One Radio..... 560
Figure 215: Time to Deliver a Typical Change to a Number of Radios..... 561
Figure 216: Time to Deliver a Typical Change to Many Radios in Single Site Mode..... 562
Figure 217: Time to Deliver a Typical Change to Many Radios in Capacity Plus Mode..... 563
Figure 218: Voice Downtime when Switching Over a Number of Radios..... 564
Figure 219: Example of a Dedicated MOTOTRBO Link System with Four Backhaul Sites..... 572
Figure 220: GPIO Pin Configurations..... 574
Figure 221: RDAC Backhaul Status..... 575
Figure 222: Juniper SRX300 Services Gateway Front View..... 582
Figure 223: Juniper SRX300 Services Gateway Rear View..... 582
Figure 224: Juniper SRX345 Services Gateway Front View..... 583
Figure 225: Juniper SRX345 Services Gateway Rear View..... 583
Figure 226: Juniper EX2300-24T Ethernet Switch Front View..... 583
Figure 227: Juniper EX2300-24T Ethernet Switch Rear View..... 583
Figure 228: Juniper SRX345 Chassis Cluster Connection Topology Diagram..... 614
Figure 229: Ports and VLANs Assignment on a Juniper EX 2300 Switch in Repeater Site with a Single Switch..... 623
Figure 230: Ports and VLANs Assignment on a Juniper EX 2300 Switch in Repeater Site with a Double Switch..... 624
Figure 231: Hub-to-Spoke VPN Overlay Tunnel Network..... 630
Figure 232: AVPN Overlay Tunnel Network Diagram..... 640
Figure 233: Start Shell Setting in Advanced Options..... 667
Figure 234: Host Network Manager..... 667
Figure 235: Appliance Settings Window Visible During Import..... 670
Figure 236: Linux Host IP Address..... 671
Figure 237: Installation of Control Stations for Unconfirmed Data..... 686
Figure 238: Installation of Control Stations for Confirmed Data..... 687
Figure 239: Horizontal Separation Isolation..... 688
Figure 240: Vertical Separation Isolation..... 689

List of Tables

Table 1: System Feature Overview....47
Table 2: Frequency Pairs....67
Table 3: Frequency Pairs....75
Table 4: Advantage Transmit Interrupt Features....89
Table 5: RAS Configuration....104
Table 6: Software Confirmed and Unconfirmed Mode....110
Table 7: Input Methods Supported in Full Keypad....113
Table 8: Performance Specification Accuracy....115
Table 9: GPS Signal Icon....116
Table 10: Service Methods....117
Table 11: Interaction between Parameters to Dictate Radio Performance....118
Table 12: Number of Windows in a 30-Second Data Frame....120
Table 13: Window Size versus Number of Windows....120
Table 14: Calculation for the Window Size with Enhanced Privacy Enabled....123
Table 15: Wait Time Before De-Allocation of Windows....123
Table 16: The System Throughput....125
Table 17: Total Number of Radios Sending ARS based on ARS Initial Delay Value....127
Table 18: Number of Radios Sending ARS Based on ARS Initial Delay Value....128
Table 19: Number of Radios Sending ARS Based on ARS Initial Delay Value....128
Table 20: Use of Precedence Designator....132
Table 21: Examples of Timing Configurations....138
Table 22: Scan Interval On Time....141
Table 23: Same Beacon Set Between Cycle Buffering Scheme....141
Table 24: Different Beacon Set Between Cycle Buffering Scheme....141
Table 25: Radio GPS Revert Channel Location Services Configuration Parameters....147
Table 26: GPS Revert Channel Location Number of Windows in a 3-Second Data Frame....148
Table 27: Outdoor Location GPS Revert Channel Data Size....149
Table 28: Indoor Location GPS Revert Channel Element Data Size for One Beacon....150
Table 29: GPS Revert Channel Wait Time Before De-allocation....150
Table 30: GPS Revert Channel System Throughput....151
Table 31: Report Channel Time Slot....153
Table 32: Number of Priority Members....158
Table 33: Voice Pretime Duration Recommendation....162
Table 34: Neighboring Sites List....164
Table 35: Basic Site Configurations....169
Table 36: Basic Site Configuration Setting....173

Table 37: Two Site Configuration in CPS....175
Table 38: Roam List Configuration....176
Table 39: Recommended Beacon Duration and Beacon Interval....178
Table 40: Roaming Interaction Summary....180
Table 41: Reception of Unprotected Calls While Privacy Configuration....185
Table 42: Reception of Protected Calls While Privacy Configuration....186
Table 43: Icons for the Privacy Status/Type....187
Table 44: CPS Programmable Pins....196
Table 45: Summarized Performance Parameters....243
Table 46: Standard and Premium Voice Announcement Feature....249
Table 47: Wi-Fi Default Profile....251
Table 48: MOTOTRBO Analog Voice Features....256
Table 49: MOTOTRBO MDC Analog Signaling Features....256
Table 50: Quik-Call II Signaling Features....257
Table 51: Analog Scan Features....257
Table 52: CPS Repeater Wide Settings....258
Table 53: Rear Accessory Port CPS Programmable Pins....259
Table 54: Rear Accessory Port Fixed Audio Pins for DR 3000....261
Table 55: Rear Panel Port Fixed Audio Pins for MTR 3000....261
Table 56: Rear Panel DB25 Port Fixed Audio Pins for SLR 5000 and SLR 8000....262
Table 57: Front Panel Audio Ports on the SLR 8000....263
Table 58: Configuration Summary Table....263
Table 59: Zetron Model 42 Trunking Controller Jumper Settings....265
Table 60: Zetron Model 42 Trunking Controller Jumper Settings....266
Table 61: Zetron Model 38 Tone Panel Switch Settings....266
Table 62: Programmable Options for ARTS....274
Table 63: Computer Specifications for Access to the Webpage of the Repeater....277
Table 64: Sample Attachment to MOTOTRBO 2-4-1 License Application....283
Table 65: System Components and Topologies....297
Table 66: Description of the Impedance Supported by the Wireline Board....302
Table 67: Repeater Specifications for DR 3000....303
Table 68: Repeater Specifications for MTR3000....303
Table 69: Mobile Components for MOTOTRBO Portable....317
Table 70: Mobile Components for MOTOTRBO Mobile....317
Table 71: MOTOTRBO Portable Average Battery Life....318
Table 72: Digital MOTOTRBO Radios in Direct Mode/Dual Capacity Direct Mode....337
Table 73: Extended Range Direct Mode Features Distribution....342
Table 74: Horizontal and Vertical Antenna Required Isolation....345
Table 75: Digital MOTOTRBO Radios in Repeater Mode....358

Table 76: Digital MOTOTRBO Radios in IP Site Connect Mode....370
Table 77: Digital MOTOTRBO Radios in Capacity Plus Single Site and Capacity Plus Multi Site Modes....385
Table 78: Site Router Hair-Pinning Requirement Overview....387
Table 79: Maximum Number of Satellite Receivers Supported per Voting Repeater per Site in a Multi-Site System....391
Table 80: System Design Considerations....395
Table 81: Voice and Data Traffic Profiles....400
Table 82: Data Application Retry Attempts and Intervals....410
Table 83: GPS Revert Channels....413
Table 84: IP Site Connect Device Bandwidth Equation....429
Table 85: Detailed Bandwidth Calculation for Repeater 1 in IP Site Connect Mode....431
Table 86: Detailed Bandwidth Calculation for Repeaters in IP Site Connect Mode....431
Table 87: IPv4 Configuration....475
Table 88: MNIS Data Gateway and DDMS Computer Specifications....508
Table 89: Codeplug Communication Requirements....512
Table 90: Examples of Possible Radio ID and Aliases....515
Table 91: CPS Option per Channel....521
Table 92: Emergency Revert and GPS/Data Revert Considerations....523
Table 93: Dynamic Mixed Mode System CPS Configuration Recommendations....537
Table 94: Radio Management Computer Specifications....565
Table 95: Configurable Timers....566
Table 96: Standalone Dedicated-Link Backhaul Configuration....573
Table 97: Hybrid Dedicated-Link Backhaul Configuration....573
Table 98: OVCM CONFIGURABLE PARAMETERS....579
Table 99: CPSS and CPMS IP Plan Summary....585
Table 100: Radio Network Subnet IP Assignment in the CPSS IP Plan....586
Table 101: Application Network Subnet IP Assignment in the CPSS IP Plan....587
Table 102: Radio Network Subnet IP Assignment in the CPMS IP Plan....588
Table 103: Application Network Subnet IP Assignment in the CPMS IP Plan....590
Table 104: Example of a Radio Network IP Plan for the Site ID = 15 in the CPMS System....591
Table 105: Example of an Application Network IP Plan for the Site ID = 15 in the CPMS System....592
Tabela 106: Description of Address Book Entries....600
Tabela 107: Capacity Plus Dynamic Source NAT Rules....602
Tabela 108: Traffic Matrix for Capacity Plus Single Site....603
Tabela 109: Traffic Matrix for Capacity Plus Multi Sites – Except NAT Topology....604
Tabela 110: Traffic Matrix for Capacity Plus Multi Sites – NAT Topology....604
Table 111: Examples of Network Interfaces....607
Table 112: Examples of Services Interfaces....607
Table 113: Examples of Special Interfaces....608

Table 114: Logical Interfaces..... 608
Table 115: Logical Interfaces in Motorola Configuration Templates.....609
Table 116: Standardized 24-Port Juniper EX2300 Ethernet Switch in CPSS and COMS systems..... 622
Table 117: Description of Address Book Entries in the No Tunnels Topology..... 627
Table 118: Description of Address Book Entries in the NAT Topology.....644
Table 119: Applications Overview..... 678
Table 120: MOTOTRBO Documentation..... 680
Table 121: Websites.....681
Table 122: Interaction Between Control Station Modem Type and Channel Type Parameters..... 682

List of Processes

Configuring the MOTOTRBO Link System: Example 2 76

List of Procedures

Configuring MOTOTRBO Link Mode on the Standard Repeater at the Origin Site 67
Configuring MOTOTRBO Link Mode on the Link Repeater at the Origin Site 69
Configuring MOTOTRBO Link Mode on the Standard Repeater at the Terminating Site 71
Configuring MOTOTRBO Link Mode on the Link Repeater at the Terminating Site 72
Configuring Radios 74
Configuring MOTOTRBO Link Mode on the Backward Link Repeater at the Interim Site 76
Configuring MOTOTRBO Link Mode on the Forward Link Repeater at the Interim Site 78
Configuring MOTOTRBO Link Mode on the Standard Repeater at the Interim Site 80
Conducting the RF Site Survey 143
Configuring IRP in RM 202
Populating the RM Server 231
Configuring Enterprise Wi-Fi Roaming Enhancement in RM 252
Activating SUM License 276
Accessing the Webpage of the Repeater 277
Downloading SLR Repeater Logs 279
Enabling Repeater Logs 280
Resetting Login Credentials/Certificate 280
Configuring Channel Lock Feature 291
Configuring Wi-Fi Roaming Feature 292
Configuring Wi-Fi Certificate Feature 292
Configuring Fall Alert in RM 293
Configuring Caller Alias in Radio Management 294
Adding the Pre-shared Key to the Radio Management 295
Securing Devices 295
Performing Repeater Factory Reset 296
Converting Existing 12.5/25 kHz Licenses 398
Migrating from IP Site Connect 452
Migrating from Capacity Plus Single Site 453
Configuring Groups 513
Configuring the Private Calls Feature 517
Configuring the All Call Feature 518
Failure Preparedness – Uninterrupted Power Supplies (Battery Backup) 535
Configuring Considerations for a Dynamic Mixed Mode System 536
Configuring Broadcast Calls 578
Configuring Unaddressed Calls 578
Configuring Open Voice Channel Mode Calls in TX Mode 580

Configuring Open Voice Channel Mode Calls in RX Mode 580
Loading Basic Configuration with Device Console Port 650
Transferring Files to and from Juniper Devices Using SCP Protocol 653
Transferring Files to and from Juniper Devices with the USB Stick 654
Loading the Configuration from a File to the Juniper SRX Router and EX Switch 655
Upgrading Juniper OS on the EX2300 Switch 656
Upgrading Juniper OS on the SRX3xx Router 657
Preparing SRX345 to Deploy Chassis Cluster 659
Loading Configuration from a File on SRX Series Chassis Cluster 660
Upgrading Juniper OS on SRX Series Chassis Cluster 661
Creating and Modifying Credentials on Juniper EX Switch and SRX Router 663
Modifying SNMP Configuration on Juniper EX Switch and SRX Router 664
Clearing Persistent MAC Addresses Table on Juniper EX Switch 664
Changing the WAN IP Address (Juniper) 665
Saving the Rescue Configuration on Juniper Devices 666
Adjusting WinSCP Configuration for Juniper Devices 666
Generating Certificates for Juniper SRX Devices 667
Reserving IP Address on DHCP Server in SRX3xx Router 674
Enabling the Port Mirroring on Juniper EX Switch 675

About MOTOTRBO IP Site Connect, Capacity Plus System Planner

The IP Site Connect, Capacity Plus System Planner is designed to provide information concerning the impact of the MOTOTRBO features on pre-sales system planning considerations.

Related Information

Related Information	Purpose
Capacity Max System Advisor Guide	Provides fault management, system, and call monitoring solutions for a Capacity Max system.
Standards and Guidelines for Communication Sites Feature Guide	Provides standards and guidelines that should be followed when setting up a communications site. Also known as R56 manual.
Capacity Max Migration Guide	Provides instructions for using the Capacity Max Bridge to migrate from the MOTOTRBO™ Connect Plus trunked radio system to the Capacity Max commercial grade trunking system.
Capacity Max Installation and Configuration Manual	Provides explanation of the entire process of configuring Capacity Max system.
Capacity Max System Operations, Troubleshooting and Maintenance Guide	Provides guidelines for better system monitoring and troubleshooting possible issues.
Capacity Max System Release Upgrade Guide	Provides instruction step by step on upgrading the system to the latest release available.
MOTOTRBO CPS and AirTracer Applications Installation Guide	Provides the installation procedures and system requirementsfor following applications: • MOTOTRBO™ Customer Programming Software • Radio Management Server and Radio Management • Device Programmer • MOTOTRBO™ AirTracer • MOTOTRBO™ RDAC • MOTOTRBO™ Tuner
Repeater Diagnostics and Control (RDAC) User Guide and Online Help	Explains the features of the MOTOTRBO™ RDAC, which is a standalone Windows application for system technicians who need to run diagnostics on the radio (repeater or base radio) that has the RDAC capability.
MOTOTRBO CPS Radio Management User Guide and Online Help	Provides information about the Customer Programming Software structure and features which allows technicians to manage all radio components, in addition with Radio Management which provides a centralized management of programming radios in-the-field.

Related Information	Purpose
MOTOTRBO Radio Management User Guide and Online Help	Provides information about the Radio Management (RM) which allows the user to manage an entire fleet of radios that are connected to the Radio Management Configuration Client (RMC).
MOTOTRBO System Design Tools	Estimates the infrastructure and loading constraints on a MOTOTRBO™ system. The System Design Tools is a down-loadable program from Motorola Online.
WAVE 5000 Solution System Planner	Provides guidance on when it is appropriate for a WAVE 5000™ deployment with a MOTOTRBO™ system.
Wave 7000 System Planner	Provides system operators' supporting the WAVE 7000™ server to collect and generate reports on statistical data on the MOTOTRBO™ system performance.
IMPRES Over Air Battery Management	Provides information about the functionality of the application managing batteries for radio fleets.
Radio Management System Planner	Provides information about Radio Management system components, installation, and troubleshooting of possible issues.

Chapter 1

Introduction

1.1 Welcome to MOTOTRBO

Improving workforce productivity and operational effectiveness requires superior communications quality, reliability, and functionality. MOTOTRBO is the first digital two-way radio system from Motorola Solutions specifically designed to meet the requirements of professional organizations that need a customizable, business critical, private communication solution using licensed spectrum. MOTOTRBO combines the best in two-way radio functionality with digital technology to deliver increased capacity and spectral efficiency, integrated data applications and enhanced voice communications.

MOTOTRBO is an integrated voice and data system solution comprising of mobile and portable radios, audio and energy accessories, repeaters, text messaging and location tracking applications, and a third-party application partner program.

Figure 1: MOTOTRBO System

This system planner enables the reader to understand the features and capabilities of the MOTOTRBO system, and provides guidance on how to deploy and configure the system and its components to take advantage of its advanced capabilities.

This system planner is divided into 5 sections, with the first being this introduction. Section 2 provides an overview of system level features. Section 3 describes the system components in more detail. Section 4 provides guidance on system design considerations including configuration of components. Section 5 provides product sales and support information.

This system planner is complementary to additional training and documentation including:

- Radio Customer Programming Software (CPS) and related training
- System workshop/system service training
- Product specification sheets

1.2

Software Version

All the features described in the System Planner are supported by the following software versions:

- Radios - R02.40.00 and above
- Repeaters - R02.40.00 and above

Chapter 2

System Feature Overview

This chapter provides an overview of all the MOTOTRBO systems.

Table 1: System Feature Overview

System	Description
IPSC	Indicates IP Site Connect feature related content.
CPSS	Indicates Capacity Plus Single Site feature related content.
CPMS	Indicates Capacity Plus Multi Site feature related content.
CPSM	Indicates Capacity Plus Single Site AND Capacity Plus Multi Site shared feature related content.

2.1 MOTOTRBO Digital Radio Technology

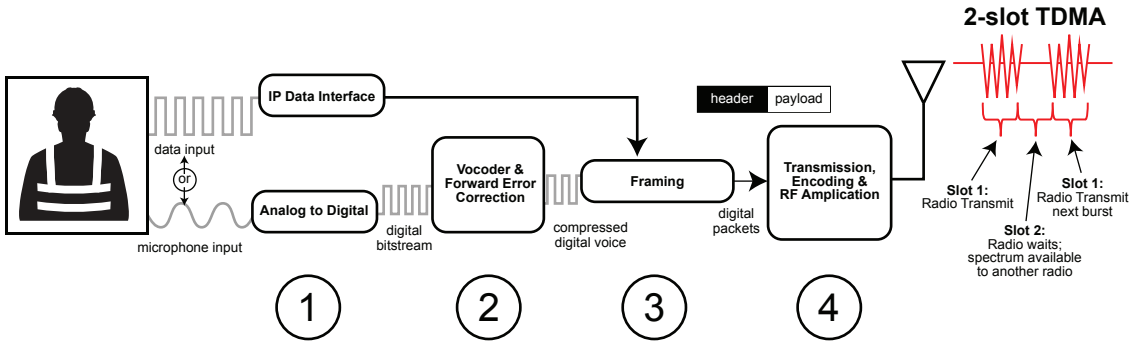
This section provides a brief overview of MOTOTRBO digital radio technology. It addresses two of the primary benefits delivered by this technology, which are the spectral efficiency and improved audio performance.

2.1.1 Digital Radio Technology Overview

The digital radio technologies employed by MOTOTRBO can be summarized as follows:

The following figure has four parts which are described in the following sections.

Figure 2: MOTOTRBO Digital Radio Technology



2.1.1.1
Analog to Digital Conversion

The first part is the analog to digital conversion.

When a radio user presses the Push-To-Talk (PTT) button and begins speaking, his voice is received by the radio microphone and converted from an acoustic waveform to an analog electrical waveform. This voice waveform is then sampled by an analog to digital converter. In typical radio applications, a 16-bit sample is taken every 8 kHz, this produces a 128,000bps (bits per second) digital bitstream, which contains far too much information to send over a 12.5 kHz or 20/25 kHz radio channel. Therefore some form of compression is required.

2.1.1.2
Vocoder and Forward Error Correction

The second part is the Vocoding and Forward Error Correction (FEC) application.

Vocoding (Voice encoding) compresses speech by breaking it into its most important parts and encoding them with a small number of bits, while greatly reducing background noise. Vocoding compresses the voice bitstream to fit the narrow (for MOTOTRBO) 6.25 kHz equivalent radio channel. The MOTOTRBO vocoder is AMBE+2TM which was developed by Digital Voice System, Inc. (DVSI), a leader in the vocoding industry. This particular vocoder works by dividing speech into short segments, typically 20 to 30 milliseconds in length. Each segment of speech is analyzed, and the important parameters such as pitch, level, and frequency response are extracted. These parameters are then encoded using a small number of digital bits. The AMBE+2TM vocoder is the first to demonstrate very low bit rates while producing toll-quality speech such as traditionally associated with wireline telephone systems.

Together with the vocoding process, FEC is also applied. FEC is a mathematical checksum technique that enables the receiver to both validate the integrity of a received message and determine which, if any, bits have been corrupted. FEC enables the receiver to correct bit errors that may have occurred due to radio frequency (RF) channel impairment. This effectively rejects noise that can distort an analog signal and by comparison enables more consistent audio performance throughout the coverage area. At this stage, the vocoder has already compressed the 128,000bps input signal to 3,600bps.

2.1.1.3
Framing

The third part is where the framing process happens.

In framing, the vocoded speech is formatted for transmission. This includes organizing the voice and any embedded signaling information (such as color code, group ID, PTT ID, call type, and others) into packets. These packets form a header and payload type of structure. The header contains the call control and ID information, and the payload contains the vocoded speech. This same structure can also relay Internet Protocol (IP) data packets. The IP packets are simply an alternative form of payload to the MOTOTRBO radio. The header information is repeated periodically throughout the transmission, thereby improving the reliability of the signaling information as well as enabling a receiving radio to join a call that may already be in progress. This condition is referred as “late entry”.

2.1.1.4
Time Division Multiple Access Transmission

Finally, the signal is encoded for a Frequency Modulation (FM) transmission. The bits contained in the digital packets are encoded as symbols representing the amplitude and phase of the modulated carrier frequency, amplified, and then transmitted.

Time Division Multiple Access (TDMA) organizes a channel into 2-time slots. A given radio’s transmitter is active only for short bursts, which provides longer battery life. By transmitting only on their alternating time

slots, two calls can share the same channel at the same time without interfering with one another, thereby doubling spectrum efficiency. Using TDMA, a radio transmits only during its time slot (it transmits a burst of information, waits, then transmits the next burst of information).

2.1.1.5
Standards Compliance

The digital protocols employed in MOTOTRBO (from vocoding and forward error correction to framing, transmission encoding, and transmission through 2-slot TDMA) are fully specified by the ETSI DMR (European Telecommunications Standards Institute Digital Mobile Radio) Tier 2 Standard, which is an internationally recognized standard with agreements among its supporting members.

NOTE: Tier 2 indicates full power conventional operation in licensed channels for professional and commercial users.

Although formal interoperability testing and verification processes for this standard have yet to fully mature, Motorola Solutions anticipates that MOTOTRBO radio systems are interoperable with other solutions that comply to the ETSI DMR Tier 2 standard.

2.1.2
Spectrum Efficiency Through 2-Slot TDMA

This section describes the spectrum efficiency through 2-slot TDMA.

2.1.2.1
Frequencies, Channels, and Requirements for Spectrum Efficiency

A radio communications channel is defined by its carrier frequency, and its bandwidth. The spectrum of available carrier frequencies is divided into major bands (such as 800/900 MHz, VHF, and UHF), and the majority of licensed channels in use today have widths of either 20/25 kHz or 12.5 kHz. As the airwaves have become increasingly crowded, new standards and technologies that allow more radio users to share the available spectrum in any given area are needed. The demand for greater spectral efficiency is being driven, in part, by regulatory agencies. In the U.S., for example, the Federal Communications Commission (FCC) requires manufacturers to offer only devices that operate within 12.5 kHz VHF and UHF channels by 2011. By the year 2013, all VHF and UHF users are required to operate in 12.5 kHz channels.

The next logical step is to further improve the effective capacity of 12.5 kHz channels. While there is no current mandate requiring a move to 6.25 kHz, such discussions are on-going at the FCC and other agencies. It's only a matter of time before the ability to carry two voice paths in a single 12.5 kHz channel, also known as 6.25 kHz equivalent efficiency, becomes a requirement in 800/900 MHz, VHF, and UHF bands. Presently, FCC rules are in place to mandate manufacturers to build radios capable of the 6.25 kHz efficiency for 800/900 MHz, VHF, and UHF bands, but the enforcement of these rules are put on hold. In the meantime, MOTOTRBO offers a way to divide a 12.5 kHz channel into two independent time slots, thus achieving 6.25 kHz-equivalent efficiency today.

2.1.2.2
Delivering Increased Capacity in Existing 12.5 kHz Channels

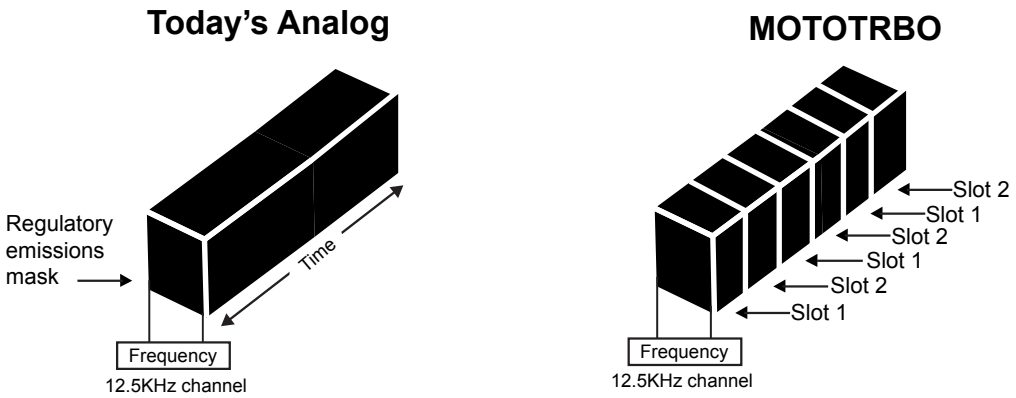
MOTOTRBO uses a 2-slot TDMA architecture. This architecture divides the channel into two alternating time slots, thereby creating two logical channels on one physical 12.5 kHz channel.

Each voice call utilizes only one of these logical channels, and each user accesses a time slot as if it is an independent channel. A transmitting radio transmits information only during its selected slot, and is idle

during the alternate slot. The receiving radio observes the transmissions in either time slot, and relies on the signaling information included in each time slot to determine which call it was meant to receive.

By comparison, analog radios operate on the concept of Frequency Division Multiple Access (FDMA). In FDMA, each transmitting radio transmits continuously on a designated channel, and the receiving radio receives the relevant transmission by tuning to the desired carrier frequency.

Figure 3: Comparison between Today's Analog and MOTOTRBO



12.5kHz Analog
- 1 voice for each 12.5kHz channel
- A single repeater for each channel

12.5kHz TDMA
- Divides existing channel into two timeslots
- Delivers twice the capacity through repeater
- Performance is same or better than 12.5kHz FDMA
- Single repeater does work of two repeaters
- Reduces need for combining equipment
- Enables 40% increase in radio battery life

TDMA thereby offers a straightforward method for achieving 6.25 kHz equivalency in 12.5 kHz repeater channels – a major benefit for users of increasingly crowded licensed bands. Instead of dividing channels into smaller slices of decreased bandwidth – which is what would be required to increase spectrum efficiency with FDMA methods, TDMA uses the full 12.5 kHz channel bandwidth, but increases efficiency by dividing it into two alternating time slots. Additionally, this method preserves the well-known radio frequency (RF) performance characteristics of the 12.5 kHz signal. From the perspective of RF physics – that is, actual transmitted power and radiated emissions – the 12.5 kHz signal of two-slot TDMA occupies the channel, propagates, and performs essentially in the same way as today's 12.5 kHz analog signals. With the added advantages of digital technology, TDMA-based radios can work within a single repeater channel to provide roughly twice the traffic capacity, while offering RF coverage performance equivalent to, or better than, today's analog radio.

2.1.2.3
2-Slot TDMA Reducing Infrastructure Equipment

2-slot TDMA essentially doubles repeater capacity. This means that one MOTOTRBO repeater does the work of two analog repeaters (a MOTOTRBO repeater supports two calls simultaneously).

This saves costs of repeater hardware and maintenance, and also saves on the cost and complexity of RF combining equipment necessary in multi-channel configurations. Just as importantly, the 2-slot TDMA signal fits cleanly into a customer's existing, licensed channels; there is no need to obtain new licenses for the increase in repeater capacity, and compared to alternative technologies that may operate on different bandwidths, there is no comparative increase in the risk of interference with or from adjacent channels.

Figure 4: Analog 2-Channel System

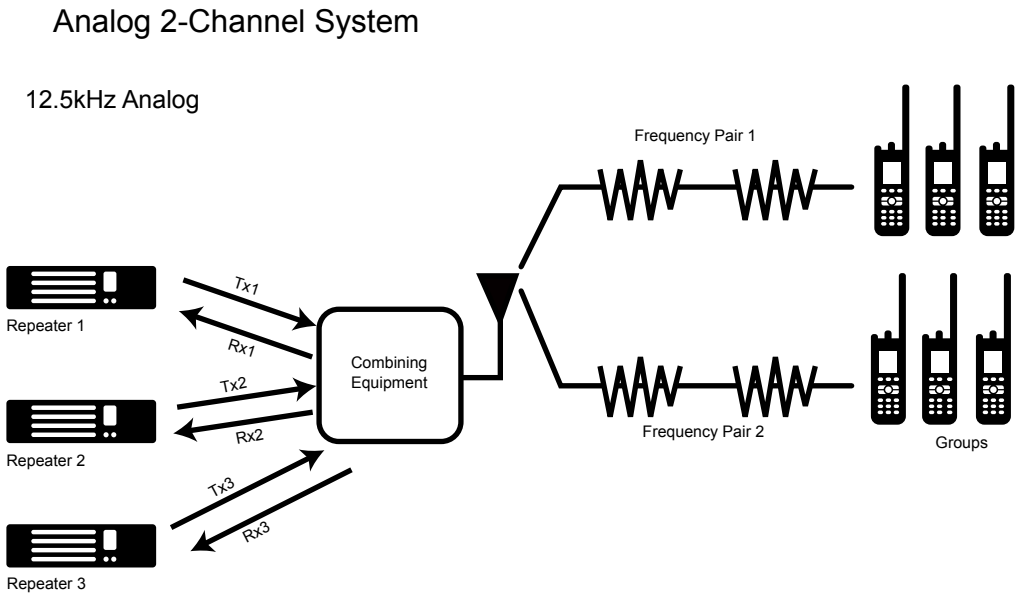
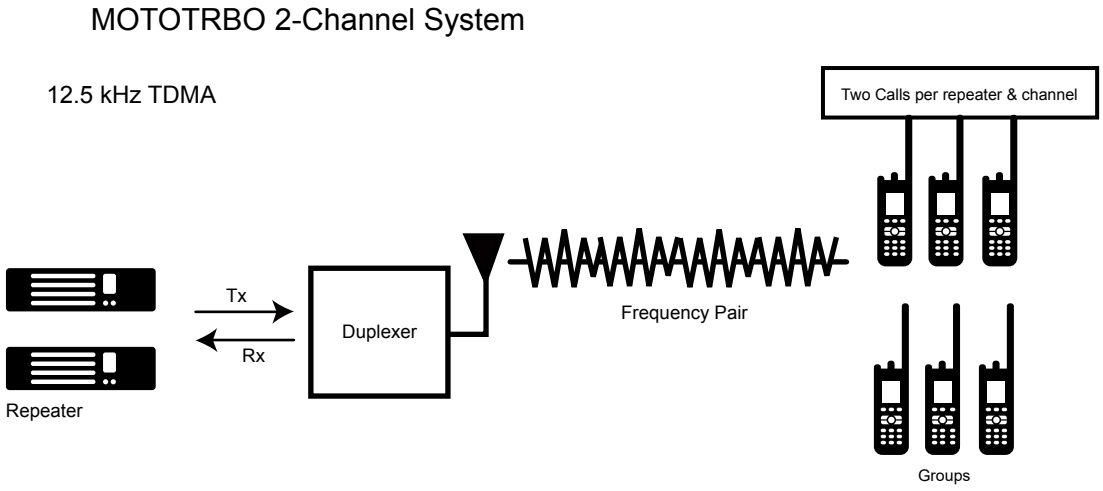


Figure 5: MOTOTRBO 2-Channel System



2.1.2.4

2-Slot TDMA Enables System Flexibility

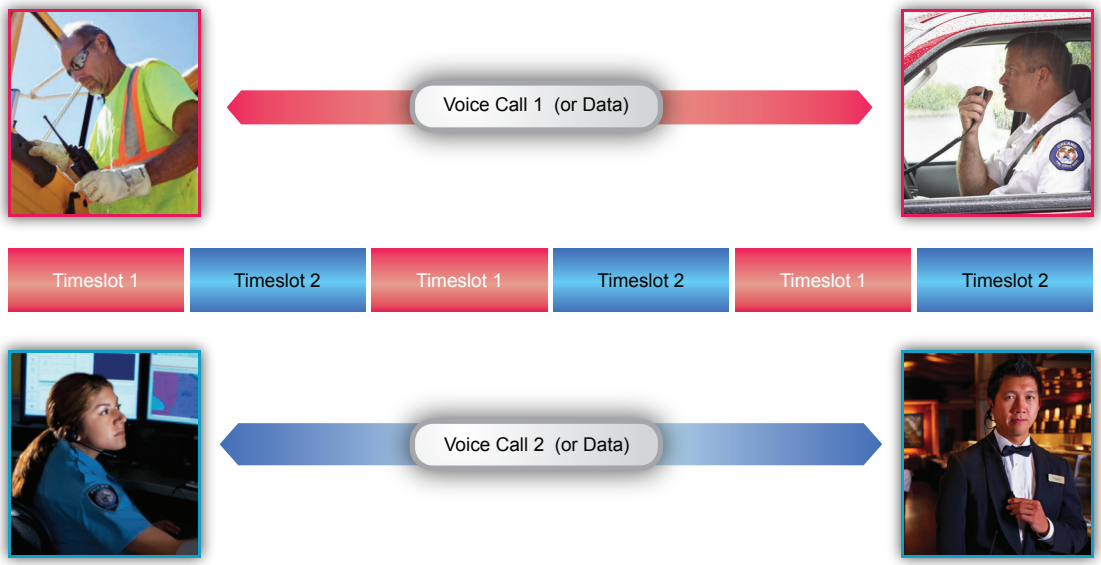
The two time slots or logical channels enabled by 2-slot TDMA can potentially be used for a variety of purposes. Many organizations deploying MOTOTRBO systems can use these slots in the following manner:

- Use both the slots as voice channels. This doubles the voice capacity per licensed repeater channel, thereby
  - increasing the number of users the system can accommodate, and
  - increasing the amount of air time the users can consume.
- Use both slots as data channels. This allows the organizations to fully deploy data transactions

- Use one slot as a voice channel, and the other as a data channel. This is a flexible solution, that allows customers to equip their voice users with mobile data, messaging, or location tracking capabilities.

In any of these scenarios, additional benefits are realized within the existing licensed repeater channel.

Figure 6: MOTOTRBO 2-Slot TDMA



NOTE: When used in direct mode without a repeater, 2-slot TDMA systems on a 12.5 kHz channel do not deliver 6.25 kHz equivalent efficiency. This is because the repeater is necessary to synchronize the time slots to enable independent parties to share them. Thus, on a direct or talkaround channel, when one radio begins transmitting, the whole 12.5 kHz channel is effectively busy, even though the transmitting radio is using only one time slot. The alternate time slot is unavailable for another, independent voice call. However, the alternate time slot can potentially be utilized as a signaling path. The ETSI DMR Tier 2 standard refers to this capability as Reverse Channel signaling, and it is envisioned to be used to deliver important future benefits to professional users, such as priority call control, remote-control of the transmitting radio, and Emergency Call pre-emption. This future capacity for reverse channel signaling is a unique capability of TDMA technology and, if supported by your system, may be deployed in both repeater and direct/talkaround configurations. At this time, the MOTOTRBO system does NOT support Reverse Channel signaling.

2.1.2.5
2-Slot TDMA System Planning Considerations

System Planning considerations associated with the increased capacity and the flexibility of the MOTOTRBO 2-slot TDMA architecture include:

- Capacity planning:
  - How many voice and data users do you have?
  - What usage profiles are anticipated?
  - How many channels and repeaters are needed?

These questions are addressed in more detail in System Design Considerations on page 395.

- Fleetmapping:
  - How to map users, voice services and data services such as messaging or location tracking to channels.

Voice and data service capabilities are described in more detail in this module and in System Components and Topologies on page 297. Fleetmapping considerations are addressed in more detail in System Design Considerations on page 395, in the MOTOTRBO Systems Training, and within the MOTOTRBO radio CPS.

- Migration Planning:
  - How to migrate existing channels to digital channels?
  - What updates to licensing requirements may be needed?

These questions are addressed in more detail in section four System Design Considerations on page 395.

2.1.3
Digital Audio Quality and Coverage Performance

This section describes how digital audio drives coverage performance. It also sets expectations for how digital audio behaves and sounds from the end-user's perspective.

2.1.3.1
Digital Audio Coverage

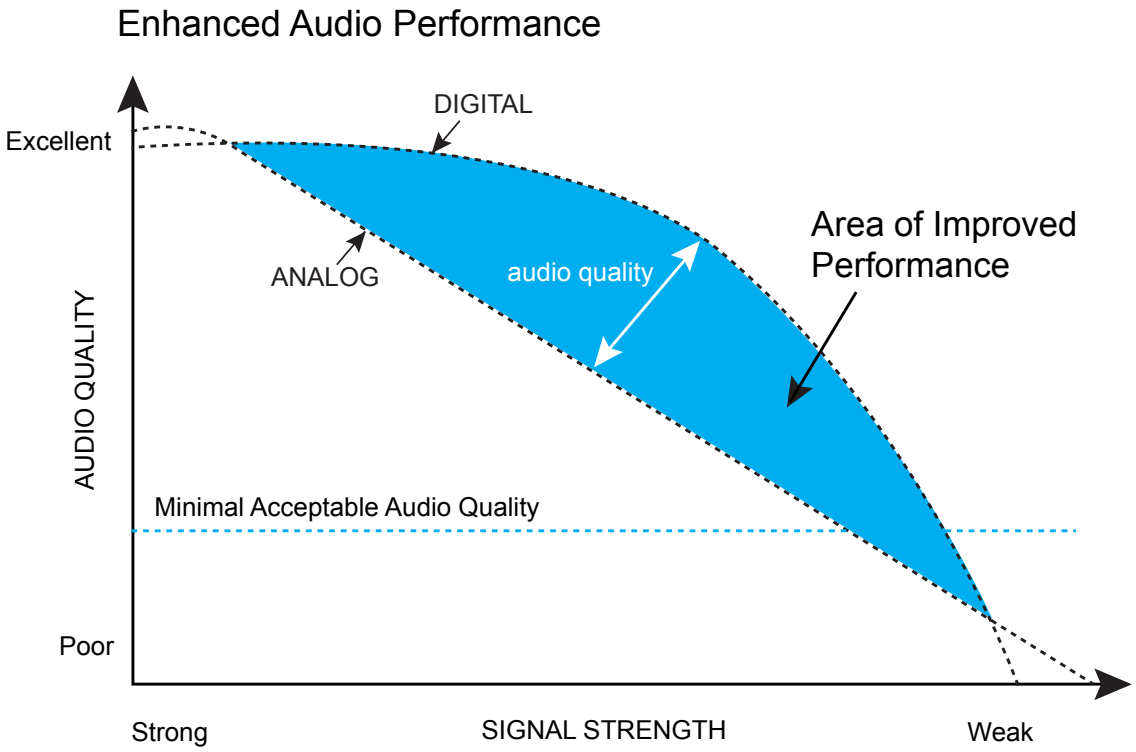
The main difference between analog and digital coverage is how the audio quality degrades throughout the coverage region. Analog audio degrades linearly throughout the region of coverage, while digital audio quality performs more consistently in the same region of coverage. A primary reason for the different degradation characteristics is the use of forward error correction coding used in digital transmissions, which can accurately deliver both audio and data content with virtually no loss over a far greater area.

It is this error protection that allows a MOTOTRBO system to provide consistent audio quality throughout its coverage area. A comparable analog system can never offer such consistency. In the MOTOTRBO system, the audio quality remains at a high level, because the error protection minimizes the noise effect.

The following figure graphically illustrates the relationship of delivered system audio quality, while comparing good to poor audio quality with strong to weak signal strength.

- In very strong signal areas the analog signal, because there is no processing, may sound slightly better than the digital audio signal.
- Digital signals increase the effective coverage area above the minimally acceptable audio quality level.
- Digital signals improve the quality and consistency of the audio throughout the effective coverage area.
- Digital signals do not necessarily increase the total distance that an RF signal propagates.

Figure 7: Comparison of Audio Quality versus Signal Strength for Analog and Digital



2.1.3.2

Predicting Digital Audio Coverage

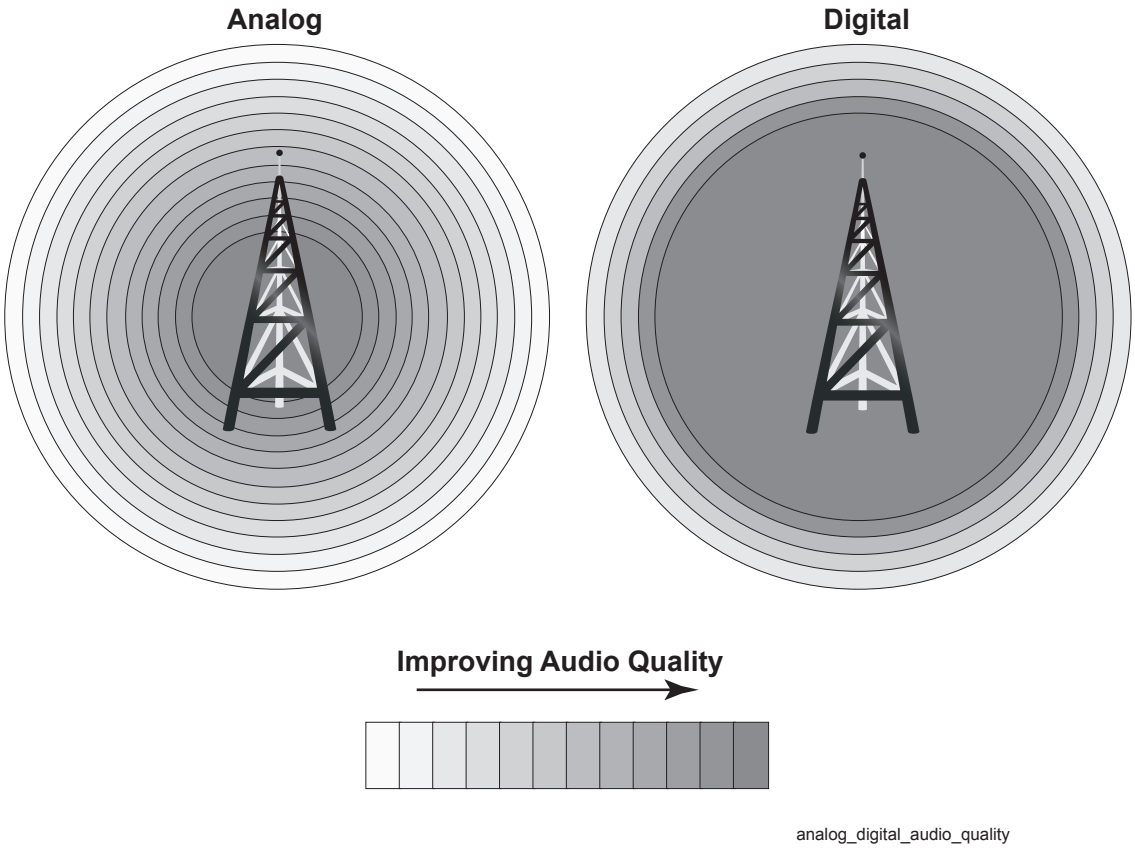
Predicting coverage for a radio site can be complicated. There are many factors that affect RF performance prediction, and generally, the more factors that can be considered, the more accurate the prediction of coverage. Perhaps the most influential factor is the selection of the RF propagation model and/or RF prediction software tools.

Coverage prediction techniques for analog and digital systems generally follow the same basic procedures, and require similar sets of input factors. Therefore, if the site's analog coverage footprint is already known, it is easier to plan the site's digital coverage footprint. This approach allows the system designer to use their existing analog site coverage prediction techniques, whether simple or complex, and then translate the results of the analog coverage prediction to predict digital coverage.

Delivered Audio Quality (DAQ) is a method to quantify audio quality. It is a measure of the intelligibility and quality of voice transported through a communications system, as defined in TIA TSB-88. DAQ reports audio quality on a 5-point scale, with a DAQ rating of three is considered as the minimal acceptable level of audio quality for public safety applications. The definition of DAQ 3 is "Speech understandable with slight effort and occasional repetition required due to Noise/Distortion.".

When comparing an analog site and a MOTOTRBO site, the relative regions of coverage offering comparable audio quality are illustrated in the following figure.

Figure 8: Differences in Analog Coverage



For a DAQ 3 audio quality, MOTOTRBO provides a greater usable range than analog, when all other factors are considered equal (for example, transmit power level, antenna height, receiver noise figures, IF filter bandwidths, no audio processing – such as Hear Clear, on the analog radios, terrain, antenna combining equipment, and others).

For an advanced, more comprehensive understanding of RF coverage prediction for the MOTOTRBO site, the reader is encouraged to obtain the TIA Telecommunications Service Bulletin TSB-88 – “Wireless Communications Systems-Performance in Noise and Interference-Limited Situations, Recommended Methods for Technology-Independent Modeling, Simulation, and Verification.”

A copy of TSB-88 can be obtained from http://www.tiaonline.org.

2.1.3.3
User Expectations for Digital Audio Performance

There are a number of differences between how digital audio behaves compared to analog audio from the end user (listener’s) perspective. Motorola Solutions has found that setting proper end user expectations in this regard is an important aspect of system planning.

What End-Users Experience with Digital Audio

- Consistent performance throughout coverage area with no gradual fade at the fringes: While analog signals slowly degrade as the receiver moves away from the transmitter, digital signals perform more consistently throughout the coverage area. However, digital signals, more abruptly, shift from “good” to “no signal”, when crossing the fringe of the coverage area. This means, users cannot rely on degrading audio quality to warn them that they are approaching the fringe of coverage. On the other hand, just

prior to the fringe of the coverage area, digital audio is still crisp and clean, whereas analog audio has excessive noise and static.

- Digital Sounds Different: The vocoding process is designed to deliver optimum audio quality with a very small number of bits. Some listeners find the resulting tonal qualities of digital speech somewhat different from what they have experienced with analog speech. Because the vocoding process is highly specialized for reproducing human speech, other sounds like music and tones are not reproduced accurately. Additionally, digital audio can introduce end-to-end audio delays. When overwhelming errors or dropouts are encountered, digital radios can generate some unique-sounding audio “artifacts”.
- Background Noise Reduction: The advanced vocoding capabilities in MOTOTRBO also include background noise reduction. Regardless of what is happening in the environment of the transmitting radio, only voice is reconstructed at the receiving radio – background noise, like machine noise, wind noise, and traffic noise, is not reconstructed, and thus, not heard. This is a key advantage of the MOTOTRBO digital voice solution over typical analog solutions, because noisy environments like factories, stores, work sites, and windy locations do NOT significantly degrade communication intelligibility.

What End-Users Do NOT Experience with Digital Audio

- Digital radio is not “CD Quality.” MOTOTRBO is the first radio in the industry to use the AMBE+2TM low bit rate vocoder to deliver communications grade voice quality. End users should not be misled into thinking that “communications grade” digital audio quality in radio systems is analogous to the high fidelity audio quality of CD’s and DVD’s.
- Digital cannot solve historic problems. System issues with coverage and interference are not necessarily eliminated by switching to digital. Adjacent or co-channel interference may sound different to a digital user, but digital technology does not solve interference issues. For example, analog interference is not heard as voice to a digital radio and vice versa, but disruption of system performance can still occur.

2.1.3.4

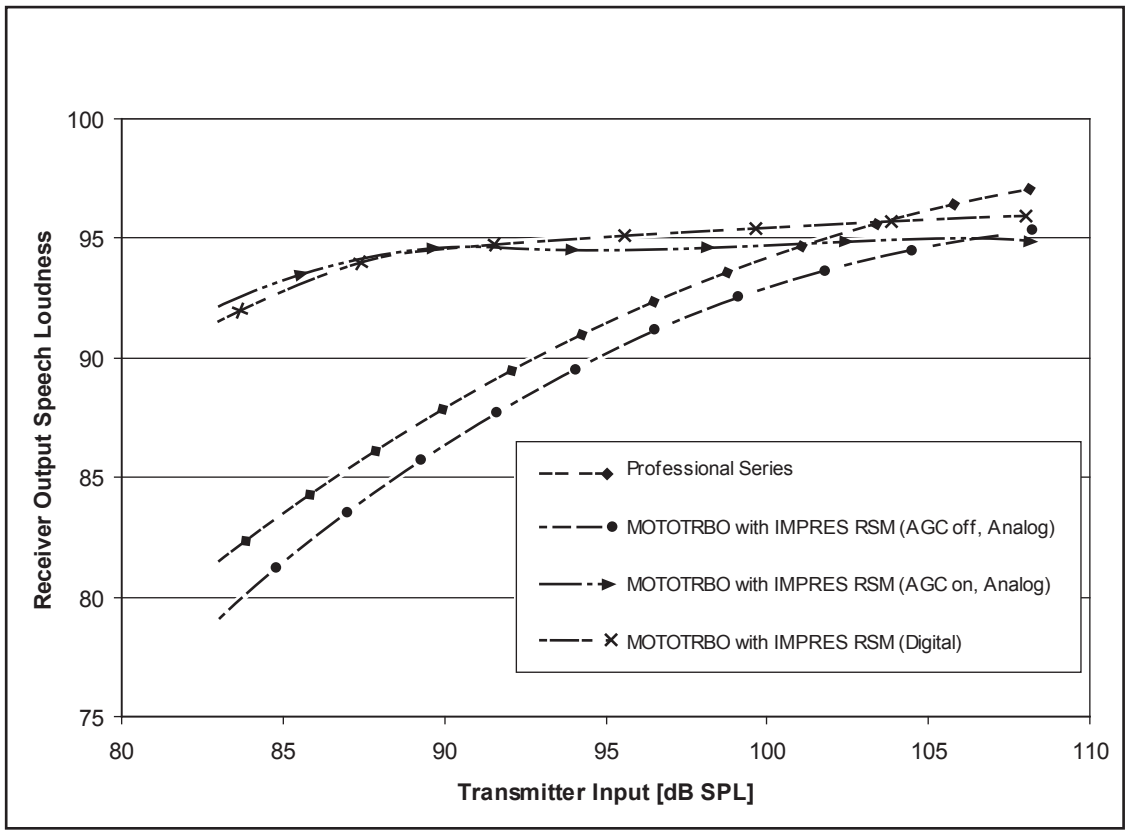
Audio Balancing

Transmitting voice over a digital air interface requires a voice coder, or vocoder for short. The vocoder used by MOTOTRBO is the Digital Voice Systems Inc. (DVSI) AMBE+2TM. This vocoder delivers excellent voice quality with robustness to both background noise and RF channel bit errors in a 6.25 kHz equivalent channel bandwidth. In order to produce optimal voice quality, the input level into the vocoder must fall within a specific amplitude range.

The diverse nature of users with respect to mouth-to-microphone distance as well as voice level and directivity can make this a bit problematic. In an effort to produce optimal voice quality over these diverse input conditions, MOTOTRBO digital always employs Automatic Gain Control (AGC) in the audio transmit path. The primary function of the transmit AGC is to produce the best voice quality possible under real life conditions. Since voice is still the main application of a two-way radio, this is a primary goal.

A secondary result of the AGC is to produce flat received speech loudness level over a range of input levels at the microphone. The usage of IMPRES Accessories extends this input range so optimal voice quality occurs over an even greater input range. The following figure illustrates this extended range flat response in the curve titled MOTOTRBO with IMPRES RSM (Digital). This same response curve can also be produced in analog mode by using an IMPRES Accessory and enabling Analog Mic AGC in the CPS General Settings. The following figure illustrates this type of response in the curve titled MOTOTRBO with IMPRES RSM (AGC on, Analog). An advantage of this type of response is that soft talkers and users that turn away from the microphone while speaking still come through loud and clear.

Figure 9: Transmit Audio Sensitivity



The flat audio response of digital is different from the traditional analog audio response. The traditional response is a linear response and the louder one speaks, then the louder the received volume. Figure 9: Transmit Audio Sensitivity on page 57 illustrates a traditional analog response in the curves titled Professional Series and MOTOTRBO with IMPRES RSM (AGC off, Analog). When Analog Mic AGC is disabled, then the Analog Mic Gain (dB) is adjustable in the CPS General Settings. Therefore, MOTOTRBO in analog mode is able to deliver the traditional analog response and is adjustable to fit into existing systems.

Examination of Figure 9: Transmit Audio Sensitivity on page 57 indicates that digital and traditional analog responses are similar at an input Sound Pressure Level (SPL) of 98 dB. Below this level, analog is quieter than digital. This is important to note as a system requiring MOTOTRBO to function as a digital radio and also as an analog radio during migration, may experience received audio level differences that are mode dependent. This could occur when scanning both digital and analog channels and the analog talker is located in a quiet environment such as an office. In quiet environments many users tend to speak softly and therefore the input falls below the equivalent response level of 98 dB SPL. Therefore, during the migration period, the analog response may be quieter than the digital response.

2.2
Basic System Topologies for Digital and Analog Operations

MOTOTRBO is a two-way radio system – conventional and trunked. In its most basic form, a MOTOTRBO system is comprised of radios that communicate with each other in the following available modes:

- Direct mode
- Repeater mode

- Through a repeater in conventional single site mode

System	Description
 IP Site Connect	MOTOTRBO system is configured through a set of repeaters in IP Site Connect mode.
 Capacity Plus Single Site	MOTOTRBO system is configured by trunking a set of repeaters in Capacity Plus Single Site mode.
 Capacity Plus Multi Site	MOTOTRBO system is configured by trunking a set of repeaters connected across multiple sites in Capacity Plus Multi Site mode.

The MOTOTRBO system can be configured to operate in analog mode, digital mode, or in both modes.

2.2.1
Repeater and Direct Mode Configurations

In direct mode, receive and transmit functions are both carried out on the same physical channel (transmit and receive frequencies are the same).

1. When operating in **Analog Direct Mode**, MOTOTRBO supports one voice path (transmit and receive) on one physical channel, and can be configured to operate in 12.5/20/25 kHz channel bandwidth systems.

   The option board interface meets the timing constraint of the MPT1327 standard, which is a signaling standard for trunked private land mobile radio system. The following features do **not** work with MPT1327:

   - VOX
   - Scan (normal and priority)
   - Battery saver
2. When operating in **Digital Direct Mode**, MOTOTRBO uses one physical channel configured for a 12.5 kHz channel bandwidth. On that one direct 12.5 kHz physical channel bandwidth, a MOTOTRBO digital system can support only one voice (or data) path at a time. Without a repeater in place to coordinate the time slot sequence among radios, only one radio can transmit at a time in order to guarantee transmissions do not overlap.

In repeater-based radio communications systems, a voice path requires a pair of channels: one for transmission, the other for reception.

2.2.1.1
Analog Repeater Mode

When operating in Analog Repeater Mode, MOTOTRBO operates similar to existing analog repeaters by supporting one voice path (transmit and receive) on one pair of physical channels, and can be configured to operate in 12.5/20/25 kHz channel bandwidth systems.

2.2.1.2
Digital Repeater Mode

When operating in Digital Repeater Mode, MOTOTRBO uses a pair of physical channels configured for 12.5 kHz channel bandwidth. Through the use of Time Division Multiple Access (TDMA) technology and the synchronization provided by the repeater, MOTOTRBO splits each 12.5 kHz channel (one transmit and one receive) into two independent time slots or logical channels within the 12.5 kHz physical channel bandwidth. This allows the user to assign voice or data traffic to either of the time slots independently. To the end user, this means they now have two voice or data channels that can be managed independently, instead of one. These two logical channels (two time slots) can transmit and receive independently of each other. The two logical channels in a 12.5 kHz channel makes the channel equivalent to a 6.25 kHz wide channel.

2.2.1.3
Dynamic Mixed Mode

When operating in Dynamic Mixed Mode (DMM), MOTOTRBO uses a pair of physical channels configured for 12.5 kHz channel bandwidth for digital operation and 12.5/20/25 kHz for analog operation.

The repeater dynamically switches between analog and digital modes based on the call it receives from radios. If an analog radio transmits, the repeater switches to analog mode to repeat the analog call. However, the repeater only repeats analog calls that are qualified by PL (DPL/TPL). If a digital radio transmits, then the repeater switches to digital mode to repeat the digital call if the call uses the right color code. While the repeater repeats one analog call at a time, it can repeat two digital calls at a time, one on each logical channel.

When a repeater repeats a new digital call that starts on one of the logical channels, the repeater does not qualify any analog call including an Emergency Call until the digital call (both the transmission and call hang time) is over and the corresponding channel hang time has expired. Upon the expiry of channel hang time, only then does the repeater start qualifying both analog and digital calls simultaneously. Similarly, if an analog call is being repeated, the repeater does not qualify any digital call including digital data and Emergency Calls on any of the two logical channels until the analog call is over and the corresponding hang time has expired.

Analog console device(s) are supported only when the repeater has not qualified an OTA digital call. If an analog console device tries to key up the repeater when a digital call has been received Over-The-Air, the analog call will be denied access. The repeater notifies the console via a channel busy tone generated over the speaker and Rx audio pins on the 4-wire repeater interface. Analog consoles do not have priority over digital calls (voice or data) in DMM mode.

Dynamic Mixed Mode is a repeater only configuration and the main functions of this feature are:

- The system requires one pair of physical channels (one Tx frequency and one Rx frequency) for both analog and digital calls, one MOTOTRBO repeater, and one set of RF equipment (antenna, combiners, couplers, LNA, and others) to enable analog and digital radio users to communicate.
- This configuration allows the user to have a mix of legacy analog radios and the digital MOTOTRBO radios in a MOTOTRBO system.
- The repeater supports two independent time slots or logical channels within the 12.5 kHz physical channel bandwidth while repeating digital calls. However, the repeater supports one voice path (transmit and receive) on a 12.5/20/25 kHz channel while repeating analog calls.

Dynamic Mixed Mode does not support the following configurations/features:

System	Description
IPSC IP Site Connect	This means that in Dynamic Mixed Mode, the repeater can only repeat the digital calls Over-The-Air and cannot send the voice/data packets over the IP network. The status of the repeater and the control of the repeater cannot be performed from a remote PC application like RDAC-IP.
CPSS Capacity Plus Single Site	This means that in Dynamic Mixed Mode, trunking the logical channels of multiple MOTOTRBO repeaters as per Capacity Plus Single Site is not supported.

- **FCC Type-I and Type-II monitoring**
  Since FCC Type-I and Type-II monitoring are not supported in single site analog operation in any of the earlier MOTOTRBO releases, it is also not supported in Dynamic Mixed Mode single site operation.
- **Transmit Interrupt Feature**
  The Voice Interrupt, Emergency Voice Interrupt, Remote Voice Dekey, and Data Over Voice Interrupt features are presently not supported in Dynamic Mixed Mode systems.
- **RDAC Over IP Feature**
  RDAC over local USB and connections via GPIO are supported. RDAC over the network is NOT supported.
- **Repeater Knockdown**
  In Dynamic Mixed Mode systems, this feature is not supported during an ongoing digital transmission.
- **PTT on a 4-wire Interface**
  In Dynamic Mixed Mode systems, this feature is not supported during a digital repeat operation.

2.2.1.4
IP Site Connect Mode

IPSC

When operating in IP Site Connect Mode, MOTOTRBO combines the logical channels of multiple MOTOTRBO systems (operating in digital repeater mode at dispersed locations) into one logical channel covering all locations.

In this mode, repeaters across dispersed locations exchange voice and data packets over an IPv4-based back-end network. There are three main functions of this mode, as follows:

- To increase the RF coverage area of a MOTOTRBO system.
- To provide voice and data communication between two or more MOTOTRBO single site systems located at geographically separate locations.
- To provide voice and data communication between two or more MOTOTRBO single site systems operating in different frequency bands (for example, 800/900 MHz, VHF, and UHF).

The backend network of an IP Site Connect system is designed to work seamlessly with internet connectivity provided by an Internet Service Provider (ISP). The system only requires that one of the repeaters have a static IPv4 or DNS address, while the others may be dynamic. Also, the system avoids the need for reconfiguration of a customer's network such as reprogramming of firewalls.

When a new call starts at one of the logical channel of a repeater, the repeater sends the call to all the repeaters and all these repeaters repeat the call on their corresponding logical channel. This allows a radio in the coverage area of any repeater to participate in the call. Thus, the coverage area of an IP Site Connect system is the sum of the coverage areas of all the repeaters. However, note that an IP Site Connect configuration does not increase the capacity (number of calls per hour) of the system. The capacity of one Wide Area Channel of an IP Site Connect system is approximately the same as that of a single repeater working in digital repeater mode.

In an IP Site Connect configuration, MOTOTRBO radios support all the features that they already support in digital repeater mode. This also includes Transmit Interrupt features that are supported on logical channels configured over wide area networks. Additionally, the radios are capable of automatically roaming from one site to another.

The IP Site Connect configuration of MOTOTRBO does not require any new hardware besides backend network devices such as routers. If a customer has multiple MOTOTRBO systems working in digital repeater mode at dispersed sites and wants to convert them into an IP Site Connect system then the repeaters and the radios should be updated with new software and the repeaters need to be connected to an IPv4-based backend network. It is possible to configure a repeater such that:

- Both logical channels work in IP Site Connect mode (over wide area).
- Both logical channels work in digital repeater mode (single site over local area).
- One of its logical channels works in IP Site Connect mode (over wide area) and the other logical channel works in digital repeater mode (single site over local area).

MOTOTRBO has three security features in the IP Site Connect configuration.

- Provides the confidentiality of voice and data payloads by extending the privacy feature, whether Basic or Enhanced, or Advanced Encryption Standard (AES), to cover the communication over the backend network.
- Ensures that all the messages between repeaters are authentic.
- Supports Secure VPN (Virtual Private Network) based communication between the repeaters for customers needing higher level of security (protection against replay attack).

The IP Site Connect configuration of MOTOTRBO provides a mechanism and a tool to remotely manage repeaters. The tool (called RDAC) receives alarms from all the repeaters, helps in diagnosis of repeaters, and provides some controls over the repeaters.

2.2.1.5
Capacity Plus Single Site Mode

CPSS

When operating in Capacity Plus Single Site Mode, MOTOTRBO trunks the logical channels of multiple MOTOTRBO repeaters (operating in digital repeater mode) at the same location.

This allows the radios to share the logical channels, resulting in less waiting time to access the system and increased channel capacity for a given quality of service. Another advantage is that the probability of all channels being busy at the same instant is low. Therefore the probability of a call being blocked is lower than when only one channel can be accessed.

Capacity Plus Single Site is a single site trunking configuration of the MOTOTRBO system. In a Capacity Plus Single Site configuration, all the “idle” radios (radios neither receiving nor transmitting) are on an idle channel called the Rest Channel. Therefore, a new call always starts on the Rest Channel. At the start of a call, the Rest Channel repeater selects one of the idle channels as the new Rest Channel, informs the radios on the current Rest Channel about the new Rest Channel, converts the current Rest Channel to a traffic channel,

and starts repeating the bursts sent by the radio. The radios that are not participating in the call (that is, destination of the call is not of their interest) move to the new Rest Channel.

If the current Rest Channel is the last idle channel (that is, all the other available channels are in use), the current Rest Channel remains as the Rest Channel. The call starts on the channel and non-participating radios stay on the channel. In this condition, non-participating radios indicate that the channel is busy through its yellow LED. If all channels are busy and a radio user initiates a call, then the radio generates a distinct tone to indicate that the system is busy. As soon as a channel becomes free in the Capacity Plus Single Site system, the non-participating radios are informed, and move to the free channel.

At the end of the call (that is, after the call hang time), the repeater also broadcasts the status of all other available channels. This triggers any radio on the channel to move to the current Rest Channel or to a channel where a Group Call of interest is active.

The Capacity Plus Single Site system has no central controller to manage the Rest Channel. The Rest Channel is managed collectively by all the trunked repeaters. A trunked repeater periodically informs the status of its channels to other trunked repeaters whenever the status of its channels change. When a new Rest Channel is selected, the selecting repeater informs all the other repeaters. The new Rest Channel is selected based on the following conditions:

- At the start of a call, the repeater of the current Rest Channel selects the new Rest Channel.
- On detection of interference or before starting CWID (BSI) transmission, the repeater of the current Rest Channel selects the new Rest Channel.
- On detection of no Rest Channel (in the event of a failure of the current Rest Channel repeater or the backend network), the repeater with the lowest ID selects the new Rest Channel.
- When a call ends on a system, if a call is in progress on the current Rest Channel, then the repeater of the current Rest Channel selects the new Rest Channel.

The Capacity Plus Single Site system does not require an exclusive control channel. The Rest Channel changes on every call; in case of an interference or if the repeater becomes unavailable due to failure. This results in the following advantages:

- Non-exclusive channels make it easier to satisfy regulator frequency coordination (where exclusive use of channels is not possible).
- Capacity Plus Single Site does not use “request and grant” mechanism to allocate channels and does not require any central controller to trunk the channels.
- The dynamic Rest Channel mechanism makes Capacity Plus Single Site very suitable for an environment where channels are shared by multiple radio systems.
- The dynamic Rest Channel mechanism also improves the reliability of the Capacity Plus Single Site system. In the event of a repeater failure, the other available repeaters automatically reconfigure themselves and continue to work as the Capacity Plus Single Site system.

The Capacity Plus Single Site system configuration of MOTOTRBO does not require any new hardware apart from backend network devices such as routers. If a customer has multiple MOTOTRBO systems working in digital repeater mode at the same site and wants to convert to a Capacity Plus Single Site system, then the repeaters and radios should be updated with the new software, and the repeaters need to be connected to an IPv4-based backend network. If one logical channel of a repeater is configured to the Capacity Plus Single Site mode, then the other logical channel will also be in the same mode.

In a Capacity Plus Single Site configuration, MOTOTRBO systems support all previous digital repeater mode features, with the exception of the following:

- Scan: Capacity Plus Single Site supports Group Scan, so a properly programmed radio listens for multiple talkgroups within a single Capacity Plus Single Site system, but does not support scanning channels of another system. Adding multiple talkgroups to the Receive list of a radio allows the user to hear the conversations of those talkgroups, and reply within the call hang time, regardless of the physical channel on which that call takes place.

- Emergency Revert Channel: Capacity Plus Single Site does not support a Revert Channel for emergency because probability of all Trunked Channels becoming busy is low. However, reverting to an emergency group is supported. This promotes a centralized handling of an emergency situation.
- IP Site Connect configuration: Capacity Plus Single Site is a single site system and therefore does not support features related to IP Site Connect configuration such as wide-area coverage and automatic roaming. However, a radio can be programmed with multiple channels in multiple zones, one of which could be a Capacity Plus Single Site system, another an IP Site Connect System, and others could be MOTOTRBO conventional channels or Analog conventional channels.
- Impolite calls: Capacity Plus Single Site supports impolite Emergency Call and impolite transmissions (group members can transmit over an ongoing call). A new call always starts on an idle channel and therefore, a radio does not start a non-Emergency Call impolitely.
- Talkaround mode: A radio can have a talkaround personality but in Capacity Plus Single Site mode, there is no talkaround option.
- monitoring of channels status: monitoring is important in a conventional system, where a radio stays on a channel. In Capacity Plus Single Site, a radio moves from one Rest Channel to another. Most of the Rest Channels are in an idle state and therefore, monitoring is not necessarily needed.
- Fragmentation of a Data Packet: Capacity Plus Single Site does not fragment a data packet before transmitting Over-The-Air. Thus, the size of an IP datagram (including IP and UDP headers) should be less than the maximum size of the Packet Data Unit. The value of the Packet Data Unit is a CPS programmable parameter with a maximum size of 1500 bytes.
- Option Board: If the Option Board feature is enabled for Capacity Plus Single Site, then the feature is automatically enabled for all trunked and Revert Channels of a Capacity Plus Single Site system. On a Capacity Plus Single Site personality, the Option Board is not aware of the transmit or receive channel. Additionally, an Option Board does not use or create Virtual Personalities in a Capacity Plus Single Site system. Hence, an Option Board will not be able to customize the current working personality.
- Transmit Interrupt: The Voice Interrupt, Emergency Voice Interrupt, Remote Voice Dekey, and Data Over Voice Interrupt features are supported on Capacity Plus Single Site systems.

Capacity Plus Single Site does not provide the following features:

- Coverage of multiple sites.
- Call queuing, priority, and preemption.
- Priority Monitor: Capacity Plus Single Site provides higher priority only to an All Call.
- Radio access control.

Greater detail on system services available in direct-mode and repeater-based system topologies

is described in System Components and Topologies on page 297.

2.2.1.6
Capacity Plus Multi Site Mode

CPMS

When operating in Capacity Plus Multi Site Mode, MOTOTRBO trunks the logical channels (that is, the TDMA slots) of multiple MOTOTRBO repeaters (operating in digital repeater mode) at multiple locations and

combines the logical channels into one logical channel. This allows radios to share the logical channels, as well as increase the RF coverage area of a MOTOTRBO system.

Capacity Plus Multi Site (CPMS) is a trunked multisite multi-channel configuration of MOTOTRBO, which combines both the Capacity Plus Single Site and IP Site Connect configurations. This combined configuration requires only software updates for radios and repeaters but does not require any new hardware.

NOTICE: Only repeaters with 32 MB of internal memory (for example, XPR 8380/XPR 8400 or MTR3000) can support the CPMS configuration.

The CPMS supports a wide variety of backend networks from a dedicated network to an Internet provided by the ISP. The CPMS requires more bandwidth over the back-end network than IP Site Connect and is designed to work seamlessly with Internet connectivity. The system requires only one of the repeaters to have a static IPv4 or DNS resolvable address. Additionally, the system avoids the need for reconfiguration of a customer's network, such as reprogramming of firewalls.

Similar to CPSS, CPMS repeaters at a site are connected over a LAN. A CPSS repeater uses multiple individual messages to communicate with the rest of the repeaters on site. However, a CPMS repeater sends a broadcast message to IPv4 Limited Broadcast Address (255.255.255.255). The broadcast messages may produce some diverse effects on the other devices present on the LAN. Therefore, a CPMS configuration requires only the CPMS repeaters and RDAC to be present on the LAN.

The call start-up of CPMS is a combination of IP Site Connect and Capacity Plus Single Site configurations with the following enhancements:

- In an IP Site Connect system, a customer can configure a logical channel as either a local channel or a wide area channel. A call over a local channel is repeated only over the local site, whereas a call over a wide area channel is repeated over all the sites where at least one channel is idle. Instead of local and wide-area channels of IP Site Connect, CPMS supports both local and wide area talkgroups. A repeater handles a local talkgroup call in the same method as in a CPSS configuration. However, a wide area talkgroup call is repeated over all the associated sites where at least one logical channel is idle.
- In an IP Site Connect system, a call starts at all sites. This is often called "All sites Light-Up". An advantage of this is the simplicity in implementation because repeaters are not required to know the list of radios present at its site. A disadvantage is that a multi-site configuration does not increase the capacity of a system but only the coverage. CPMS makes the following enhancements:
  - The CPMS allows defining a talkgroup as a wide area talkgroup. A wide area talkgroup call "lights-up" only the sites which are statically associated with the talkgroup. The call is rejected when a radio tries to initiate a wide area Group Call from a site not associated with the talkgroup.
  - The talkgroups not defined as wide-area are local talkgroups. A local call "lights-up" only one site where the initiating radio is located.
  - The CPMS Private Call initially "lights-up" all the sites but after approximately 400 milliseconds, the call continues only at the sites (at most two) where the source radio or destination radio are present.
- In CPMS, a wide area non-Emergency talkgroup call starts only if all the associated sites have idle channels. This is defined as "All Start". Additionally, the CPMS allows a customer to reserve a number of logical channels for wide-area talkgroup calls only. This improves the success of "All Start" for the wide-area talkgroup calls.
- An exception to the "All Start: rule (for all wide-area talkgroup calls) is when all channels a the destination site(s) are unusable (due to interference, BSI transmission or HW failure). The call source site reporter is able to continue the wide-area call setup process excluding unusable site(s).
- Just like a CPSS, the CPMS system has no controller. Repeaters of one site trunk the logical channels available at its site. The trunking process in CPMS is similar to that of CPSS. Repeaters from one site do not participate in trunking the RF resources of another site. Each site trunks its channel.

2.2.1.7

MOTOTRBO Link Mode

MOTOTRBO Link Mode is a configuration that enables Over-The-Air (OTA) backhaul through repeaters. This functionality is useful in areas where no site link connectivity exists.

When operating in MOTOTRBO Link Mode, MOTOTRBO supports chaining together a series of repeaters using a DMR channel as the backhaul link mechanism. In this mode, repeaters across dispersed locations exchange voice and data packets over a DMR-based OTA protocol with two timeslots.

The sites are linked or chained together using DMR channels that are dedicated for the sole purpose of linking the sites. Each site must contain at least one repeater that performs either the role of a Link or Standard Repeater. The Backhaul Link Repeater is a repeater dedicated to linking two sites together by forwarding the call data between the adjacent sites in the chain. A Standard Repeater can be conceptualized as a tap that is dropped into the network at some sites for subscriber radios to receive and/or transmit new calls into the network.

Within a backhaul site, the Standard and Link repeaters have connectivity to each other through an Ethernet connection to a Local Area Network (LAN). Every backhaul site must reside in its own IP subnet. The repeaters synchronize their timeslot timing by using General Purpose Input/Output (GPIO) pins on the accessory connector allocated for slot synchronization. Within a backhaul chain, connectivity between sites is available through the DMR channels in the Link repeaters. All backhaul sites and repeaters within the backhaul chain are timeslot timing aligned.

MOTOTRBO supports Dedicated-Link Backhaul system mode with the following configurations:

Standalone Dedicated-Link Backhaul
The system consists of one MOTOTRBO Link chain, which includes no more than nine MOTOTRBO Link sites.

Hybrid Dedicated-Link Backhaul
The system consists of one IPSC Backhaul network and one or more standalone MOTOTRBO Link chains. The Proxy repeater is responsible to bridge the calls between IPSC Backhaul network and the backhaul chain.

NOTE: Only SLR Series Repeaters (for example, SLR 1000/SLR 5000/SLR 8000) and second generation subscribers can support the MOTOTRBO Link configuration.

When a subscriber radio initiates a call (group or private), the Standard repeater receives the call and forwards it to an adjacent backhaul site by a link repeater/channel, and repeated by the Standard repeaters at all adjacent sites along the backhaul chain. The subscriber radio talk permit tone is only played when a call has been set up across the whole backhaul chain of repeaters. During the voice call set up, the Standard repeater transmits a Control Signaling Block (CSBK) to the subscriber that confirms that it has won the right to transmit on the channel. During the data call set up, the subscriber confirms that it has won the right to transmit on the channel but retries when it fails to win the channel until the maximum number of retries is exceeded.

Since the MOTOTRBO Link configuration uses daisy-chaining, each new site that is added to the chain increases the transmission delay required for a call to be transmitted from the origin of the chain to a terminating site in the chain. To enable a good user experience with minimal delay, a MOTOTRBO Link chain of repeaters is limited to chaining together up to nine sites with eight OTA links. And, MOTOTRBO Link systems are not expected to be heavily loaded systems with many users per site.

In a MOTOTRBO Link configuration, MOTOTRBO systems support all previous IP Site Connect repeater mode features, except for the following:

Auto Roaming
MOTOTRBO supports the ability to automatically roam between sites of one MOTOTRBO Link chain. Auto roaming between MOTOTRBO Link chains or/and IP Site Connect backhaul sites is not supported.

Enhanced Channel Access
MOTOTRBO only supports Backhaul Channel Access (BCA) with a TRART mechanism as channel access rule during call setup phase. This should be based on to the TRT mechanism for ECA with the “R1” phase replaced with the “R1-A” phase that is more similar to what is used for CPMS.

Remote Diagnostic and Alarm Control (RDAC)
MOTOTRBO supports only remotely monitor presence and alarm status from backhaul chain repeaters (No remote control command is supported).

Remote Repeater Programming (RRP)
MOTOTRBO supports RRP feature on IP Site Control backhaul repeaters (include the Proxy repeater) same as legacy IPSC systems. The Standard and Link repeaters do not support RRP.

A MOTOTRBO Link system does not support the following features:

- Transmit Interrupt
- Digital Telephone Patch
- Digital Voting
- Confirmed Group Data
- GPS Revert, Data Revert
- Enhanced/Scheduled GPS
- Repeater Call monitoring (RCM)
- CSBK Data

2.2.1.7.1
Hardware and Software Requirements

MOTOTRBO Link Mode software and hardware requirements are listed in this section.

- SLR 5000/8000/1000 series repeaters with R2.9 firmware or newer.
- Custom DB25-DB25 sync cable, see Figure 220: GPIO Pin Configurations on page 574.
- DP/DM4000 or DP3441/3661/e series radios with R2.9 firmware or newer.
- DP1400/2400e/DM2600/ as well as SL4010e/SL1600/SL2600/ portables with the latest firmware.
- Peripheral hardware for the repeaters such as duplexers, ethernet switches, and cabling.
- CPS 16.0 or later, alternatively Radio Management R2.9 or newer.
  Note: Using an Ethernet crossover cable to connect back to back two repeaters at a given backhaul site is not recommended.

Not supported:

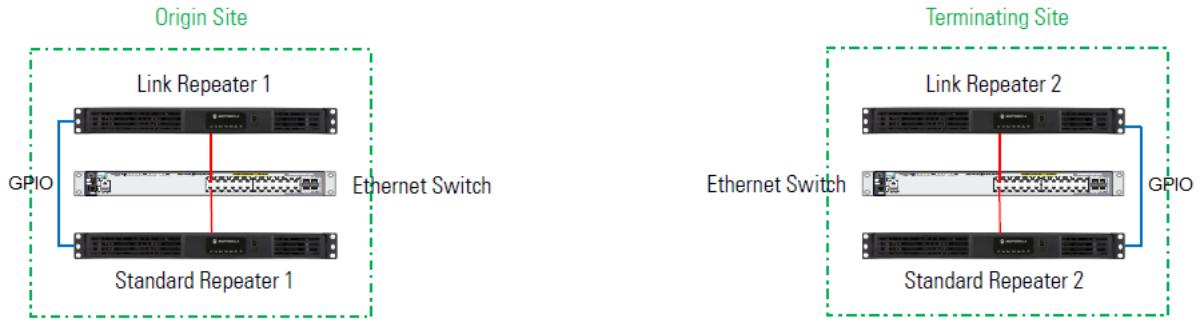
- DR 3000 and MTR3000 irrespective of memory size.
- First generation DP36xx; DP34xx; DM36xx and DM34xx.

2.2.1.7.2

MOTOTRBO Link System: Example 1

This section contains an exemplary configuration of a system.

Figure 10: MOTOTRBO Link System: Example 1



NOTE: The following devices support the GPIO4 function selection:

- SLR1000 repeaters - Pin #4
- SLR 5000 and SLR 8000 repeaters - Pin # 23
- MOTOTRBO Light Subscribers - Pin # 8
- MOTOTRBO Portable - Pin # 12

Table 2: Frequency Pairs

	TX	RX
Standard Repeater 1	1	2
Link Repeater 1	3	4
Link Repeater 2	4	3
Standard Repeater 2	5	6

NOTE:

- TX1 and RX2 can be reused on the standard repeater 2 if your spectrum licensing conditions permit, and there is no coverage overlap.
- The link repeaters should be set to the lowest RF power possible that supports a reliable link. In most cases, full power is a waste.
- Adequate RF filtering must be used on each site.
- Careful attention is needed when choosing frequencies, having multiple transmitters on the same site can result in intermodulation.

2.2.1.7.2.1

Configuring MOTOTRBO Link Mode on the Standard Repeater at the Origin Site

Use this procedure to configure MOTOTRBO Link Mode on the standard repeater.

Procedure:

1. In the CPS, select the ***<Repeater>*** and ensure that the Firmware Version is R2.9 or newer.

where the ***<Repeater>*** is the name of the repeater

2. From the ***<Repeater>*** drop-down list, select **General Settings** and perform the following actions:
   a. In the **Radio Name** field, enter the ***<name of the repeater>***
   b. In the **Radio ID** field, enter the ***<repeater ID>***

   NOTE: The Radio ID for each repeater in the system must be unique.

   Step example:

3. From the ***<Repeater>*** drop-down list, select **Accessories** and perform the following actions:
   a. In the **GPIO4** field (Pin #23), select **Site Slot Sync Input**.

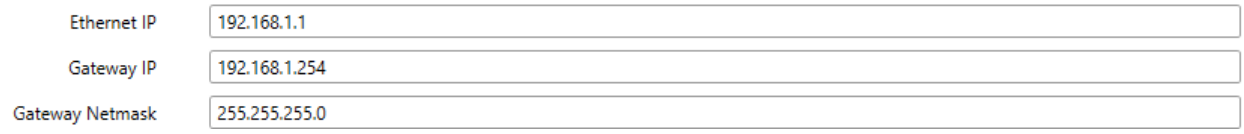
   IMPORTANT: One repeater cannot configure 2 pins at the same time even if leaving the unused pin not connected. Sync input and sync output cannot be enabled at the same time.

   b. Set the **Active Level** to **Low**.
   c. Select the **Debounce** check box.

   Step example:

4. From the ***<Repeater>*** drop-down list, select **Network** and enter the required network settings.

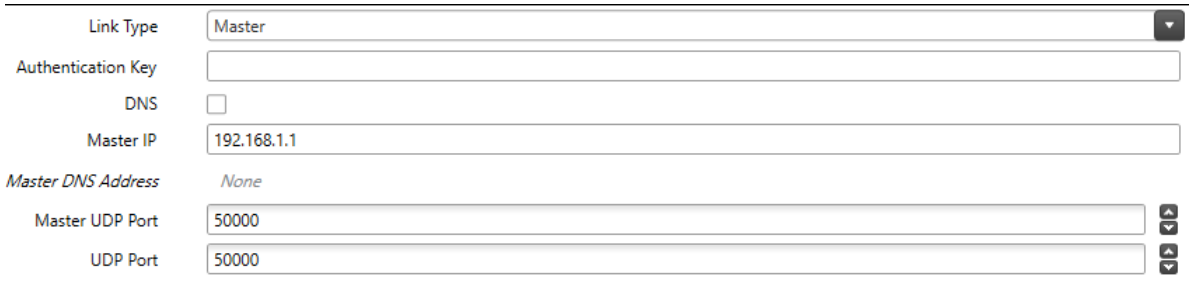
   Step example:



5. From the ***<Repeater>*** drop-down list, select **Link Establishment** and perform the following actions:
   a. From the **Link Type** drop-down list, select **Master**.
   b. Clear the **DNS** check box.
   c. In the **Master IP** field, enter the ***<Master IP address>***.
   d. In the **Master UDP Port** field, enter the ***<Master UDP Port address>***.
   e. In the **UDP Port** field, enter the ***<UDP Port address>***.

   IMPORTANT: Every repeater on the same site must have the same ***<UDP Port address>*** value.

   Step example:



6. From the ***<Repeater>*** drop-down list, select **MOTOTRBO Link**, and perform the following actions:

a. From the **Link Mode** drop-down list, select **Dedicated Link**.
b. From the **Site Type** drop-down list, select **Origin Site**.
c. From the **Repeater Type** drop-down list, select **Standard Repeater**.
d. Clear the **GPIO Slot Timing Master** check box.
e. From the **Maximum Number of Links** drop-down list, select ***<number of links>***.

   where the ***<number of links>*** is the number of sites of the longest backhaul chain minus 1 In the Example 1, this value is **1**. In the Example 2, this value is **2**.
f. From the **Link Beacon Interval (sec)** drop-down list, select **60**.
g. Select the **IP Site Connect MOTOTRBO Link Site** check box.

Step example:

7. From the ***<Repeater>*** drop-down list, select **Channels** → **Zone1** → **Channel1**.
8. From the **IP Site Connect** drop-down list, select **Slot 1 & Slot 2**.

   NOTE: This parameter differs depending on the site structure. In this example, the parameter is **Slot 1 & Slot 2**.

2.2.1.7.2.2 Configuring MOTOTRBO Link Mode on the Link Repeater at the Origin Site

Use this procedure to configure MOTOTRBO Link Mode on the link repeater.

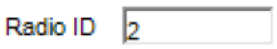
Procedure:

1. In the CPS, from the ***<Repeater>*** drop-down list, select **General Settings**, and in the **Radio ID** field, enter the `repeater ID`.

   where the ***<Repeater>*** is the name of the repeater

   NOTE: The Radio ID for each repeater in the system must be unique.

   Step example:

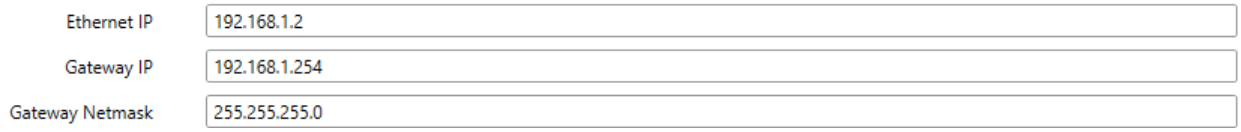
2. From the ***<Repeater>*** drop-down list, select **Accessories** and perform the following actions:
   a. In the **GPIO6** field (Pin #8), select **Site Slot Sync Output**.

      IMPORTANT: One repeater cannot configure 2 pins at the same time even if leaving the unused pin not connected. Sync input and sync output cannot be enabled at the same time.
   b. Set the **Active Level** to **Low**.
   c. Select the **Debounce** check box.

   Step example:

3. From the ***<Repeater>*** drop-down list, select **Network** and enter the required network settings.

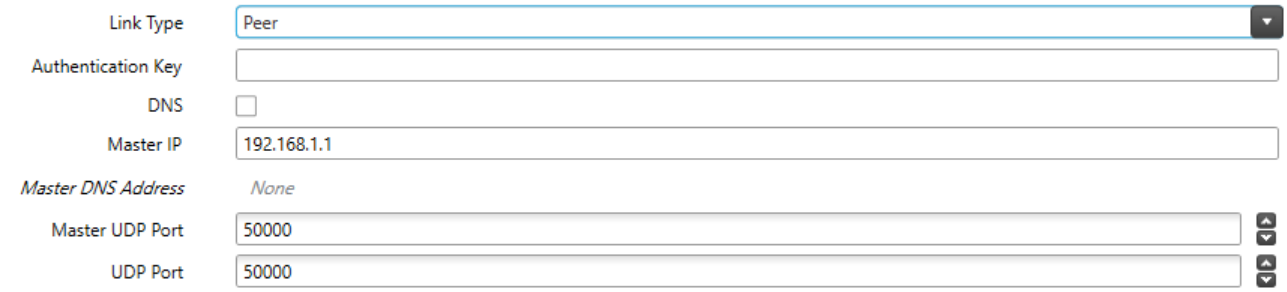
Step example:



4. From the ***<Repeater>*** drop-down list, select **Link Establishment** and perform the following actions:
   a. From the **Link Type** drop-down list, select **Peer**.
   b. Clear the **DNS** check box.
   c. In the **Master IP** field, enter the ***<Master IP address>***.
   d. In the **Master UDP Port** field, enter the ***<Master UDP Port address>***.
   e. In the **UDP Port** field, enter the ***<UDP Port address>***.

   IMPORTANT: Every repeater on the same site must have the same ***<UDP Port address>*** value.

Step example:



5. From the ***<Repeater>*** drop-down list, select **MOTOTRBO Link**, and perform the following actions:
   a. From the **Link Mode** drop-down list, select **Dedicated Link**.
   b. From the **Site Type** drop-down list, select **Origin Site**.
   c. From the **Repeater Type** drop-down list, select **Link Repeater**.
   d. Select the **GPIO Slot Timing Master** check box.
   e. From the **Maximum Number of Links** drop-down list, select ***<number of links>***.

      where the ***<number of links>*** is the number of sites of the longest backhaul chain minus 1. In the Example 1, this value is **1**. In the Example 2, this value is **2**.
   f. From the **Link Beacon Interval (sec)** drop-down list, select **60**.
   g. Clear the **IP Site Connect MOTOTRBO Link Site** check box.

Step example:

6. From the ***<Repeater>*** drop-down list, go to **Channels** → **Zone1** → **Channel1**
7. From the **IP Site Connect** drop-down list, select **Slot 1 & Slot 2**.

2.2.1.7.2.3

Configuring MOTOTRBO Link Mode on the Standard Repeater at the Terminating Site

Use this procedure to configure MOTOTRBO Link Mode on the standard repeater.

Procedure:

1. In the CPS, from the ***<Repeater>*** drop-down list, select **General Settings**, and in the **Radio ID** field, enter the ***<repeater ID>***.

   where the ***<Repeater>*** is the name of the repeater

   NOTE: The Radio ID for each repeater in the system must be unique.

   Step example:

2. From the ***<Repeater>*** drop-down list, select **Accessories** and perform the following actions:

   a. In the **GPIO4** field (Pin #23), select **Site Slot Sync Input**.

      IMPORTANT: One repeater cannot configure 2 pins at the same time even if leaving the unused pin not connected. Sync input and sync output cannot be enabled at the same time.

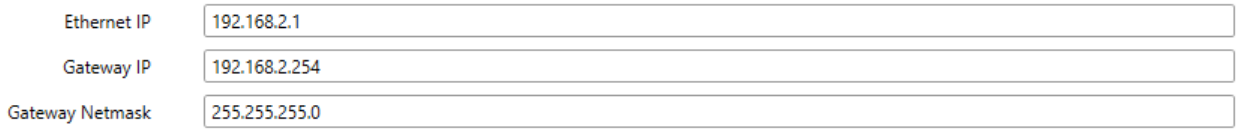
   b. Set the **Active Level** to **Low**.

   c. Select the **Debounce** check box.

   Step example:

3. From the ***<Repeater>*** drop-down list, select **Network** and enter the required network settings.

   Step example:

4. From the ***<Repeater>*** drop-down list, select **Link Establishment** and perform the following actions:

   a. From the **Link Type** drop-down list, select **Master**.

   b. Clear the **DNS** check box.

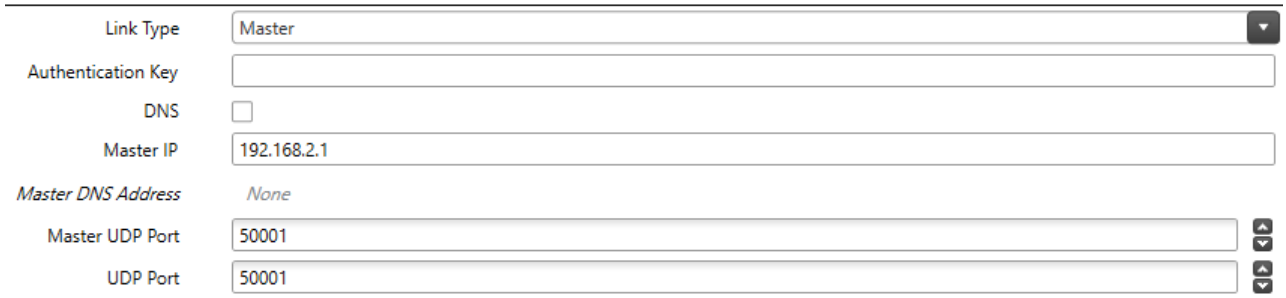
   c. In the **Master IP** field, enter the ***<Master IP address>***.

   d. In the **Master UDP Port** field, enter the ***<Master UDP Port address>***.

   e. In the **UDP Port** field, enter the ***<UDP Port address>***.

      IMPORTANT: Every repeater on the same site must have the same ***<UDP Port address>*** value.

Step example:



5. From the ***<Repeater>*** drop-down list, select **MOTOTRBO Link**, and perform the following actions:
   a. From the **Link Mode** drop-down list, select **Dedicated Link**.
   b. From the **Site Type** drop-down list, select **Terminating Site**.
   c. From the **Repeater Type** drop-down list, select **Standard Repeater**.
   d. Clear the **GPIO Slot Timing Master** check box.
   e. From the **Maximum Number of Links** drop-down list, select the ***<number of links>***.

      where the ***<number of links>*** is the number of sites of the longest backhaul chain minus 1
      In the Example 1, this value is **1**. In the Example 2, this value is **2**.
   f. From the **Link Beacon Interval (sec)** drop-down list, select **60**.
   g. Clear the **IP Site Connect MOTOTRBO Link Site** check box.

Step example:

6. From the ***<Repeater>*** drop-down list, go to **Channels** → **Zone1** → **Channel1**
7. From the **IP Site Connect** drop-down list, select **Slot 1 & Slot 2**.

NOTE: This parameter differs depending on the site structure. In this example, the parameter is **Slot 1 & Slot 2**.

2.2.1.7.2.4 Configuring MOTOTRBO Link Mode on the Link Repeater at the Terminating Site

Use this procedure to configure MOTOTRBO Link Mode on the link repeater.

Procedure:

1. In the CPS, from the ***<Repeater>*** drop-down list, select **General Settings**, and in the **Radio ID** field, enter the ***<repeater ID>***.

   where the ***<Repeater>*** is the name of the repeater

NOTE: The Radio ID for each repeater in the system must be unique.

Step example:

2. From the ***<Repeater>*** drop-down list, select **Accessories** and perform the following actions:
   a. In the **GPIO6** field (Pin #8), select **Site Slot Sync Output**.

      IMPORTANT: One repeater cannot configure 2 pins at the same time even if leaving the unused pin not connected. Sync input and sync output cannot be enabled at the same time.

   b. Set the **Active Level** to **Low**.
   c. Select the **Debounce** check box.

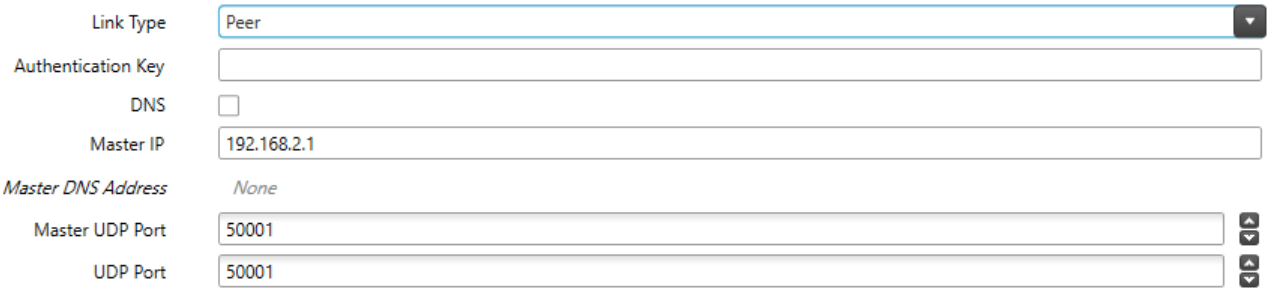
3. From the ***<Repeater>*** drop-down list, select **Network** and enter the required network settings.

Step example:

4. From the ***<Repeater>*** drop-down list, select **Link Establishment** and perform the following actions:
   a. From the **Link Type** drop-down list, select **Peer**.
   b. Clear the **DNS** check box.
   c. In the **Master IP** field, enter the ***<Master IP address>***.
   d. In the **Master UDP Port** field, enter the ***<Master UDP Port address>***.
   e. In the **UDP Port** field, enter the ***<UDP Port address>***.

      IMPORTANT: Every repeater on the same site must have the same ***<UDP Port address>*** value.

Step example:



5. From the ***<Repeater>*** drop-down list, select **MOTOTRBO Link**, and perform the following actions:
   a. From the **Link Mode** drop-down list, select **Dedicated Link**.
   b. From the **Site Type** drop-down list, select **Terminating Site**.
   c. From the **Repeater Type** drop-down list, select **Link Repeater**.
   d. Select the **GPIO Slot Timing Master** check box.
   e. From the **Maximum Number of Links** drop-down list, select ***<number of links>***.

      where the ***<number of links>*** is the number of sites of the longest backhaul chain minus 1
      In the Example 1, this value is **1**. In the Example 2, this value is **2**.
   f. From the **Link Beacon Interval (sec)** drop-down list, select **60**.

g. Clear the **IP Site Connect MOTOTRBO Link Site** check box.

Step example:

6. From the ***<Repeater>*** drop-down list, go to **Channels** → **Zone1** → **Channel1**
7. From the **IP Site Connect** drop-down list, select **Slot 1 & Slot 2**.

2.2.1.7.2.5 Configuring Radios

Use this procedure to configure the radios in the MOTOTRBO Link System.

Procedure:

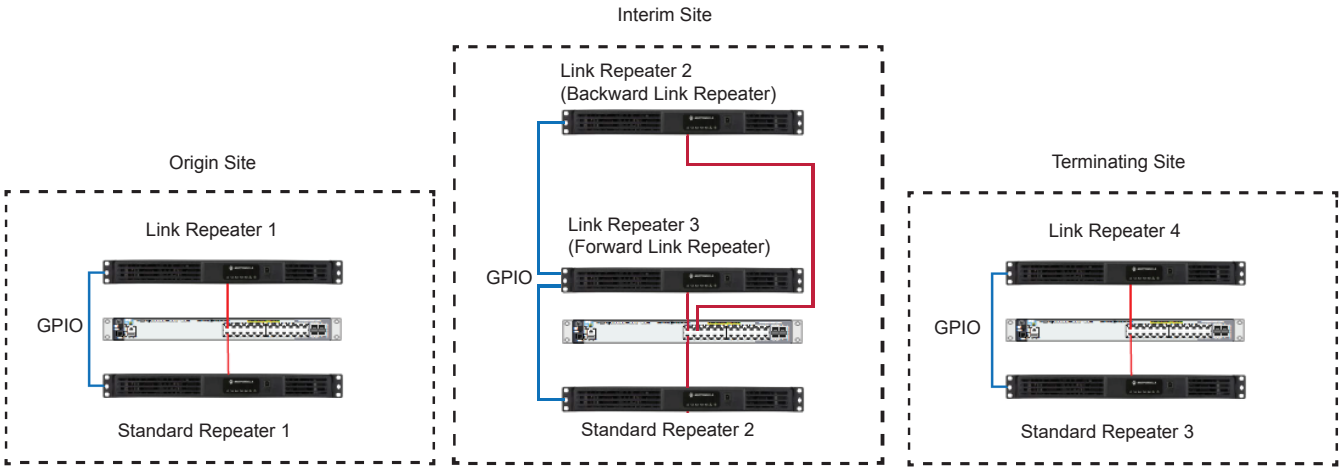
1. In the CPS, select the ***<Radio name>*** and ensure that the Firmware Version is R2.9 or newer.
   - where ***<Radio name>*** is the name of the radio
2. Select ***<Radio name>*** → **Channels** → **Zone1** → **IPSC Group 101**.
3. Ensure that the MOTOTRBO Link check box is selected in all channels in the Zone and Channel Pool.

2.2.1.7.3

MOTOTRBO Link System: Example 2

This section contains an exemplary configuration of a system.

Figure 11: MOTOTRBO Link System: Example 2



NOTE: The following devices support the GPIO4 function selection:

- SLR1000 repeaters - Pin #4
- SLR 5000 and SLR 8000 repeaters - Pin # 23
- MOTOTRBO Light Subscribers - Pin # 8
- MOTOTRBO Portable - Pin # 12

Table 3: Frequency Pairs

	TX	RX
Standard Repeater 1	1	2
Link Repeater 1	3	4
Link Repeater 2	5	3
Link Repeater 3	4	6
Link Repeater 4	6	5
Standard Repeater 2	7	8

	TX	RX
Standard Repeater 3	9	10

NOTE:

- TX1 and RX2 can be reused on the standard repeater 2 or 3 if your spectrum licensing conditions permit, and there is no coverage overlap.
- Careful attention is needed when choosing frequencies, having multiple transmitters on the same site can result in intermodulation.
- The link repeaters should be set to the lowest RF power possible that supports a reliable link. In most cases, full power is a waste.
- Adequate RF filtering must be used on each site.

IMPORTANT:

- Forward Link Repeater is a repeater at the Interim Site which receives data from the Terminating Link direction (in this example Link Repeater 3 Rx frequency 6 equals Link Repeater 4 Tx frequency 6), and transmits data to the Origin Link direction (Link Repeater 3 Tx frequency 4 equals Link Repeater 1 frequency 4).
- Backward Link Repeater is a repeater at the Interim Site which receives data from the Origin Link direction (Link Repeater 2 Rx frequency 3 equals Link Repeater 1 Tx frequency 3), and transmits data to Terminating Link direction (Link Repeater 2 Tx frequency 5 equals Link Repeater 4 Rx frequency 5).
- Forward Link Repeater at the Interim Site has to be Slot Timing Master.

2.2.1.7.3.1

Configuring the MOTOTRBO Link System: Example 2

Follow this procedure to set up the MOTOTRBO Link System shown in example 2.

Process:

1. Configure the standard repeater 1. See Configuring MOTOTRBO Link Mode on the Standard Repeater at the Origin Site on page 67.
2. Configure the link repeater 1. See Configuring MOTOTRBO Link Mode on the Link Repeater at the Origin Site on page 69.
3. Configure the link repeater 2. See Configuring MOTOTRBO Link Mode on the Backward Link Repeater at the Interim Site on page 76.
4. Configure the link repeater 3. See Configuring MOTOTRBO Link Mode on the Forward Link Repeater at the Interim Site on page 78.
5. Configure the link repeater 4. See Configuring MOTOTRBO Link Mode on the Link Repeater at the Terminating Site on page 72.
6. Configure the standard repeater 2. See Configuring MOTOTRBO Link Mode on the Standard Repeater at the Interim Site on page 80.
7. Configure the standard repeater 3. See Configuring MOTOTRBO Link Mode on the Standard Repeater at the Terminating Site on page 71.
8. Configure the radios. See Configuring Radios on page 74.

2.2.1.7.3.1.1

Configuring MOTOTRBO Link Mode on the Backward Link Repeater at the Interim Site

Use this procedure to configure MOTOTRBO Link Mode on the link repeater.

Procedure:

1. In the CPS, select the ***<Repeater>*** and ensure that the Firmware Version is R2.9 or newer.

   where the ***<Repeater>*** is the name of the repeater

2. From the ***<Repeater>*** drop-down list, select **General Settings** and in the **Radio ID** field, enter the ***<repeater ID>***.

   NOTE: The Radio ID for each repeater in the system must be unique.

   Step example:

3. From the ***<Repeater>*** drop-down list, select **Accessories** and perform the following actions:

   a. In the **GPIO4** field (Pin #23), select **Site Slot Sync Input**.

      IMPORTANT: One repeater cannot configure 2 pins at the same time even if leaving the unused pin not connected. Sync input and sync output cannot be enabled at the same time.

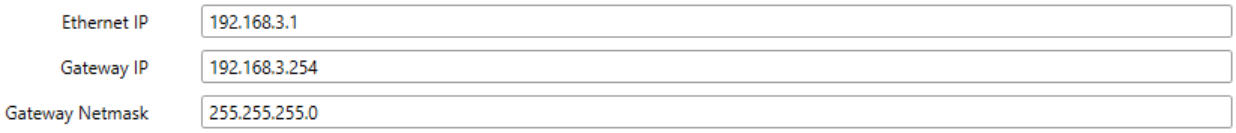
   b. Set the **Active Level** to **Low**.

   c. Select the **Debounce** check box.

   Step example:

4. From the ***<Repeater>*** drop-down list, select **Network** and enter the required network settings.

   Step example:

5. From the ***<Repeater>*** drop-down list, select **Link Establishment** and perform the following actions:

   a. From the **Link Type** drop-down list, select **Peer**.

   b. Clear the **DNS** check box.

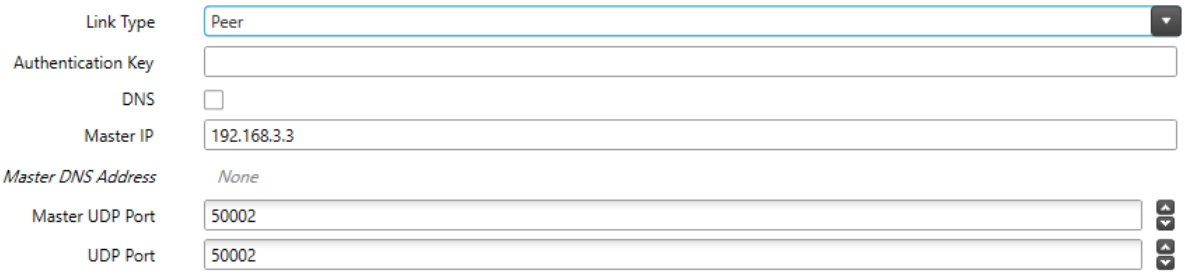
   c. In the **Master IP** field, enter the ***<Master IP address>***.

   d. In the **Master UDP Port** field, enter the ***<Master UDP Port address>***.

   e. In the **UDP Port** field, enter the ***<UDP Port address>***.

      IMPORTANT: Every repeater on the same site must have the same ***<UDP Port address>*** value.

   Step example:

6. From the ***<Repeater>*** drop-down list, select **MOTOTRBO Link**, and perform the following actions:

a. From the **Link Mode** drop-down list, select **Dedicated Link**.
b. From the **Site Type** drop-down list, select **Interim Site**.
c. From the **Repeater Type** drop-down list, select **Link Repeater**.
d. Clear the **GPIO Slot Timing Master** check box.
e. From the **Maximum Number of Links** drop-down list, select ***<number of links>***.

   where the ***<number of links>*** is the number of sites of the longest backhaul chain minus 1 In the Example 2, this value is **2**.
f. From the **Link Beacon Interval (sec)** drop-down list, select **60**.
g. Clear the **IP Site Connect MOTOTRBO Link Site** check box.

Step example:

7. From the ***<Repeater>*** drop-down list, go to **Channels** → **Zone1** → **Channel1**
8. From the **IP Site Connect** drop-down list, select **Slot 1 & Slot 2**.

2.2.1.7.3.1.2 Configuring MOTOTRBO Link Mode on the Forward Link Repeater at the Interim Site

Use this procedure to configure MOTOTRBO Link Mode on the link repeater.

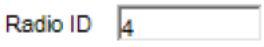
Procedure:

1. In the CPS, from the ***<Repeater>*** drop-down list, select **General Settings**, and in the **Radio ID** field, enter the ***<repeater ID>***.

   where the ***<Repeater>*** is the name of the repeater

   NOTE: The Radio ID for each repeater in the system must be unique.

   Step example:

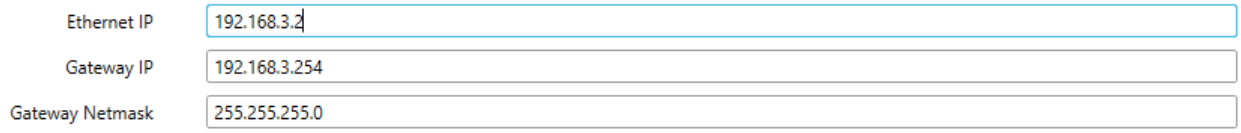
2. From the ***<Repeater>*** drop-down list, select **Accessories** and perform the following actions:
   a. In the **GPIO6** field (Pin #8), select **Site Slot Sync Output**.

      IMPORTANT: One repeater cannot configure 2 pins at the same time even if leaving the unused pin not connected. Sync input and sync output cannot be enabled at the same time.
   b. Set the **Active Level** to **Low**.
   c. Select the **Debounce** check box.

   Step example:

3. From the ***<Repeater>*** drop-down list, select **Network** and enter the required network settings.

Step example:



4. From the ***<Repeater>*** drop-down list, select **Link Establishment** and perform the following actions:
   a. From the **Link Type** drop-down list, select **Peer**.
   b. Clear the **DNS** check box.
   c. In the **Master IP** field, enter the ***<Master IP address>***.
   d. In the **Master UDP Port** field, enter the ***<Master UDP Port address>***.
   e. In the **UDP Port** field, enter the ***<UDP Port address>***.

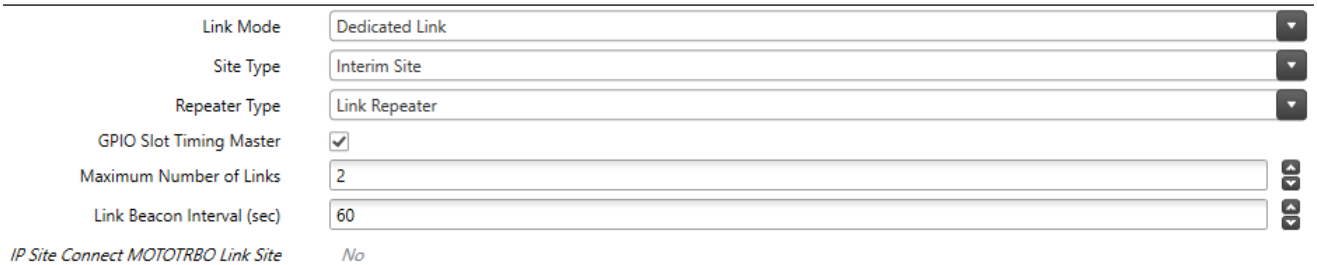
   IMPORTANT: Every repeater on the same site must have the same ***<UDP Port address>*** value.

Step example:

5. From the ***<Repeater>*** drop-down list, select **MOTOTRBO Link**, and perform the following actions:
   a. From the **Link Mode** drop-down list, select **Dedicated Link**.
   b. From the **Site Type** drop-down list, select **Interim Site**.
   c. From the **Repeater Type** drop-down list, select **Link Repeater**.
   d. Select the **GPIO Slot Timing Master** check box.
   e. From the **Maximum Number of Links** drop-down list, select ***<number of links>***.

      where the ***<number of links>*** is the number of sites of the longest backhaul chain minus 1
      In the Example 2, this value is **2**.
   f. From the **Link Beacon Interval (sec)** drop-down list, select **60**.
   g. Clear the **IP Site Connect MOTOTRBO Link Site** check box.

Step example:



6. From the ***<Repeater>*** drop-down list, go to **Channels → Zone1 → Channel1**
7. From the **IP Site Connect** drop-down list, select **Slot 1 & Slot 2**.

2.2.1.7.3.1.3

Configuring MOTOTRBO Link Mode on the Standard Repeater at the Interim Site

Use this procedure to configure MOTOTRBO Link Mode on the standard repeater.

Procedure:

1. In the CPS, from the ***<Repeater>*** drop-down list, select **General Settings**, and in the **Radio ID** field, enter the ***<repeater ID>***.

   where the ***<Repeater>*** is the name of the repeater

   NOTE: The Radio ID for each repeater in the system must be unique.

   Step example:

2. From the ***<Repeater>*** drop-down list, select **Accessories** and perform the following actions:

   a. In the **GPIO4** field (Pin #23), select **Site Slot Sync Input**.

      IMPORTANT: One repeater cannot configure 2 pins at the same time even if leaving the unused pin not connected. Sync input and sync output cannot be enabled at the same time.

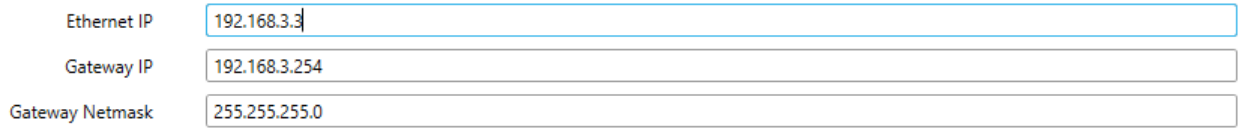
   b. Set the **Active Level** to **Low**.

   c. Select the **Debounce** check box.

   Step example:

3. From the ***<Repeater>*** drop-down list, select **Network** and enter the required network settings.

   Step example:

4. From the ***<Repeater>*** drop-down list, select **Link Establishment** and perform the following actions:

   a. From the **Link Type** drop-down list, select **Master**.

   b. Clear the **DNS** check box.

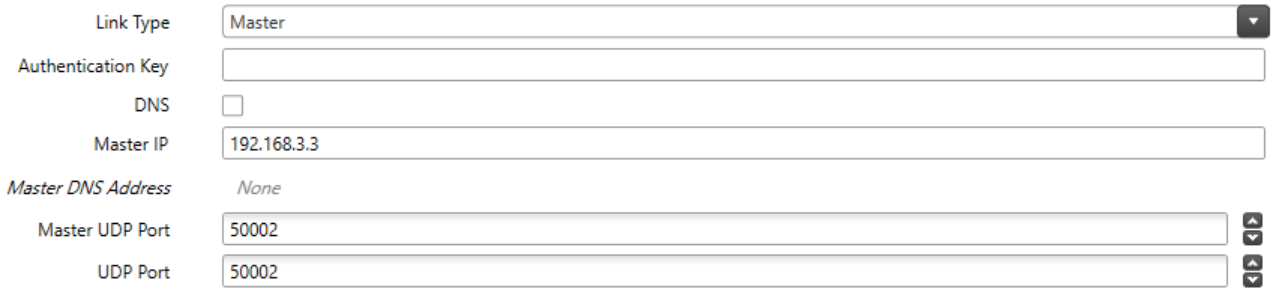
   c. In the **Master IP** field, enter the ***<Master IP address>***.

   d. In the **Master UDP Port** field, enter the ***<Master UDP Port address>***.

   e. In the **UDP Port** field, enter the ***<UDP Port address>***.

      IMPORTANT: Every repeater on the same site must have the same ***<UDP Port address>*** value.

   Step example:

5. From the ***<Repeater>*** drop-down list, select **MOTOTRBO Link**, and perform the following actions:
   a. From the **Link Mode** drop-down list, select **Dedicated Link**.
   b. From the **Site Type** drop-down list, select **Interim Site**
   c. From the **Repeater Type** drop-down list, select **Standard Repeater**.
   d. Clear the **GPIO Slot Timing Master** check box.
   e. From the **Maximum Number of Links** drop-down list, select the ***<number of links>***.

      where the ***<number of links>*** is number of sites of the longest backhaul chain minus 1
      In the Example 1, this value is **1**. In the Example 2, this value is **2**.
   f. From the **Link Beacon Interval (sec)** drop-down list, select **60**.
   g. Clear the **IP Site Connect MOTOTRBO Link Site** check box.

   Step example:

6. From the ***<Repeater>*** drop-down list, go to **Channels** → **Zone1** → **Channel1**
7. From the **IP Site Connect** drop-down list, select **Slot 1 & Slot 2**.

   NOTE: This parameter differs depending on the site structure. In this example, the parameter is **Slot 1 & Slot 2**.

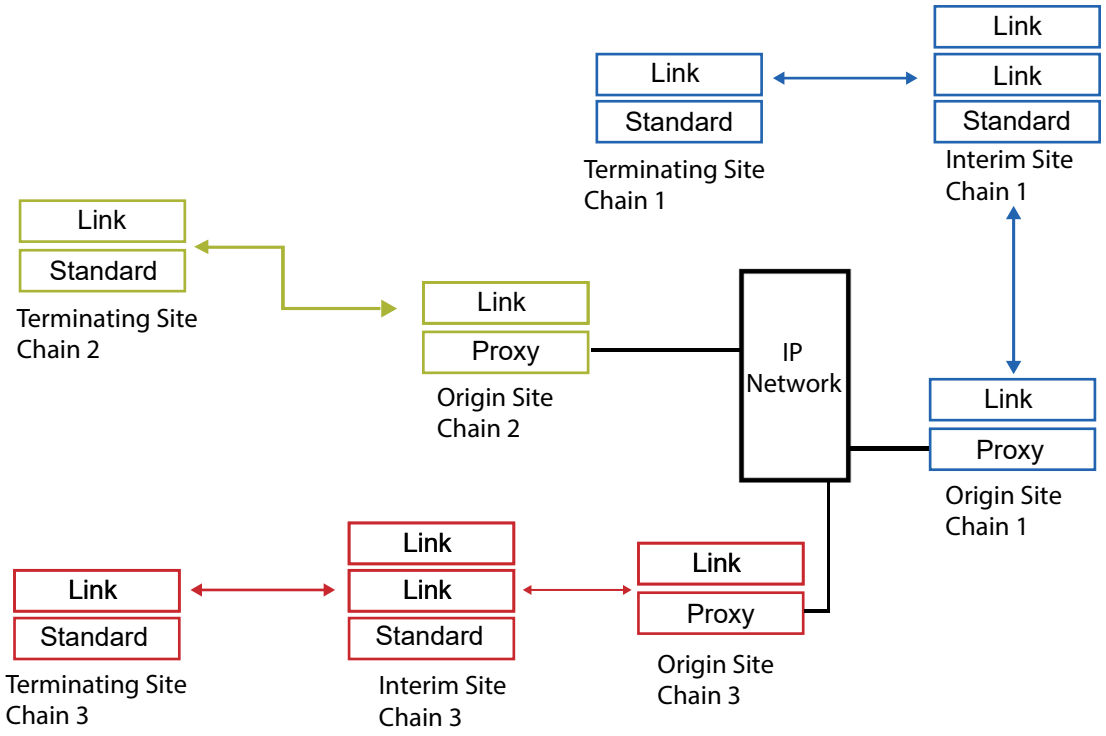
2.2.1.7.4

MOTOTRBO Link System: Example 3

This section contains an exemplary configuration of a system with several backhaul chains.

Figure 12: MOTOTRBO Link System: Example 3

The following figure is an example hybrid system of three backhaul chains connected by IP.



2.2.2

MOTOTRBO Supports Analog and Digital Operation

The MOTOTRBO system can be configured to operate in analog mode, digital mode, or in Dynamic Mixed Mode.

The system can consist of multiple repeaters. A single MOTOTRBO repeater configured to operate in Dynamic Mixed Mode can dynamically switch between analog and digital modes depending on the type of call it receives.

NOTE: A repeater in Dynamic Mixed Mode system cannot be part of multiple repeater system in which the repeaters are connected over the network for IP Site Connect, Capacity Plus Single Site, or Capacity Plus Multi Site operation.

MOTOTRBO portable and mobile radios can communicate in analog and digital. The mobile or portable radio user selects the mode of operation (analog or digital), and physical and logical channel using his channel selector knob (each channel selection position is configured for a particular call type on either a digital channel that specifies both frequency and time slot, or an analog channel that specifies both frequency and 25 kHz or 12.5 kHz bandwidth). Radio channels are either analog or digital. This is configured by the CPS. The radio can scan between analog and digital channels.

Greater detail on channel planning and configuration is provided in System Design Considerations on page 395.

2.2.3
MOTOTRBO Channel Access

Channel access dictates what conditions a radio is allowed to initiate a transmission on a channel. The channel access rules of MOTOTRBO are governed by the mobile and portable radios. It is the radio's responsibility to assess the state of the system, and utilize its channel access rules to decide whether to grant the call to the user.

In repeater systems, it is the repeater's responsibility to:

- Identify if a channel is busy, or
- Identify if a channel is idle, or
- Inform for which radio the channel is reserved.

The repeater does not block or deny any channel access from radios on its system, but will not repeat transmissions from another system.

There are two main types of channel access in a MOTOTRBO system: Polite and Impolite access. In the configuration software, channel access is referred to as the Admit Criteria. MOTOTRBO supports the following Admit Criteria:

- Always: This criteria is often referred to as "Impolite" channel access, and can be applied to analog and digital channels.
- Channel Free: This criteria is often referred to as "Polite to All", and can be applied to analog and digital channels.
- Color Code Free: This criteria is sometimes referred to as "Polite to Own Color Code" or "Polite to Own System", and is applied only to digital channels.
- Correct PL: This criteria is sometimes referred to as "Polite to Other System", and is applied only to analog channels. The radio checks for a PL match prior to allowing a transmission.

Channel access methods must be specified for each channel in the radio CPS. The TX (Transmit) parameters for each defined channel contains an "Admit Criteria" selection that must be set to one of the values described above.

All these channel access options govern how standard group voice calls and Private Calls access the system. Not all transmission types utilize these settings. For example, emergency voice calls always operate impolitely. This gives emergency voice calls a slightly higher priority over existing traffic on the channel. Data calls are always polite. Since a data call can be queued and retried, its priority is considered lower than voice.

Note that a "polite" radio user attempting a voice call will be polite to data, but an impolite user may not. Control messages (used for signaling features) are also always polite. The exception is the emergency alarm. Emergency alarms are sent with a mix of impolite and polite channel access, in order to optimize the likelihood of successful transmission.

When the Admit Criteria is either Channel Free or Correct PL, a configurable RSSI threshold is provided per channel in the radio. If the received signal strength is less than the configured RSSI threshold, the signal is considered as an interference and the radio gets channel access when the user initiates a new call. However, if the received signal strength is greater or equal to the configured threshold, the channel is considered busy and the radio does not get channel access when the user initiates a new call. It is the responsibility of the site planner or the service provider to set the RSSI Threshold to an appropriate value considering the RF interference and also ensure that the desired signal strength is more than the configured threshold. The default value of RSSI Threshold is -124 dBm. The configurable range is between -124 dBm to -80 dBm. When a value of -124 dBm is selected, subscriber does not get channel access if carrier activity is detected due to interference on the channel when the user initiates a new call. A value of -124 dBm is very sensitive to RF interference.

When operating in IP Site Connect mode, the repeaters also check the channel for interference before transmitting. This is required since even though the source radio checks the channel at one site, it does

not mean there is no interference at another site. Therefore, a repeater checks for Over-The-Air interference before waking up and transmitting. The repeater always acts with an Admit Criteria of Channel Free and has a configurable signal strength threshold. Although one site may be busy, the other non-busy sites continue with the call.

2.2.3.1
Impolite Operation

Impolite operation is also known as the admit criteria of "Always".

When configured for impolite operation, a radio does not check for an idle channel prior to allowing a transmission. From the user's perspective, the radio simply transmits when the PTT is pressed. However, on a digital repeater channel, the radio checks if the repeater is hibernating. Transmission does not proceed, if the repeater is hibernating and the radio is unable to wake it.

NOTE: When a radio is utilizing impolite operation, it is possible that it is transmitting on top of another user's transmission which causes RF contention at the target. When RF contention occurs between digital transmissions, it is impossible to predict which signal is usable. If one transmission is much stronger than the other, it is received instead of the weaker signal. But in most cases, the two transmissions on the same frequency and time slot results in both transmissions being unusable. Thus, it is recommended that only disciplined users are granted the right to use impolite operation. Further, those impolite users are encouraged to utilize the busy channel LED on their radio to determine, if the channel is idle prior to transmitting.

System	Description
IPSC IP Site Connect	When operating in IP Site Connect mode, it is important to understand that impolite channel access only occurs at the local site. If a call is taking place on the IP Site Connect system, and the original source of that call is at the same site as the interrupting "impolite" radio, RF contention occurs and it is unclear which source is successful. If the original source of the call is at a different site from the interrupting radio, the original call continues at all other sites except where the interrupting radio is located.
CPSS Capacity Plus Single Site	When operating in Capacity Plus Single Site mode, the impolite operation is supported only in Emergency Calls.
CPMS Capacity Plus Multi Site	When operating in Capacity Plus Multi Site mode, the impolite operation is supported only in Emergency Calls.

2.2.3.2
Polite to All Operation

Polite to all operation is also known as the admit critearia of "Channel Free".

When configured for Polite to All operation, the radio checks if channels are idle or busy, prior to allowing a transmission. The radio is polite to all analog or digital transmissions, another system's transmission, or other traffic on your system. This option is often used, when there are neighboring communications systems, to prevent radio users from disrupting other transmissions. However, when this option is used, any strong signal on the channel blocks other users from transmitting.

2.2.3.3
Polite to Own Digital System Operation

This criteria applies only to digital channels, and also known as the admit criteria of "Color Code Free".

When configured for Polite to Own Digital System operation, the radio checks for an idle or busy channel, prior to allowing a transmission. This operation is similar to the Polite to All operation with exception that the radio is not polite to analog systems or other system transmissions. It is only polite to other traffic in its own system. This option is often used when there are no neighboring communications systems, or when there is no concern about interfering with radios in neighboring communication systems.

2.2.3.4
Polite to Other Analog System Operation

This criteria applies only to analog channels, and also known as the admit criteria of "Correct PL".

When configured for Polite to Other Analog System operation, the radio checks for an Idle or busy channel, prior to allowing a transmission. This operation is similar to the Polite to All operation with exception that the radio is not polite to analog systems with the same PL. It is polite to other system transmissions. The radio checks for a PL match prior to allowing a transmission.

2.2.3.5
Polite, Impolite or Voice Interrupt In A Call

This is also known as "In Call Criteria", and applies only when the radio is participating in an active call.

The radio can optionally allow others that are part of the call to transmit impolitely (Always), to automatically clear the channel using the Voice Interrupt feature prior to beginning the voice transmission (Voice Interrupt), or to follow the previously configured channel access (Follow Admit Criteria). If configured for an In Call Criteria of Always, the user receives a Talk Permit Tone when they press the PTT while receiving a transmission for them. In other words, a radio has the ability to transmit over another user while listening to their transmission. However, when this happens, the other party does not stop transmitting and therefore RF contention can occur which may corrupt both transmissions. The In Call Criteria of Voice Interrupt is an alternative to the In Call Criteria of Impolite.

The Voice Interrupt option has advantages including the ability to avoid the previously described RF contention issue by clearing the channel prior to beginning a transmission, which yields a higher probability of successfully communicating with the intended target radio(s), as compared with the RF contention encountered with impolite transmissions. However, Voice Interrupt has disadvantages including a longer channel access time when an interruption is necessary, due to the signaling having to complete the interruption and handoff.

If configured for an In Call Criteria of Voice Interrupt, the radio user receives a Talk Permit Tone when PTT is pressed while receiving an interruptible voice transmission and the channel is successfully cleared down. In other words, a radio user has the ability to clear the channel of another user’s interruptible voice transmission before beginning their own voice transmission when both radios are participating in the same voice call (for example, both are members of the same group during a Group Call, or both are participating in the same Private Call). Depending on the radio’s CPS configuration, the radio user whose transmission was interrupted may or may not receive a Talk Prohibit Tone until the user releases the PTT. If the channel is not successfully cleared down, the user typically receives a Channel Busy Tone until the PTT is released.

NOTE: For the Voice Interrupt feature to operate consistently, all radios using the channel should be provisioned with the ability to be interrupted. However, not all need to be provisioned with the Voice Interrupt capability.

If some radios are provisioned without the ability to be interrupted (for example, normally desirable for a supervisor’s radio), then those transmissions cannot be interrupted and the radio user receives a Channel Busy tone if the Voice Interrupt feature is attempted while receiving an uninterruptible voice transmission.

If configured for Follow Admit Criteria and the previously configured channel access (Admit Criteria) is set to either Channel Free or Color Code Free, the user receives a Transmit Denial Tone when they press the PTT while receiving a transmission for them. Users must wait until the user stops transmitting and call hangtime starts before they are granted a transmission. Utilizing the Channel Free Tone helps train users from transmitting too early. Although a setting of Always may be useful for speeding up conversations for well disciplined users, it may cause undisciplined users to “step over” other users. Therefore, it is recommended that most users are provisioned with an In Call Criteria of Follow Admit Criteria.

2.2.3.6
Repeater Wake-up Provisioning

When there is no inbound traffic for a specified duration (Subscriber Inactivity Timer), the repeater stops transmitting and enters an inactive state. In this inactive state, the repeater is not transmitting, but instead it is listening for transmissions. When the user or radio needs to transmit through the repeater, the radio sends a wake-up message to the repeater.

Upon receiving the wake-up message, the repeater activates and begins transmitting idle messages. The radio then synchronizes with the repeater before it begins its transmission.

The repeater wake-up sequence is configurable within the radio. The number of wake-up attempts (“TX Wakeup Message Limit“) and the time between the attempts (“TX Sync Wakeup Time Out Timer”) may be altered if required to operate with other vendor’s systems. It is recommended that these values remain at default while operating on MOTOTRBO systems.

2.3
Digital Voice Features

It is not recommended to delete a contact from the digital contact list because each contact can be tied to a cross-functional fleet of systems and devices communicating together. This may cause the radio to work incorrectly.

2.3.1
Group Calls

The digital group is a way of enabling groups to share a channel without distracting and disrupting one another. Because two-way radios are well suited for “one-to-many” types of calls, the Group Call is the most common call in a MOTOTRBO system. Hence, the majority of conversations takes place within a group.

System	Description
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	The Capacity Plus Single Site and Capacity Plus Multi Site systems allow a radio user to leave a Group Call and start another voice or emergency or control call (for example, Call Alert, Radio Check, Radio Inhibit/Uninhibit, and others) while the radio is busy listening in to a Group Call. The radio moves to the current Rest Channel and starts a new call on the Rest Channel. If a user starts a non-Emergency Call when all channels are busy, then the call fails, and the radio stays on the traffic channel.

Individual radios that need to communicate with one another are grouped together, and configured to be members of a group. A transmitting radio can be heard by all the radios within the same group, and on the same logical channel (frequency and time slot.) Two radios cannot hear each other, if they are on the same logical channel (frequency and time slot) but on different groups. Two radios on different logical channels cannot hear each other, even if they are placed in the same group.

In MOTOTRBO Digital Conventional systems, capabilities for Group Calls are configured with the portable and mobile radio CPS. The repeater does not require any specific configuration for groups. Radios can be configured to enable the user to select among multiple groups using the radio channel selector knob or buttons, or using the radio menu contacts list. Which group a radio user hears on a given channel depends on a configurable parameter called the RX Group List. A call preceding tone can be provisioned to alert the target user of the incoming Group Call. This can be enabled or disabled per Group. An introduction to configuring Group Calls and RX Group Lists is provided in System Design Considerations on page 395 of this document.

Groups are defined according to the organizational structure of the end user. When planning for groups, customers should think about:

- which members of the functional workgroups in their organization that need to talk with one another,
- how those workgroups interact with members of other workgroups, and
- how users will collectively share the channel resources.

Greater detail on the fleetmapping process is provided in System Design Considerations on page 395 of this document.

2.3.2
Private Calls

MOTOTRBO provides the capability for a user to place a Private Call directly to another radio, even if they are not in the same group. However, for this action to take place both radios need to be on the same channel and time slot.

This feature allows a radio user to carry a one-to-one conversation that is only heard by the two parties involved. For example, an employee may use a Private Call to privately alert a specific manager about a security incident, rather than placing a Group Call that would be heard by the whole group. Though Private Calls utilize the signaling capabilities in MOTOTRBO systems to govern which radios are allowed to participate, the use of a Private Call does not necessarily imply the use of encryption or scrambling.

Private Calls can be configured as confirmed or unconfirmed on a per channel basis. For confirmed Private Calls, the calling radio transmits a short control signal message to the target radio. This signaling verifies the presence of the target radio before being allowed to start the call. The receiving user does not need to manually “answer” this signal, but rather the receiving radio automatically responds to the setup request. Once the receiving radio replies to the setup request, the initiating radio sounds a Talk Permit tone and starts the call. The receiving radio sounds a Private Call indication to the user, prior to relaying the received voice. Once a Private Call is set up, subsequent transmissions do not require the call setup messaging. For unconfirmed Private Calls, the calling radio does not transmit any control signaling before being allowed to start the call. Although there is no confirmation the radio is present on the system, an audible indication from the target user may act as confirmation. For example, “Joe, are you there?”, “Yes, go ahead.”.

It is important to understand the advantages and disadvantages of confirmed and unconfirmed operation as it relates to performance. In general, confirming radio presence increases the setup time (voice access time) of a Private Call since the user must wait for the control signaling to go through the radio network before acquiring a talk permit tone. Although this may take more time, it does guarantee that the target radio is present prior to providing the talk permit tone. When operating on an IP Site Connect system that is connected through the public Internet, this time may be longer than when operating on a single site since the control messaging may be traversing through the Internet. If the target radio is scanning or roaming, the setup time of a confirmed Private Call may increase due to the fact that the first control message may not successfully reach the scanning or roaming radio. The second attempt, which contains a preamble, has a higher likelihood of reaching the scanning or roaming radio.

Since unconfirmed Private Calls do not transmit any control signaling, the additional setup time is not required and therefore the voice access time is shorter. Because setup messaging is not used prior to starting the call, it is possible that scanning or roaming radios may arrive late to a call. This could cause the user to miss the first few words of the transmission (no more than what is lost while scanning for a Group Call).

In addition, the user must utilize an audible acknowledgment to validate presence when configured with unconfirmed Private Calls since no control messaging is used to confirm radio presence.

In MOTOTRBO systems, capabilities for Private Calls are configured with the portable and mobile radio CPS. The repeater does not require any specific configurations for Private Calls. Radios can be configured to allow the user to select the recipient of a Private Call using the radio menu contacts list. Private Calls can also be mapped to a channel selection or a programmable button. Users can also manually dial the destination Radio ID with the radio keypad. This means a radio can make a Private Call to any other radio that is on the channel, regardless of whether the radio has created a CPS Private Call entry for the target radio. A call receive tone, or call preceding tone, can be configured to alert the target user of the incoming Private Call. This can be enabled or disabled per individual radio. Greater detail on the fleetmapping process that governs who is allowed to make Private Calls and to whom, as well as an introduction to the CPS configuration section for Private Calls, is provided in System Design Considerations on page 395.

2.3.3
All Call

All Call is a one way voice call between a privileged operator and all users on a logical channel. The transmitting radio utilizes a special All Call group that every radio on the same system and logical channel (regardless of group) receives.

As an All Call is considered a one-way transmission, users cannot talk back to an All Call. If the user transmits after receiving an All Call, they transmit using their currently selected group. An All Call follows the Admit Criteria of the selected channel. More information on the Admit Criteria is provided in Channel Access Configuration on page 527.

All Calls do not communicate across different time slots or channels within the system. The ability to initiate an All Call is only programmed into radios that are used in supervisory roles. All other radios monitor All Call transmissions by default. This feature is very useful when a supervisor needs to communicate with all the users on a logical channel, rather than just a particular group or individual.

In MOTOTRBO systems, capabilities for All Calls are configured with the portable and mobile CPS. The repeater does not require any specific configurations for All Calls. Radios can be configured to enable the user to select an All Call through the radio menu contacts list. All Calls can also be mapped to a channel selection or a programmable button. A call receive tone, or call preceding tone, can be configured to alert the target user of the incoming All Call. Greater detail on the fleetmapping process governs who is allowed to make All Calls, as well as an introduction to CPS configuration section for All Calls, is provided in System Design Considerations on page 395 of this document.

2.3.4
DTMF Hot Keypad

When this feature is enabled, the numeric keypad allows live dialing during dispatch operation. During a voice call, the user can transmit the following characters using a MOTOTRBO radio with keypad: 0 1 2 3 4 5 6 7 8 9 * #. These characters are encoded as dual tone multi frequency (DTMF). These DTMF tones enable the user to communicate with a device connected to a Control Station using the numeric keypad.

This feature is supported in single site conventional, IP Site Connect, Capacity Plus Single Site and Capacity Plus Multi Site system configurations. This feature is also supported by radios in analog mode.

WARNING: A phone patch call needs other call processing requirements in addition to DTMF tones, simply connecting an APP box to the Control Station does not enable the phone patch call capability. If phone patch calls need to be supported, please use the configurations defined in the DTP feature. See Digital Telephone Patch (DTP) on page 457.

2.4

Advantage Transmit Interrupt

The Advantage Transmit Interrupt feature is a suite of features proprietary to Motorola Solutions. This feature generally allows a radio to shut down an ongoing clear Basic Privacy or Enhanced Privacy interruptible voice transmission, and potentially initiate a new transmission. Transmit Interrupt is independent of call type, therefore it applies to Group Calls, Private Calls, Emergency Calls and All Calls. This feature also applies to Private Calls that are initiated through remote monitor command, and Group Calls that are initiated via emergency remote monitor.

NOTE: For software version R01.06.00, this feature is supported on digital direct channels and digital repeater channels.

System	Description
IPSC IP Site Connect	For software version R01.06.00, this feature is supported on IP Site Connect local channels. For software version R01.07.00 or later, this feature is supported on IP Site Connect wide area channels. For IP Site Connect wide area channels, a repeater can use this feature to stop a voice transmission where a radio continues to transmit even after failure of arbitration. This also provides feedback to the transmitting radio that the transmission is not repeated Over-The-Air and allows the radio to participate in a call started by another radio.
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	For software version R01.07.00 or later, this feature is supported on Capacity Plus Single Site system configurations and Capacity Plus Multi Site system configurations.

To support different use cases, Advantage Transmit Interrupt has four unique variations:

Table 4: Advantage Transmit Interrupt Features

Feature	Description
Voice Interrupt	This feature allows a radio that is unmuted to an interruptible voice call, to stop the ongoing voice transmission and initiate its own voice transmission to the same call membership. Voice Interrupt is typically used during a prolonged voice transmission when “late-breaking” or urgent information becomes available, and it is necessary to disseminate the information to the group as quickly as possible.
Emergency Voice Interrupt	This feature allows a radio to stop any ongoing interruptible voice transmission, and initiate its own emergency transmission. Emergency Voice Interrupt gives a radio an improved access to the radio channel, in an emergency condition.
Remote Voice Dekey	This feature allows a radio to stop an ongoing interruptible voice transmission. It is typically used by a supervisor to remotely dekey a radio that is inadvertently transmitting (for example, the PTT is inadvertently pressed for an extended period of time) and occupying the radio channel.

Feature	Description
Data Over Voice Interrupt	This feature allows a third-party data application on an option board or attached PC to control the radio in order to stop any ongoing interruptible voice transmission and initiate its own data message transmission. The application can also specify in the data message, an option to discard itself, if an ongoing voice transmission is not interruptible. This feature is useful in situations where data traffic is more important than voice traffic. Data Over Voice Interrupt is not used by any data applications native to the radio (for example, Text Message, Location, and Telemetry do not use Data Over Voice Interrupt).

While receiving a Direct Mode/Dual Capacity Direct Mode (DCDM) on page 328 transmission, a radio may use the Advantage Transmit Interrupt feature to remotely dekey the transmitting radio and begin its own Direct Mode or Repeater Mode on page 345 transmission. Similarly, while receiving a Repeater Mode transmission, a radio may use the Transmit Interrupt feature to remotely dekey the transmitting radio, and begin its own Repeater Mode transmission. However, the radio may not use the Advantage Transmit Interrupt feature to remotely dekey the transmitting radio's Repeater Mode transmission and begin its own Direct Mode transmission. This scenario is not supported because Advantage Transmit Interrupt dekeys only the radio's transmission within a channel (timeslot), but does not dekey the repeater which remains keyed on the Direct Mode carrier frequency, and supports two channels (timeslots). The repeater is not dekeyed because this may interfere undesirably with a call in the other channel (timeslot) supported by that repeater.

Provisioning of the Advantage Transmit Interrupt feature in general, is separated into two basic categories:

- Radios that have the ability **for voice transmissions to be interrupted**.
- Radios that have the ability **to initiate transmit interrupt commands**.

NOTE: The radios may be provisioned with none, one, or both of these capabilities.

There are a few important items to consider before provisioning of the Advantage Transmit Interrupt feature:

- The Advantage Transmit Interrupt feature is supported in digital direct mode and single site repeater mode
- Because the Advantage Transmit Interrupt features are proprietary to Motorola Solutions and use some proprietary signaling (that is, manufacturer-specific extensions that comply to the ETSI DMR Tier 2 standards), non-Motorola Solutions radios may not be able to unmute to an interruptible voice transmission and Motorola Solutions radios may not be able to interrupt a non-Motorola Solutions radio's voice transmission. Hence, it is highly recommended to assign radios to separate groups and/or channels. This classifies radios provisioned with Transmit Interrupt capability from the radios that are not provisioned with the capability.
- In Direct Mode, Advantage Transmit Interrupt can typically clear an interruptible voice transmission from the channel in less than two seconds. In Single Site Repeater Mode, Advantage Transmit Interrupt can typically clear an interruptible voice transmission from the channel in less than three seconds. The Advantage Transmit Interrupt feature provides one automatic retry in the event that the first interrupt attempt fails due to corrupt signaling (for example, RF coverage degradation, signaling collisions with other radios, and others). The retry essentially doubles the times mentioned. If the radio user still needs to interrupt after the failed retry, the user needs to initiate another service request.
- VOX is not compatible with the Advantage Transmit Interrupt feature. Therefore, VOX is prevented from operating when any of the Transmit Interrupt features are enabled.

System	Description
IPSC IP Site Connect	The Advantage Transmit Interrupt feature is supported on both local and wide area slots of the IP Site Connect mode
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	The Advantage Transmit Interrupt feature is supported on both local and wide area slots of the Capacity Plus Single Site and Capacity Plus Multi Site system configurations. In Capacity Plus Single Site and Capacity Plus Multi Site configurations, an All Call can only be stopped by Emergency Voice Interrupt. Voice Interrupt, Remote Voice Dekey, or Data Over Voice Interrupt features are not supported.

NOTE: For the Advantage Transmit Interrupt feature to operate consistently, all radios using the channel should be provisioned with the ability to be interrupted. If some radios are provisioned without the ability to be interrupted (for example, normally desirable for a supervisor's radio), then those radios' transmissions cannot be interrupted.

2.4.1
Transmit Interrupt Capable System Upgrade

There are several considerations when upgrading a deployed system that presently do not support the Transmit Interrupt feature, to become Transmit Interrupt capable.

NOTE: For systems that use a DR 3000 repeater, the repeater software version must be upgraded to R01.06.00, or later.

For systems that do not use privacy exclusively (Voice and Data Privacy on page 181), radio transmissions with privacy disabled and interruptible voice enabled cannot be received by radios using software versions prior to R01.06.00.

For systems that use privacy exclusively, there are no major concerns receiving radio transmissions with both privacy and interruptible voice enabled; provided the older release supports the type of privacy being used by the radio provisioned with software version R01.06.00 or later.

To minimize service disruption during the upgrade period, systems that do not use privacy exclusively may be upgraded using the following approach:

- Provision new radios with software version R01.06.00 or later. Configure two channels; one channel with Transmit Interrupt features enabled, and the other channel with all Transmit Interrupt features disabled. During the upgrade, the channel with all Transmit Interrupt features disabled is used.
- Individually upgrade previously deployed radios to software version R01.06.00 or later, and provision with the two channels described above. The channel with all Transmit Interrupt features disabled is then used during the upgrade.
- For systems that use a repeater, the repeater may be upgraded to be Transmit Interrupt capable at any time. Finally, once all radios have been upgraded to the compatible software version, the channel with the Transmit Interrupt features enabled is used by all radios on the system.

2.5
Digital Signaling Features

Digital calls utilize digital vocoding and error correction coding processes, and a digital call occupies a single logical channel (frequency and TDMA time slot).

Within a given time slot, the digital call is organized into voice information and signaling information. Included in the signaling information is an identifier used to describe the type of call that is transmitted within the time slot (for example, Group Call, All Call, or Private Call). Signaling information also includes identification information and/or control information, which is used to notify listeners on a voice call of system events and status (for example, the ID of the transmitting radio and the group ID). Because this information is repeated periodically during the course of the call, this embedded signaling allows users to join a voice transmission that is already in progress and still participate in the call. This is referred to as Late Entry, and is an advantage over analog signaling schemes.

2.5.1
PTT ID and Aliasing

The PTT ID and Aliasing feature allows the target radio to identify the originator of a call.

If programmed with the radio Customer Programming Software (CPS), a user friendly alphanumeric name or “alias” can also be displayed. These user friendly aliases are also used when initiating voice calls and digital signaling features. The alias information in the transmitting radio should correspond with the alias information in the receiving radio. The transmitting Radio ID is sent Over-The-Air and, if there is an alias for that ID in the receiving radio, the receiving radio displays the alias. If no alias is configured at the receiving radio for that ID, then only the ID of the transmitting radio is shown.

2.5.2
Radio Enable/Disable

A radio can be enabled or disabled in either of the following ways:

- By another radio, typically in a supervisory role, that sends Inhibit/Uninhibit command using Over-The-Air signaling. This radio-to-radio enable/disable can be done in the following three methods:
  - Device Authentication: Both the target radio (the one to be disabled) and the supervisory radio (the one to disable the target radio), are configured with some keys from the enhanced privacy or AES. Once the target radio receives the inhibit/uninhibit command from the supervisory radio, it sends back a message to challenge the supervisory radio and the supervisory radio responds. If both radios share the same key, the supervisory radio is able to respond correctly then the target radio can be enabled/disabled; otherwise, the target radio can’t be enabled/disabled.
  - User Authentication: This is similar to the Device Authentication. The only difference is that the supervisory user must manually key in a passphrase, when challenged by the target radio, while it is not needed in Device Authentication scenario.
  - Without Authentication: Once the target radio receives the inhibit/uninhibit command from the supervisory radio, it enables/disables itself immediately without challenging the supervisory radio or radio user.
- By a third-party application connected to the system, that sends Inhibit/Uninhibit command using the third-party application.

NOTE: If the target radio is enabled/disabled through either of the methods listed, it can be disabled/enabled through the same or a different method.

2.5.2.1
Over-The-Air Signaling Enable/Disable

The Radio Disable feature can be used to stop any inappropriate use of a radio, or to prevent a stolen radio from functioning. In MOTOTRBO systems, Radio Disable is configured in the portable and mobile radios with the CPS.

To allow a radio to use this function, it must be enabled in the CPS **Menu** settings. To permit (or prevent) a radio from receiving and responding to this command, go to the **Signaling Systems** settings in the CPS.

When disabled, the radio's display blanks and the radio is no longer able to make or receive calls. The radio can still be turned on and off; this indicates that the radio has not failed, but is disabled. Once disabled, a radio can also be enabled through the CPS. All radios are configured to accept Inhibit commands by default, but this can be disabled through the CPS.

For Over-The-Air radio enable signaling to be successful, the target radio must be turned on and be within coverage of the site it was disabled at. This is important since a disabled radio locks onto the site or channel on which it was disabled, even after a power cycle. To receive an enable command Over-The-Air, the radio also has to be within coverage of the site where the disabling occurred. This may also be accomplished by communicating with the radio on the talkaround frequency of the site in which it was disabled.

2.5.3
Remote Monitor

The Remote Monitor feature allows a remote user to activate a target radio’s microphone and transmitter for a period of time. A call is silently set up on the target radio, and its PTT is controlled remotely without any indications given to the end user. The duration that the target radio transmits after receiving a Remote Monitor command is set in the target radio through the CPS. When receiving the Remote Monitor command, the target radio initiates a Private Call back to the originator of the Remote Monitor command.

This feature is used to ascertain the situation of a target radio which is powered-on, but is unresponsive. This is beneficial in a number of situations including:

- Theft
- Incapacity of the radio user
- Allowing the initiator of an Emergency Call to communicate hands-free in an emergency situation

In MOTOTRBO systems, Remote Monitor is configured in portable and mobile radio through the CPS. To allow a radio to use this function, it must be enabled in the CPS **Menu** settings. To permit (or prevent) a radio from receiving and responding to this command, go to the **Signaling Systems** settings in the CPS. When a radio is configured to decode the remote monitor command, the duration that the target radio transmits after receiving a Remote Monitor command is also set in the CPS **Signaling Systems** settings of the target radio.

The Remote Monitor feature may be activated on a disabled radio. Remote Monitor could also be programmed to be activated on radios that are in emergency mode only.

When a radio operates in conventional single site/IPSC system configuration, talkaround mode, or direct mode/dual capacity direct mode, an optional authentication procedure can be added into the remote monitor/ emergency remote monitor operations. After the initiating radio sends out the remote monitor request to the target radio, instead of keying up and responding immediately, the target radio sends a challenge to the initiating radio to ensure the initiating device/user is legitimate. Only after reception of a valid response from the initiating radio, the target radio keys up for the remote monitor procedure. If there is no valid response from the initiating radio, the target radio does not key up, and the remote monitor session ends.

In order to enable this optional authentication procedure, both the target radio and initiating radio must have enhanced privacy or symmetric keys enabled. This authentication does not depend on these privacy features, but it uses the privacy key from these privacy methods.

There are two types of authentication which are the device authentication and user authentication. The authentication type is selected and configured in the target radio through Radio Management (RM)-CPS.

Device Authentication

Device authentication is used to authenticate the initiating radio only, so the authentication is transparent to the initiating radio user and the radio user does not need to take any action.

The target radio is configured to use device authentication. No additional configuration is needed for the initiating radio.

In order for the initiating radio to be a “legitimate” one, in its privacy key set (enhanced privacy or symmetric keys), it must have the privacy key that the target radio uses to generate the challenge. The target radio always uses the first privacy key in its privacy key set that is associated with its current personality. If the current personality is not associated with any privacy method, the radio uses the first privacy key from its radio wide key set pools by the following order: symmetric keys, then enhanced privacy key set.

When the initiating radio user initiates a remote monitor, the target radio sends a message to challenge the initiating radio. Upon receiving the challenge, the initiating radio uses the privacy key in its privacy key set to respond to the challenge. After receiving the response to the challenge, the target radio verifies that the response is correct. If the response is correct, the target radio transmits, and if the response is incorrect, the target radio does not transmit.

User Authentication

User authentication is used to authenticate both the initiating radio and the radio user.

The configuration is the same as the device authentication, except that the target radio must be configured for user authentication and provisioned with an additional passphrase.

For the initiating radio and radio user to be “legitimate”, the initiating radio must have the privacy key, as in the device authentication scenario. Also, the initiating radio user must know the passphrase that is configured in the target radio.

The authentication procedure is similar to that in the device authentication except that: when challenged by the target radio, the initiating radio user must enter the passphrase manually from the radio keypad. If the passphrase entered matches the passphrase provisioned in the target radio, the authentication procedure succeeds, and the remote monitor process continues. Otherwise, the remote monitor process stops, and the target radio does not key up and respond.

2.5.4 Radio Check

The Radio Check feature checks if a radio is active in a system without notifying the user of the target radio. Besides the Busy LED, there is no other audible or visual indication on the checked radio. The receiving radio automatically and silently responds with an acknowledgment to the initiating radio.

This feature is used to discreetly determine if a target radio is available. For example, if a radio user is non-responsive, Radio Check could be used to determine if the target radio is switched on and monitoring the channel. If the target radio responds with an acknowledgment, the initiator could then take additional action such as using the Remote Monitor command to activate the target radio’s PTT.

In MOTOTRBO systems, Radio Check is configured in portable and mobile radios through CPS. To allow a radio to use this function, it must be enabled in the CPS **Menu** settings. All MOTOTRBO radios receive and respond to a Radio Check. This feature cannot be turned off in the CPS.

2.5.5
Call Alert

The Call Alert feature allows a radio user to essentially page another user. When a radio receives a Call Alert, a persistent audible and visual alert is presented to the user. The initiator of the Call Alert is also displayed. If a user is away from his radio at the time of the reception, the alert remains until the user clears the Call Alert screen. If the user presses the PTT while the Call Alert screen is active, they starts a Private Call to the originator of the Call Alert.

For in-vehicle applications, this is often used in conjunction with the Horn and Lights option. When a user is away from his vehicle, a Call Alert can initiate the vehicle's horn and lights to sound and flash, which notifies the user to return to the vehicle and call the originator.

In MOTOTRBO systems, Call Alert is configured in portable and mobile radio through CPS. To allow a radio to use this function, it must be enabled in the CPS **Menu** settings. All MOTOTRBO radios receive and respond to a Call Alert. This feature cannot be disabled using the CPS).

2.5.6
Remote Voice Dekey

The Remote Voice Dekey feature allows a radio user to stop any interruptible voice transmission, except for All Calls. This ability to remotely stop an interruptible voice transmission is provisioned into the radio through the CPS and accessed using a programmable button.

NOTE: For the Remote Voice Dekey feature to operate consistently, all radios using the channel should be provisioned with the ability to be interrupted. However, not all must be provisioned with the Remote Voice Dekey capability.

If some radios are provisioned without the ability to be interrupted (for example, normally desirable for a supervisor's radio), then those radios' transmissions cannot be interrupted and the radio user receives a Remote Voice Dekey Failure Tone if Remote Voice Dekey is attempted while receiving an uninterruptible transmission. The radios that are provisioned without the ability to be interrupted (for example, a supervisor's radio) may still be provisioned with the Remote Voice Dekey feature, which gives those radios the ability to interrupt another radio's interruptible voice transmission.

For this feature, the initiating radio is not required to be a member of the voice call that is being interrupted. Therefore, it is possible to interrupt a voice call, and then initiate a new call to a different group or individual. Once the original voice transmission is terminated via the Remote Voice Dekey feature, the interrupting radio user can initiate a new call through any of the available call initiation methods.

When the programmable button is pressed and an interruptible voice transmission is on the channel, the radio attempts to stop the interruptible voice transmission. If the radio succeeds at interrupting the voice transmission, the radio user receives a Remote Voice Dekey Success Tone when the channel is successfully cleared down. If the radio fails to interrupt the voice transmission, then the radio user typically receives a Remote Voice Dekey Failure Tone. Depending on the radio's CPS configuration, the radio user whose transmission was interrupted may or may not receive a Talk Prohibit Tone until the PTT is released.

2.6
Digital Emergency

MOTOTRBO offers a variety of emergency handling strategies that fits the customer's organizational needs. In its basic form, MOTOTRBO provides the ability for a radio user in distress to send a confirmed emergency alarm message, and emergency voice to a user on a supervisory radio.

The emergency alarm message contains the Radio ID of the initiator. Upon reception of an emergency alarm, the supervisor receives audible and visual indications of the emergency and the initiating Radio ID is displayed. Depending on configuration, emergency voice may follow between the initiator and the supervisor.

Once the supervisor handles the emergency situation (solves the problem), he clears the emergency on the supervisor radio. Once the initiator clears his emergency on the initiator radio, the emergency is considered over.

NOTE: A radio does not roam while reverted to a channel due to an emergency or when Active Site Search is disabled. See Site Roaming on page 163 for details on the interactions between emergency and roaming.

Each mobile radio can program the Emergency Alarm to any of the programmable buttons, whereas for the portable radio the Emergency Alarm can only be programmed to the orange button. The Emergency Alarm can also be triggered externally through a footswitch for a mobile application or any other applicable accessory. Pressing the emergency button causes the radio to enter emergency mode, and begin its emergency process.

When a user presses the Emergency button, the radio gives audible and visual indications to show that it has entered emergency mode. There is a CPS configurable option available, referred to as Silent Emergency, which suppresses all indications of the emergency status on the user's radio. This feature is valuable in situations where an indication of an emergency state is not desirable. Once the user breaks radio silence by pressing the PTT and speaking, the Silent Emergency ends, and audible and visual indications return.

When the user's radio is in the emergency mode, various other features are blocked that may distract him from his communication with the supervisor. For example, the user is not able to initiate other features such as Scan, Private Call, or other command and control functions.

Once the emergency is complete (for example, turn off and turn on the radio, or long/short press of the emergency button depending on the radio configuration) these abilities return.

The emergency sequence is generally made up of two major parts:

- the signaling and
- the following voice call.

The emergency alarm is sent first, and depending on configuration is commonly followed up by an Emergency Call.

An emergency alarm is not a data service, but rather a confirmed command and control signaling that is sent to a group. More than one radio can be configured on the system to monitor that group, and be designated to acknowledge emergency alarms for that group. These radios are considered acknowledging supervisors. There is no user level acknowledgment. The supervisor radio automatically acknowledges the emergency, and provides an alert to the supervisor radio user. There are other radios that are designated to only monitor emergency alarms, but are not permitted to acknowledge them; these users are commonly referred to as non-acknowledging supervisors. Thus, sending the emergency alarm to a group allows for multiple supervisors to receive the emergency alarm indication. It is important that only one acknowledging supervisor should be configured per group and slot; otherwise there may be contention between the acknowledgements.

The supervisors retain a list of received emergency alarms so that they can keep track of multiple emergencies. Once cleared, the emergency alarm is removed from the list, and the next one is displayed. These emergencies are displayed in a last-in-first-out sequence. The supervisor has the ability to hide the emergency alarm list, so he can contact service personnel to attend to the received emergency situation. The channel where the emergency alarm was received is displayed to aid the supervisor when changing channels.

If the user follows up the Emergency Alarm with a voice call while in the emergency mode, his transmission contains an embedded emergency indication. Any radio user can be configured to display this embedded emergency indication. Emergency Calls are always processed with an admit criteria of Always. This allows the Emergency Call to transmit regardless of the current channel activity. If there is another radio currently transmitting, contention may occur.

The initiating radio supports a feature that is tied to silent emergency and the Emergency Call. The "Unmute Option" prevents the radio from receiving voice traffic after initiation of a Silent Emergency. In situations where an indication of an emergency state is not desirable, it is important to be able to mute incoming voice,

that may give away the initiators emergency state. Once the user breaks radio silence by pressing the PTT and speaking, the radio returns to its normal unmute rules.

Silent emergency and the unmute options have no effect on data. It is the responsibility of the end user to make sure data is not sent to a terminal that would divulge any emergency state. Transmission of data does not clear Silent Emergency.

The channel and group on which a user transmits his emergency is crucial to properly contacting a supervisor. MOTOTRBO offers the ability for a user to transmit the emergency on a selected channel or to automatically change to a predetermined channel to transmit his emergency.

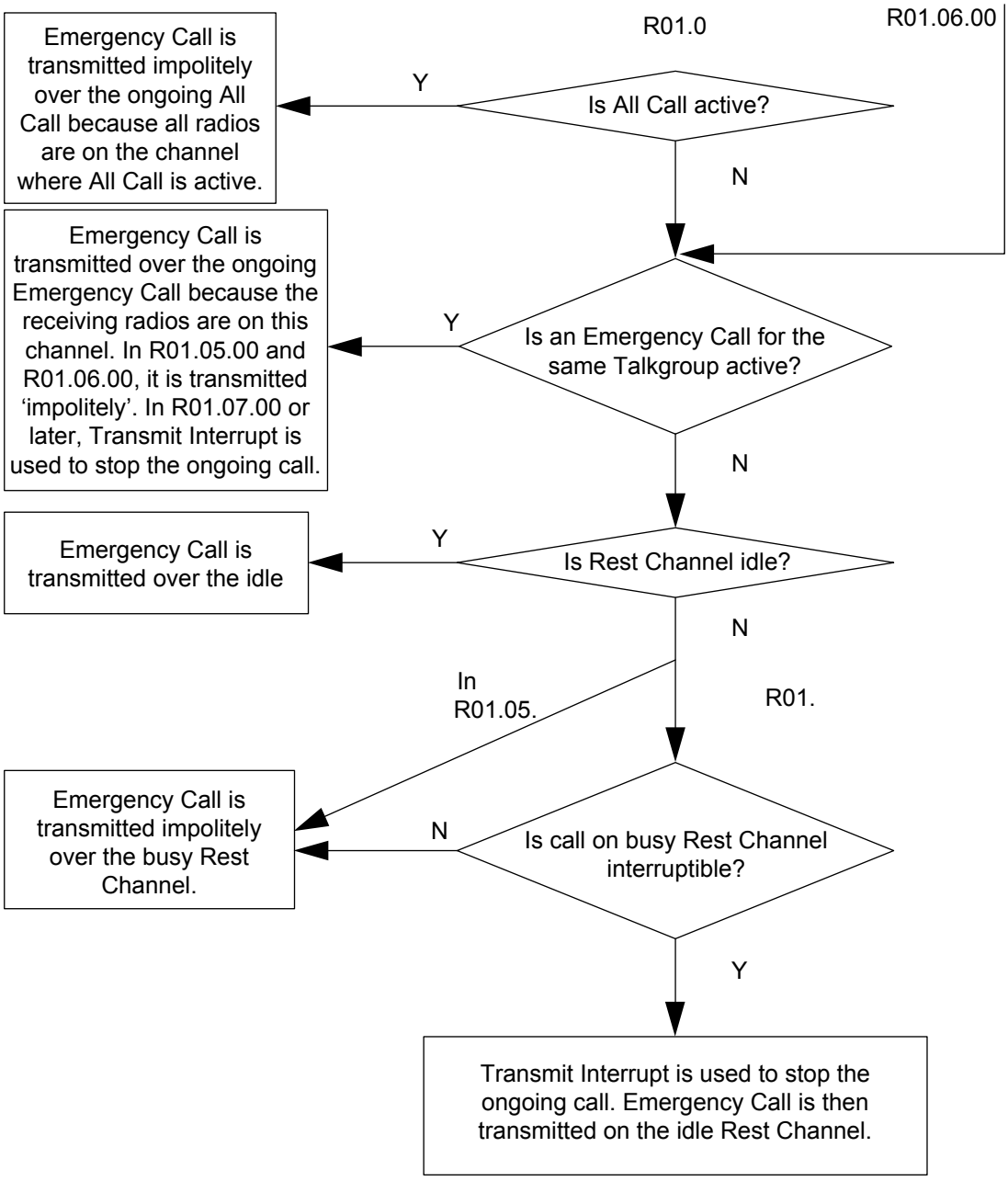
Transmitting an emergency on a selected channel (referred to as a “tactical” emergency) is often useful on small systems where there are only a few groups of users. Each group has its own specified user that handles emergencies.

Automatically changing to a predetermined channel, referred to as “reverting”, is often useful in systems that have a dispatch style emergency strategy. Users in various groups and channels are configured to revert to a specific channel and group to process an emergency. This allows one user to monitor an “Emergency” group, and all other users revert to him in case of an emergency. This minimizes the possibility of supervisors missing emergencies on one channel, while monitoring other channels. After the emergency is cleared, all users revert back to the selected channel they were on before the emergency. In MOTOTRBO systems, the Emergency Revert Channel is configured in portable and mobile radio CPS at the Digital Emergency Systems settings.

System	Description
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	The Capacity Plus Single Site and Capacity Plus Multi Site systems do not support a Revert Channel for emergency. The start of an Emergency Call is announced over all busy channels. This allows a listening radio that is interested in joining the Emergency Call, to leave its channel and join the Emergency Call. A radio is interested in an Emergency Call if the emergency group is either the Tx-Group, or is in the Rx-Group list of the radio. A radio listening to an Emergency Call (for example, e1) joins another Emergency Call (for example, e2), only if the e2’s group has a higher priority than the e1’s group. The first priority is the Tx-Group, followed by any Rx-Group in the Rx-Group list of the radio. The Capacity Plus Single Site and Capacity Plus Multi Site systems ensure that an Emergency Call should start on a channel where the users monitoring the “Emergency” group are present. There are some behavior differences in software versions R01.05.00 – R01.07.00. This is shown in the following flowchart: **NOTE:** In software version R01.05.00, an Emergency Call may not be serviced if ALL of the following scenarios occur: ● All Trunked Channels are busy. ● A call for the emergency talkgroup is active on a channel. ● A radio powers on or joins the system after a long fade and the radio initiates an Emergency Call. In this instance, there is no radio to service the Emergency Call on the busy Rest Channel.

System	Description
	There are three major methods to process the emergency alarm and the Emergency Call; all are configurable through the CPS. They are Emergency Alarm Only, Emergency Alarm and Call, and Emergency Alarm with Voice to Follow. The Capacity Plus Multi Site system handles an Emergency Call at the source site in the same way as in a R01.07.00 Capacity Plus Single Site system. If a Rest Channel is busy at a destination site, and the call is interruptible, then the ongoing call is interrupted for the Emergency Call to proceed. However, if the ongoing call is not interruptible, the Emergency Call starts impolitely. **NOTE:** The impolite Emergency Call is sent to the sites associated with the emergency talkgroup.

Figure 13: Digital Emergency Flowchart



Notes A radio does not provide any audible indication to the user when the radio switches channels. However, the group display on the radio changes.

2.6.1
Emergency Alarm Only

When configured for Emergency Alarm Only, the emergency process only consists of the emergency alarm part. The number of emergency alarm attempts and their admit criteria are configurable, and can even be set to retry indefinitely. The number of alarm attempts are controlled by CPS parameters in the **Digital Emergency System** settings. These parameters include the number of polite and impolite retries. The alarm

is initially sent regardless of channel activity, and once the configured impolite attempts are exhausted, the polite retries are executed when the channel is idle.

The Emergency Alarm Only ends when:

- an acknowledgment is received,
- all retries are exhausted,
- the user manually clears the emergency, or
- the user pushes the PTT.

No voice call is associated with the emergency when operating as Emergency Alarm Only. Pressing the PTT clears the emergency, and a standard voice call is processed.

2.6.2
Emergency Alarm and Call

When configured for Emergency Alarm and Call, the emergency consists of the emergency alarm process followed by the ability to perform an Emergency Call. The number of emergency alarm attempts and their admit criteria are configurable, and can even be set to retry indefinitely. The alarm is initially sent regardless of channel activity, and once the configured impolite retries are exhausted, the polite retries are executed when the channel is idle.

Emergency alarm stops when:

- an acknowledgment is received, or
- all retries are exhausted.

The radio still remains in an emergency state. Any follow up PTT initiates an Emergency Call, and the call includes an embedded emergency indication. If the user presses the PTT before the radio sends an emergency alarm, the radio stops sending the alarm, and starts the Emergency Call. While in the emergency mode, all subsequent voice transmissions are Emergency Calls. The user remains in emergency mode until he manually clears emergency. The only way to reinitiate the emergency alarm process is to reinitiate the emergency.

System	Description
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	The following example illustrates the interaction between an Emergency Call and an All Call: An All Call is occurring on Channel 1, and Channel 2 is the Rest Channel. The radio initiating an Emergency Call leaves Channel 1, moves to Channel 2, and starts the Emergency Call. The start of the Emergency Call is announced on Channel 1. This triggers the radios that want to participate in the Emergency Call to leave Channel 1 and move to Channel 2.

2.6.3
Emergency Alarm with Voice to Follow

When configured for Emergency Alarm and with Voice to Follow, the emergency consists of sending a single emergency alarm, and followed by an automatic transmission of an Emergency Call. This is referred to as hot microphone.

The radio only sends one emergency alarm regardless if there is channel activity, and then without waiting for an acknowledgment the radio immediately activates the microphone and initiates an Emergency Call without the need of the user pressing the PTT. The duration of the hot microphone state is configurable through the CPS in the Digital Emergency Systems settings. This transmission is considered an Emergency Call, and therefore includes the embedded emergency indication. Once this hot microphone duration expires, the radio

stops transmitting, but remains in the emergency mode. Any follow up PTT initiates an Emergency Call, and includes the embedded emergency indication. The user remains in the emergency mode until he manually clears his emergency. The only way to reinitiate the emergency alarm and the hot microphone is to re-initiate the emergency.

It is important to note that when configured for Emergency Alarm with Voice to Follow, the radio continues to transmit voice for the duration of the provisioned hot microphone timer. Since voice has priority over data, any data is queued while voice is transmitting, including the GPS update that was triggered by the emergency. The GPS data cannot be delivered until after the radio stops transmitting voice, and after the repeater hangtime has expired. The GPS data has no additional priority over other data queued in the radios, or over any traffic on the channel. Therefore, its delivery may be delayed if the radio in emergency has pending data queued or if the channel is busy processing other traffic.

It is recommended when utilizing Emergency Alarm with Voice to Follow and GPS, that the hot microphone timer be at maximum 30 seconds. There are a few reasons for this. First of all, data messages do not stay in the queue forever, 30 seconds is short enough so to give the GPS data a chance to be transmitted without timing out. Second, if the hot microphone timer is longer than 30 seconds, and the GPS update rate is around the same value, then other GPS messages may start to fill up in the queue while the voice transmission is processing. This not only occurs with the radio in emergency, but with all other radios since the channel is busy. Therefore when the voice call ends, all radios attempt to access the channel with their GPS data which increases the likelihood of collisions and lost messages. Finally, understand that while the user is transmitting due to its hot microphone timer, there is no way to communicate back to them. Most users can explain their situation in less than 30 seconds and require some feedback from the emergency dispatcher much sooner. That is why it is recommended to keep this value low and if additional monitoring is required, the remote monitor feature can be utilized. Only use a long hot microphone timer in specialized applications.

Also, since the emergency alarm itself is not acknowledged nor retried, its reliability is less than that of the standard Emergency Alarm and Emergency Alarm Only and Call. These considerations should be taken into account when choosing to operate with Emergency Alarm with Voice to Follow.

2.6.4
Emergency Voice Interrupt for Emergency Alarm

The Emergency Voice Interrupt feature, when enabled in a radio, is used during the initiation of an emergency condition when an interruptible voice transmission is already taking place on the channel.

When an emergency is initiated with Emergency Voice Interrupt enabled, the radio attempts to interrupt an ongoing, interruptible voice transmission on the channel. The radio then uses the established procedures for either Emergency Alarm or Emergency Alarm with Call, depending upon the CPS configuration. For the Emergency Voice Interrupt for Emergency Alarm feature, the radio is not required to be a member of the voice call being interrupted.

NOTE: For the Emergency Voice Interrupt for Emergency Alarm feature to operate consistently, all radios using the channel should be provisioned with the ability to be interrupted. However, not all need to be provisioned with the Emergency Voice Interrupt for Emergency Alarm capability.

If some radios are provisioned without the ability to be interrupted (for example, normally desirable for a supervisor’s radio), then those radios’ transmissions cannot be interrupted and the radio user instead transmits the Emergency Alarm in accordance with the configuration of the polite and impolite Emergency Alarm fields in the CPS, if Emergency Alarm is attempted while receiving another radio’s uninterruptible transmission.

If the interruption of the voice transmission is successful, the radio uses the established procedures for either Emergency Alarm or Emergency Alarm with Call, depending upon the CPS configuration, once the channel has been cleared. Depending on the radio’s CPS configuration, the radio user whose transmission was interrupted may or may not receive a Talk Prohibit Tone until the PTT is released.

If the interruption of the voice transmission fails, the radio then uses the established procedures for either Emergency Alarm or Emergency Alarm with Call, depending upon the CPS configuration. However, the

probability of success diminishes because the original voice transmission had not been successfully cleared from the channel.

If the voice call on the channel is not transmitting an interruptible voice signal, the radio uses the established procedures for either Emergency Alarm or Emergency Alarm with Call, depending upon the CPS configuration, again with a lower probability of success.

2.6.5
Emergency Voice Interrupt for Emergency Voice

The Emergency Voice Interrupt feature, when enabled in a radio, is used during the initiation of an emergency voice transmission, primarily when an interruptible voice transmission takes place on the channel and the radio does not belong to that voice transmission.

The radio attempts to interrupt the voice transmission, and then uses the established procedures for Emergency Voice Transmissions, when all of the following conditions are met:

- Emergency Voice Interrupt is enabled.
- The radio is in an emergency condition (for example, the designated Emergency button was pressed previously).
- Another radio's interruptible voice transmission is taking place on the channel.
- The radio in the emergency condition does not belong to the other radio's voice transmission (that is, the radio in the emergency condition is not receiving the other radio's voice transmission).
- The radio user in the emergency condition requests an Emergency Voice Transmission.

The Emergency Voice Interrupt for Emergency Voice feature is not used when the radio belongs to the voice call is being interrupted. Instead, when the radio belongs to the call on the channel (that is, the radio that is receiving the voice transmission), the "In Call Criteria" is used rather than the Emergency Voice Interrupt feature. This is because some systems may disallow radios to interrupt any call to which they belong. In this case, the user must wait until the receiving transmission has finished, before beginning their Emergency Voice transmission.

The Emergency Voice Interrupt for Emergency Voice feature is also capable of interrupting an All Call provided the All Call is transmitting interruptible voice.

NOTE: For this feature to operate consistently, all radios using the channel should be provisioned with the ability to be interrupted. However, not all need to be provisioned with the Emergency Voice Interrupt for Emergency Voice capability.

If the radio succeeds at interrupting the voice transmission, the radio uses the established procedures for Emergency Voice Transmissions, once the channel has been cleared. Depending on the radio's CPS configuration, the radio user whose transmission was interrupted may or may not receive a Talk Prohibit Tone until the PTT is released. If the radio fails to interrupt the voice transmission or the voice transmission is not interruptible, the radio also uses the established procedures for Emergency Voice Transmissions. However, the probability of success diminishes because the original voice transmission had not been successfully cleared from the channel.

2.6.6
Emergency Search Tone

This Emergency Search Tone is optional for all MOTOTRBO radios (version R02.00.00 onwards) excluding MOTOTRBO Light, and can be enabled or disabled via CPS configuration.

This feature is available in direct mode (12.5e or 6.25e) and Conventional Single Site.

System	Description
IPSC IP Site Connect	This feature is available in the IP Site Connect.
CPMS Capacity Plus Single Site and Capacity Plus Multi Site	This feature is available in the Capacity Plus Single Site and Capacity Plus Multi Site.

If enabled, when the radio initiates an emergency, it plays out a loud and attention grabbing tone (Emergency Search Tone), to help people around to locate and identify the emergency initiator. This Emergency Search Tone is for the emergency initiating radio only, and not for the emergency receiving radios. This tone starts when the emergency starts and ends when the radio exits the emergency. The tone is temporarily suspended, when the radio is transmitting or receiving voice/data/CSBK calls.

If enabled, this Emergency Search Tone is played out regardless if the CPS “All Tone Disabled” option is turned on or not.

NOTE: The Emergency Search Tone feature is disabled on a transmitting radio whenever the Emergency Call is acknowledged by a Receiving/Acknowledging radio. If the Emergency Call is not acknowledged, the Emergency Search Tone is emitted by the transmitting radio and continues to be emitted as expected.

This tone is mutual exclusive with the Silent Emergency feature. That is, if the Silent Emergency is enabled for the radio, this feature is disabled automatically regardless if this tone is CPS enabled or not.

Also, it is CPS configurable to specify where to route this Emergency Search Tone/incoming voice, either the radio’s internal speaker or the accessory. When an accessory is not attached, it is always routed to the radio’s internal speaker automatically.

2.7 Restricted Access to System

Restricted Access to System (RAS) supports all existing ADP interfaces and is supported in all MOTOTRBO system configurations including Conventional Single Site.

System	Description
IPSC IP Site Connect	This feature is supported by IP Site Connect
CPSM	This feature is supported by Capacity Plus Single Site and Capacity Plus Multi Site

System	Description
Capacity Plus Single Site and Capacity Plus Multi Site	

This feature supports all existing ADP interfaces and is supported in all MOTOTRBO system configurations including Conventional Single Site.

The Restricted Access to System (RAS) feature prevents unauthorized subscriber users from using the repeaters in the system to transmit to their targeted user or user groups. Additionally, RAS provides limited protection to prevent unauthorized subscribers from listening to any voice/data/CSBK transmission repeated from the RAS enabled repeaters. The unauthorized subscriber device could be a Motorola Solutions subscriber, or a DMR-compatible subscriber from other vendors. However, RAS is not a privacy feature and if voice privacy is a concern, Basic Privacy, or Enhanced Privacy should be used. See Types of Privacy on page 182 for details.

This feature provides two methods to prevent a subscriber from accessing the system: RAS Key Authentication and Radio ID Range Check. These two methods are independent of each other and may be enabled/disabled separately or together. When used together, they provide a robust and flexible way to control the subscribers' access to the system.

2.7.1
Restricted Access to System Key Authentication

In this method, both the repeater and subscriber are configured with a secret Restricted Access to System (RAS) key through CPS.

When a subscriber transmits, the subscriber uses its configured RAS key to encode the bursts. When a repeater receives the bursts, the repeater also uses its configured RAS key to decode the bursts. If the RAS keys in the subscriber and repeater are the same, the repeater decodes and repeats the bursts successfully. However, if the subscriber does not have a RAS key or its RAS key does not match the one configured in the repeater, the decoding process in the repeater fails, and the transmission is blocked at the repeater. Therefore, the bursts from the unauthorized subscriber are not repeated and cannot reach the targeted user or user group.

This method is secure and difficult to break or circumvent, because the RAS ID length ranges from 6 to 24 characters. The algorithm is very robust. However, this method requires CPS configurations in the subscriber's codeplug, resulting in more time and extra effort, when changes have to be made to a fleet of radios.

The RAS key authorization is disabled by default. The following table shows the default settings for RAS configuration in a repeater and a subscriber:

Table 5: RAS Configuration

RAS Configuration	Default Setting
In a repeater all RAS configuration is performed in the 'Security' section and therefore applies to all channels in the repeater.	Authentication = Disabled
	Authentication Key Alias = Default
	Authentication Key = None
In a subscriber, most RAS configuration is performed in the 'Security' section.	Key Alias = Default
	Key Value = 000000 (By default)
In a subscriber the enablement of RAS is on a per channel basis.	RAS Alias = Default (In a channel)

The following are several scenarios when adding these RAS key authentication enabled repeaters/radios into an existing system:

- If cloning is utilized on the device, there are no new configuration steps when deploying into an existing system utilizing RAS or an existing system not utilizing RAS.
- If cloning is not utilized and the existing system is RAS disabled, the RAS enabled repeaters/radios need to be RAS disabled using the CPS/RM tool, before they can be used in the system.
- If cloning is not utilized and the existing system is RAS enabled with a customer chosen RAS key, the RAS enabled repeaters/radios (with the default RAS key) need to be re-programmed with the customer chosen RAS key using the CPS/RM tool.

2.7.2
Radio ID Range Check

In this method, up to 64 Radio ID ranges can be provisioned in the repeaters. Each of these Radio ID ranges may be configured as allowed or left as un-configured. If the Radio ID is within any of the allowed Radio ID ranges when the repeater receives a transmission from a subscriber, the repeater repeats it normally. However, if the subscriber's Radio ID is not within any of the allowed Radio ID ranges, the repeater blocks the transmission. Hence, the transmission from unauthorized subscribers are not repeated and cannot reach the targeted user or user group.

This method only requires configurations in the repeaters. Therefore, it is very easy to make changes quickly. However, an unauthorized user may analyze the radio transmission Over-The-Air, or use other means to guess some allowed Radio IDs and create clones of authorized IDs, thus gaining access to use the repeater.

2.8
Digital Voting

The digital voting feature is the voting solution for MOTOTRBO digital radio systems. To achieve the best voting result, the voting selection is executed at the smallest possible level, known as the burst level, and is called continuous voting. MOTOTRBO digital voting is available in all system configurations including Digital Conventional Single Site.

System	Description
IPSC IP Site Connect	This feature is supported by IP Site Connect
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	This feature is supported by Capacity Plus Single Site and Capacity Plus Multi Site

In a two-way radio system, a receive-and-transmit repeater is typically located at an elevated area such as the top of a hill or tall building, and has a high powered transmitter so that all the subscribers operating within the desired service area can receive signals at an acceptable strength. However, the mobile and portable subscribers typically have considerably smaller transmitted power because of size and cost considerations. The result is that while all the subscribers within the service area of the repeater can receive the transmissions, the repeater may not receive the transmissions from the subscribers, or may receive the

transmissions at signal strengths that are too low to provide reliable communications. In other words, the talk-in range of the repeater is typically significantly less than its talk-out range.

To resolve this imbalance, multiple receive-only repeaters (satellite receivers) can be installed at various locations throughout the service area to relay the radio's transmission to the repeater. Once a satellite receiver receives an acceptable signal transmitted by the radio, the signal can be relayed back to the repeater over the IP network. Then the repeater repeats the relayed signal at a sufficiently high power level such that all radios in the service area are able to receive it.

However, depending on where the transmitting radio is, the repeater itself (via its internal receiver) and other satellite receivers may also receive the radio's transmission at an acceptable signal strength level. In this case, the repeater receives multiple copies of the same transmission from different receivers, selects one best copy of the received transmission, and ignores the rest. This selection is accomplished by a "voting" process. Typically, the voting process analyzes each received signal and determines which one is the best based on the signal-to-noise ratio of the signal or a bit error rate.

By selecting the best signal copy among all the receivers, an additional benefit of voting is reducing the effects of local interference or fading, thus improving voice and data quality.

NOTE: Digital voting is available starting from software version R02.30.02 onwards. Any repeaters or radios prior to those versions must be upgraded in order to operate properly in a voting enabled system. Radios with firmware: R01.11.02 and above for MOTOTRBO, R02.06.04 and above for MOTOTRBO 2.0 are compatible with digital voting.

2.9 CSBK Data

This feature aims to improve the data communication performance and reliability, by using a data transmission method called "CSBK data", whereby a single CSBK is used to transmit the ARS, GPS and XCMP device raw data. The OTA transmission time is reduced to one burst. Therefore chances of channel collision are reduced, and the system capacity of enhanced GPS is enlarged greatly.

An XCMP device can send multiple single CSBKs to other XCMP devices; the same CSBK can be transmitted repetitively to improve reliability.

NOTE: The XCMP device here refers to an option board (OB) or a non-IP peripheral device.

2.9.1 Supported Data Service

The following is a listing of the CSBK data services supported:

- ARS data that originates from the radio or the server.
- GPS data that originates from the radio or the XCMP device targeted to the server.
- Raw data that originates from the XCMP device and targeted to the server.
- Data from XCMP device to XCMP device can be sent as one CSBK or multiple single CSBKs. Multiple single CSBKs are only supported in direct mode.

2.9.2 Impacted Features

The following is a listing of the impacted CSBK Data features:

Enhanced GPS
CSBK data follows the existing Enhanced GPS rule when the window sizes are 5, 6, 7, 8, 9, 10. Enhanced GPS with window sizes 5, 6, 7, 8, 9, 10 are compatible with CSBK data compression. Window sizes 1 and 2 are introduced to generate high data throughput.

Battery Save and Scan Preamble
CSBK data follows the unconfirmed data method for Battery Save and Scan Preamble CSBK. There is no preamble for the CSBK data targeted to the server.

Enhanced Channel Access
CSBK data follows the unconfirmed data method for ECA.

GPS Revert
Location CSBK data follows the unconfirmed GPS data method for GPS revert.

2.9.3
Improved Third-Party Interfaces

The following is a list of improved third-party interfaces categorized by repeater and radio:

- Repeater
  - Repeater Call Monitor – monitors CSBK data
  - Wireline Protocol – routes CSBK data to the wireline gateway
- Radio
  - XCMP – transmits as CSBK data, and transmits at the Enhanced GPS channel
  - ARS – transmits as CSBK data
  - LRRP – transmits as CSBK data

2.9.4
Affected System Components

The following is a list of system components affected by the CSBK data feature:

- Repeater – only supported by MTR3000 and 32 MB DR 3000 Series
- Radio – only supported by R02.08.10.00 and later
- CPS
- MNIS
- ARS (DDMS), LRRP and Raw Data Applications

2.10
Digital Audio

The SLR 8000 repeater provides integrated speaker and connector for an external microphone on its front panel. Digital Audio supports speaker and microphone in digital mode, as done in analog mode. Digital audio features include digital audio receive and digital audio transmit.

Digital audio receive plays back the voice from the speaker when an DMR voice call is repeated at the SLR 8000 repeater. The playback of the receive audio from the speaker is only supported in the Conventional Single Site, IP Site Connect, Capacity Plus Single Site, Capacity Plus Multi Site, Connect Plus, and Capacity Max system configurations. CPS provides configurations for the speaker phone to play back as follows:

- none (digital audio receive at FP is de-activated),

- audio received on slot 0 (one of the two digital channels),
- audio received on slot 1 (another digital channel), or
- mix of audio received on slot 0 and slot 1 (both digital channels).

Digital audio transmit transmits the microphone audio OTA as a DMR voice call. The voice call can be an individual or talkgroup voice call. Digital audio transmit is supported only in a conventional single site system.

The DMR voice call is supported by microphone audio and is a clear voice call without basic or enhanced privacy, and it is not Transmit Interruptible. CPS provides configuration to enable microphone audio to be transmitted on Slot 1 (one of the two digital channels), or Slot 2 (another digital channel). CPS also supports configurations that allow the user to configure the preempt priority of OTA transmitting, among multiple transmission requests. The requests can be from a local audio (front panel microphone), repeat audio (non-emergency voice call), or an emergency repeat audio (emergency voice call). CPS also provides configuration to set a Target ID for the microphone audio transmission. The Target ID includes:

- Call type (individual or talkgroup call)
- Target subscriber Radio ID

2.11
Confirmed Group Data

Confirmed Group Data is the most efficient way of sending a message, when the same data is required to be sent to ‘n’ radios, and then sending one data message to a talkgroup, where all ‘n’ radios are member of the talkgroup. The DMR Protocol does not support confirmation of a data packet sent to a group.

The disadvantage of unconfirmed data packet is that the reliability of transferring the data decreases rapidly as the size of data messages increases. For example, if the reliability of one unconfirmed data burst (12 bytes) is 98%, then the reliability of 32 bursts (384 bytes), is only 52% = (0.98)32.

NOTE: A confirmed data is more reliable because it uses SARQ (Selective Automatic Repeat Request), where the sender tries multiple times to transfer the part of the message, which was received by the target incorrectly.

MOTOTRBO provides a proprietary method to transfer data messages to a group in a confirmed way. The transfer has the following constraints:

- The data messages can be transferred only from a data application (that is only through the MNIS Data Gateway). The source cannot be a radio and it is not sent through a Control Station.
- The maximum number of blocks in the message is limited to 40. This limits the size of the message to 636 bytes, including IP and UDP headers.
- The maximum number of target radios for a message is limited to 200. The target radios must be MOTOTRBO radios.
- The target radios of a message must be members of a talkgroup.
- A radio, which is participating in a Confirmed Group Data suspends the Priority Scan during the Confirmed Group Data.
- The transfer is supported only in the repeater mode (Not in direct mode).
- The transfer is supported only in the single site conventional, IP Site Connect, Capacity Plus, or Capacity Max Systems.

The data application requests to transfer a data message to a set of radios by providing the data payload, a list of recipient radios, and a talkgroup to the MNIS Data Gateway.

NOTE: The destination talkgroup must be an Rx member in all the recipient radios.

The MOTOTRBO system forms and transmits a confirmed packet data unit (PDU) in the same way as an individual data packet. After transmitting the PDU, the system polls all the recipient radios one by one for their acknowledgments on the trunked channel. If the response from one or more radios is negative for the whole PDU or for few blocks, then the system follows the SARQ procedure, which at a high level is similar to the SARQ procedure for individual data packets.

After the SARQ procedure is completed, the MNIS Data Gateway returns to the source (data application) and confirms the success or failure of the transfer for each recipient radio.

In good signal condition (that is when all radios receive the PDU correctly on the first attempt), the method takes (p+r+9) * 0.06 seconds of over the air time; where ‘p’ is the number of blocks in the PDU and ‘r’ is the number of recipient radios.

2.12 MOTOTRBO Integrated Data

This section describes the MOTOTRBO Integrated Data.

2.12.1 MOTOTRBO Integrated Data Overview

When performing in digital mode, any MOTOTRBO radio can be used as an integrated voice and data radio, where the radio can send voice as well as data messages on a given logical channel. This does not refer to data services like enabling users to surf the web, send video images, or synchronize their office desktops. This is not the right technology for such bandwidth-hungry applications. However, it is a great technology for productivity-enhancing applications like messaging, location based services, simple database queries, barcode reading, and fill-in-the-form type of applications. Additionally, it is built into the MOTOTRBO system, so there are no monthly fees or dependencies on public carrier services, and customers control what applications their users can access.

The MOTOTRBO system provides reliable data communications throughout the same areas where the system provides readily usable voice communications. However, there is a trade-off between the desired RF coverage area for data and the data throughput of the system. Extending the range of a system's operation requires more data message retries to successfully complete confirmed transactions, thus lowering throughput.

Integrating voice and data on the same channel brings several benefits. These include:

- Use of one RF channel for both voice and data.
- Use of one system infrastructure for both voice and data.
- Use of one subscriber to send and retrieve both voice and data messages Over-The-Air.

Integrating voice and data on the same channel also brings several considerations. These include the following:

- Traffic loading
- Customer application requirements
- Contention of voice and data.

System Design Considerations on page 395 provides practical guidance on the above considerations.

MOTOTRBO supports data services in a number of ways.

- MOTOTRBO allows radios to send “unit-to-unit” and “unit-to-group” data packets. It supports confirmed and unconfirmed delivery of a data packet. The following table shows the confirmed and unconfirmed mode for all the software versions.

Table 6: Software Confirmed and Unconfirmed Mode

Call Type/Release	R01.01.00 – R01.03.00	R01.04.00	R01.05.00 – R01.06.00
Unit-to-Unit	Confirmed	Confirmed	CPS selectable for a personality. Confirmed (by default)
		Exception: In IP Site Connect, location data is always sent unconfirmed.	
Unit-to-Group		Unconfirmed	

NOTE: If some of the radios are still running on older software versions like R01.00.00 or R01.01.00, then the radios must select the unit-to-unit data as confirmed mode.

- MOTOTRBO also enables infrastructure and/or PC based applications by supporting Internet Protocol (IP) addressing and IP packet data services. Rather than relying upon external modems, MOTOTRBO radios can connect directly to computer equipment with standard USB interfaces. This simplifies and lowers the cost of integrating with applications, and at the same time expands the universe of potential applications that organizations can deploy.
- MOTOTRBO supports a Third-Party Application Partner Program. This program includes a complete application developer's kit that fully describes interfaces for IP data services, command and control of the radio, and for option boards that can be installed in the radio.

For some infrastructure based data applications, the radio must first complete a registration process before data messages can be exchanged between the radio and the infrastructure based application. Registration has no impact on voice operation, aside from utilizing the same channel. Polite voice calls have to wait until an in-progress registration completes before it can use the channel, while impolite voice calls can transmit on top of a registration transmission. A radio does not have to register for voice services. A radio registers when the radio powers up in a data capable mode, or changes into a data capable mode. A radio registers with a Presence Notifier may also be utilized with third-party applications. The Presence Notifier informs the data Application Servers that the registered radio is "on the system" and available for services.

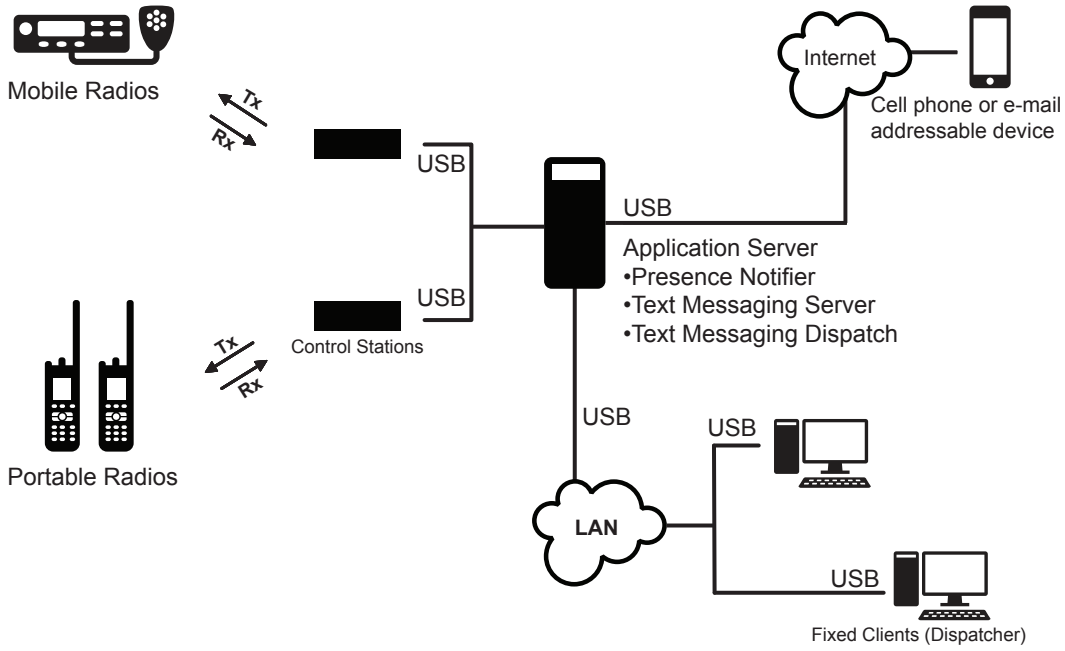
In MOTOTRBO systems, the codeplug configuration determines whether or not a radio attempts to register on the selected channel. This is defined through the ARS parameter which is enabled or disabled through the settings within each channel. It must be set to enabled for those channels that are utilized for data communications with infrastructure based applications. Besides device registration, if enabled through CPS, the radio also allows the radio user to register using their user id with the support from additional third-party application.

2.12.2
Text Messaging Services

Multiple MOTOTRBO system components interact together to deliver text messaging services. These include the built-in text messaging capabilities of MOTOTRBO subscriber radios and the third-party Text Messaging Services application. The services provided by each of these components are described in the following subsections.

The following figure shows a sample MOTOTRBO Text Messaging system configuration. See System Components and Topologies on page 297 for more details on setting up your MOTOTRBO system.

Figure 14: Text Messaging Services



See MOTOTRBO Network Interface Service on page 315 and MOTOTRBO Device Discovery and Mobility Service on page 327 for details on data communication with applications through a repeater network interface, instead of a Control Station.

2.12.2.1
Built-In Text Messaging Service

The built-in text messaging feature allows MOTOTRBO portable and mobile radio users to send and receive information in a text format. This feature provides a useful alternative to voice on the MOTOTRBO system. The built-in text message service is fully accessed from the menu system on MOTOTRBO radio models with keypads and displays. Some aspects of this service are also available to non-display models.

2.12.2.1.1
Services Provided to a Radio User

Using the built-in text messaging services, a radio user can create, send, receive, store and display a text message. The following capabilities are included:

- A radio user can create a text message in one of two ways: Quick text or limited free-form text messages. Quick text messages are pre-defined using CPS. This allows a user to choose from commonly sent messages without having to retype the content. Once selected, the user is allowed to edit any part of the Quick text message prior to sending. The CPS allows you to define 10 Quick Text messages.
- A radio user can select to send a text message to other radios. Messages can be sent to an individual or to a group. When a message is sent to an individual, the sender receives an acknowledgment once the recipient receives the message. If all delivery retry attempts were exhausted, a failure indication will be generated. With messages addressed to a group, the sender only receives confirmation that the message was transmitted and does not receive confirmation from any of the intended recipients.
- When receiving a text message, the user is notified of a new message by an icon, display string, and an audible tone if enabled in the codeplug through the CPS.

- Messages are received only if the radio is currently in digital mode of operation. A radio user should enter Scan mode to receive messages if multiple channels are being utilized. System planning considerations associated with data and scan are discussed in System Design Considerations on page 395.
- A user can store up to 30 received or sent text messages at a time. The user is notified once the Inbox and Sent folder storage becomes full. Once full, subsequent new messages automatically cause the oldest messages to be deleted. Messages are not deleted when the radio is turned off.
- A user can store up to 30 draft text messages in the Drafts folder at a time. Once full, subsequent new drafts automatically cause the oldest draft(s) to be deleted. A user can opt to Send, Edit, or Delete the drafts in the Drafts folder. The user can opt to Save a text message that is being written or edited to the Drafts folder. If a high priority event causes the radio to exit the text message editing screen, the current text message is automatically saved into the Drafts folder. A draft that is sent is deleted from the Drafts folder and stored to the Sent folder.
- The user can scroll through messages and select any message to read, reply to, forward, save or delete.

2.12.2.2
Predictive Text Entry

Predictive text entry is now available for text messaging in MOTOTRBO software version R02.10.00. Previous releases supported the multi-tap input method whereby the user repeatedly presses the same key to cycle through the letters for that key. For example, to type the word “the” using multi-tap method, the radio user presses the buttons “8-tuv”, “4-ghi” twice, and “3-def” twice. However, with predictive text, each key press results in a prediction, therefore they only have to press “8-tuv”, “4-ghi”, and “3-def”, which generates “the”.

Predictive text may take some time to master for some radio users. Therefore, there is an option to return to the multi-tap input method when necessary. Although once mastered, predictive text entry can lower the number of overall keystrokes utilized when typing a text message, making text messaging quicker and easier.

Predictive text also provides additional functions:

Smart Punctuation
For alphabetic languages, the radio includes punctuation intelligently based on the input key. For example, after the radio user presses “2-abc”, “2-abc”, “6-mno”, “1 -,.?” and “8-tuv”, the word “can’t” is predicted.

Word Prediction
The radio can learn the common word sequences the radio user uses often. This function predicts the next word after the user enters the first word of the sequence that is frequently used. This can be enabled or disabled through the utilities menu.

Sentence Capitalization
The radio can automatically capitalize the first word of a sentence for alphabetic languages. This function can be enabled or disabled through the utilities menu.

Word Correction
The radio can supply alternative choices when the input word is not recognized by the radio dictionary. For example, if the radio user incorrectly types “thsi”, the radio autocorrects to “this”. This function can be enabled or disabled through the utilities menu.

Auto Accenting
Mostly used with non-English words, the radio automatically adds an accent to words such as “cafe".

User Defined Words

A radio user can add words that are not in the standard dictionary, such as names, e-mail addresses, and instant messaging IDs.

NOTE: Predictive text is only supported in color display models – the 5-line full keypad portables and the 4-line alphanumeric mobiles in software version R02.10.00 or later. Mobiles require a four-way navigation microphone with keypad.

The following input methods are supported on the 5-line full keypad portables and 4-line alphanumeric mobiles in software version R02.10.00 or later:

Table 7: Input Methods Supported in Full Keypad

Language Keypad	5-Line Full Keypad Portable Support	4-Line Alphanumeric Keypad Mobile Support
Roman Keypad (English, Spanish, Portuguese, French Italian, German, Polish, Turkish, Chinese Pinyin)	✓	✓
Simplified Chinese Keypad (PinYin, Stroke)	✓	✗
Traditional Chinese Keypad (ZhuYin)	✓	✗
Korean Keypad	✓	✗
Cyrillic Keypad (Russian)	✓	✗

2.12.2.3 ETSI DMR Standard Text Messaging

System	Description
IPSC IP Site Connect	This feature is available in IP Site Connect (both local and wide area channels).

To fulfill an optional DMR Standard Text Messaging format interoperability, ETSI DMR standard text messaging is available in addition to (Motorola Solutions) proprietary text messaging. However, DMR standard text messaging has the following limitations:

- works only for radio to radio text messaging;
- available in Conventional Single Site (both local and wide area channels);
- only supported on MOTOTRBO 2.0 radios (including the SL series);

DMR standard or proprietary Text messaging can be selected through a CPS option. The radio can receive both DMR standard and proprietary text messages regardless of the CPS selection. The radio also replies in-kind, meaning the reply follows the received text message format (DMR standard or Motorola Solutions proprietary). However, while initiating a radio to radio text message, the initiating radio always follows the CPS configuration (DMR standard or Motorola Solutions proprietary text message).

2.12.2.4
ETSI DMR Tier 2 UDP/IP Header Compression

There are three choices for header compression: ETSI DMR Tier 2 UDP/IP Header Compression (DMR), Motorola Solutions legacy Header Compression (MSI), or do not use header compression (none). DMR header compression and MSI header compression are not interoperable. DMR header compression is supported only in the newer version radios/repeaters (R02.40.00 or later) of MOTOTRBO 2.0 series, and provides improved retry reliability compared to MSI header compression and should therefore be used in preference with both DMR Tier 2 text messaging and Motorola text messaging but only if supported by all radios in the fleet to maintain interoperability.

Header Compression selection is configurable through CPS. The following are the recommendations for selecting the appropriate option.

- Select ‘DMR’ Header Compression when using ETSI DMR Tier 2 text messaging (the entire fleet supports software version R02.40.00 or later).
- Select ‘DMR’ Header Compression if using Motorola text messaging and the entire Radio and Repeater fleet has software version R02.40.00 or later.
- Select ‘DMR’ Header Compression if the entire Radio and Repeater fleet supports “DMR”, that is, their software version is R02.40.00 or later.
- Select ‘MSI’ or ‘none’ Header Compression if not all the radio/repeater fleet support “DMR”. This is for backward compatibility. Older radios/repeaters (prior to software version R02.40.00) only support MSI header compression or no header compression.
- Select ‘MSI’ or ‘none’ Header Compression if not all the radio/repeater fleet support software version R02.40.00 or later. This is for backward compatibility. Older radios/repeaters (prior to software version R02.40.00) only support MSI header compression or no header compression.

2.12.3
Location Services

The MOTOTRBO location feature allows a dispatcher to determine the current location of a radio on a display map. The dispatcher can obtain the radio’s location alone (latitude/longitude) or the location combined with other information about the environment (horizontal speed, direction, and others) that allows value-added services, such as tracking of resources.

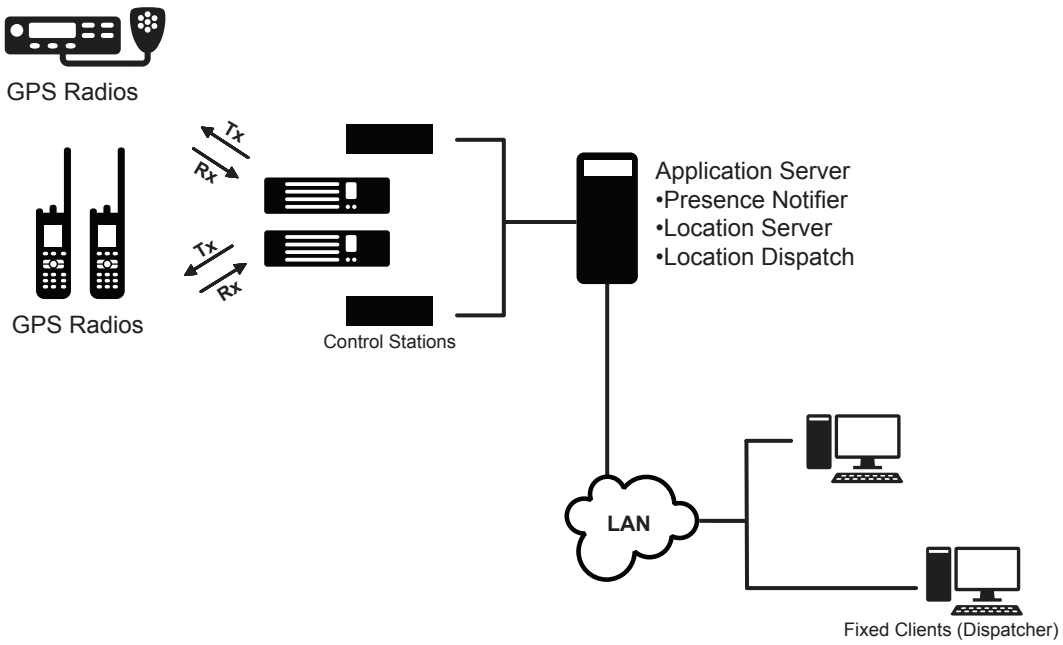
MOTOTRBO systems enable location services through two complementary functions. First, the MOTOTRBO mobile and portable radio portfolio includes models that are equipped with a built-in Global Positioning System (GPS) receiver. The acquisition of location data is done by a GPS receiver inside the radio and is dependent on the GPS receiver receiving accurate signals from the earth-orbiting GPS satellites. However, the GPS receiver may not work well indoors or in environments where the sky is largely obscured.

Using the integrated data services capability of the MOTOTRBO system, GPS equipped mobiles and portables are able to transmit their location coordinates, over the radio system, to a receiving application that displays the radios’ geographic locations on a high resolution map. This third-party receiving application is the second part of the system.

Third-party location service applications are also supported. MOTOTRBO provides a location interface to third-party location services applications.

See MOTOTRBO Network Interface Service on page 315 and MOTOTRBO Device Discovery and Mobility Service on page 327 for details on data communication with applications through a repeater network interface, instead of a Control Station.

Figure 15: Location Services



2.12.3.1

Performance Specifications

Table 8: Performance Specification Accuracy

GPS Transmitter	Portable	Mobile
TTFF (Time to First Fix) Cold Start	< 2 minutes	< 1 minute
TTFF (Time to First Fix) Hot Start	< 10 seconds	
Horizontal Accuracy	< 10 meters	

NOTE: Accuracy specifications are for long-term tracking (95th percentile values > 5 satellites visible at a nominal -130 dBm signal strength).

The definitions for some of the terms stated in Table 8: Performance Specification Accuracy on page 115 are as follows:

Cold Start

A cold start scenario occurs when the radio is first powered up, and the GPS receiver is attempting to acquire its first position lock. In this scenario, the GPS receiver only has a valid almanac stored; it does not have any valid satellite ephemeris data nor valid real-time clock synchronization. Almanac data is stored in a non-volatile (persistent) memory, and is valid for approximately one year. The GPS receiver regularly updates the almanac data; therefore it is always valid unless the radio is powered off for more than one year. The almanac data provides a mapping of the GPS satellites' position in the sky in relation to a real-time clock.

Hot Start

A hot start scenario occurs when the GPS receiver attempts to acquire a new location fix after a previous fix had occurred recently. In this scenario, the GPS receiver has valid satellite ephemeris data, a valid almanac, and valid real-time clock synchronization.

Time to First Fix

Time to First Fix (TTFF) indicates the time the GPS receiver takes to determine its first or subsequent position lock. This is determined largely by the time taken to download a full satellite ephemeris or satellite orientation packet with a data rate of 50 bits per second (bps), as well as, how long it takes for the GPS receiver to reach the relevant satellite in its Scan List. In a cold start, the Scan List includes all of the 24 orbiting satellites. The GPS receiver samples each satellite for a certain amount of time to determine if it is visible or not before moving to the next satellite. The receiver continues to do this until it detects a certain number of visible satellites and can determine an approximate location, thus helping the receiver to truncate the Scan List. In a hot start, the receiver already has most, if not all, the data needed to calculate its position. Therefore, no scanning is needed and minimal downloading is necessary to calculate position, resulting in a lower time to acquire a positional fix.

Horizontal Accuracy

Horizontal Accuracy indicates a radius length from the reported point location. The latitude and longitude reported is equivalent to a point in the center of a circle, with the horizontal accuracy value as the radius of the circle. The true position should be within this location range.

2.12.3.2

Services Provided to a Radio User

When the location service is disabled, the radio does not provide any location updates to a location Application Server. An icon is displayed on the radio if the location service is enabled. The absence of this icon indicates that the location service is disabled. The icon shows a full satellite dish when good GPS signals are detected and an empty satellite dish when the radio is receiving poor GPS signals.

Table 9: GPS Signal Icon

Good Signal	Poor Signal	Disabled
		no icon

The radio does not display its current location on its screen. With the exception of pressing the Emergency button, a radio user cannot trigger a location update to a location Application Server. In general, the radio user does not have to take any action in this process; the radio transmits the location coordinates automatically over the system.

2.12.3.3

Services Provided to a Location Application

For all the services, a third-party location Application Server is required to send an explicit request to the radio. A radio does not provide unsolicited location update to a location Application Server. When the radio turns on and/or selects a properly configured channel (that is, the previously mentioned “ARS Parameter”), the radio registers with the presence service. The location application thus learns that this radio is on the air, and will make an explicit request for location updates if it is configured to track the location of the radio.

The GPS equipped radios transmit an update of their location coordinates over the radio system in response to three service methods which are described in the following table.

Table 10: Service Methods

Service Method	Definition
Single Location Update	The location Application Server wants to know the current location of a radio user. In this case, the application sends a request for a single location update.
Periodic Location Updates	Single location update is used to track the location of a radio user by a location Application Server, but is an inefficient use of air interface. Location tracking allows a location Application Server to periodically get the location of a radio user by sending a single location request that contains the time interval between updates. The radio continues to update its location periodically at the specified time interval until the request is canceled by the location Application Server. The location tracking application can configure the radio to provide updates as frequently as once every 10 seconds. The default value is once every 10 minutes. The rate of update is configurable in increments of one second and must be matched with the resource capabilities of the radio system and the needs of the end-user. This is discussed further in System Design Considerations on page 395.
On Emergency	A radio sends its location after the user triggers an emergency alarm or an emergency alarm and call request. The location update is sent only to the location Application Server which had previously sent an active location request for location updates from that radio upon an emergency event. This location update is sent by the radio only after the processing of emergency is completed. For example, for Emergency Alarm with Call, the location data is only sent after the emergency alarm is acknowledged and the initial Emergency Call is completed. This happens because the location data is sent as a data burst which has lower priority than the voice call.

2.12.3.4
GPS (GNSS) Revert Channel

The GPS Revert Channel feature allows system operators a configurable option to off load radio transmitted location updates onto a programmed digital channel that differs from the digital Selected Channel. This feature effectively removes Location Update traffic from the Selected Channel in order to free up that channel to accommodate increased voice loads and/or to enhance the user experience by reducing the number of channel busies during voice call requests. This feature also allows a large group to communicate on a single voice channel while sending location updates on multiple GPS Revert Channels to accommodate larger Location Update loads. This increases the Location Update throughput associated with radios belonging to a single group.

Each channel programmed into the radio has a configurable CPS option to designate the GPS transmission channel on which it transmits Location Update messages. The CPS options for the GPS transmission channel are **Selected**, **All**, and **None**. Choosing **Selected** means that the GPS updates are transmitted on the current channel. In the case of **All**, a single channel must be chosen from the list of all channels. This chosen channel is known as the GPS Revert Channel and this is where GPS updates are transmitted on. It is understood that there may be instances when the radio is known to be out of range. In order to extend battery life, minimize time away from the Selected Channel, and/or to efficiently use frequency resources in these situations, the radio can also be configured to disable the transmission of Location Update messages on a per channel basis by using the selection **None**. A radio is shown as present to the dispatcher when a radio is switched from a GPS enabled channel to a GPS disabled channel until the presence indication duration is exceeded.

To configure the radio to support Location Updates, there are a few parameters that must be managed correctly. How these parameters interact to dictate the radio's performance is shown in the following table. These parameters are the radio-wide GNSS setting that resides in the **General Settings** CPS folder, and the **ARS** and GPS Revert settings that are present for each channel defined in CPS. In this case, the channel being defined is titled "Channel1". Also, in the case where a GPS Revert Channel (GPS1) is selected, this requires that GPS1 has already been defined as a channel in CPS.

Table 11: Interaction between Parameters to Dictate Radio Performance

General Settings: GNSS	Channels: Zone1 Channel1 ARS	Channels: Zone1 Channel1 GPS Revert	Result
Not Enabled	Not Enabled	Not Selectable	GPS Chip: Disabled Presence: Disabled Location: Disabled
Not Enabled	Enabled	Not Selectable	GPS Chip: Disabled Presence: Enabled Location: Disabled
Enabled	Not Enabled	Not Selectable	GPS Chip: Enabled Presence: Disabled Location: Disabled
Enabled	Enabled	None	GPS Chip: Enabled Presence: Enabled Location: Disabled
Enabled	Enabled	Selected (Channel1)	GPS Chip: Enabled Presence: Enabled Location: TX on Channel1
		GPS1	GPS Chip: Enabled Presence: Enabled Location: TX on GPS1

NOTE: Not Selectable means the setting cannot be configured as the option is grayed out.

2.12.3.5

Enhanced GPS (GNSS) Revert Channel

System	Description
IPSC IP Site Connect	This feature is supported in repeater mode only and works in IP Site Connect mode of operation. Only GPS data (unconfirmed only) is supported on the Enhanced GPS Revert Channel in IP Site Connect mode
CPSM	This feature is supported in repeater mode only and works in Capacity Plus Single Site and Capacity Plus Multi Site modes of operation. In Capacity Plus Single Site and Capacity Plus Multi Site modes,

System	Description
Capacity Plus Single Site and Capacity Plus Multi Site	ARS Registration Message is also supported on the Enhanced GPS Revert Channel.

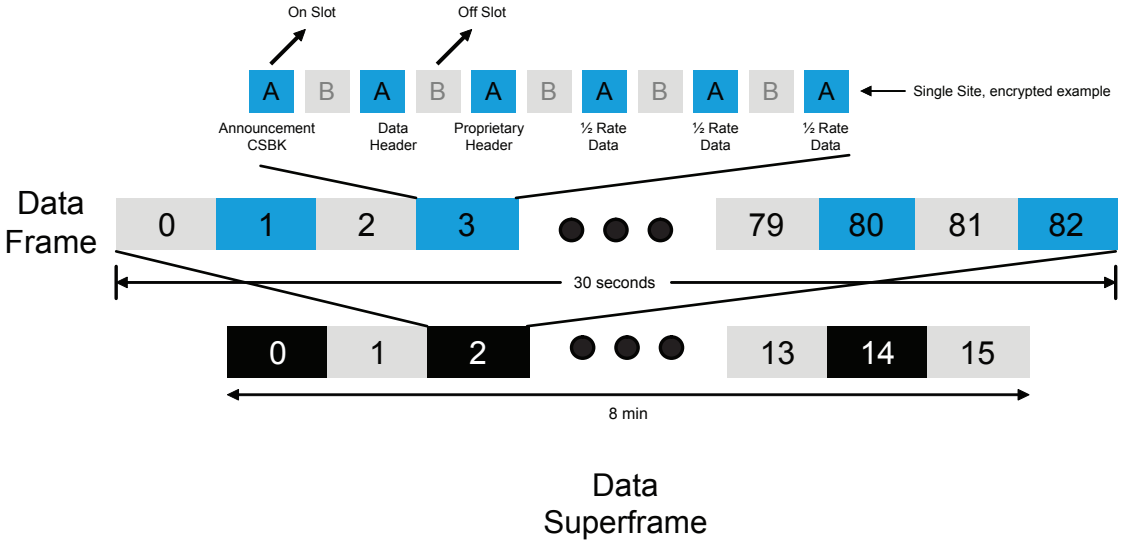
NOTE: This feature is supported in repeater mode only and works in single-site mode of operation. Only GPS data (unconfirmed only) is supported on the Enhanced GPS Revert Channel in conventional mode for single-site mode. There is no support for voice or other non-GPS data on the Enhanced GPS Revert Channel. Data from option board interface is also not supported over an Enhanced GPS Revert Channel.

The Enhanced GPS Revert Channel is an enhancement of the GPS Revert channel functionality that supports higher throughput and increased reliability. Similar to the former feature, a subscriber offloads location responses routed to a server, to a Revert Channel. The primary difference lies in the method a subscriber accesses the channel. In the GPS Revert Channel feature, subscribers access a channel in a desynchronized manner and may therefore cause transmission collisions. The probability of collision increases with the number of transmissions made over the channel and collisions adversely affect the reliability of transmissions.

This enhanced feature enables subscribers to access a channel in a synchronized manner, which eliminate collisions and allow them to use the channel efficiently. The synchronization between subscribers is achieved by a repeater that divides a logical channel into groups of contiguous bursts defined as “windows”. This allows subscribers to make reservations for these windows in which GPS data can be transmitted. This is a slot wide configuration. The windowed data structure consists of an eight minute data superframe. Within the eight minute data superframe, there are 16 data frames, each 30-second in duration This data superframe is repeated over and over again. Both the data frame and superframe always have the same size for every windowed GPS Revert Channel.

Within a 30-second data frame, there are windows that can be reserved by subscribers for GPS data transmission. The number of windows within a 30-second data frame depends on the size of each window. A window consists of an announcement slot in the beginning followed by bursts of GPS data. The following figure shows the windowed data structure for a window size of six (one announcement + five bursts of GPS data).

Figure 16: Windowed Data Structure for a Window Size of Six



The window size is dependent on the amount of GPS data to be sent, the privacy mode and header compression usage. Based on window size, the number of windows in a 30-second data frame is shown in the following table:

Table 12: Number of Windows in a 30-Second Data Frame

Window Size (Includes Announcement Burst)	Number of Windows (in a 30-second data frame)
5	100
6	83
7	71
8	62
9	55
10	50

The CSBK data feature introduces a 7.5-second data frame; within a 2-minute data superframe, there are 16 data frames. This feature compresses the GPS and ARS data into one single CSBK, with window size 1 and is only supported with the MNIS. This is because the repeater's outbound data is not transmitted over the air.

A window size 2 is supported by a Control Station and MNIS. In order to ease system migration when enabling the CSBK data feature, a window size of 5-10 can be considered as it works best with the feature.

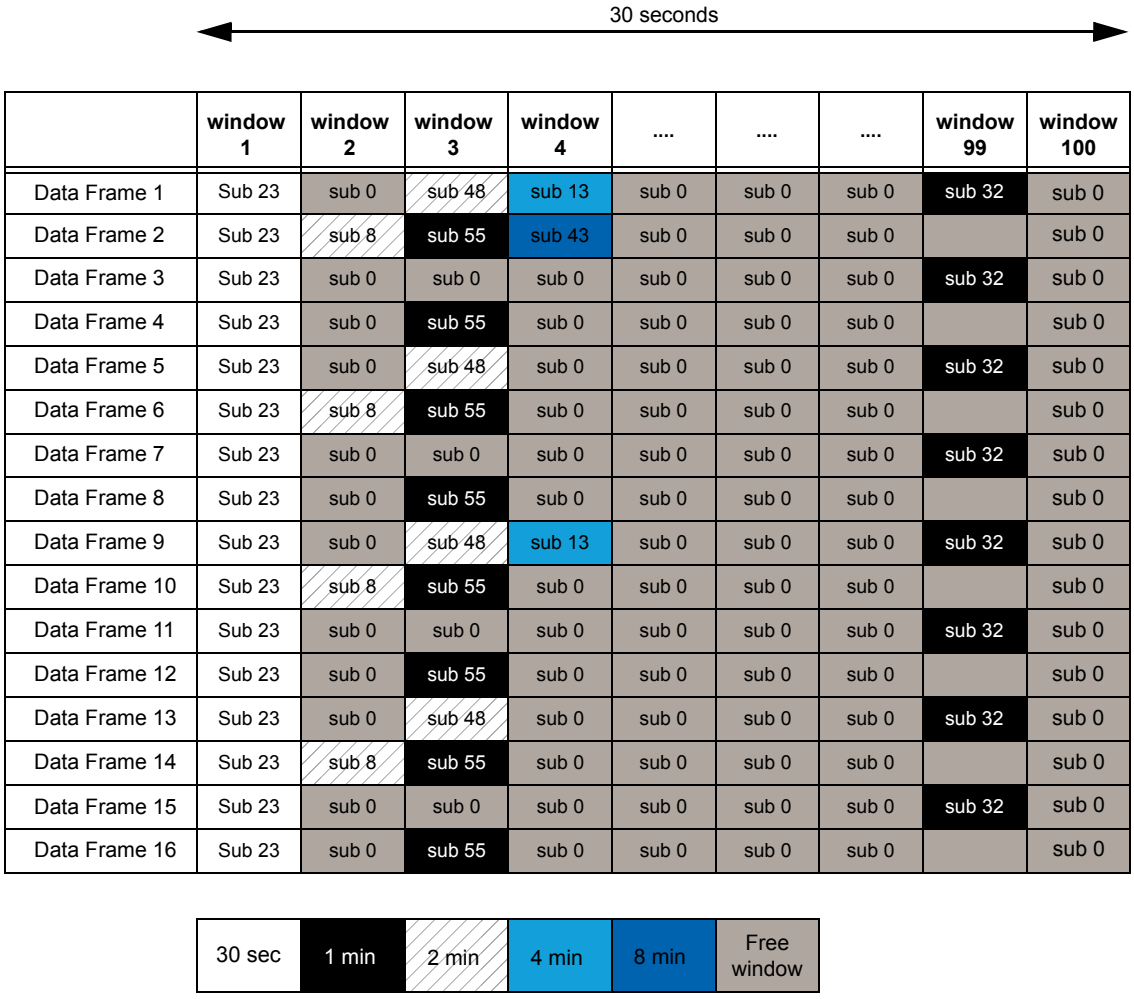
Based on window size, the number of windows in a 7.5-second data frame is shown in the following table.

Table 13: Window Size versus Number of Windows

Window Size (Includes Announcement Burst)	Number of Windows (in a 7.5-second data frame)
1	125
2	62

A repeater's slot that is configured with "Enhanced GPS" maintains allocations of all the windows. At the beginning of every window, the repeater sends an announcement containing the current window number, data frame and the ID of the subscriber for the next reserved window. The following figure shows the scheduling of different subscribers in a window map for a given data superframe.

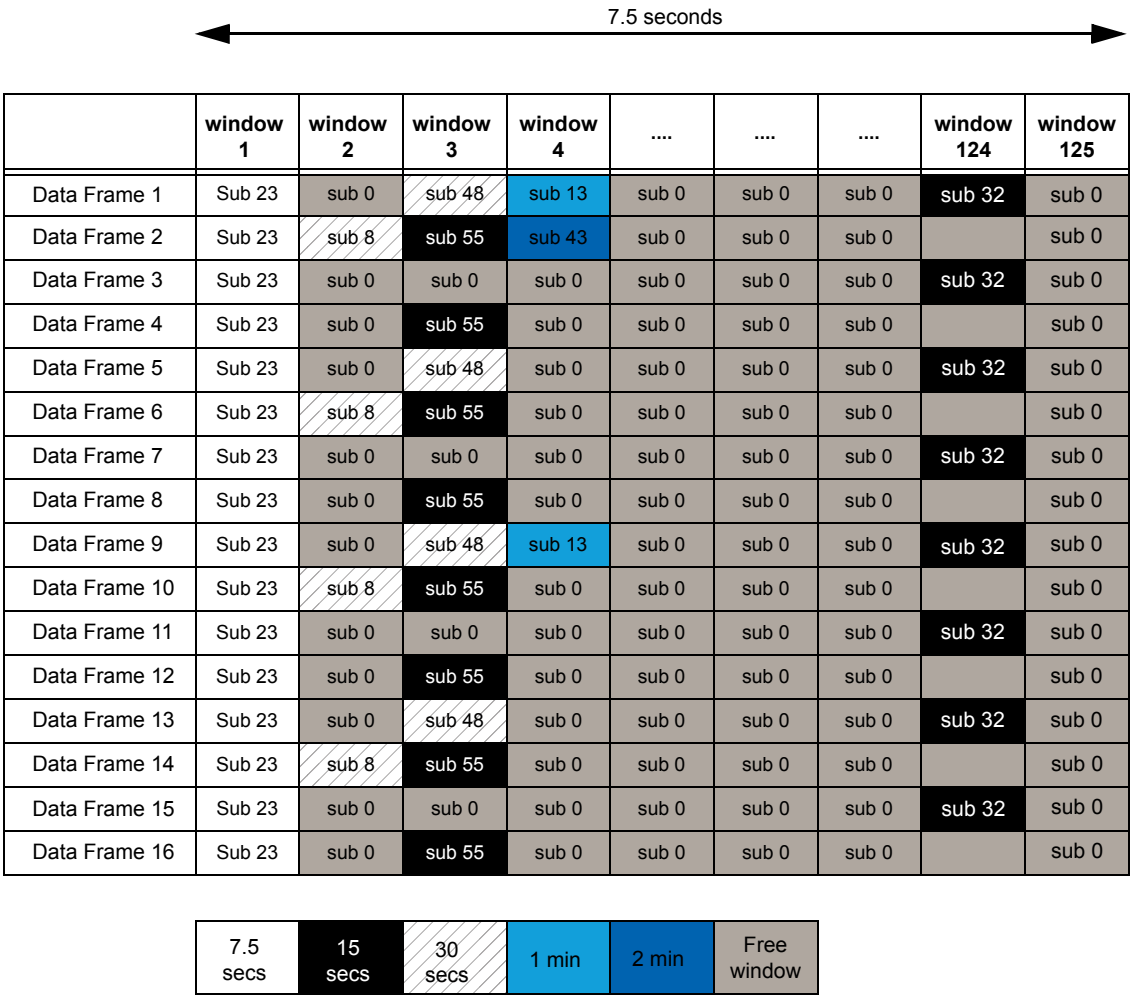
Figure 17: Subscriber Scheduling in a Window Map with 30 Seconds Data Frame



This windowed data structure with an 8-minute data superframe and a 30-second data frame allows this enhanced feature to support update rates of 0.5, 1, 2, 4 and 8 minutes in addition to one-time updates.

The following figure shows the scheduling of different subscribers in a window map for a given data superframe when the window size is 1 with a 7.5-second data frame.

Figure 18: Subscriber Scheduling in a Window Map with 7.5-Second Data Frame



This windowed data structure with a 2-minute data superframe and a 7.5-second data frame allows this enhanced feature to support update rates of 7.5, 15, 30, 60 and 120 seconds in addition to one-time updates.

Before sending a location response, a subscriber requests a window for reservation (for one-time location response) from the repeater, or a set of periodic windows for periodic location responses. The repeater allocates window(s) (if available) and informs the subscriber in a grant message. The subscriber stores the window timing, reverts to the Enhanced GPS Revert Channel before the allocated window arrives, and verifies its reservation by listening to a confirmation grant from repeater. The subscriber then sends its location response in the reserved window.

Since subscribers only send their location response in their reserved windows, collisions do not happen here. The benefits of using Enhanced GPS Revert Channel methodology are as follows:

- Support for up to 360 location responses per minute per repeater using both slots, while running at 90% capacity, and decrease in the number of channels and associated hardware needed for GPS data transmission.
- Increased GPS reliability due to the drastic reduction of collision among subscribers sending GPS data. For more details on reliability based on voice loading on primary channel, see Enhanced GPS Revert – Loading and Reliability on page 414.
- More control over system throughput, by allowing users to choose the most appropriate window size, based on the location response characteristics needed.

- For a window size of 1, support up to 1808 location responses per minute per repeater using both slots, while running at 90% capacity is possible. According to the memory limitation, 3616 radios for a 2-minute update per repeater using both slots cannot be supported, the maximum number of radios allowed is only 2200. If there are more than 2200 radios, it is recommended to configure the two scheduled slots with two repeaters to share the loading.
- For a window size of 2, support up to 896 location responses per minute per repeater using both slots, while running at 90% capacity is allowed.

When the CSBK data feature is enabled, the GPS and ARS data are compressed into a single CSBK data. Window size 1 is only supported by MNIS mode because the window announcement gets transmitted through the repeater's outbound air interface, while window size 2 is supported by both the Control Station and MNIS mode. Window size 2 is supported for Control Station mode, while window size 2 and 1 are supported with the MNIS. A window size ranges from 5 to 10. In order to ease system migration when enabling the CSBK data feature, a window size of 5 to 10 can be considered as it is quite compatible with the CSBK data feature. The size depends on the following factors:

- The parameters that the application has requested in a location response, such as longitude, latitude, time, altitude, velocity, direction, and so on.
- Whether IP/UDP headers compression is enabled.

The following table shows the calculation for the window size with enhanced privacy enabled.

Table 14: Calculation for the Window Size with Enhanced Privacy Enabled

Requested Element	LRRP Response Size (bytes)
Latitude + Longitude	11
Time	6
Request ID **	3
Speed_hor *	3
Direction_hor	2
Altitude *	3
Radius *	2
* Variable sized fields	
** Assume that Request ID value is smaller than 256.	

The following calculations assume GPS data is unconfirmed and "Compressed UDP Data Header" is selected in the CPS.

For No Privacy: *WindowSize* = ((*LRRPResponseSize* + 1) ÷ 12) + 3

For Enhanced Privacy: *WindowSize* = ((*LRRPResponseSize* + 1) ÷ 12) + 4

If a subscriber is out of range or its battery is dead, GPS data is not sent GPS during its reserved windows, so the repeater also has a mechanism to free up the windows reserved for that subscriber. The repeater waits for a certain period of time before releasing the windows and this time is dependent on the cadence rate of the subscriber's location request. The table below summarizes the amount of time the repeater waits before de-allocating windows for a subscriber.

Table 15: Wait Time Before De-Allocation of Windows

Update Rate	Wait Time Before De-allocation (minutes)
30 seconds	5

Update Rate	Wait Time Before De-allocation (minutes)
1 minute	5
2 minutes	10
4 minutes	20
8 minutes	30

In a subscriber, it is highly recommended to keep the Enhanced GPS Revert Channel in the **Channel Pool** in the CPS. This prevents the user from accessing the Enhanced GPS Revert Channel that may affect GPS reliability. A channel can be configured as an Enhanced GPS Revert Channel by selecting the field **Enhanced GNSS** in the channel settings. In order to send responses to the Enhanced GPS Revert Channel, the GPS Revert Channel setting of the home channel has to be set to **Enhanced GNSS**.

In a multisite system with roaming enabled, all sites are recommended to use the same setting and window size as an Enhanced GPS Revert Channel. This can be configured through the Enhanced GPS Revert Channel of the Home Channel.

In a multisite system with roaming enabled, all sites are recommended to use the same setting and window size as an Enhanced GPS Revert Channel. This can be configured through the Enhanced GPS Revert Channel of the Home Channel.

In a repeater, the CPS allows either one or both slots to be configured as Enhanced GPS. The window size in the repeater's Enhanced GPS slot should match the window size in the subscribers. One slot can be configured for regular Data Revert and the other slot can be configured for Enhanced GPS Revert. The repeater CPS also allows a user to choose the maximum percentage of windows that are used for periodic updates. The possible values are 90%, 75%, 60%, and 45%. The rest of the windows are used for one-time updates and also to empty out queued data. When a subscriber is participating in a voice call, chances are it may miss its windows. This leads to windows getting queued up in the subscriber. When this happens, the subscriber can make one time requests to ask for additional windows to empty out its queue.

In a situation whereby a system has heavy voice loading, the subscriber may start to miss their reserved windows quite frequently. Hence, in such a scenario it is advised to run the system at 60% or 45% capacity so the rest of the windows can be used to clear up the queued data. For more information on system reliability based on voice call loading, see Enhanced GPS Revert – Loading and Reliability on page 414.

System	Description
IPSC IP Site Connect	In an IP Site Connect system where a Revert Channel is a wide area channel, only one repeater's slot needs to be selected with periodic window reservation (90%, 75%, 60%, and 45%). For all the other peers (excluding Capacity Plus Multi Site), this value should be set to **None**.
CPMS Capacity Plus Multi Site	In a Capacity Plus Multi Site system where a Revert Channel is a wide area channel, only one repeater's slot needs to be selected with periodic window reservation (90%, 75%, 60%, and 45%). For all the other peers (excluding IP Site Connect), this value should be set to **None**.

For all modes, it is not recommended to have any non-GPS data on the GPS Revert Channel. The only exception is Capacity Plus Single Site and Capacity Plus Multi Site modes where ARS data is also supported on the GPS Revert Channel. The system throughput is dependent on the window size selected for the system and the percentage of windows reserved for periodic updates.

The following table summarizes system throughput:

Table 16: The System Throughput

Window Size	Number of Updates per Minute per Slot			
	90%	75%	60%	45%
1	904	752	600	456
2	448	376	304	224
5	180	150	120	90
6	150	125	100	75
7	128	107	86	64
8	112	93	75	56
9	100	83	66	50
10	90	75	60	45

NOTE: These numbers are based on good signal conditions. The actual throughput and reliability may vary with RF conditions and voice call loading. For more details on loading-reliability relationship, see Enhanced GPS Revert – Loading and Reliability on page 414.

The Enhanced GPS feature can be configured in the following manner:

- Conventional Single-Site Mode
  - One slot for voice, one slot for Enhanced GPS Revert
  - One slot for GPS Revert, one slot for Enhanced GPS Revert
  - Both slots for Enhanced GPS Revert

System	Description
IPSC IP Site Connect	• One slot for voice, one slot for Enhanced GPS Revert • Both slots for Enhanced GPS Revert • Both slots for Enhanced GPS Revert
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	• One slot of data revert repeater for GPS/ARS, one slot for all other data • Both slots for Enhanced GPS Revert

If digital voting is enabled in a system with Enhanced GPS, some of the window sizes cannot be used for the Enhanced GPS feature:

- Capacity Plus Single Site
  - If the system is a single site system, all window sizes 1 to 2 with CSBK data feature enabled, or 5 to 10 may be used. Examples of such systems are Conventional Single Site.

System	Description
IPSC IP Site Connect	• If the system is a single site IP Site Connect system, all window sizes 1 to 2 with CSBK data feature enabled, or 5 to 10 may be used. • For multisite IPSC or Capacity Plus Multi Site, if the IP delay between sites is up to 60 milliseconds, the window size must be 1 or 2 with CSBK data feature enabled, or 7, or bigger. If the IP delay is up to 90 milliseconds, the window size must be 1 or 2 with CSBK data feature enabled, or 8, or bigger. Otherwise, the GPS data may not be transmitted nor received properly.
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	If the system is a single site Capacity Plus Single Site or Capacity Plus Multi Site system, all window sizes 1 to 2 with CSBK data feature enabled, or 5 to 10 may be used.
CPMS Capacity Plus Multi Site	For multi-site Capacity Plus Multi Site, if the IP delay between sites is up to 60 milliseconds, the window size must be 1 or 2 with CSBK data feature enabled, or 7, or bigger. If the IP delay is up to 90 milliseconds, the window size must be 1 or 2 with CSBK data feature enabled, or 8, or bigger. Otherwise, the GPS data may not be transmitted nor received properly.

For more information, see Single Site Conventional on page 355, IP Site Connect Mode on page 361, and Capacity Plus Single Site Mode on page 371.

2.12.3.5.1

ARS Initialization Delay

Upon power on, subscribers normally register with the Presence Notifier by sending ARS messages immediately. In a scenario where a user has a system with many subscribers powering on within a short time, there can be many collisions between ARS registration messages. To reduce collisions, a user can configure the maximum value of an initial random delay for ARS registration through the CPS. This field is called “ARS Initialization Delay” and has a range of 0 minutes to 4 hours with a default value of 0 minutes.

A value of “0 minutes” defines that the ARS registration message is sent out between 5 seconds and 15 seconds and this feature is essentially not delayed (5 seconds to 15 seconds was the existing delay in ARS registration prior to R01.07.00). If a user selects a value of “30 minutes”, then the subscriber randomly chooses a time between 5 seconds and 30 minutes and sends the ARS when this random time elapses. This randomization of time between different subscribers sending the ARS reduce ARS collisions at power on.

When to use:

- This feature can be used with Enhanced GPS to avoid collisions among large number of subscribers sending ARS messages in a short period of time. However, the user must enable “Persistent LRRP Request” in the CPS to ensure that GPS data is still sent even if ARS is delayed.
- This feature can be used in any scenario where large number of subscribers power on, in a short period of time and delay in ARS registration message is permitted.

When not to use:

- This feature should not be used in situations where ARS registration message is immediately needed. For example; text messaging from server to subscriber may not work properly if this feature is enabled.

The following table summarizes the recommended ARS initialization delay value when ARS is sent on the Enhanced GPS channels in trunked systems (Capacity Plus Single Site and Capacity Plus Multi Site modes). The value varies with the window size and periodic loading percentage for the system.

Table 17: Total Number of Radios Sending ARS based on ARS Initial Delay Value

Total Number of Radios Sending ARS based on ARS Initial Delay Value									
Window Size	Periodic Loading (%)	30 mins	60 mins	90 mins	120 mins	150 mins	180 mins	210 mins	240 mins
1	90	100	200	300	400	500	600	700	800
	75	250	500	750	1000	1250	1500	1750	2000
	60	400	800	1200	1600	2000	2400	2800	3200
	45	550	1100	1650	2200	2750	3300	3850	4400
2	90	144	288	432	576	720	864	1008	1152
	75	360	720	1080	1440	1800	2160	2520	2880
	60	576	1152	1728	2304	2880	3456	4032	4608
	45	816	1632	2448	3264	4080	4896	5712	6528
5	90	60	120	180	240	300	360	420	480
	75	150	300	450	600	750	900	1050	1200
	60	240	480	720	960	1200	1440	1680	1920
	45	330	660	990	1320	1650	1980	2310	2640
6	90	48	96	144	192	240	288	336	384
	75	123	246	369	492	615	738	861	984
	60	198	396	594	792	990	1188	1386	1584
	45	273	546	819	1092	1365	1638	1911	2184
7	90	42	84	126	168	210	252	294	336
	75	105	210	315	420	525	630	735	840
	60	168	336	504	672	840	1008	1176	1344
	45	234	468	702	936	1170	1404	1638	1872
8	90	36	72	108	144	180	216	252	288
	75	93	186	279	372	465	558	651	744
	60	150	300	450	600	750	900	1050	1200
	45	204	408	612	816	1020	1224	1428	1632
9	90	33	66	99	132	165	198	231	264
	75	81	162	243	324	405	486	567	648
	60	132	264	396	528	660	792	924	1056
	45	183	366	549	732	915	1098	1281	1464
10	90	30	60	90	120	150	180	210	240

Total Number of Radios Sending ARS based on ARS Initial Delay Value									
Win-dow Size	Peri-odic Load-ing (%)	30 mins	60 mins	90 mins	120 mins	150 mins	180 mins	210 mins	240 mins
	75	75	150	225	300	375	450	525	600
	60	120	240	360	480	600	720	840	960
	45	165	330	495	660	825	990	1155	1320

In conventional mode, when ARS is sent on the Home channel, the table below can be used as a guideline to choose the delay values based on voice call loading and the number of subscribers in the system.

Table 18: Number of Radios Sending ARS Based on ARS Initial Delay Value

Number of Radios Sending ARS Based on ARS Initial Delay Value								
	30 mins	60 mins	90 mins	120 mins	150 mins	180 mins	210 mins	240 mins
No Voice	300	600	900	1200	1500	1800	2100	2400
Low Voice **	51	102	153	204	255	306	357	408
High Voice **	24	48	72	96	120	144	168	192

** See Voice and Data Traffic Profile on page 400 for the definitions of “High Voice”, and “Low Voice”.

In conventional mode with CSBK data feature enabled, the table below can be used as a guideline to choose the delay values. When the ARS initial delay value is zero, the number of radios illustrated in the following table guarantees successful ARS registration of most radios within five minutes. Based on Figure 143: Number of Users per Slot versus User Experience on page 401, a large number of radios can cause poor user experience for voice calls – numbers larger than 102 with a Low Voice profile and numbers larger than 48 with High Voice profile are not recommended.

Table 19: Number of Radios Sending ARS Based on ARS Initial Delay Value

Number of Radios Sending ARS Based on ARS Initial Delay Value									
	0 mins	30 mins	60 mins	90 mins	120 mins	150 mins	180 mins	210 mins	240 mins
No Voice	40	600	1200	1800	2400	3000	3600	4200	4800
Low Voice **	15	102	–	–	–	–	–	–	–
High Voice **	10	48	–	–	–	–	–	–	–

** See Voice and Data Traffic Profile on page 400 for the definitions of “High Voice”, and “Low Voice”.

2.12.3.6
Data Revert Channel

CPSM

A Capacity Plus Single Site system extends the “GPS Revert Channel” feature to the “Data Revert Channel” feature. This feature is available only in Capacity Plus Single Site and Capacity Plus Multi Site modes as a configurable option.

The Data Revert Channel feature allows system operators to offload all data messages from radios to a Server (for example, registration messages, location responses, text messages to the Server, and their Over-The-Air acknowledgments, and others) onto programmed digital channels (called Data Revert Channels). Data messages (including their Over-The-Air acknowledgments) from radio-to-radio and from the Application Server to radios are always sent over the Trunked Channels.

The Data Revert Channel feature is optional. In the absence of this feature, data messages are sent over the Trunked Channels. This feature should be used when there is a need to reduce data traffic from the Trunked Channels. Data Revert Channels frees up the Trunked Channels and the Trunked Channels can accommodate increased voice loads. This also enhances the user experience by reducing the number of busy channels during voice calls.

Data Revert Channels are exclusively used by the system for transporting data packets. They are not used for voice communication. As Data Revert Channels offload most of the data communication from the Trunked Channels, they facilitate more voice communication over these channels. Data Revert Channels are especially useful for transporting location responses.

Each channel programmed into a radio has a configurable CPS option to designate the GPS transmission channel on which the radio transmits Location Update messages. The CPS options for the GPS transmission channel are **Trunked**, **Revert**, and **None**. Choosing **Trunked** means that the data messages to the Server are transmitted on the Rest Channel. In the case of **Revert**, data messages to the Server are transmitted over one of the Revert Channels that are programmed into the subscriber. There may be instances when the radio is known to be out of range. In order to extend battery life, minimize time away from the Rest Channel, and/or to efficiently use frequency resources in these situations, the radio can also be configured to disable the transmission of data messages on Revert Channels by using the selection **None**. To configure a radio to support data messages, there are a few parameters that must be managed correctly. How these parameters interact to dictate the radio’s performance is shown in Table 11: Interaction between Parameters to Dictate Radio Performance on page 118.

2.12.3.7
Global Navigation Satellite System

The Global Navigation Satellite System (GNSS) feature is available for MOTOTRBO 2.0 GNSS models only. This feature adds another independent satellite system (GLONASS or Beidou) to work with GPS.

- GLONASS (Global Navigation Satellite System) is a Russian global satellite system consisting of 24 satellites, designed to provide positioning and velocity determination for government and civilian use.
- Beidou is a satellite navigation system created by the People's Republic of China, named after the Chinese constellation.

GLONASS or Beidou alone is slightly less accurate than GPS. However, the GNSS models, combining GPS and GLONASS/Beidou, improves time to fix (TTF) and accuracy over GPS alone with the increased number of satellites. The Radio menu shows the numbers of GPS and GLONASS/Beidou satellites separately in the GPS info.

The default GNSS setting could be “GPS+Beidou”, “GPS+GLONASS”, “Beidou Only” or “GLONASS Only” depending on the countries that the GNSS radio models are sold. The User can change the GNSS setting through the CPS configuration. A GNSS radio can also be configured with “GPS only” mode, for example for power saving consideration.

2.12.3.8
GPIO Triggered Event Driven and Distance Driven Location Update

GPIO Triggered Event Driven Location Update is triggered by the radio’s GPIO status change. The location information, timestamp and the GPIO Pin Status are combined as one location update. Therefore it’s easy for the location application to know when and where a GPIO Pin status change is triggered.

NOTE: Both features are for MOTOTRBO 2.0 radios only (excluding the SL series)

Distance Driven Location Update is triggered when the distance traveled by a radio from the last update exceeds specific values defined in the location server application. This feature reduces the number of location updates over the air when a radio is not moving or moving slowly.

2.12.4
Telemetry Services

The MOTOTRBO radios incorporate telemetry functionality that is only supported in the digital mode of operation. Both the MOTOTRBO portable and mobile radio support General Purpose Input/Output (GPIO) lines on the radio accessory connector.

With this telemetry functionality, the originating radio can send a telemetry command to another radio. Sending the telemetry command can be triggered either by GPIO pins or a programmable button. In either case, the telemetry command can be sent out on the “normal traffic” channel (for example, the selected channel for single site conventional systems). Alternatively, in firmware versions R01.08.00 and R01.08.10, if the telemetry command is triggered by a programmable button, the telemetry command can be sent out on a CPS configured telemetry channel that is selected from the “Channel Pool” or visible zone channels.

NOTE: When sending the telemetry command on the CPS configured telemetry channel (that is, not the “normal traffic channel”), neither preambles nor retries are used. To avoid missing the telemetry message, it is recommended for the receiving radio not to scan other channels, when listening on the telemetry receiving channel.
Regardless of whether the home channel is analog or digital, when the telemetry revert functionality is initiated via predefined buttons, the radio leaves any ongoing call and initiates the telemetry command transmission on a digital Revert Channel.

Telemetry commands instruct GPIO pins on the target radio to be set, clear, toggle or pulse. The telemetry commands can also be used to query the status of GPIO pins at the target radio.

At the receiving end, the basic built-in telemetry functionality allows the target radio to translate the received telemetry command and to trigger GPIO action. The telemetry functionality also enables the target radio to display a programmed Text Status Message or act on a telemetry command received from the originating radio responding to an event at the originating radio's GPIO pins. The Telemetry Text Status Message is provisioned in the source telemetry radio and is displayed as a pop-up alert at a target radio through the telemetry application. Since the Telemetry Text Status Message is not sent as a standard text message, it is not saved in the Inbox or indexed. Furthermore, its target can only be another radio since it must be received and processed by the telemetry application within the radio.

It is possible for the message to be forwarded to an external computer connected to the radio, or the option board, where a customer supplied application could monitor and take an action. MOTOTRBO provides a telemetry interface for third-party telemetry applications.

Telemetry Over-The-Air signaling utilizes the data service similar to the way that text messaging works. It can co-exist with voice and text messaging. If telemetry messages are expected to occur often, for example 30 radios sending telemetry once every five minutes, this may affect performance of other services on the channel. This should be taken into consideration when determining the data load versus quality of service of a channel.

2.12.4.1
Physical Connection Information

The MOTOTRBO portable offers three GPIO pins, and the MOTOTRBO mobile offers five GPIO pins for telemetry. These GPIO pins can be set to high or low, toggled, or pulsed for a configured duration. A pin can be configured to be active high or active low. It is recommended to use an AC-powered MOTOTRBO mobile for most extended telemetry applications. Motorola Solutions does not currently offer external hardware for telemetry configuration.

The GPIO lines have a 4.7k ohm pull-up resistor tied to a regulated 5 VDC supply within the mobile radio. The regulated supply remains on as long as power is supplied to the mobile, even if the mobile is turned off so the pull-ups are active even when the radio is off.

When configured as input, the voltages of the GPIO lines should be within the range of 0 VDC to 5.5 VDC.

- 0 VDC to 0.8 VDC are interpreted as low level
- 2.2 VDC to 5.5 VDC are interpreted as high level

When configured as output, the GPIO are able to source a current of 1mA maximum at the following levels:

- 4.7 VDC to 5.5 VDC for a high level
- 0 VDC to 0.8 VDC for a low level

2.12.4.2
Telemetry Examples

See Text Messaging in DCDM on page 329 and Telemetry Commands in DCDM on page 331 for diagrams and descriptions of the following simple telemetry examples in both direct and repeater mode.

- Send Telemetry Command from Radio to Another Radio to Toggle an Output Pin
- Send Telemetry Message from Radio to Another Radio when Input Pin State Changes
- Send Telemetry Command to Toggle an Output Pin from Radio to Another Radio when Input Pin State Changes

2.12.5
Data Precedence and Data Over Voice Interrupt

Data applications on the internal option board, or running on an attached PC, are able to request priority treatment of data messages, and Data Over Voice Interrupt independently. To facilitate this, the data application designates the precedence of each data message as being Immediate, Priority, or Routine. When the radio receives a data message for transmission from an internal option board or attached PC application, the radio determines the precedence requested for the data message, and processes the data message accordingly.

The use of the precedence designators can be summarized in the following table:

Table 20: Use of Precedence Designator

Precedence designator	Usage
Immediate Precedence	Used to place data near the top of the queue and request the Data Over Voice Interrupt feature.
Priority Precedence	Used to place the data near the top of the queue without invoking the Data Over Voice Interrupt feature.
Routine Precedence	Used to place the data at the bottom of the queue.

Immediate precedence is used to automatically clear the channel of voice calls by using the Data Over Voice Interrupt feature prior to beginning the data transmission. This capability departs from the typical behavior of a radio system, which normally gives priority to voice calls over pending data calls. Depending on the radio's CPS configuration, the radio user whose transmission was interrupted may or may not receive a Talk Prohibit Tone until the user releases the PTT.

For the Data Over Voice Interrupt feature to operate consistently, all radios using the channel should be provisioned with the ability to be interrupted. If some radios are provisioned without the ability to be interrupted (for example, normally desirable for a supervisor's radio), then those radios' transmissions cannot be interrupted, and the data message are placed near the top of the data queue (behind any existing queues for Immediate precedence data messages). When Immediate precedence is designated and a data (or control) transmission occupies the channel, the radio must wait for the channel to become clear before initiating the data transmission.

Priority precedence is used to ensure that the data message is transmitted before any Routine precedence data messages, and after any existing Immediate precedence data messages. Priority precedence does not use the Data Over Voice Interrupt capability. When either Priority or Routine precedence is designated, the radio must wait for the channel to become clear before initiating the data transmission.

NOTE: The Data Precedence and Data Over Voice Interrupt features do not need to be configured in the radio or repeater via the CPS because these features are always available.

For more information on the Data Precedence and Data Over Voice Interrupt features, please refer to the MOTOTRBO Option Board ADK Development Guide on the MOTODEV Application Developers website https://mototrbodev.motorolasolutions.com

2.12.6
Enhanced Job Tickets

MOTOTRBO Job Tickets also known as "Work Tickets" allow the system dispatcher server application to manage the flow of tasks by sending and assigning Job Tickets (tasks) to one or multiple radios. The radio users work on the assigned tasks and move the tasks to different preconfigured states such as "New" state, "In Progress" state, and others, according to the progress of the tasks. The modified tasks are sent back from the radio to the dispatcher Application Server.

A number of MOTOTRBO application developer program solutions can create and manage job tickets which makes this feature extremely useful in service organizations (for example the hotel staff, taxi, security staff, and others). The enhanced Job Tickets application is not compatible with the legacy Text Message based Job Tickets application.

2.12.6.1
Job Tickets Registration

The Subscriber Unit ID (SUID) and User ID registrations are supported through the ARS registration system topology. The PC Job Tickets application supports the Conventional, IP Site Connect and Capacity Plus Multi Site ARS Presence Interface. The PC Job Tickets presence application may register to the Presence

Interface for receiving the Radio subscriber's presence (SUID and User ID) and associate them for device and user level Job Tickets management. Job Tickets Registration is also supported on the Conventional system.

System	Description
 IP Site Connect	The Job Tickets Registration is supported on IP Site Connect mode.
 Capacity Plus Multi Site	The Job Tickets Registration is supported on Capacity Plus Multi Site mode.

2.12.6.2

Common Job Tickets Data Communication

An Enhanced Job Tickets Protocol (EJTP) specification is defined for message exchanges between the communicating devices. The JTP can be communicated over a variety of transport mechanisms. The messages exchanged by JTP are XML documents. The design allows for extension to support future Job Ticket requirements. Job Tickets Data Communication is also supported on the Conventional system.

System	Description
 IP Site Connect	The Job Tickets Data Communication is supported on IP Site Connect mode.
 Capacity Plus Multi Site	The Job Tickets Data Communication is supported on Capacity Plus Multi Site mode.

In order to address the limited OTA Radio network bandwidth available, the encoding of JTP messages are based on the Motorola Solutions Binary Extensible Markup Language (MBXML) for OTA LMR Radio network transfer. MBXML was explicitly designed to efficiently encode JTP XML documents.

The Subscriber Unit supports a Radio Management (RM) configurable Job Tickets Application Server SUID and UDP port for the Subscriber Unit, for sending Subscriber created Job Tickets to the Application Server. The MNIS application supports routing of the Job Tickets data application to the connected Job Tickets application. The JT Application Server IP address is derived from the Subscriber IP address mapping scheme. The Subscriber Unit sends locally created ticket to this IP address. See the following examples:

- CAI Network = 10 (RM configurable)
- JT Server SUID = 2 (RM configurable)
- JT Server IP Network = CAI Network + 1 (derived)
- JT Server IP Address = (JT Server IP Network + JT Server SUID) = (11.0.0.2) (derived)

The Subscriber Unit supports a fixed internal receive UDP port (0x0FAD), for receiving Job Tickets Protocol IP datagram. The PC Job Tickets server application can send tickets to an individual or a group of Subscriber Units through the MNIS interface. When the Subscriber Unit sends the response to the received Job Ticket, it uses the source IP address and UDP port from the received message as the destination address and port.

The Subscriber Unit supports a CPS/RM configurable “Forward to PC” function for forwarding the Subscriber Unit received Job Tickets UDP datagram to the Subscriber connected PC network (that is the CAI+1 network) as a pass-through operation. All Job Tickets targeted to the Subscriber internal Job Tickets UDP port and IP address are forwarded to the locally connected PC network.

The Job Tickets application IP datagram are sent through the system Trunk Channel between the Subscriber Unit and the MNIS. The MNIS application supports the routing of the data to/from the PC Job Tickets application. The maximum Job Ticket data payload size is 1000 bytes.

2.12.6.3
Common Job Tickets Inbox Folders

The Subscriber Unit supports storing or sorting two types of Job Tickets Menu inbox messages like “My Tasks” and “Shared Tasks”. The “Shared Tasks” is a public type which could be accessed by any user. The “My Tasks” is a private type which can only be accessed by the matching User ID that has logged in to the Subscriber Unit. Job Tickets Data Communication is also supported on a Conventional system.

System	Description
IPSC IP Site Connect	The Job Tickets Data Communication is supported on IP Site Connect mode.
CPMS Capacity Plus Multi Site	The Job Tickets Data Communication is supported on Capacity Plus Multi Site mode.

The Job Tickets dispatcher server application sends the tickets to the specified User ID or as a public message type. If the dispatcher sends the ticket to the specified User ID and the user is not logged in, the Subscriber Unit just stores the message without providing any user feedback. When the matching User ID is logged into the Subscriber Unit, the private messages are accessible.

The Status Folder are CPS or RM configurable for the Job Tickets inbox messages. Both “My Tasks” and “Shared Tasks” folders share the same Status Folders configuration. The Job Tickets Inbox stores up to 500 received messages for both “My Tasks” and “Shared Tasks”. When the Job Ticket status is modified, the Subscriber Unit sends a response message to the server application and move the ticket to the corresponding Status Folder. When the Subscriber Unit’s Job Ticket Inbox is full, the oldest completed task will be deleted for storing the new incoming message. The Subscriber Unit sends onetime broadcast message for the deleted message to the Job Tickets server application.

2.12.6.4
Subscriber Created Job Tickets

The Subscriber Unit supports the creation of new Job Ticket, and sends it to the preconfigured Job Tickets server application IP Address and UDP port.

The new ticket creation is governed by the CPS or RM preconfigured templates. After the ticket has been sent to the server application successfully, the ticket is stored in the Job Ticket outbound “Sent Tasks” folder.

A success or failure icon is used for message sent status. The user can resend the failure messages through the Sent Tasks menu. The Job Tickets “Sent Tasks” folder can store up to 30 created tickets. When the “Sent Tasks” folder is full, the oldest ticket is deleted to allow a newly created ticket to be stored.

2.12.6.5
All Job Tickets Deletion

The portable or mobile radio supports a Customer Programmable Software (CPS) or Radio Management (RM) configurable field, for deleting all Job Tickets at power up. If Delete All Job Tickets is enabled, the radio deletes both public and private Job Tickets at power up.

2.12.6.6
MNIS Network

The following are the three types of MNIS Networks:

CAI Network

This field must be the same as CAI (Comment Air Interface) Network assignment of the radios. The radio has multiple CAI IP addresses such as Internal Network Address, External Network Address, and Bluetooth Network Address. The addresses are Class A addresses using the network IDs such as CAI Network, CAI Network+1, and CAI Network+2. As a default CAI Network setting, the CAI IP addresses have Class A network IDs of 12, 13 and 14. Typically one would leave the assignment to the default unless the radio IP addresses resulting from the default setting would conflict with IP addresses of other devices on the customer’s network. For more information, see MOTOTRBO Network Interface Service (MNIS) and Device Discovery and Mobility Service (DDMS) on page 489.

CAI Group Network

This field must be the same as CAI (Comment Air Interface) Network assignment of the talkgroup, and also must be the same as CAI Group Network assignment of the radios. The talkgroups have Multicast IP addresses with network ID of CAI Group Network. The consideration are similar as CAI Network applies for CAI Group Network.

Job Tickets UDP Port

This field represents the Job Tickets Data Application UDP port. Since most of the MOTOTRBO Job Tickets applications use this port as default, typically a user leaves the assignment to the default. If there is port conflict, this port could be changed.

NOTE: See Data Applications and MNIS Deployments on page 499 for other MNIS configuration to deploy a system.

2.13
Indoor Location

This section describes the indoor location operation in conjunction with the outdoor location support, such as GPS.

The indoor location feature is supported in Single Site Capacity Plus, Multi Site Capacity Plus, IP Site Connect, Capacity Max, Connect Plus, and Conventional digital operation modes. The indoor location configurations and operation along with outdoor location operation are described in this section.

NOTE: Indoor location updates cannot be sent over CSBK calls.

2.13.1
iBeacon

iBeacon is Apple's implementation of Bluetooth Low Energy (BLE) wireless technology to create a different way of providing location-based information and services to iPhones and other iOS devices.

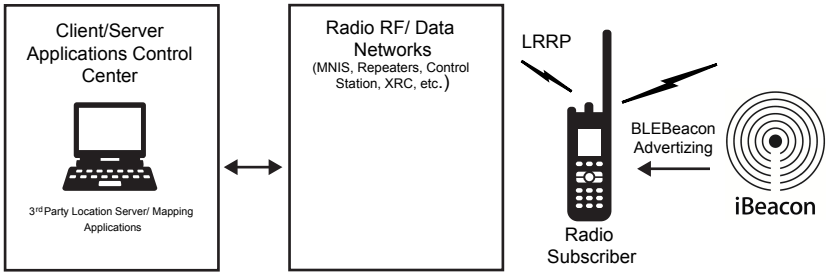
The iBeacon is the dominant beacon devices in the market today. The iBeacon is not the only beacon device on the market. There are other non-Apple beacons in the market, but MOTOTRBO only supports iBeacon in release 2.5. Apple does not develop the beacons. They are manufactured by third-parties such as Estimote, Roximity & Gimbal. Estimote is the preferred iBeacon vendor for MOTOTRBO internal test and development.

2.13.2
Indoor Location Operation

MOTOTRBO radio software listens for the signal transmitted by the ibeacons and it sends the data from the radio to the server application, which requested for the beacons data. The beacons data are mapped to the strategically deployed indoor location, and presented to the user via a mapping application.

The indoor location operation leverages the same outdoor (that is, GPS) location request/response system topology and LRRP protocol to support both indoor and outdoor location request/response messaging. The indoor location data is encapsulated in the LRRP protocol with or without the outdoor (that is, GPS) location data. Thus, either indoor and/or outdoor data can be requested by the LRRP initiating application. The radio sends a response message according to the LRRP request. The LRRP initiator can request for one or more iBeacon data set.

Figure 19: Indoor Location Operation



2.13.3
iBeacon Configuration and Operation Parameters

When selecting an off-the-shelf iBeacon for indoor location deployment, it is recommended that the following iBeacon device protocol attributes and operation parameters should be programmable:

UUID
Is a region identifier that distinguishes your iBeacons from others.

Major
Is used to group a related set of iBeacons for location mapping.

Minor
Is used to identify an individual iBeacons for location mapping.

Tx Power
Two's complement of measured beacon Tx power. The actual Tx power can be calculated as a two's complement of the data: (0xC5 = 197 => 256-197 = -59 dBm). Tx power is the strength of the signal measured at 1 meter from the iBeacon.

BLE Advertisement Time Interval

Specifies the beacon periodic advertisement broadcast interval.

NOTE: It is important to understand that there is a beacon battery life. When the beacon device is configured for more frequent broadcast transmission, it consumes more power.

Omni-Directional Antenna with Configurable Range.

Specifies the configurable range for Omni-Directional Antenna.

NOTE: Not all parameters are used for their indoor location deployment, as it depends on the customer's requirements.

2.13.4
iBeacon Deployment Considerations

When selecting an off-the-shelf iBeacon for indoor location deployment, it is important that the device vendor provides the software tools for the remote fleet management and analytics.

For example, Estimote provides a fleet management tool (iOS and Android base) for batch beacon update. Once the user starts the batch update, new configurable settings are applied to beacons when the user is in range. The update continues in the background, therefore the Estimote application does not have to be active during the process. When the user leaves the range of beacons, the update stops and then seamlessly continues in the background once the user is back in range. The application remembers the beacons, which are pending update. Estimote provides iOS and Android base application for beacon site survey proposes, and it can even modify the beacon configurable parameters as needed.

2.13.4.1
iBeacon UUID and Radio Operation Considerations

The iBeacon vendor ships the iBeacon devices with the same vendor UUID in all iBeacon devices. When deploying a system, the site must be surveyed to track for other people's iBeacon devices to ensure your iBeacon UUID is not the same as the other collocated party's iBeacon devices.

Only the desired UUIDs are programmed into the Radio for iBeacon device detection. The iBeacon devices must be programmed with the same UUID within the same site or region. If the site happens to have two different iBeacon system deployments with the same UUID, and the radio detects the other party's collocated iBeacons, it impacts the radio iBeacon device detection performance, buffering scheme, and unnecessary Radio OTA report overhead. When the radio detects the UUID from a different iBeacon system deployment, the third-party mapping application filters for their deployed unique iBeacon Major or Minor value for mapping purpose.

2.13.4.2
iBeacon BLE Advertisement Time Interval and Radio Scan Mode Operation Considerations

The following are the iBeacon BLE Advertisement Interval Rate and Scan Mode Operation parameters considerations:

Scan Mode

Is a Radio Management (RM) or Customer Programmable Software (CPS) configurable parameter. This field is used for configuring the Bluetooth advertisement scan bandwidth. When "Normal" is selected, the radio uses 50% of the 100ms Bluetooth scan advertisement bandwidth to perform scan within the "Scan Interval On Time". If "Aggressive" is selected, the radio uses 75% of the 100ms Bluetooth scan advertisement bandwidth to perform the scan within the "Scan Interval On Time". The "Scan Mode" is only available when the radio is not associated to a Wi-Fi access point. If the radio is associated to a Wi-Fi

access point, then the radio automatically uses only 20% of the 100ms Bluetooth scan advertisement bandwidth to perform scan within the “Scan Interval On Time”.

Scan Interval On Time

Is an RM or CPS configurable parameter. It instructs the Radio to turn on BLE scanning for the configured time. The “Scan Interval On/Off Time” is a duty cycle. When the Indoor Location is turned on, the radio performs the BLE scan continuously base on this duty cycle until it is turned off by the user.

Scan Interval Off Time

Is an RM or CPS configurable parameter. It instructs the radio to turn off BLE scanning for the configured time.

The iBeacon BLE Advertisement Interval Rate is configured in the iBeacon device for a specific timing deployment need. This beacon advertisement interval rate is configured to meet each deployment timing requirements. On the radio CPS, the “Scan Mode” field is used for configuring the Bluetooth scan advertisement bandwidth. When “Normal” is selected, the radio uses 50% of the radio Bluetooth advertisement scan bandwidth to perform scan within the configured “Scan Interval Time = ON” time. If “Aggressive” is selected, the radio uses 75% of the radio Bluetooth advertisement scan bandwidth to perform the scan within the configured “Scan Interval Time = ON” time. If the radio is connected to a Bluetooth headset, the Bluetooth advertisement scan bandwidth is reduced. The “Scan Mode” is only available when the radio is not associated to a Wi-Fi access point. If the radio is associated to a Wi-Fi access point, then the radio automatically uses only 20% of the Bluetooth advertisement scan bandwidth to perform scan. Misalignment of the iBeacon Advertisement Interval which lands on the Radio advertisement scan OFF window may cause the radio unable to detect the beacons. A detailed timing calculation must be performed to align the radio Bluetooth scanning and beacon advertisement interval for better beacon detection performance. It is also recommended to use two beacons or more to cover the radio walk-path at one location, to provide better beacon detection performance. A detailed site survey must be done for every deployed beacon coverage spot.

The following table shows the examples of timing configurations:

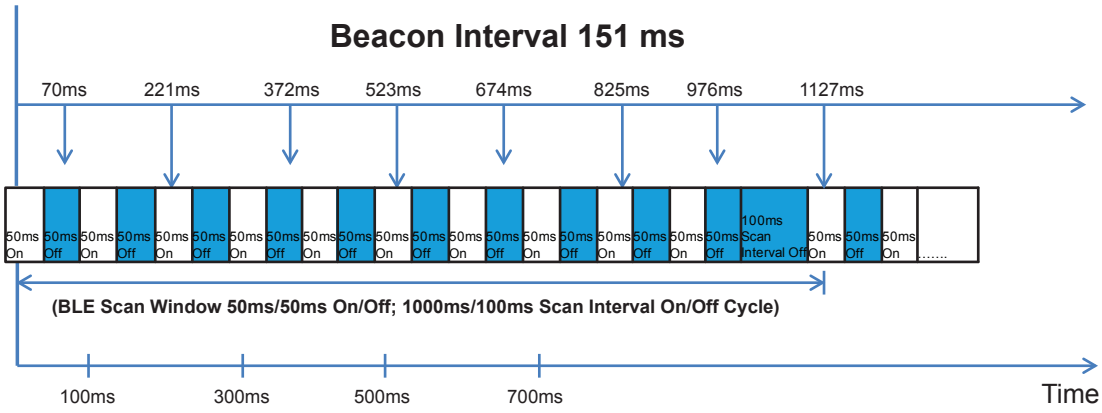
Table 21: Examples of Timing Configurations

Operation Example	Timing Configuration
Radio Bluetooth or WiFi Coexistence Operation	iBeacon Device BLE Advertisement Interval Rate (programmable in the iBeacon device)
Bluetooth Only	The Radio BLE scan advertisement bandwidth is only 50% in every 100ms duty cycle within the configured “Scan Interval On Time”. The iBeacon BLE Advertising Interval Rate value last 2 digits should be configured to end with 51ms (that is 151ms, 251ms, 551ms, and others) when possible. This configuration allows the radio to better distribute the Scan advertisement bandwidth on/off cycle. This is for better alignment with the iBeacon Advertising Interval, for better detection performance. For example, see Figure 20: Beacon Interval of 151ms and Radio Normal Scan Mode Detection Alignment on page 139. If the suggested time increment is not supported, the beacon interval should be configured in such a way that it could get best possible alignment to land on the radio BLE scan advertisement On window.
Bluetooth and WiFi Coexisted	When WiFi connection is active, the radio scan advertisement bandwidth is 20% in every 100ms duty cycle within the configured “Scan Interval On Time”. The iBeacon BLE Advertising Interval Rate value last 2 digits should be configured to end with 81ms (that is 181ms, 281ms, 381ms, and others) when possible. This configuration allows the radio to better distribute the Scan advertisement bandwidth on/off cycle. This helps to better align with the iBeacon Advertising Interval

Operation Example	Timing Configuration
	for better detection performance. A faster iBeacon BLE Advertisement Time Interval Rate is desired in this mode for better detection performance.

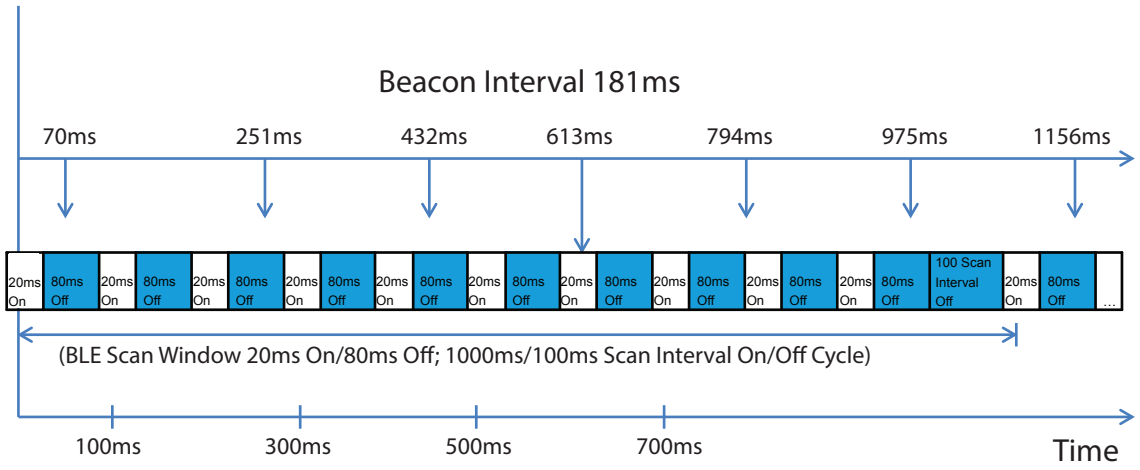
The following figure assumes that there is no interference, good RF condition, and that the radio is able to detect the beacon in the 50ms scan on window (Hit), and unable to detect the beacon in the 50ms scan off window (Miss). It assumes the beacon initial random starting point is at the 70ms time mark with a beacon interval of 151ms. When the beacon advertising is aligned within the Hit window, it is a successful detection. When the beacon advertising is aligned within the missed window, it is a failed detection. In this example, the number of Hit within a scan interval cycle is 3 (at 221ms, 523ms, and 825ms). For other beacon interval value, which may not be aligned with the radio scan advertisement on window, it may not able to detect the beacon at all. User must calculate the probability of the beacon interval and radio scan advertisement window alignment to optimize detection performance.

Figure 20: Beacon Interval of 151ms and Radio Normal Scan Mode Detection Alignment



The following figure assumes there is no interference, good RF condition and the radio is able to detect the beacon in the 20ms scan on window (Hit), and unable to detect the beacon in the 80ms scan off missed window. It assumes the beacon initial random starting point is at the 70ms time mark with a beacon interval of 181ms. When the beacon advertising is aligned within the Hit window, it is a successful detection. When the beacon advertising is aligned within the missed window, it is a failed detection. In this example, the number of Hit within a scan interval cycle is 1 (at 613ms) only. For other beacon interval value, which may not be aligned with the radio scan advertisement on window, it may not able to detect the beacon at all. User must calculate the probability of the beacon interval and radio scan advertisement window alignment to optimize detection performance.

Figure 21: Beacon Interval of 181ms and Radio WiFi Coexistence Mode Detection Alignment



2.13.4.3

Radio CPS Configurable Scan Interval On/Off Time Operation Considerations

The CPS configurable “Scan Interval On/Off Time” is used for turning on/off the Bluetooth scanning for iBeacon devices.

The actual scan active duty cycle is controlled by the predefined BLE Scan Advertisement bandwidth. See iBeacon BLE Advertisement Time Interval and Radio Scan Mode Operation Considerations on page 137 for more information. The radio buffers the detected iBeacon devices in every Bluetooth Scan Interval Time On/Off cycle in the volatile memory. The same iBeacon may be detected multiple times within a Bluetooth Scan Interval On cycle, but the radio only stores it once at the end of each cycle. For example, “Scan Interval On Time = 5 sec; Scan Interval Off Time = 100ms”, if a same beacon is detected multiple times within this duty cycle, the radio only stores the most recently detected beacon. One or more beacons may be detected within each cycle.

In between each “Scan Interval On/Off Time” duty cycle, if the exact same set of beacon(s) is detected, the radio only updates the previous beacon set with the most recently detected beacon(s) set’s RSSI and Timestamp value. In between each “Scan Interval On/Off Time” duty cycle, if a different set of beacon(s) is detected, the radio inserts the most recently detected beacon(s) set into the buffer. See Table 23: Same Beacon Set Between Cycle Buffering Scheme on page 141 and Table 24: Different Beacon Set Between Cycle Buffering Scheme on page 141 for more information. The Radio can buffer up to 200 beacons. When the buffer is full the oldest beacon is removed for the newly detected beacon. The radio always reports from the most recent to the oldest detected beacons.

The Scan Interval time On/Off cycle may be treated as an Indoor Location buffer sampling rate. In some scenarios the “Scan Interval On time” may be longer than the other. It depends on the number of co-located iBeacon devices, beacon Interval Rate, Scan Interval On/Off Time and Scan Mode selected. See the following table for suggested minimum “Scan Interval On Time” configuration. A detailed site survey is needed to fine tune the timing configuration for the different use case deployment requirement. The minimum allowed Scan Interval On/Off increment time is 100ms. The following table uses the “Scan Interval Off Time =100ms”.

The recommended minimum “Scan Interval On Time” for a typical one to five co-located beacons should be as followed:

Table 22: Scan Interval On Time

Beacon Advertisement Interval Rate	Recommended Minimum Scan Interval On Time (ms)
>900ms and <1000ms	5000
>800ms and <900ms	5000
>700ms and <800ms	4500
>600ms and <700ms	4500
>500ms and <600ms	4000
>400ms and <500ms	3500
>300ms and <400ms	3000
>200ms and <300ms	2500
>0ms and <200ms	2000

The following table shows the example of same beacon set detected between the cycle buffering scheme:

Table 23: Same Beacon Set Between Cycle Buffering Scheme

1st Scan Interval On/Off Cycle Detected Beacon	Beacon Stored After 1st Cycle	2nd Scan Interval On/Off Cycle Detected Beacon	Beacons Stored after 2nd Cycle
Beacon # 1	Beacon # 1	Beacon # 1	Beacon # 1
Beacon # 2	Beacon # 2	Beacon # 2	Beacon # 2

The following table shows the example of different beacon set detected between the cycle buffering scheme:

Table 24: Different Beacon Set Between Cycle Buffering Scheme

1st Scan Interval On/Off Cycle Detected Beacon	Beacon Stored After 1st Cycle	2nd Scan Interval On/Off Cycle Detected Beacon	Beacons Stored after 2nd Cycle
Beacon # 1	Beacon # 1	Beacon # 3	Beacon # 3
Beacon # 2	Beacon # 2	–	Beacon # 1
–	–	–	Beacon # 2

2.13.4.4

iBeacon Advertisement Tx Power and iBeacon RF Site Survey Considerations

The iBeacon vendor advertises a set of optimal distance relative to the beacon advertisement Tx Power level. There are many factors that can alter the beacon devices RF transmission performance such as the antenna design, antenna placement, device housing material, device orientation, obstruction, and others. Each iBeacon Tx Power is programmed for each deploying location and validate the beacon RF detection distance.

A detailed beacon RF site survey is needed for each deploying beacon at different location. A careful beacon RF site survey technique may help operation performance. It is also recommended to perform the site survey

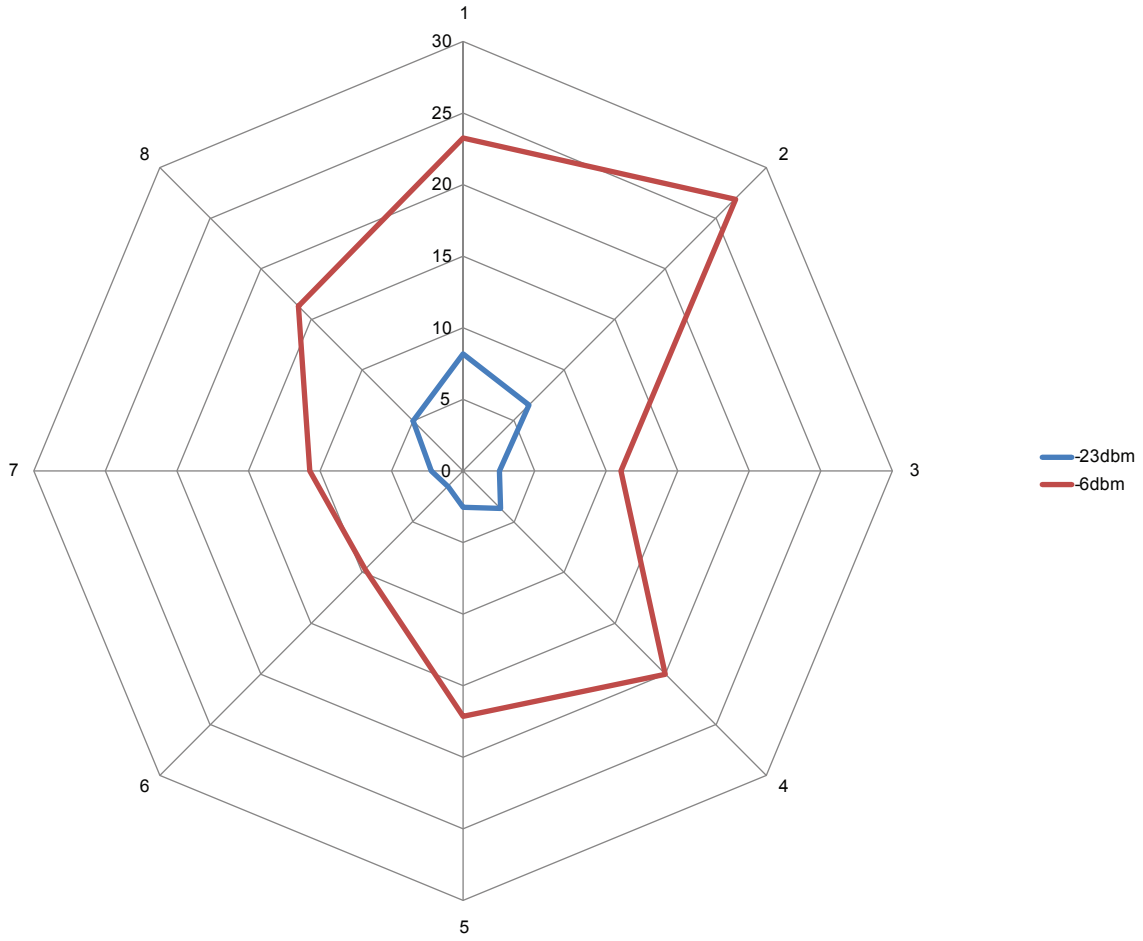
with the MOTOTRBO radio along with another off-the-shelf device like the cell phone, to validate the beacon performance.

Figure 22: Beacon RF Site Survey on page 142 is an example of actual beacon RF site survey data. The following are the parameters:

- Beacon Advertisement Time Interval = 851ms
- Radio Scan Interval On/Off = 5sec/100ms
- Beacon Tx Power = -6dBm and -23dBm
- Distance Scale = 5 meter/Unit
- Use the MOTOTRBO radio for detecting the beacon

NOTE: It is strongly suggested that it should be used as reference only and should not be used as an exact value for the system deployment without validation.

Figure 22: Beacon RF Site Survey



Based on the beacon detection distance/coverage area plot in Figure 22: Beacon RF Site Survey on page 142, even when the beacon is placed on the ground in an open space, the detection distance varies from point to point. Quadrant 1–2 has the best distance and coverage area, and quadrant 5–7 has the worst

coverage. User can conclude that the beacon RF coverage is not a perfect circle. This is why a beacon RF site survey is needed when deploying every beacon.

NOTE: Most of the off-the-shelf iBeacon device vendors would not advise the user on the Bluetooth antenna location in the device. As a conclusion on where the beacon antenna is placed, user can point between Point 1 and 2, because it has the best distance and coverage area from both plots with different Tx Power.

2.13.4.4.1
Conducting the RF Site Survey

The following are the procedures to conduct the site survey:

Procedure:

1. Place the beacon on the ground in an open space without any obstruction at the origin point “0”. See Figure 22: Beacon RF Site Survey on page 142.
2. Hold the MOTOTRBO radio in the hand for detecting the beacon.

   It is also recommended to use a mobile phone that can detect the iBeacon to perform the survey simultaneously.
3. Walk from out-of-range point to in-range point direction, toward to the beacon with the radio in direct line-of-sight with the beacon.

   NOTE: It is very important to avoid walking the opposite way. When the user is in between the radio and the beacon, it may block the RF energy and cause unpredictable result.
   This beacon RF site survey technique provides a better beacon deployment in different situations.
4. Start walking from Point 1 (at the 30 meter mark) toward the beacon at the Scan Interval On/Off cycle time for every 1 meter (1m in 5 seconds) and record the beacon detection distance result on both Radio.
5. Repeat Step 4 for Point 1 to Point 8.

   The beacon distance detection result is plotted in Red for the -6dBm Tx Power, and the -23dBm Tx Power is plotted in Blue.

2.13.4.5
Other iBeacon Deployment Considerations

Once the beacon RF coverage is known, it is static for the deployment. However, the environment around the beacon may change such as obstruction may move in and block the beacon. To minimize this uncertain environment which may impact the beacon performance, a strategic beacon placement is important at deployment.

For example, if the iBeacons are being deployed in a shopping mall, it is preferred not to mount the beacon at human body waist level, because there could be many people around and block the beacon from the radio user under Indoor Location tracking.

The human body RF blocking concern should be taken into consideration when deploying the iBeacon devices. If the human body is in between the radio and beacon, it blocks most of the beacon RF energy which may reach the radio. The radio may not be able to detect the beacon even when it is within the beacon RF line-of-sight coverage. This situation happens when the portable radio is wore on the human body. The solution is to deploy multiple co-located beacons in different points to cover the human body factor use case. For example, in a hallway beacon deployment case, the beacons should be placed and interleaved on both side of the hallway with the desired distance coverage.

The other complicated consideration is the radio under Indoor Location tracking may move in at different speed. User must know the use case condition/requirements for configuring the iBeacon devices and radio parameters. The radio may move in/out of the beacon coverage at different time. If the radio stays within the coverage for less than the required beacon detection time, it may not detect the beacon. For example, with the 851ms Beacon Interval time and radio operates in Bluetooth 50% scan duty cycle, it may take up to 2x851ms to detect the beacon. This assumes there is no Bluetooth interference. For example, in Figure 22: Beacon RF Site Survey on page 142 and -23dBm Tx Power, if the radio user walks from Point 3 toward to Point 7 in one meter per second, the user should spend about five seconds within the beacon RF coverage range, and the radio should be able to detect the beacon. If the radio user runs at five meters per second, and stays within beacon coverage range about one second, the radio may not detect the beacon.

2.13.4.6

Indoor Location Deployment Requirement Checklist

Each iBeacon configuration, mounting, environment, and others may be different, even for a single end-to-end Indoor Location deployment, such as a shopping mall. To deploy each iBeacon, a detailed planning and requirement considerations are mandatory.

The following requirement checklist guides the user to configure the Application Server/Map, Radio and iBeacon.

- How many beacons should the Application Server request from the radio for Indoor Location tracking, distance triangulation, tracking history, and others? How should the server/mapping application filter for its own deployed iBeacon devices?
- Will the radio be connected to other Bluetooth devices and/or WiFi AP while under Indoor Location tracking enable mode? Is the beacon Advertisement Interval configuration aligned with the radio operation modes according the recommendation?
- What is the desired radio Customer Programmable Software (CPS) configurable Scan Interval Time On/Off rate? Is the value configured according to the recommended rules?
- What is the maximum number of co-located beacons that the radio has to detect within a Scan Interval Time On/Off period (100 co-located beacons should require a longer time to detect than a five co-located beacons case)? If there are large numbers of co-located beacons, the collision rate is higher thus the detection performance could be poor?
- What supports the radio moving speed (walking or running) for passing through the beacon RF coverage area? What is the desired radio beacon detection time?
- How is the radio be worn or attached (portable radio on human body or mobile radio mounted in warehouse forklift)?
- What is the required iBeacon Advertisement Interval speed to cover the radio movement conditions?
- Is the iBeacon Advertisement Interval time value configured according to the recommended rule and value for best detection performance in different Bluetooth/WiFi operation mode?
- What is the required iBeacon RF coverage range/Tx Power setting?
- What is the best iBeacon mounting location for the best RF coverage condition?
- What is the deploying beacon location environment (shopping mall with high human traffics which may block beacon RF)?
- How many beacons do you need to cover an area to provide the best coverage without blind spot?
- What is the distance accuracy requirement?
- What is the required beacon battery life?
- Have you performed a site survey for other people’s iBeacon which may have the same UUID?
- Have you performed an iBeacon RF range site survey for every deployed beacon?

2.13.5
iBeacon OTA Parameters

The following iBeacon data attributes can be requested through the LRRP Application Server messages. These data are encapsulated in the LRRP response message.

UUID
Is a region identifier that distinguishes customers iBeacons from others.

Major
Is used to group a related set of iBeacons for location mapping.

Minor
Is used to identify individual iBeacons for location mapping.

Tx Power
Two's complement of measured Tx power. The actual Tx power can be calculated as a two's complement of the data: (0xC5 = 197 => 256-197 = - 59 dBm). Tx power is the strength of the signal measured at one meter from the iBeacon.

Timestamp
Is a one second counter parameter to determine the time between beacon detection.

RSSI
Is the beacon Tx RSSI level received by the radio.

2.13.6
Radio Indoor Location Configuration and Operation Parameters

The indoor location feature depends on the Radio Bluetooth LE technology and operation. The Bluetooth feature must be turned on for indoor location to operate.

The following radio Indoor Location CPS configurable parameters should be supported for Indoor Location operation:

- Indoor Location – This field is used to enable or disable the Indoor Location feature. If it's enabled, the radio starts scanning for the beacon by default. The Menu or Programmable Button can be used to turn on/off scan.
- Scan Mode – This field is used for configuring the Bluetooth advertisement scan bandwidth. When "Normal" is selected, the radio uses 50% of the 100ms Bluetooth scan advertisement bandwidth to perform scan within the "Scan Interval On Time". If "Aggressive" is selected, the radio uses 75% of the 100ms Bluetooth scan advertisement bandwidth to perform the scan within the "Scan Interval On Time". The "Scan Mode" is only available when the radio is not associated to a Wi-Fi access point. If the radio is associated to a Wi-Fi access point, then the radio automatically uses only 20% of the 100ms Bluetooth scan advertisement bandwidth to perform scan within the "Scan Interval On Time".
- Beacon UUID – Up to 20 programmable UUID shall be supported, and the radio listens to the configured UUID only. At least one UUID must be programmed in the radio. Otherwise, the feature is considered disabled. A LRRP request message can be used to instruct the radio to listen to any iBeacon device, but the LRRP request is not remembered after the radio powers off.
- Scan Interval On Time – This instructs the radio to turn on BLE scanning for the configured time. The "Scan Interval On/Off Time" is a duty cycle. When the Indoor Location is turned on, the radio performs the BLE scan continuously based on this duty cycle until it is turned off by the user.
- Scan Interval Off Time – This instructs the radio to turn off BLE scanning for the configured time.

2.13.7
Radio Indoor/Outdoor Location Application Services

A location Application Server is required to send an explicit LRRP request to the radio, for all the services. A radio does not provide unsolicited location update to a location Application Server. When the radio turns on and/or selects a properly configured channel, the radio registers with the presence service (that is, ARS, Connect Plus or Cap Max registration). The location Application Server learns that this radio is on the air, and makes an explicit request for location updates when it is configured to track the indoor/outdoor location of the radio.

The outdoor (that is, GPS) and indoor location equipped radios transmit an update of their location coordinates and/or iBeacon data over the radio system in response to four service methods, as follows:

- Single Location Update – The location Application Server wants to know the current location of a radio user. In this case, the application sends a request for a single location update.
- Periodic Location Updates – The location tracking allows a location Application Server to periodically get the location of a radio user, by sending a single location request that contains the time interval between updates. The radio continues to update its location periodically at the specified time interval until the request is canceled by the location Application Server. The location tracking Application Server can configure the radio to provide update rate base on the system's data throughput resource capabilities. The fastest supported indoor and outdoor (that is, GPS) location update interval is 30 seconds. The radio supports the stored persistent LRRP update base on the Application Server request too.
- On Emergency – A radio sends its location after the user triggers an emergency alarm or an emergency alarm and call request. The location update is sent only to the location Application Server, which had previously sent an active location request for location updates from that radio upon an emergency event. This location update is sent by the radio only after the processing of emergency is completed. For example, for Emergency Alarm with Call, the location data is only sent after the Emergency Alarm is acknowledged and the initial Emergency Call is completed. This happens because the location data is sent as a data burst which has lower priority than the voice call.
- On GPIO Trigger (Mobile radio only) – A radio sends its location after the location configured GPIO triggers a level transition. The location update is sent only to the location Application Server, which had previously sent an active location request for location updates from that radio upon an event.

This beacon data is sent in the LRRP update from the most recent to the least recent, up to the requested number of beacons. Once the beacon data is sent, it is removed from the radio buffer. The radio keeps the most recent beacon in the buffer as the last known location. If no new beacon is detected in the subsequent scan cycle, the radio reports the last known beacon data plus up to the requested number of beacons available in the buffer.

2.13.8
Third-Party Location Application Services

The third-party location services application consists of an Application Server and location clients. The Application Server requests, receives, and stores the location data of the radios. The location clients get the location data from the Application Server for managing and displaying the radios' locations on a map. The types of available indoor/outdoor location services (that is, indoor location iBeacon distance triangulation/ approximation and others) are third-party application dependent.

2.13.9

Radio GPS Revert Channel Location Services

The GPS Revert Channel feature is applicable to Digital Conventional mode only, and it allows system operators a configurable option to off-load radio transmitted location updates onto a programmed digital channel that differs from the digital Selected Channel.

This feature effectively removes Location Update traffic from the Selected Channel in order to free up that channel to accommodate increased voice loads and/or to enhance the user experience by reducing the number of channel busies during voice call requests. This feature also allows a large group to communicate on a single voice channel while sending location updates on multiple GPS Revert Channels to accommodate larger location update loads. This increases the location update throughput associated with radios belonging to a single group.

Each channel programmed into the radio has a configurable CPS option to designate the location (that is, indoor and/or outdoor location) transmission channel on which it transmits location update messages. The CPS options for the **GPS Transmission Channel** are **Selected**, **Channel** and **None**. Choosing **Selected** means the location updates are transmitted on the current channel. In the case of **Channel**, a single channel must be chosen from the list of all channels. This chosen channel is known as the “GPS Revert” channel and this is where location updates are transmitted. There may be instances when the radio is known to be out of range of any Control Station accepting location updates. In order to extend battery life, minimize time away from the Selected Channel, and/or to efficiently use frequency resources in these situations, the radio can also be configured to disable the transmission of location update messages on a per channel basis by using the selection **None**. A radio is shown as present to the dispatcher when a radio is switched from a location (that is, indoor and/or outdoor) enabled channel to a location disabled channel, until the presence indication duration is exceeded.

To configure the radio to support location updates, a few parameters must be managed correctly. How these parameters interact to dictate the radio’s performance is shown in the following table. The **GPS** and **Indoor Location** settings reside in the Radio Wide General Settings CPS folder. The “Indoor Location” service must be purchased for it to be shown on the CPS menu. The CPS configurable **ARS** and **GPS Revert** settings are present for each channel. When Revert Channel (that is, RevertChan1) should be used, it must be created by CPS. When a **GPS Revert** channel is **Selected**, it uses the currently selected channel for location transmission.

Table 25: Radio GPS Revert Channel Location Services Configuration Parameters

Radio Wide		Channel Wide	
GPS	Indoor Location	ARS	GPS Revert
Do not care	Do not care	Disabled	Disallowed
Enabled	Do not care	Enabled	Allowed
Do not care	Do not care	Disabled	Disallowed
Do not care	Enabled	Enabled	Allowed

See Radio Enhanced GPS Revert Channel Location Services on page 148 for more details on existing GPS Revert support.

2.13.10

Radio Enhanced GPS Revert Channel Location Services

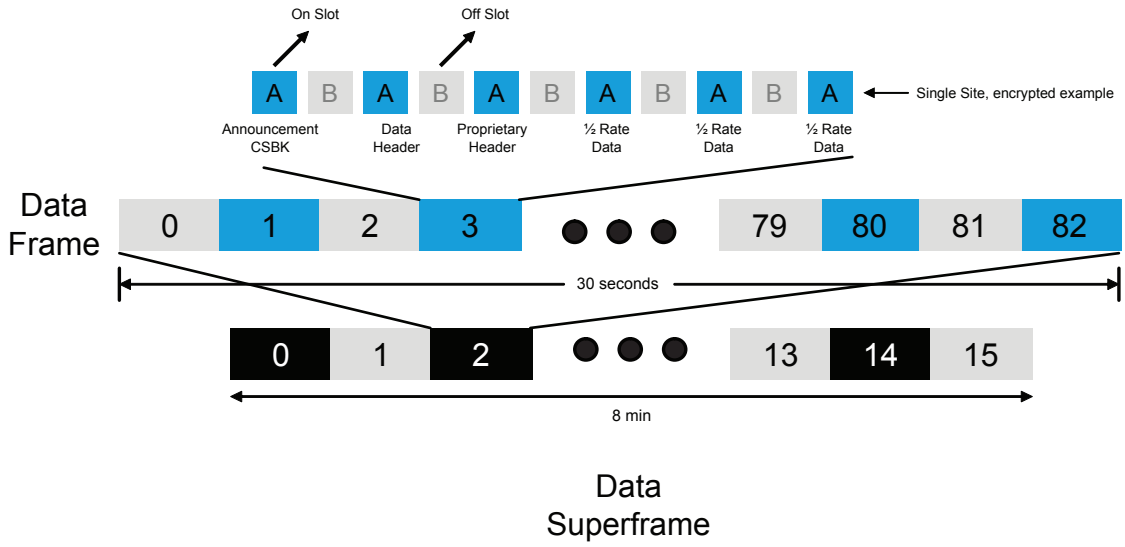
The Enhanced GPS Revert Channel is an enhancement of the GPS Revert Channel functionality that supports higher throughput and increased reliability. Similar to the former feature, a subscriber offloads location responses routed to a server, to a revert channel.

The primary difference lies in the method a subscriber accesses the channel. In the GPS Revert Channel feature, subscribers access a channel in a desynchronized manner and may therefore cause transmission collisions. The probability of collision increases with the number of transmissions made over the channel and collisions adversely affect the reliability of transmissions.

This enhanced feature enables subscribers to access a channel in a synchronized manner, which eliminate collisions and allow them to use the channel efficiently. The synchronization between subscribers is achieved by a repeater that divides a logical channel into groups of contiguous bursts defined as “windows”. This allows subscribers to make reservations for these windows in which GPS data can be transmitted. This is a slot wide configuration. The windowed data structure consists of an eight minute data super frame. Within the 8-minute data super frame, there are 16 data frames, each is 30 seconds in duration. This data super frame is repeated over and over again. Both the data frame and super frame always have the same size for every windowed GPS Revert Channel.

Within a 30-second data frame, there are windows that can be reserved by subscribers for GPS data transmission. The number of windows within a 30-second data frame depends on the size of each window. A window consists of an announcement slot in the beginning followed by bursts of location (that is, indoor and/or outdoor GPS) data. The following figure illustrates the windowed data structure for a window size of six (one announcement + five bursts of location data).

Figure 23: GPS Revert Channel Location Windows Data Structure for a Window Size of Six



The window size is dependent on the amount of location (that is, indoor and/or outdoor GPS) data to be sent, the privacy mode and header compression usage. Based on window size, the number of windows in a 30-second data frame is shown in the following table.

Table 26: GPS Revert Channel Location Number of Windows in a 3-Second Data Frame

Window Size (Includes Announcement Burst)	Number of Windows (In a 30-second data frame)
5	100

Window Size (Includes Announcement Burst)	Number of Windows (In a 30-second data frame)
6	83
7	71
8	62
9	55
10	50

A repeater's slot that is configured with "Enhanced GPS" maintains allocations of all the windows. At the beginning of every window, the repeater sends an announcement containing the current window number, data frame and the ID of the subscriber for the next reserved window. Before sending a location response, a subscriber requests a window for reservation (for one-time location response) from the repeater, or a set of periodic windows for periodic location responses. The repeater allocates window(s) (if available) and informs the subscriber in a grant message. The subscriber stores the window timing, reverts to the Enhanced GPS Revert Channel before the allocated window arrives, and verifies its reservation by listening to a confirmation grant from repeater. The subscriber then sends its location response in the reserved window. Since subscribers only send their location response in their reserved windows, collisions do not happen here. Hence, this methodology promotes the following benefits:

- Support for up to 360 location responses per minute per repeater using both slots, while running at 90% capacity, and decrease in the number of channels and associated hardware needed for GPS data transmission.
- Increased GPS reliability due to the drastic reduction of collision among subscribers sending GPS data.
- More control over system throughput, by allowing users to choose the most appropriate window size, based on the location response characteristics needed.

This feature is supported in repeater mode only and works in IPSC single or multi-sites, Capacity Plus single or multi-sites and Capacity Max modes of operation. Only unconfirmed data is supported on the Enhanced GPS Revert Channel in conventional mode (both single-site and IPSC). In Capacity Plus Single Site mode, ARS Registration Message is also supported on the Enhanced GPS Revert Channel. There is no support for voice on the Enhanced GPS Revert Channel. A window size ranges from 5 to 10. The size depends on the following factors:

- The parameters that the application has requested in a location response for outdoor location, such as longitude, latitude, time, altitude, velocity, direction, suaddr, and others.
- The parameters that the application has requested in a location response for indoor location, such as UUID, Major, Minor, Timestamp, Tx Power, and RSSI.
- Whether IP/UDP headers compression is enabled.

The following table shows an example calculation for the window size with enhanced privacy enabled. The total LRRP response message size includes the IP header, Privacy header, LRRP header, Indoor and Outdoor location data element.

Table 27: Outdoor Location GPS Revert Channel Data Size

Requested Element	Element LRRP Response Size (bytes)
Latitude + Longitude	11
Time	6
Request ID *	3
Speed_hor *	3

Requested Element	Element LRRP Response Size (bytes)
Direction_hor	2
Altitude *	3
Radius *	2
* Indicates variable field sizes	

Table 28: Indoor Location GPS Revert Channel Element Data Size for One Beacon

Requested Element	Element LRRP Response Size (bytes)
Beacon-Major-Minor-Timestamp	9
Beacon-Major-Minor-Tx Power- RSSI-Timestamp	11
Beacon-UUID-Major-Minor-Tx Power- RSSI-Time-stamp	27
Beacon-UUID	18

NOTE: If more than 1 beacon data is requested in the request element, the indoor location token header shall be shared with multiple beacon response message thus the response size is should be calculated as followed:

Example for “bcon-maj-min-time” response element:

- 1 Beacon Response Size = Header 3 bytes(1 byte Beacon Info Token + 1 byte Beacon Request Element + 1 byte Length + 6 bytes Beacon Data Payload = 9 bytes
- 2 Beacon Response Size = Header 3 bytes(1 byte Beacon Info Token + 1 byte Beacon Request Element + 1 byte Length + 12 bytes Beacon Data Payload = 15 bytes

The following calculations assume GPS data is unconfirmed and “Compressed UDP Data Header” is selected in the CPS. The total LRRP response message size shall include the UDP/IP header, Privacy header, LRRP header, Indoor and Outdoor location data element.

- For No Privacy
  WindowSize= ((LRRPResponseSize+1)÷12)+3
- For Enhanced Privacy
  WindowSize= ((LRRPResponseSize+1)÷12)+4

For windows de-allocation, if a subscriber is out of range or its battery is dead, it will not send location data during its reserved windows. Thus, the repeater also has a mechanism to free up the windows reserved for that subscriber. The repeater waits for a certain period of time before releasing the windows and this time is dependent on the cadence rate of the subscriber’s location request. The following table summarizes the amount of time the repeater waits before de-allocating windows for a subscriber.

Table 29: GPS Revert Channel Wait Time Before De-allocation

Update Rate	Wait Time Before De-allocation (minutes)
30 seconds	5
1 minute	5
2 minutes	10
4 minutes	20
8 minutes	30

In a subscriber, it is highly recommended to keep the Enhanced GPS Revert Channel in the **Channel Pool** in the CPS. This prevents the user from accessing the Enhanced GPS Revert Channel that may affect GPS reliability. A channel can be configured as an Enhanced GPS Revert Channel by selecting the field **Enhanced GNSS** in the channel settings. In order to send responses to the Enhanced GPS Revert Channel, the GPS Revert Channel setting of the home channel has to be set to **Enhanced GNSS**.

In a multisite system with roaming enabled, all sites are recommended to use the same setting and window size as an Enhanced GPS Revert Channel. This can be configured through the Enhanced GPS Revert Channel of the Home Channel.

In a multisite system with roaming enabled, all sites are recommended to use the same setting and window size as an Enhanced GPS Revert Channel. This can be configured through the Enhanced GPS Revert Channel of the Home Channel.

In a repeater, the CPS allows either one or both slots to be configured as Enhanced GPS. The window size in the repeater's Enhanced GPS slot should match the window size in the subscribers. One slot can be configured for regular Data Revert and the other slot can be configured for Enhanced GPS Revert. The repeater CPS also allows a user to choose the maximum percentage of windows that will be used for periodic updates. The possible values are 90%, 75%, 60%, and 45%. The rest of the windows are used for one-time updates and also to empty out queued data. When a subscriber is participating in a voice call, chances are it may miss its windows. This will lead to windows getting queued up in the subscriber. When this happens, the subscriber can make one time requests to ask for additional windows to empty out its queue.

In a situation whereby a system has heavy voice loading, the subscriber may start to miss their reserved windows quite frequently. Hence, in such a scenario it is advised to run the system at 60% or 45% capacity so the rest of the windows can be used to clear up the queued data.

In an IP Site Connect system where a Revert Channel is a wide area channel, only one repeater's slot needs to be selected with periodic window reservation (90%, 75%, 60%, and 45%). For all the other peers, this value should be set to **None**.

For all modes, it is not recommended to have any non-GPS data on the GPS Revert Channel. The only exception is Capacity Plus Single Site mode, where ARS data is also supported on the GPS Revert Channel. The system throughput is dependent on the window size selected for the system and the percentage of windows reserved for periodic updates. The following table summarizes system throughput:

Table 30: GPS Revert Channel System Throughput

Window Size	Number of Updates per Minute per Slot			
	90%	75%	60%	45%
5	180	150	120	90
6	150	125	100	75
7	128	107	86	64
8	112	93	75	56
9	100	83	66	50
10	90	75	60	45

NOTE: These numbers are based on good signal conditions. The actual throughput and reliability may vary with RF conditions and voice call loading.

The Enhanced GPS feature can be configured in the following manner:

- Conventional single-site and IPSC modes:
  - One slot for voice, one slot for Enhanced GPS Revert
  - One slot for GPS Revert, one slot for Enhanced GPS Revert

- Both slots for Enhanced GPS Revert

- Capacity Plus Single Site mode:
  - One slot of data revert repeater for GPS/ARS, one slot for all other data
  - Both slots for Enhanced GPS Revert

2.13.11
Connect Plus Fast GPS Location Services

When the location application requests a periodic location update, each Subscriber Unit (SU) that has compatible radio and Option Board (OB) firmware is assigned the following information.

Periodic Update Report Channel (Fast GPS Report Channel)

- Decodes expected Frame # and Window # of the SU (OB) in the Control Channel (CC) Control Signaling Block (CSBK) and informs to which repeater and slot it should trunk.
- Communicates to the OB through Over the Air (OTA) messaging from controller. It is not programmed in the OB.
- The Controller determines which specific repeaters and slots to use in Report Channels. The Network Manager (NM) provides two user-configurable settings that determine which channel the controller uses:
  - The maximum number of slots to use in Report Channels. This cannot exceed the number of report channel licenses for the XRC site.
  - Repeaters and slots that are NOT to be used as Report Channels (exclusion list).
- The Controller loads the Report Channels one at a time and as fully as possible before assigning radios to a new Report Channel. This allows the slot to be used as a voice trunk until the number of reporting SUs has grown to a point that it requires its use as a Report Channel.
- The Controller assigns SUs to a Report Channel before activating the Report Channel.
- When necessary, the Controller can temporarily suspend reporting on a Report Channel. The SUs are not reassigned to a different channel during the temporary suspension.
- When necessary, the Controller can reassign Report Channels.
- The use of Report Channels is a purchasable feature (on a per-channel basis).

Window Number

The SU (the OB) scans Control Channel messaging for its assigned Window Number (SUs assigned to even-numbered windows) or the Window preceding its assigned Number (SUs assigned to odd-numbered windows). This causes the SU to trunk immediately (even numbers) or after a short delay (odd numbers) to its preassigned Report Channel if:

- The Frame Number is an expected Frame in which the SU reports (Based on the Initial Frame and Frame interval information provided to the SU).
- The SU determines (from the same CSBK) if preassigned Report Channel is active (such as accepting reports).

Initial Frame Number (0-15)

The SU begins reporting when it decodes its Initial Frame Number and Window Number.

Report Interval

- When SU sees its Windows Number, it reports to subsequent Frame Numbers based on its Report Interval.
- The Report Interval is assigned according to the SUs Update Interval.
- The Update Intervals shown on the chart are supported initially.

Assignment is made when system first delivers the periodic Location Request to the SU and/or each time the SU registers (and re-registers on a site). This info is put into a new Registration Response CSBK.

Control Channel downlink sends a CSBK that announces the Frame Number and Window Number. The CSBK is sent for every even-numbered window (beginning with Window zero).

SUs assigned to even-numbered windows

After the SU decodes expected frame number and window number in the Control Channel message, it moves to its preassigned Report Channel, transmits the Periodic Location Update through the DMRII unconfirmed method, and then returns to CC time slot.

SUs assigned to odd-numbered windows

SUs search for for the even-numbered window that precedes their assigned window. Once SU detects the even-numbered preceding window, it starts a short delay timer before moving to its preassigned Report Channel slot. The delay timer is determined by the window size, which is also communicated in the CC CSBK. This allows two SUs to be assigned to the same traffic channel slot by the same message, at slightly different times.

The Report Channel Time Slot table shows the frame and window structure on each Report Channel time slot.

The frame and window number given on the CC down link applies to all Report Channels. The Report Channel downlink transmits only idles. The number of frames per cycle is always 16. After 16 frames, it cycles back to Frame 1. In this example, it takes 30 seconds to a single frame (supports update intervals of 30 sec to 8 min).

Table 31: Report Channel Time Slot

Window ↓	Frame →															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
70	70	70	70	70	70	70	70	70	70	70	70	70	70	70	70	70

The number of Windows per frame varies, and depends on:

- Report Size in bursts (set with the Network Manager). In this example, Report Size=5 bursts (300 ms).
- Number of slots of padding placed between each report. In this example, Padding=120ms.
- Length of time required to send a single frame (depends on fastest supported update interval). In this example: 30 sec.

2.14
Scan

MOTOTRBO supports scanning of analog voice, digital voice, data, and digital signaling through a repeater or directly from another radio. MOTOTRBO radios scan channels or groups, or both. In Capacity Plus Single Site and Capacity Plus Multi Site modes, it scans the groups only.

When scanning channels, the radio continuously searches a list of channels for activity of interest. When activity of interest is found, the radio stops and switches to that channel. When finished, the radio continues scanning the channels in the list.

The set of channels to be scanned (or scan members) are determined by a configured Scan List. A radio can have multiple Scan Lists, and each channel in a radio can be associated with a different Scan List. Scan Lists can contain only analog channels, only digital channels, or a mixture of both analog and digital channels. Once Scan is started, the radio scans through each Scan member of the associated Scan List for the selected channel.

The CPS allows a user to create, edit, or delete Scan members in a Scan List, as well as associate a Scan List to a channel. The user can start or stop Scan, and also add or remove Scan members of a Scan List using the radio's interface. Changes to the Scan List made via the radio front panel user interface are permanent, that is, not affected by power cycle (*). Note that Scan and Roam are mutually exclusive on a channel within CPS.

NOTE: This is different from the other supported feature – Nuisance Channel Delete: A channel with unwanted activity is called a Nuisance Channel. The user can remove a Nuisance Channel from the Scan List temporarily by using the Nuisance Channel Delete feature.

When the radio is scanning, and it detects a digital Scan member in its Scan List, it looks for transmissions targeted towards the group associated with that channel. The radio also looks for transmissions targeted towards itself (for example, Private Calls or signaling commands). The radio can be configured such that replies that occur within a specified duration is transmitted to the same group and channel (this reply is called talkback). If the reply occurs outside of this duration, it is considered a new transmission.

There are also options for where new voice transmissions (outside of the previously mentioned duration) are transmitted while scanning. Voice can be configured to transmit on the selected channel (the channel from which Scan was started), another predetermined channel, or on the last landed channel for voice (the last channel that Scan "locked-on-to"). Data and digital signaling are always transmitted on the selected channel. The last landed channel is not updated for data and digital signaling.

Priority levels can also be configured for members of a Scan List. There are three levels of priority within a Scan List – Priority-1, Priority-2, and Non-Priority. The Priority-1 and Priority-2 channels are scanned more often than the Non-Priority Scan members. Priority Scan is available with any mix of analog, digital, talkaround or repeater channels.

The Scan List can be configured to have one Priority-1 member and one Priority-2 member; the remaining are considered Non-Priority. When scanning, these priorities affect the order of scanning. The following represents the scan order of Scan List: Priority-1, Non-Priority-1, Priority-2, Non-Priority-2, Priority-3, Non-Priority-3, and others However, the radio may reorder Non-Priority scan members in order to optimize the efficiency of the scan.

In the CPS, there are two parameters associated with Scan Lists – Set/Clear Priority-1 and Set/Clear Priority-2. These are used to mark a Scan List member as Priority 1 and Priority 2; unmarked list members are "non priority".

While scanning, the radio can accept data (for example, text message, location, telemetry, or terminal (PC) data). However this is only applicable if the data is received on its selected (home) channel.

NOTE: In MOTOTRBO radios with software versions R01.04.00 or later, various enhancements were made to the scan engine to improve scanning performance. This has caused some features, such as scanning for Group Text Messaging and Emergency Alarms, to no longer be backward compatible with older software versions. All equipment must be upgraded for these features to perform correctly.

2.14.1
Priority Sampling

When scanning, if some activity of interest is found, the radio stops and switches to that channel. If the activity of interest is incoming data addressed to the scanning radio, an individual voice call, or it is on a Priority-1 scan member, scanning completely stops for the duration of the call. But if the activity is a voice Group Call on a Priority-2 or a Non-Priority scan member, the radio continues to periodically scan higher priority scan members.

For example, if the radio is receiving voice on a Non-Priority scan member, then the Priority-1 and Priority-2 scan members are scanned periodically. In this case, the order of scan is: Priority-1, Priority-2, Priority-1, Priority-2, and others. If the radio is receiving voice on a Priority-2 scan member, then only the Priority-1 scan member is scanned periodically. If a transmission of interest is found on the higher priority member, the radio switches to that member to monitor the transmission. If it is not of interest, it returns to the previously monitored member. Priority Sampling does not occur when transmitting.

Because the radio is currently receiving voice, leaving the current scan member to scan a higher priority member causes the radio to temporarily leave the current transmission. This causes an audio hole in received audio that is being played through the radio's speaker. Thus, the intervals during which the radio samples the higher priority members, essentially, becomes the audio holes that are introduced into the currently monitored voice. If there are two priority channels configured, this time is how often a sample is taken of either one. Therefore, one particular channel is sampled at a rate of double the priority sampling duration. A balance between how often an audio hole is introduced and how often a channel is sampled needs to be achieved to ensure that transmissions are not missed and to prevent introducing too many audio holes. This interval is CPS configurable through the "Priority Sample Time" interval parameter. Since the radio only samples at the rate of the Priority Sample Time, it is important to understand that if sampling for data, the Scan Preamble must be set to double the Priority Sample Time.

The user experiences few to no audio holes if they are currently unmuted to a lower priority voice while the priority member is in the other timeslot of the same repeater. In this situation, the radio uses the embedded signaling in the repeater to monitor activity in the other timeslot. This should be taken into consideration when deciding which identifiers are assigned to which channels and slots.

Not all identifiers are uniquely identified in the embedded signaling because they are compressed into smaller identifiers. If the system contains two or more identifiers that share the same compressed identifier, the radio incurs additional audio holes to validate the actual uncompressed identifier matches.

Duplicate compressed identifiers can be avoided if kept within a 256 ID range where the first ID of the range is an integer multiple of 256. For example if group and individual identifiers are kept between 0 and 255, or 256 and 511, or 512 and 767, and others, they will have unique compressed identifiers and no audio hole is experienced while priority sampling the other timeslot.

Setting a busy channel as a priority channel can cause excessive audio holes in non-priority audio as the radio checks each new transmission on the priority channel to determine if it is call of interest. If the priority channel has many short transmissions that are not of interest, the radio is forced to incur at least one audio hole for each. Therefore, it is recommended, that if possible, high priority transmissions should be isolated on channels that are not overly utilized by other traffic.

2.14.2
Channel Marking

In addition to configuring the sampling interval for Priority Sampling, MOTOTRBO offers a way to mitigate the duration of the audio hole itself with a feature called Channel Marking. Although relatively short, it does take time to determine if a transmission is of interest on a particular scan member. During this time, there is an audio hole in the scanned audio.

The Channel Marking feature introduces logic that assumes that if a transmission was recently identified as not of interest, there is no need to fully review it at every scan interval. Additionally, if the type of transmission

is of the same type as the transmission identified as not of interest before, there is a high likelihood it is the same transmission. Therefore, the radio only needs to identify the type of transmission taking place, which is beneficial as identifying a transmission type takes much less time than fully identifying if a transmission is not of interest. This assumption is made for a pre-determined number of times, after which, the scan member is fully reviewed again. This method changes the experienced audio holes from long audio holes every priority scan interval to one long audio hole followed by numerous short audio holes, and then another long audio hole, and so on.

This feature can greatly increase audio quality while a radio is in priority sampling mode. The drawback to channel marking is the assumption that the target of a transmission has not changed. The scanning radio does not know if the target has changed until the next full inspection. The system should be configured in such a way using CPS parameters to achieve a balance which delivers improved audio quality without sacrificing too much flexibility to consistently locate new transmissions which otherwise would be of interest. It is recommended that Channel Marking is set as Enabled in most scenarios.

However, if there is an analog signal on a digital priority channel, the radio incurs a medium size audio hole on every sample even if channel marking is enabled. The radio spends this time searching for synchronization that is not present. It is recommended that the priority traffic be placed on a channel that has limited analog interference (that is, shared use).

2.14.3
Scan Considerations

The ability to scan multiple channels is an advantage when a user must be aware of activity on numerous channels. MOTOTRBO offers the ability to scan a list of analog and digital channels (frequency and slot) within the same Scan List (often referred to as a Channel Scan List). This feature is incredibly useful when planning to migrate from analog to digital, or when a user must monitor multiple repeater frequencies and slots at the same time. When operating in digital, MOTOTRBO also provides the ability to scan multiple groups on a channel (slot). This is often referred to as a Group Scan.

A Group Scan is an optimized way to scan for multiple groups on the same channel (slot). The radio monitors the channel from either the repeater or directly from another radio to determine which group is currently transmitting. If the group transmitting is one specified in the Group Scan List, the radio stops and listens. The radio is allowed to talkback to the group for the duration of the call hang time. This call hang time overrides the TX Contact Name setting of the channel. Because only one call takes place on a channel (slot) at any given time, the scanning radio will not miss a transmission of interest, regardless of the length of the group list. A Group Scan is configured by creating a group list and adding groups already in the Contacts folder. This group list can then be selected as the RX Group List of a particular Channel. The Group Scan does not have the advanced features and configuration options of a channel scan. For example, once configured via CPS, the Group Scan cannot be turned on or off and members cannot be added or removed. Furthermore, the configurable scan options (Scan Hang time Timer, Talkback, and others) do not control the Group Scan. The Group Scan should be used in simple systems where no advanced scan options are required. If advanced scan options and features are required, a Channel Scan should be configured instead.

A Channel Scan scans a list of different channels within a system – analog or digital. A Channel Scan is different from a Group Scan since the radio must change frequencies and sometimes even modulations (analog to digital) in order to scan for activity. Unlike a Group Scan where only one call occurs at any given time, when scanning different channels (analog or multiple digital slots), there can be calls taking place on any or all of the channels. Because the radio cannot be everywhere at once, there is a possibility that the radio misses a transmission of interest. Because of this, it is recommended that the number of channels in a Channel Scan List is kept to a minimum. The larger the Scan List, the more likely a user misses, or join late, a transmission of interest during busy times.

System	Description
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	In Capacity Plus Single Site and Capacity Plus Multi Site modes, MOTOTRBO radios only support Group Scan. • All idle radios can perform a Group Scan at the start of a call. A call always starts on the Rest Channel and all idle radios are on the Rest Channel. • At the end of a call, the participating radios are informed about the ongoing calls, allowing them to perform a Group Scan. • When a radio powers on or when it comes into coverage, it searches the channels and joins a call of interest (if any). If all the channels are busy, then a radio may not join an ongoing call of interest.

2.14.3.1

Scanning and Preamble

Since data and digital signaling messages are typically shorter in duration than voice transmissions, it can be difficult for a scanning radio to detect such messages. This is especially true as the number of Scan List members increases because the amount of time between a scanning radio's repeated visits to a particular Scan List member increases, making it less likely to be on the channel at the exact moment that the data or digital signaling message begins.

Another factor is the amount of activity on each Scan List member; basically, the more active each Scan List member is, the more likely that the radio is suspending its scan operations to receive on each of those Scan List members, further increasing the likelihood that the radio will not receive the data or digital signaling on another Scan List member. To improve the likelihood of receiving data and digital signaling messages, the duration of these message types can be extended by preceding the message with special preamble signaling. The amount of preamble signaling to use can be configured into the initiating radio and the amount of preamble to use is dependent upon the number of Scan List members in the target radios' Scan List and whether priority scan is being used. Since this added signaling increases the amount of airtime used for data and digital signaling messages, there is a trade-off between increased channel loading and increased likelihood of receiving data and digital signaling messages while scanning.

Figure 24: Number of Analog Scan List Members

Number of Digital Scan List Members	Number of Analog Scan List Members																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	-	-	480	480	480	720	720	720	960	960	960	960	1200	1200	1200	1440	1440
1	-	-	720	720	720	960	960	960	960	1200	1200	1200	1440	1440	1440	1440	-
2	480	720	720	960	960	960	960	1200	1200	1200	1440	1440	1440	1680	1680	-	-
3	720	960	960	960	1200	1200	1200	1200	1440	1440	1440	1680	1680	1680	-	-	-
4	960	960	1200	1200	1200	1200	1440	1440	1440	1680	1680	1680	1680	-	-	-	-
5	960	1200	1200	1200	1440	1440	1440	1680	1680	1680	1680	1920	-	-	-	-	-
6	1200	1200	1440	1440	1440	1680	1680	1680	1680	1920	1920	-	-	-	-	-	-
7	1200	1440	1440	1680	1680	1680	1680	1920	1920	1920	-	-	-	-	-	-	-
8	1440	1680	1680	1680	1920	1920	1920	1920	2160	-	-	-	-	-	-	-	-
9	1680	1680	1920	1920	1920	1920	2160	2160	-	-	-	-	-	-	-	-	-
10	1680	1920	1920	1920	2160	2160	2160	-	-	-	-	-	-	-	-	-	-
11	1920	1920	2160	2160	2160	2400	-	-	-	-	-	-	-	-	-	-	-
12	1920	2160	2160	2400	2400	-	-	-	-	-	-	-	-	-	-	-	-
13	2160	2400	2400	2400	-	-	-	-	-	-	-	-	-	-	-	-	-
14	2400	2400	2640	-	-	-	-	-	-	-	-	-	-	-	-	-	-
15	2400	2640	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
16	2640	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Suggested guidelines for the amount of preamble duration to use with Scan Lists not using priority is provided in the following table. Scan preambles are not required for Capacity Plus Single Site and Capacity Plus Multi Site modes.

The preamble duration should be increased when Scan List members tend to carry lots of traffic or long transmissions. If no radios in the system will use the scan feature, then the amount of preamble may be set to zero.

The preamble duration should be increased when priority scan is being used because the priority channels are scanned more frequently in a full scan cycle. The preamble duration should also be increased when the selected channel or DTC is a dual capacity direct mode channel because the scanning radio needs to scan the beacon monitoring channel.

The following table suggests guidelines for the amount of preamble duration to use, with or without a dual capacity direct mode selected channel or DTC in a digital-only Scan Lists using priority.

Table 32: Number of Priority Members

		Number of Priority Members					
		Without DCDM DTC/Selected Channel			With DCDM DTC/Selected Channel		
		0	1	2	0	1	2
Number of Digital Scan List Members	0	–	–	–	–	–	–
	1	–	–	–	–	–	–
	2	480	480	480	960	960	960
	3	720	960	960	1200	1440	1200
	4	960	1200	960	1440	1920	1440
	5	960	1440	1200	1680	2640	1920
	6	1200	1680	1440	1920	3120	2640
	7	1200	1920	1680	2400	3840	3120
	8	1440	2400	1920	2640	4320	3840

Number of Priority Members						
9	1680	2640	2400	2880	4800	4320
10	1680	2880	2640	3120	5520	4800
11	1920	3120	2880	3360	6000	5520
12	1920	3360	3120	3840	6720	6000
13	2160	3840	3360	4080	7200	6720
14	2400	4080	3840	4320	7680	7200
15	2400	4320	4080	4560	8400	7680
16	2640	4560	4320	4800	8640	8400

If data and digital signaling is not carried on any of the non-priority channels and is only carried on one of the priority channels (which must be the selected channel for data messages), then the amount of scan preamble to use can be as specified in the first row of the Priority Scan table, above, regardless of the number of non-priority Scan List members.

2.14.3.2
Channel Scan and Last Landed Channel

A Channel Scan can be configured by selecting a group of already configured channels within a radio using the CPS, and adding them to a Scan List. Each channel is then configured to use this Scan List of channels. When scan is activated on a channel that contains a Channel Scan List, the MOTOTRBO radio checks for activity on each of the channels on the list.

While scanning a digital channel for activity, all Groups specified in the channel's RX Group List will be monitored.However if the radio is configured with a Channel Scan that contains channels that are configured with a RX Group List (a Group Scan), then only the Last Landed Channel is remembered by the radio, not the Last Landed Channel and Group. This means that voice transmissions are transmitted on the TX Call Member configured for the channel that was the Last Landed Channel, not the Group in the Receive Group List of channel that was the Last Landed Channel. Note that if a transmission is made within the call hang time of the scanned transmission, it will be targeted towards the landed channel and group. If it occurs after the call hang time has expired, it will be targeted towards the TX Call Member.

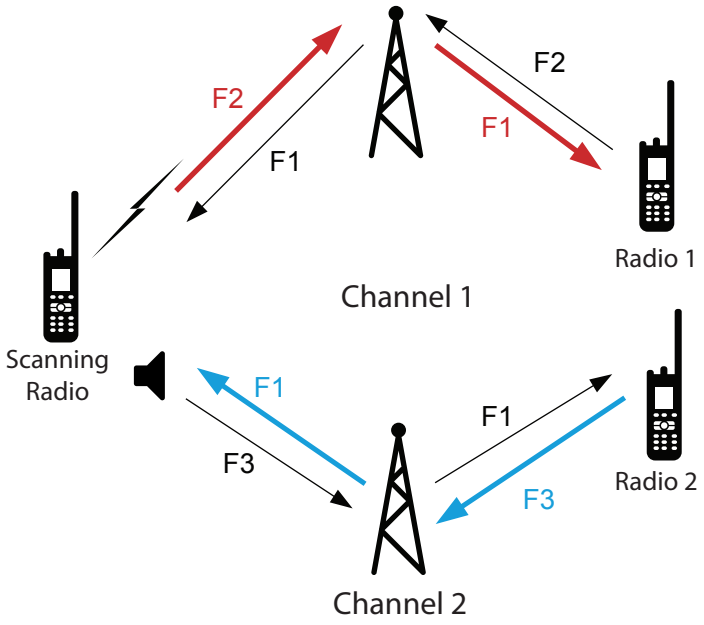
When using the Last Landed Channel option, it is recommended for each group to have its own configured channel. This way there is only one group associated with a channel, essentially making the Last Landed Channel and the Last Landed Group the same.

2.14.3.3
Scan Members with Similar Receive Parameters

When adding members to a Scan List, it is important to be conscious of the differences and similarities between their receive parameters. A Scan List that contains scan members with the same receive parameters but different transmit parameters may result in misdirected reply transmissions. This is best explained by first describing the simplest example of such a scenario.

In this example, a Scan List contains two scan members, Channel 1 and Channel 2. Channel 1 is an analog channel configured for carrier squelch with a receive frequency of F1 and a transmit frequency of F2. Channel 2 is an analog channel configured for carrier squelch with a receive frequency of F1, but with a transmit frequency of F3. A Scan List such as this implies that there is a repeater that is transmitting on F1 and receiving on F2, and another that is transmitting on F1 and receiving on F3. See the following figure .

Figure 25: Misdirected Response While Scanning

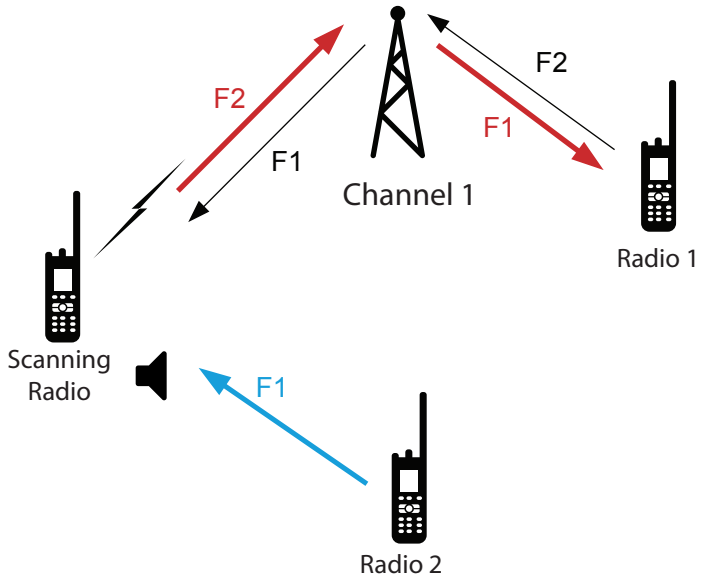


Since the radio only listens and qualifies using the receive parameters while scanning, the scanning radio could monitor a transmission from either repeater on either scan member. It does not know if it has actually landed on the correct channel or not. It only knows that the receive parameters have been qualified for the current channel being scanned. In other words, it does not know if the transmit parameters of the channel it has landed on matches the receive parameters of the radio that is has monitored. If the radio has landed on the wrong channel, when the radio user replies, the radio transmits on the wrong frequency. The result are a misdirected reply about half the time.

This scenario can be avoided by making at least one of the receive parameters unique. In an analog system, this could be done with the use of PL or DPL. In a digital system, this can be done by using a unique color code or unique group per channel. This will allow the scanning radio to only “land” on the channel where all receive parameters match and therefore properly direct the user’s reply.

Similar problems can occur if one scan member has fewer qualifiers than the others. Taking the example in the following figure, Channel 1 is still an analog channel configured for carrier squelch with a receive frequency of F1 and a transmit frequency of F2. However, Channel 2 is now a digital channel configured for Color Code 1 and Group 10 with a receive frequency of F1 and a transmit frequency of F3. The receive parameters in this example are different, but Channel 1 has few qualifiers. Channel 1 is configured to land on any transmission that breaks squelch. This means that any transmission that occurs on Channel 2 is heard on Channel 1 as an analog signal. This Scan List not only results in misdirected replies, but it also results in a digital transmission being played out the speaker as analog. The net result is undesirable sounds presented through the user’s speaker. This type of configuration should be avoided at all times. This could be avoided by utilizing a PL or DPL on the analog channel instead of only carrier squelch.

Figure 26: Misdirected Response While Scanning



Another similar problem occurs when the unique receive parameters between scan members are missing or cannot be determined. One scenario where this occurs is while scanning two slots of a repeater and a transmission is received directly from a subscriber on the same frequency. A radio in repeater mode can receive a transmission directly from a radio. However, in direct mode, slot numbering is not utilized. Therefore, if a radio is scanning two scan members with the same qualifiers with the exception of the unique slot number, when it receives a transmission without a slot number, either scan member monitors it and "land". When the user replies, the transmission is returned through the repeater on whichever slot assigned to the scan member it was monitored on. Depending on the configuration of the direct mode radio and its proximity to the repeater, the transmission may or may not be monitored. This can be managed by having different groups configured for each slot. This ensures that each slot has unique identifiers besides just the slot number. However, this does not help if the subscriber in direct mode is out of range of the repeater. This is why it is not good practice to transmit in direct mode in the RF range of the repeater.

Generally, these scenarios can be avoided if Scan Lists are created with scan members that have unique receive parameters.

2.14.3.4

Voice Transmission Reception Improvement While Scanning

In conventional system modes (Direct Mode, Single Site Repeater Mode and IPSC Mode) when a radio is scanning a number of channels for voice calls, it can miss the beginning of the voice call. The probability of missing the beginning of the transmission and joining through late entry increases as the number of scan channels increase.

To reduce the probability of missing the beginning of the voice transmission, radios can now be configured to send a larger number of voice headers preceding the voice payload. Configuration is radio wide and named 'Voice Pretime Duration'. This increases the amount of time between the user PTT and speaking. Speaking too early results in truncated audio and the issue is not resolved. Therefore it is highly recommended that Talk Permit Tone (TPT) is enabled.

The following table indicates the recommended amount of ‘Voice Pretime Duration’ to be added to per number of scan channels. Analysis shows that when no activity exists on any of the scan channels, the probability of receiving a new voice transmission without missing the beginning is above 70%. This additional time increases the time between PTT and speaking. It is highly recommended that TPT is enabled in order to reduce truncated audio.

Table 33: Voice Pretime Duration Recommendation

Number of Scan Channels	Voice Pretime Duration (ms)
2	60
3	180
4	240
5	360
6	480
7	600
8	660
9	780
10	900
11	1020
12	1200
13	1380
14	1500
15	1680
16	1800

2.14.3.5
Disable Scan Hangtime for Voice Calls

When scan is enabled after a radio receives voice transmission and call hangtime expires, the radio waits for additional scan hangtime to expire before resuming scanning.

In deployments where it is desirable to resume scanning immediately after expiration of voice call hangtime, scan hangtime for voice can now be reduced to 0 second. Coupling this with a 0 second hangtime would result in a radio resuming scanning immediately after the voice transmission ends. Configuration is in the scan list and is named ‘Voice Scan Hangtime’.

2.14.3.6
Unconfirmed Group Data Scanning

Radios can be configured to receive unconfirmed group data on channels other than the selected channel, when the selected channel is a digital channel.

The use case being accommodated here is broadcast data messages that do not need a response. It should be noted that a user sending a response to the group data source radio (individual data message) would be transmitted on the responding radio selected channel, which would be the incorrect channel. Since scanning for individual data messages is not supported, it is important if this scenario is to be supported, that the user selects the correct channel before sending the individual data message response.

2.14.4
Transmit Interrupt and Scan

Some of the Transmit Interrupt features and scan can be used together. However, there are a few interactions that need to be taken into consideration, as discussed in the following paragraphs.

Firstly, since scan is not permitted when the radio is in an emergency mode of operation, Emergency Voice Interrupt and scan do not have any direct interactions to consider because these two features are mutually exclusive. However, if a radio is in scan mode when the radio user initiates an emergency condition, the radio first exits the scan mode of operation, and then enters the emergency mode of operation (optionally following emergency revert procedures). At this point, Emergency Voice Interrupt could be invoked, if the feature has been configured in accordance with the Emergency Voice Interrupt operation as described previously.

The second interaction to consider occurs when the radio is provisioned for both the Scan Priority Sampling and a Transmit Interrupt feature. Priority Sampling is temporarily suspended when a Transmit Interrupt request is pending. This is necessary to ensure that the radio user's transmit request takes priority over the radio's receive activities.

Thirdly, the radio can be configured with the scan feature such that replies occurring within a specified duration are transmitted to the same group and channel (this reply is called talkback). A reply that occurs outside of this duration is considered a new transmission.

If the radio is provisioned for Transmit Interrupt and talkback, then Transmit Interrupt is applied to the same group and channel, when the radio user invokes a Transmit Interrupt feature while receiving. If the designated transmit channel is busy and the radio is not a member of the ongoing call, then the Voice Interrupt request is simply denied.

Recall the options for new voice transmissions – outside of the previously mentioned duration – are transmitted while scanning; include the selected channel (the channel from which scan was started), another predetermined channel, or on the last landed channel for voice. Data and digital signaling are always transmitted on the selected channel. The last landed channel is not updated for data and digital signaling. In the event that the channel selected for a new transmission is busy, a Transmit Interrupt feature may be invoked on that channel if so provisioned on that channel. However, the radio must additionally be a member of the call in progress for Voice Interrupt to be invoked.

Finally, a radio's interruptible voice transmission periodically stops transmitting momentarily, and "listens" to the channel to determine whether it is being requested to stop its transmission. When a radio is scanning channels and testing the channel for presence of a carrier while another transmitting radio is listening to the channel for Transmit Interrupt signaling, the scanning radio may conclude that the channel has no activity and moves on to the next channel in the Scan List. However, this occurrence should happen only occasionally. It is most likely that the next time the scanning radio visits the channel, it does not occur at the moment that the transmitting radio has suspended its transmission. The net result is that the time taken to detect channel activity for an interruptible voice transmission may increase slightly, versus uninterruptible voice transmissions. Since the repeater is transmitting continuously even during interruptible voice calls, this is only a concern when scanning channels that may contain interruptible voice Direct Mode transmissions.

2.15
Site Roaming

The Master repeater distributes the list to all the repeaters at the site.

The Rest Channel repeater of a site periodically broadcasts the Rest Channels of all neighboring sites Over-The-Air. The radio searches through the list of sites and selects the one with the strongest signal, and identifies this site as its current home site. The radio remains on this home site until the signal strength has dropped below a programmable threshold or when it has lost communications with the home site, at which time it attempts to find a better home site. If available, this process takes around 60 seconds in an IP Site Connect system, and around 10 seconds in a Capacity Plus Multi Site system. If a better home site is not

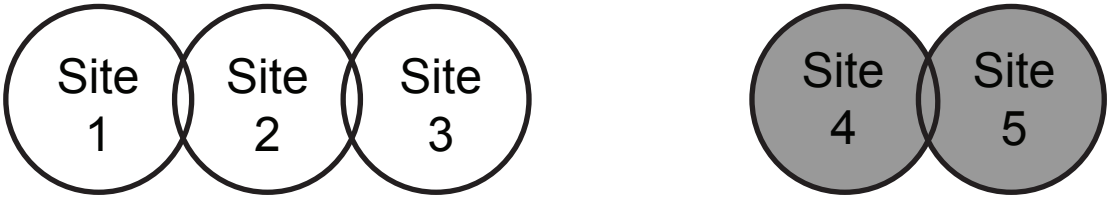
found, it remains on the previous home site and continues searching. Note that roaming occurs while the user is not in a call. Roaming is not supported while the user is in a call.

Automatic roaming involves scanning, which requires a radio to leave the Home channel for a short duration. This may cause the radio to make a late entry, or to miss a data/control call (without preambles). A stationary radio user may suspend the automatic roaming feature by using the Site Lock/Unlock features. The Site Lock/Unlock feature can be activated through the menu or a programmable button. An icon is shown on the radio display to indicate the status of automatic roaming.

Automatic roaming uses signal strength (RSSI) to select the Home channel. The signal strength is not always the best indication of the reception quality, especially when co-channel interference exists. If poor reception is encountered while automatic roaming is on, then the user can request the radio to find another channel. Automatic roaming, when activated through the menu/programmable button, allows the user to find another channel. The radio then responds to the user on the failure or success of the search. The radio LED indicates when the radio is roaming.

An example of neighboring sites is shown in the following figure. The Neighboring Sites List of a 'site A' should only identify the sites to which a radio can roam from site A.

Figure 27: Example of Neighboring Sites



For example, if the coverage areas of the sites are as shown in Figure 27: Example of Neighboring Sites on page 164, the Neighboring Sites Lists can be concluded in the following table:

Table 34: Neighboring Sites List

Site ID	Neighboring Sites List
1	2
2	1, 3
3	2
4	5
5	4

The radios can be programmed with all the six sites as neighbors to each other. However, this causes inefficiency and potentially slows down the roaming from one geographically adjacent site to another.

The radio has two methods in which it accomplishes the act of roaming; a passive method and an active method.

System	Description
IPSC IP Site Connect	MOTOTRBO supports the ability to automatically roam between sites of an IP Site Connect system. In an IP Site Connect system, a portable or mobile is configured with a roam list that contains a list of channels, each of which is one site (one repeater) of an IP Site Connect system (wide area system).

System	Description
	The process of searching for a better home site takes around 60 seconds in a IP Site Connect system. In IP Site Connect mode, the radio display indicates which site the radio is currently on, when the user enables Site Lock/Unlock via a button press
CPMS Capacity Plus Multi Site	MOTOTRBO supports the ability to automatically roam between sites of a Capacity Plus Multi Site system. In a Capacity Plus Multi Site system, the Master repeater is configured with a list of neighboring sites for each site. The process of searching for a better home site takes around 10 seconds in a Capacity Plus Multi Site system. In Capacity Plus Multi Site, the radio display indicates which site the radio is currently on, when the user presses a button preprogrammed as the “Site Alias”. A wide area talkgroup call is broadcasted over all the sites associated with the talkgroup. When a Group Call is dropped at a site due to poor reception, the radio roams and joins the call (as late entry) after landing on another site. This only happens if the site is associated with the talkgroup and the call has not ended. A Private Call is repeated over at most two sites. Therefore the radio can join the call (as late entry), only if the radio roams between those two sites.

2.15.1
Passive Site Searching

While passively roaming, the radio temporarily leaves the current home channel and inspects other sites to decide if a better site is available.

It is important to note that since the radio is temporarily away from the home channel, it is possible to miss the beginning of a transmission (late entry). Because of this, it is not advisable or required to perform passive roaming all the time. Therefore, the radio should only passively search for a better site when the current home site is no longer desirable. If the radio is within good coverage of a site, there is no need to search for a better site. In other words, the radio should only passively roam when the radio has moved far enough away from the site that its signal strength has degraded below an acceptable value or when its signal is no longer present. The signal strength threshold to initiate the Passive Site Search (Roaming RSSI Threshold) is configurable through the CPS. See Configuring the Roaming RSSI Threshold on page 168 for suggestions on setting the Roaming RSSI Threshold for various site configurations and scenarios.

Initiating Passive Site Search and selecting sites based on signal strength works well when the repeater is transmitting, but the MOTOTRBO repeater does perform in a shared-use environment and is required to de-key when not in use. If there is no activity on a system, the Passive Site Search cannot detect any repeaters and therefore is unable to determine at which site the radio should be on. Therefore, the repeater can be configured to transmit a beacon, called a roaming beacon. Roaming beacons are periodic short transmissions by a repeater when the repeater is neither transmitting nor having interference from other systems.

During times of no activity, the radio utilizes the signal strength of the beacon to determine when it should roam and which site it should roam to. If the radio does not receive a beacon in the expected duration, it assumes it is out of range of the repeater or that the repeater has failed and tries to roam to another site. See Beacon Duration and Beacon Interval Settings on page 177 for suggestions on setting the beacon duration and interval for various site configurations and scenarios.

The radio does not perform Passive Site Search while:

- transmitting,
- receiving a call of interest,
- in emergency,
- in good RF coverage,
- in talkaround (direct) mode,
- radio disabled,
- received call alert,
- monitor mode, or
- while in active menu.

System	Description
IPSC IP Site Connect	In IP Site Connect, the Passive Site Search method has the radio searching through a list of sites and selecting the one with the strongest signal. The duration of the beacon is a function of the number of sites in the IP Site Connect system and therefore in the roam list. The interval of the beacon is a function of the shared use rules of the channel and how quickly a radio is required to roam when there is no activity. The duration and interval of the roaming beacon are programmable, in an IP Site Connect system only. The radio does not perform Passive Site Search while on a channel that has scan list in IP Site Connect mode.
CPMS Capacity Plus Multi Site	In Capacity Plus Multi Site, the radio searches through a list of neighboring sites and selects the one with the strongest signal. This method is utilized whenever the site is unlocked. It relies on repeater transmissions in order for the subscriber to determine which site has the strongest signal strength. Since it is expected that the radio encounters other activity while performing the Passive Site Search, it qualifies the signal using the sites' programmed color code prior to selecting it as the new home. In addition, it sorts the sites in the roam list according to their signal strength in order to optimize follow up roams. Sites that have been detected in previous roam attempts and are assumed to be near by are searched before those that have not been detected before. Also, while roaming, the radio inspects the current home site in between other sites in order to minimize the time away. This strategy provides priority to the last home site and minimizes missing any transmissions while performing the roam attempt. In Capacity Plus Multi Site, the roaming beacon duration and interval are not configurable. The roaming beacon interval is five times the "lost detection beacon interval" of Capacity Plus Single Site. The duration of the roaming beacon, in Capacity Plus Multi Site consists of only one burst and is appended at the end of every fifth sequence of the Lost Detection Beacons. **NOTE:** The "lost detection beacons" are transmitted periodically by the Rest Channel repeater when the repeater is not transmitting. The detection of the beacon by a radio indicates that the radio is in the coverage area of the repeater.

2.15.2

Active Site Searching

The Active Site Search method consists of the radio sending wake-up messages to each repeater in its sorted roam list until it finds an active site. This method is utilized when the user or radio initiates a transmission and the home site repeater cannot be awoken, or when the user initiates a Manual Site Roam.

In most cases, the Passive Site Search determines and selects the correct site if the radio is in the unlocked state. It may be possible that the radio has roamed into a new site and has yet to receive a beacon.

When the user presses the PTT or a data transmission is requested, the radio tries to wake the Home channel repeater. This Home channel repeater is chosen from the repeaters at the radio's current home site which was determined by the Passive Site Search.

If the repeater does not wake up, the radio repeats this process for all the sites. If a repeater wakes up, the radio synchronizes itself with the repeater, completes the transmission and make the new site the home site. If the end of the roam list is reached and a site is not found, the user receives a failure indication.

This entire process of discovering and synchronizing with an active repeater increases the voice access time of the transmission (time from PTT to Talk Permit Tone). However, this increase only occurs for one transmission since the next transmission proceeds regularly on the new site.

NOTE: Wake-up messages are always sent politely. This means that if the radio detects an interfering signal, the radio does not transmit a wake-up message on that roam list member. Instead, it continues performing an Active Site Search on the next roam list member.

If the user requests a Manual Site Roam, be it through a button press or menu item, the radio actively searches for the next available site using the process described above. The Manual Site Roam does not necessarily find the best site, but rather allows the user to move to the next site that is in range and transmitting. If no site is found, a negative indication is provided to the user. If in direct mode, a successful site search changes the new channel found to repeater mode. An unsuccessful site search remains in direct mode.

NOTE: Generally, the radio does not perform any Passive Site Search during an emergency. No automatic roaming is performed when the radio is reverted during an emergency. However, when configured to a non-revert emergency channel and with Active Site Search enabled, the radio will perform Active Site Search automatically whenever the RSSI of the repeater drops below the programmed threshold or if it no longer detects repeater beacons. Note that Manual Site Roam is supported while in an emergency. See Emergency Revert, GPS/Data Revert, and Roaming Interactions on page 179 for more details.

If this is still not acceptable in the area of operation, the radios should have automatic Active Site Search disabled, the Manual Site Roam button removed, and the beacon interval should be configured as short as possible. This ensures that the Passive Site Search finds new sites quickly and the user has no method to initiate an Active Site Search.

NOTE: If Active Site Search is disabled, there is no roaming while in an emergency

System	Description
IPSC IP Site Connect	In an IP Site Connect system, the beacon interval is usually in the range of minutes and it typically takes approximately a minute for a radio user to move out of range of one site and into the range of another during Passive Site Search. Until a new site is found, the radio considers the previous site as the home site. For IP Site Connect, the radio chooses the single repeater at its home site channel.

System	Description
	It is important to note that Active Site Search causes wake-up messages to be transmitted on each roam list member's frequencies until a site is found. This may not be agreeable in some areas where frequency overlap and sharing is common. In order to minimize the number of un-wanted transmissions, the radio transmits one polite wake-up message. If a radio sends frequent GPS location updates while out of range, the radio limits the Active Site Search to only occur once every 30 seconds. This scenario is applicable in an IP Site Connect system only.
CPMS Capacity Plus Multi Site	In Capacity Plus Multi Site the radio chooses the current Rest Channel repeater at its home site. The radio then tries to wake a repeater at the home site. If the radio has lost the previous site and is searching for a new site, all transmissions by the radio fail. Otherwise, the radio tries to wake the Rest Channel repeater.

2.15.3

Roaming Considerations

This section describes the roaming considerations.

2.15.3.1

Configuring the Roaming RSSI Threshold

The Roaming RSSI Threshold is a CPS configurable parameter that controls the signal strength, that a subscriber needs to reach before searching for another site.

This RSSI roaming threshold can be CPS configured as either system wide, where every site in the system has the same threshold, or on a per site basis, where each site may have its own roaming RSSI threshold, and this roaming RSSI threshold may be different from site to site.

2.15.3.1.1

System Wide Roaming RSSI Threshold

If the Roaming RSSI Threshold is configured as system wide, and the RSSI measurement of the currently determined home site is above the specified Roaming RSSI Threshold, then the radio remains on that site and not roam.

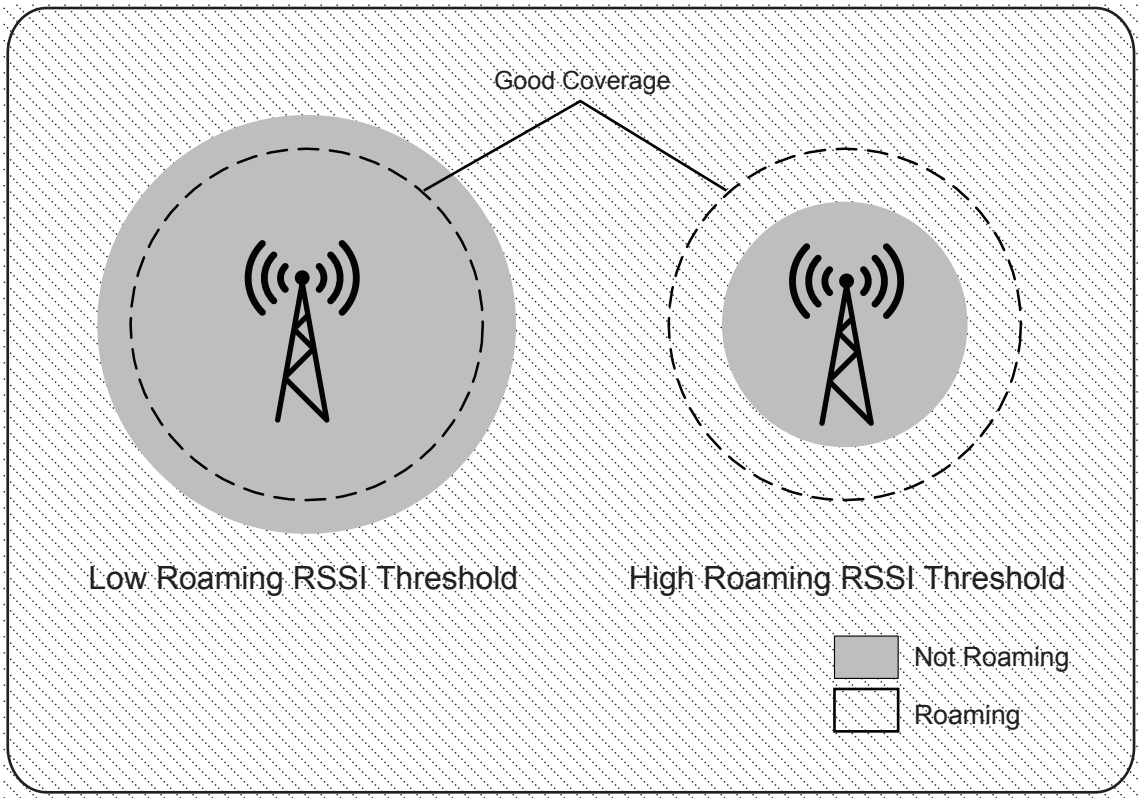
Once the RSSI measurement drops below the threshold it begins a Passive Site Search process to find a site with higher signal strength. This parameter essentially controls the distance away from a site a subscriber will begin looking for another site. In real life environments RF coverage is seldom a perfect circle, but to simplify this explanation, coverage is abstracted as a circle.

It is important to note that while passively roaming the radio temporarily leaves the current home site to determine if a stronger site is available. Since the radio is temporarily away from the home channel, it is possible to miss the beginning of a transmission (for example, enter the call late). Because of this, it is not advisable to perform passive roaming all the time.

The setting of the Roaming RSSI Threshold is a balance between when a radio leaves one site and look for the next versus how often the radio performs roam and therefore increase the chances of late entry to voice calls. If the Roaming RSSI Threshold is too low, the radio remains on a low signal strength home site even though there might be a stronger site available. If the Roaming RSSI Threshold is too high, the radio is roaming in full coverage of a repeater and causing late entry when not required. The following figure shows the impact of the Roaming RSSI Threshold value in relationship to the good coverage line (dotted) which most system coverage is

designed to meet. Note that the Roaming RSSI Threshold is a negative number therefore a high value is -80 dBm and a low value is -120 dBm. The colored area is where the radio would roam.

Figure 28: Roaming Triggered by Roaming RSSI Threshold Value



The default value of the Roaming RSSI Threshold is -108 dBm. It can be programmed for anything between -80 dBm and -120 dBm. A value of -108 dBm is approximately 80% of the good coverage. Therefore roaming occurs in the outer 20% of coverage. The default value is acceptable for most configurations but may not be optimal in a some particular configurations. Before setting the Roaming RSSI Threshold, one must consider the customer's site configuration.

Consider the following four basic site configurations:

Table 35: Basic Site Configurations

Configuration	Description
Dense Overlapping Coverage (Urban)	This type of coverage consists of dense sites with generous overlap. This coverage type is often found in large cities or highly populated areas. Overlapping sites utilize different frequencies. Non-overlapping sites may share frequencies, but those that do share frequencies need to have different color codes if they need to be distinguished while roaming. This type of coverage is highly likely to encounter a shared use on one or all of its sites. A radio user may be within coverage of three to four sites at a time. The time it takes a radio user to move from the coverage of one site to another is in the range of 10 minutes.
Isolated No Lapping Coverage (Rural)	This type of coverage consists of isolated sites with little to no overlap. This coverage type is often used for isolated sites in rural areas, although could be used to cover a single part of a small city. Non-overlapping sites may share frequencies, but those that do share frequencies

Configuration	Description
	need to have different color codes if they need to be distinguished while roaming. This type of coverage is less likely to encountered shared use although possible. A radio user will only be within coverage of one site at any time. The time it takes a radio user to move from the coverage of one site to another is in the range of multiple hours.
Corridor Coverage	This type of coverage consists of in-series slightly overlapping sites. This coverage type is often used for covering highways, train tracks, shore lines, or rivers. Frequency re-use is common in this configuration since one site only overlaps with its two adjacent sites. Non-overlapping sites may share frequencies, but those that do share frequencies need to have different color codes if they need to be distinguished while roaming. A radio will only be within coverage of one to two sites at a time. The time it takes a radio user to move from the coverage of one site to another is in the range of an hour.
Multi-Floor Coverage	This type of coverage consists of dense extremely close sites with short range coverage and generous overlap. This coverage type is often used for covering tall buildings, or deep tunnels. Frequency re-use is not common due to the small coverage footprint usually implemented with in-building radiax antenna systems. This coverage type also often encounters quick signal strength drop offs due to the nature of in building coverage. Non-overlapping sites may share frequencies, but those that do share frequencies need to have different color codes if they need to be distinguished while roaming. A radio will only be within coverage of one to two sites at a time. The time it takes a radio user to move from the coverage of one site to another is in the range of one minute.

Reference the following diagrams.

Figure 29: Dense Overlapping Coverage (Urban)

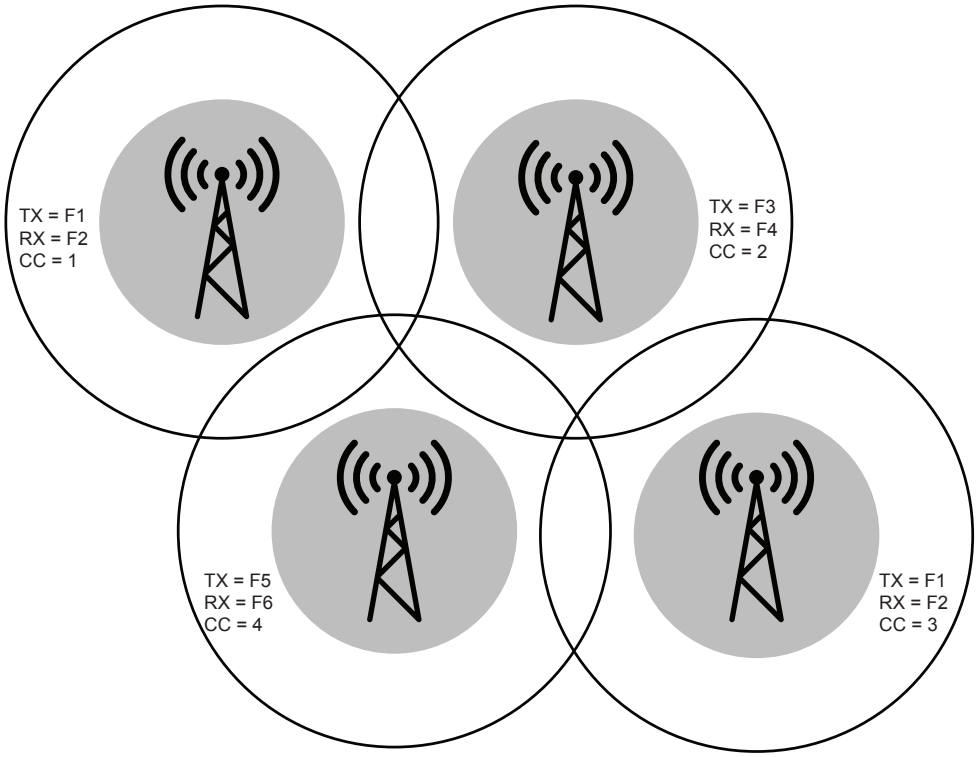


Figure 30: Isolated No Overlapping Coverage (Rural)

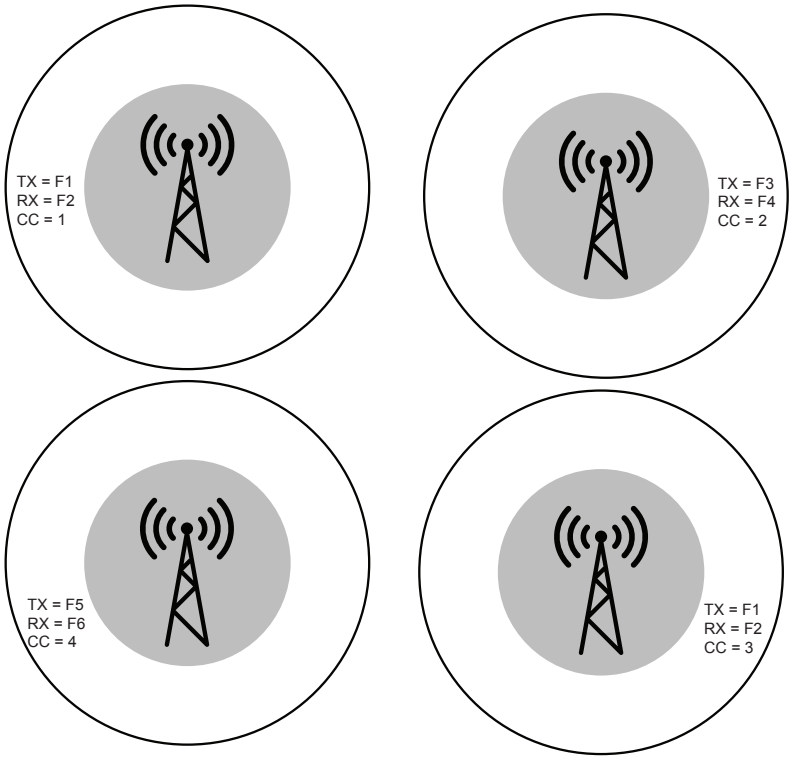


Figure 31: Corridor Coverage

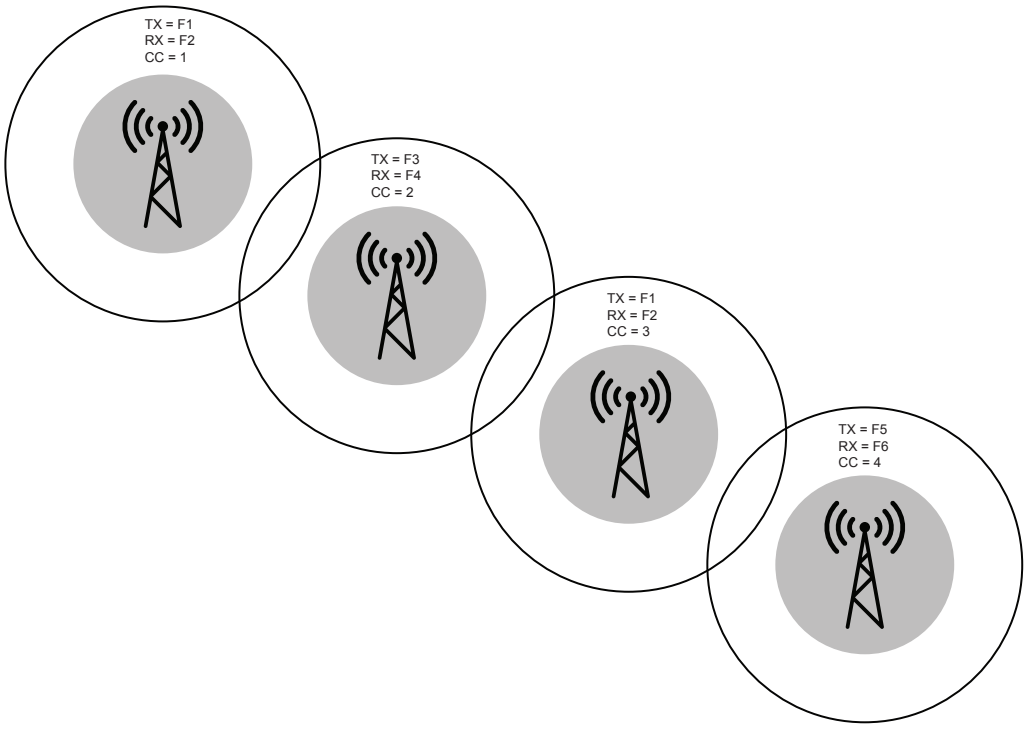
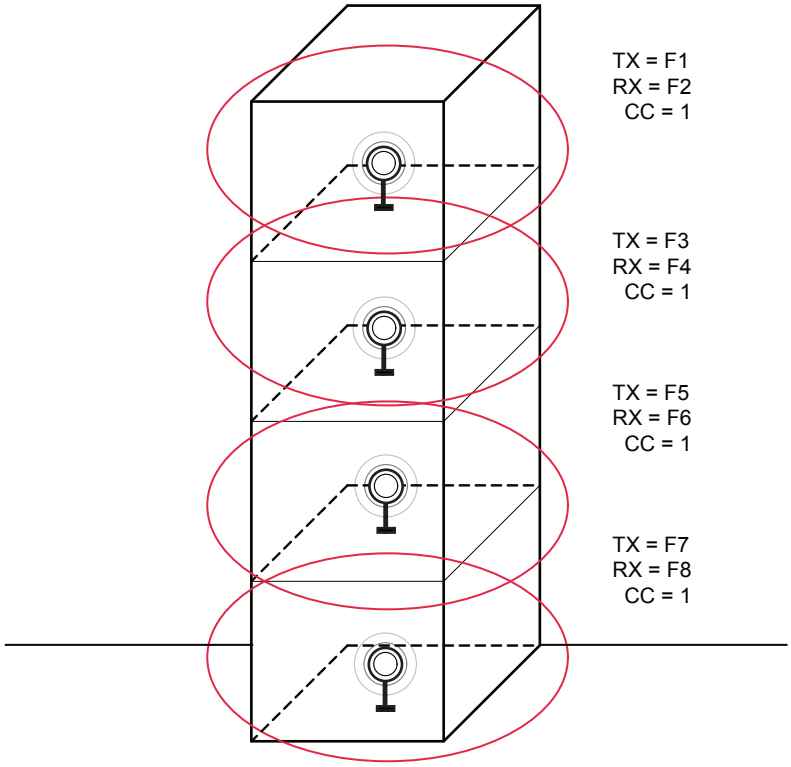


Figure 32: Multi-Floor Coverage



The site configuration should be taken under consideration when the Roaming RSSI Threshold is set. For example if the customer has a “Isolated No Overlapping Coverage” the threshold can be set to its lowest value of -120 dBm. Because there is no overlap, there is no reason for the radio to start roaming until well outside of the coverage range of the repeater. For extremely close sites with large overlaps and quick signal drop off like the “Multi-Floor Coverage”, it might be better to set to it to a higher value so that the radios search for stronger sites closer to the repeater. The following table is the suggested setting for each basic site configuration. Many radio systems have a combination of site configurations so the system designer must take all configurations into consideration and choose an appropriate value.

Table 36: Basic Site Configuration Setting

Site Configuration	Recommended Roaming RSSI Threshold	% of Outer Range Radio Will Roam
Isolated No Overlapping Coverage (Rural)	–120 dBm	Out of Range
Corridor Coverage	–110 dBm	10%
Dense Overlapping Coverage (Urban)	–108 dBm	20%
Multi-Floor Coverage	–102 dBm	50%

It is important to note that the preceding Roaming RSSI Thresholds assume the outbound and inbound RF coverage of the system is balanced. In other words, when a radio is within good outbound coverage of the repeater the radio’s inbound transmission can reach the repeater. Since the roaming algorithm uses the outbound transmission to determine when to roam, having an unbalanced system can cause radios not to

roam even though they can no longer reach the repeater. This can lead to radio transmissions that do not reach the repeater and are therefore not repeated.

One method to rectify this problem is to lower the output power of the repeater. This decreases the outbound coverage area, but ensures that if a subscriber can hear the repeater well, it can respond successfully. If lowering the output power is not desirable, the Roaming RSSI Threshold needs to be raised higher (less negative) than the recommended values. This forces the radios to roam to another site within very good RF coverage of another. This value may be different for portables and mobiles since they have different output power and therefore different inbound coverage. Portables may need a higher (less negative) Roaming RSSI Threshold than mobiles.

Also note that there is one Roaming RSSI Threshold per roam list. This means that if one site has an inbound outbound imbalance and another does not, it may be difficult to find the correct Roaming RSSI Threshold to exactly accommodate both sites. In other words if you set the threshold to roam correctly on the imbalanced site, it may end up roaming too early on a balanced site.

2.15.3.1.2
Per Site Roaming RSSI Threshold

When the Roaming RSSI Thresholds for all the sites of the system are configured the same, it may cause a radio to roam very often between sites, especially when the radio is moving around high buildings in a city.

System	Description
IPSC IP Site Connect	This per site configuration is available to MOTOTRBO radios (version R02.00.00 onwards) in IP Site Connect.
CPMS Capacity Plus Multi Site	This per site configuration is available to MOTOTRBO radios (version R02.00.00 onwards) in Capacity Plus Multi Site.

This frequent roaming may cause large audio holes or let the radio miss calls. This situation can be improved if we could lower the Roaming RSSI Threshold of the site that the radio is currently in, but still at acceptable level. When the current site's RSSI is above that lowered threshold, the radio will not roam even if the radio detects a higher RSSI from adjacent sites. In this way, the radio could avoid frequent roaming.

Thus, if audio holes/missing calls from frequent roaming is a problem for the system, we may consider to configure the Roaming RSSI Threshold on a per site basis. That is, each site in the roaming list can be configured to have its own Roaming RSSI Threshold, and this threshold may be different from site to site. When the threshold is configured on a per site basis, as long as the current site's RSSI >= its configured Roaming RSSI Threshold, the radio does not roam. When roaming, the radio uses the relative RSSI value, to decide which site to roam to. The relative RSSI value is, the "current RSSI – its CPS configured Roaming RSSI Threshold" value.

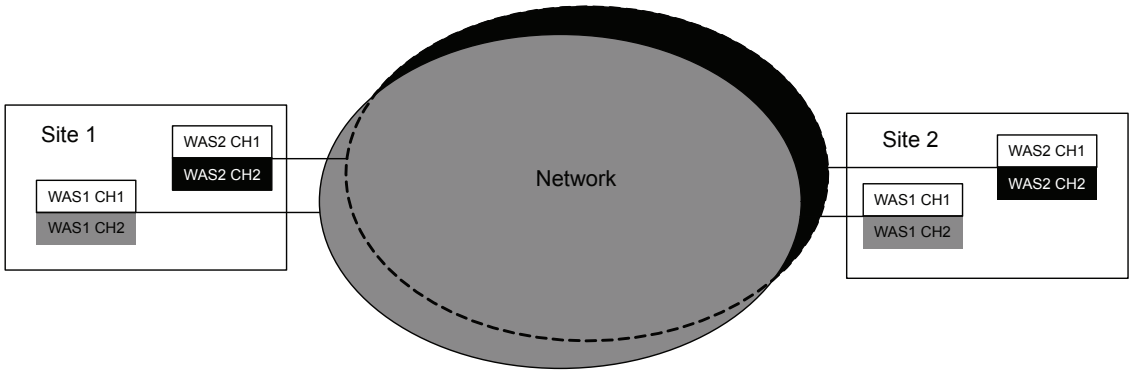
2.15.3.2
Roam List Configuration

IPSC

When configuring a Roam List it is important to keep in mind that a system can contain more than one IP Site Connect system, or also known here as a wide area system.

A wide area system is made up of one or two wide area channels. Each wide area channel is an individual voice path, in other words, the users on the same wide area channel monitors each other on any site. The following figure shows a system with 2 sites, 2 wide area systems, each with 2 wide area channels. Wide Area System 1, Channel 1 (WAS1 CH1) represents a wide area channel in wide area system 1.

Figure 33: Two Wide-Area Systems (Each with Two Wide-Area Channels)



Each wide area channel should have its own roam list. The roam list should contain one logical channel from each site that corresponds to the wide area channel. A logical channel is defined as the frequency pair, color code, timeslot combination. If there are multiple personalities (CPS Channels) that reference the same logical channel, only one should be added to the wide area channel roam list. Only wide area channels should be added to the roam list.

The following table shows an example of the two site configuration in CPS. For clarification, the colors match those of Figure 33: Two Wide-Area Systems (Each with Two Wide-Area Channels) on page 175.

Table 37: Two Site Configuration in CPS

Zone/Folder (Alias)	Personality(CPS Channel)# – Alias	Logical Channel			Group	Roam List # – Alias
		Frequency Pair	Color Code	Time Slot		
Zone 1 (Site 1)	1 – SITE 1 TGA	1	1	1	TGA	1 – WAS1 CH1
	2 – SITE 1 TGB	1	1	2	TGB	2 – WAS1 CH2
	3 – SITE 1 TGC	2	1	1	TGC	3 – WAS2 CH1
	4 – SITE 1 TGD	2	1	2	TGD	4 – WAS2 CH2
Zone 2 (Site 2)	5 – SITE 2 TGA	3	2	1	TGA	1 – WAS1 CH1
	6 – SITE 2 TGB	3	2	2	TGB	2 – WAS1 CH2
	7 – SITE 2 TGC	4	2	1	TGC	3 – WAS2 CH1

Zone/Folder (Alias)	Personality(CPS Channel)# – Alias	Logical Channel			Group	Roam List # – Alias
		Frequency Pair	Color Code	Time Slot		
	8 – SITE 2 TGD	4	2	2	TGD	4 – WAS2 CH2

The roam lists are configured, as follows:

Table 38: Roam List Configuration

Roam List # – Alias	Personality (CPS Channel) # – Alias
1 – WAS1 CH1	1 – SITE 1 TGA
	5 – SITE 2 TGA
2 – WAS1 CH2	2 – SITE 1 TGB
	6 – SITE 2 TGB
3 – WAS2 CH1	3 – SITE 1 TGC
	7 – SITE 2 TGC
4 – WAS2 CH2	4 – SITE 1 TGD
	8 – SITE 2 TGD

As can be seen there are 4 roam lists required for the 4 wide area channels. Each roam list contains only one personality that references the desired logical channel at each site. Although not necessary, personalities that correspond to a site can be placed together in their own zone (or folder). This helps further remove the concept of site from the radio user and allow the site roaming feature to choose the appropriate site. If they must manually choose a site, they can change zones. Using the actual name of the site as the zone alias helps clarify this to the end user, but it is not required. Since the same group is mapped to the same dial position in each zone, the user has the same group selected as they change through the sites (zones). In this example the personalities are aliased with the group names, but other aliases that define Site, Channel, or Group name can be used. If there are more than one group per wide area channel, a roam list can be created for each group to utilize. It is important to understand that when the radio determines a new home site to be one of the roam list members, it only utilizes the logical channel attributes of the roam list member. The remaining attributes are used from the selected personality.

The following logical channel attributes of the home site are utilized:

- Transmit Frequency and Transmit Reference Frequency,
- Receive Frequency and Receive Reference Frequency,
- Color Code,
- Time Slot,
- Talkaround Setting,
- GPS Revert Channel
- Emergency System (Including Emergency Revert Channel)

Take specific note of the GPS Revert and Emergency Revert Channels. Because physical channels are different per site, the Revert Channels must change when the radio roams to another site. It is recommended that emergency settings (other than Revert Channel) should be the same for all personalities within a roam list. Otherwise the radio may perform an emergency differently as it moves from one site to another.

The remaining personality attributes (Transmit and Receive Group List, Channel Access, and others) are used from the currently selected channel regardless of which site the radio is currently roamed to. It is good practice to make these parameters identical for personalities within a roam list so that the radio acts the same regardless if it roams to the personality or if the user selects the personality.

2.15.3.3
Scan or Roam

When selecting a roam list for a personality to utilize, one notices that a personality cannot contain a roam list and a Channel Scan List.

MOTOTRBO does not currently support the ability to roam between sites and then scan channels at a particular site. Therefore while on a particular personality, a user has the ability to roam or scan channels, not both.

2.15.3.4
Beacon Duration and Beacon Interval Settings

IPSC

If there is no activity on a system, the repeaters hibernate and the radio's Passive Site Search is not able to determine the signal strength and determine which site is the best, as repeaters are not transmitting.

Due to this, the repeater can be configured to transmit a beacon when not active and there is no other interfering signal. During times of no activity, the subscriber utilizes the signal strength of the beacon to determine when it should roam and which site it should roam to. If the subscriber does not receive a beacon in the expected duration, it assumes it is out of range of the repeater (or the repeater has failed) and attempts to roam to another site.

Both the beacon duration and the interval are programmable through CPS. The beacon duration is only configured in the repeater, but the beacon interval is programmed in both the repeater and the radio.

The duration and interval of the beacon is a function of the Over-The-Air shared use rules in the customer's region. The beacon duration is dependent on the number of sites in the IP Site Connect system and therefore in the roam list. The beacon interval is dependent on how quickly the radio is expected to roam to and from a site when there is no activity. The minimal duration and interval need to be met while keeping within the shared use guidelines of the region.

The ratio of the beacon duration and beacon interval equate to how often the repeaters transmit while there is no inbound radio activity, (the beacon transmit ratio). This ratio is not directly programmed into the system, but is rather a guideline for setting the Beacon Duration and Interval. If on a shared use frequency the beacon transmit ratio should be kept low. The target ratio is between 5% and 10%. In other words, if there is a need to increase the beacon duration, the beacon interval must also increase in order to keep the correct ratio.

If the beacon duration is configured too short it can be difficult for a roaming radio to detect it. This is especially true as the number of sites increases. As the amount of time between a roaming radio's repeated roam attempts to a particular site increases, it is less likely to be inspecting the site at the exact moment that the beacon is transmitted. Recall that the home site is sampled in between other sites, which increases the overall cycle time. A user is typically within the coverage of no more than 4 sites at any given time, therefore even with a large roam list, most of the sites have no activity and can be inspected very quickly. If numerous sites have shared-use frequencies (interference) the radio takes longer to get through its roam list and this increases the time between inspections of one particular site. Note that because the roam list is sorted by signal strength, the nearer sites are inspected first. Alternatively, if a user is transitioning to a site that they have not visited lately, the first roam may take slightly longer, but once it is has been detected this site moves to the front of the roam list. To improve the likelihood of receiving the beacon, the beacon duration should be

increased. It is safer to have a beacon duration longer than shorter, but keep in mind that if the duration is increased, the beacon interval must be increased to meet the beacon transmit ratio

The beacon interval controls how quickly a radio can roam to a site and how quickly it roams away from a site when there is no activity. When roaming with no system activity, a radio needs to see a beacon in order to roam to a new site. If the repeater beacon is sent out every one minute, the radio may be one minute deep into the site before it sees the site and roams to it. Similarly, when roaming with no system activity, a radio may be one minute outside of the site before it attempts to roam.

The impact of this value often changes based on how quickly the users are traveling. For example a car driving 60 m.p.h. can cover a mile a minute and therefore is one mile into or out of a site before roaming. This could be acceptable for site configurations such as the “Isolated No Overlapping Coverage” or the “Corridor Coverage”, but the “Dense Overlapping Coverage” coverage type may require a quicker beacon since it both triggers the leaving and entering of sites. Note again that if the user initiates a transmission before the passive roam finds the beacon, the radio attempts to wake-up the site repeater.

A one minute beacon interval may not be an issue for users on foot unless the sites are very close like in the “Multi-Floor Coverage” example. In this case a user in an elevator can move between sites at a very high rate. A one minute interval may cover the entire duration of an elevator ride from the first floor to the top. Here, it is recommended to keep the beacon interval in the range of 20 seconds. Note that a beacon transmit ratio of a 5% may not be achievable for systems with a high number of repeaters. In this case the designer may either decide to abandon the target beacon transmit ratio since in-building coverage usually does not propagate very far or have neighbors to interfere with, or lower the beacon duration to only cover the max number of overlapping sites a radio may ever see.

The following table is the recommended beacon duration and beacon interval (8% beacon transmit ratio) for a varying number of sites. The default value is a 4.32 second Beacon Duration with a 60-second Beacon Interval.

Table 39: Recommended Beacon Duration and Beacon Interval

Number of Sites in Wide Area System	Beacon Duration (sec.)	Beacon Interval (sec.)
2	0.72	10
3	1.92	30
4	3.12	40
5	4.32*	60*
6	5.52	70
7	6.72	90
8	7.92	100
9	9.12	120
10	10.32	130
11	11.52	150
12	12.72	160
13	13.92	180
14	15.12	190

Number of Sites in Wide Area System	Beacon Duration (sec.)	Beacon Interval (sec.)
15	16.32	210

NOTE: * Default Values - If shared use is not a problem in the customer's region, the beacon transmit ratio become less important and it may be desirable to increase the beacon duration and decrease the beacon interval past what is identified here. If the automatic Active Site Search feature is going to be disabled, it is advisable to lower the beacon interval as much as possible since radios rely only on it to find the appropriate site.

2.15.3.5
Emergency Revert, GPS/Data Revert, and Roaming Interactions

System	Description
IPSC IP Site Connect	Emergency Revert and GPS Revert are specific to the current home site of an IP Site Connect system. This is important since a Revert Channel of one site is most likely not a revert channel of another site. Although it is possible to revert while roaming, roaming while reverted is limited.
CPMS Capacity Plus Multi Site	Data Revert is specific to the current home site of a Capacity Plus Multi Site system. This is important since a Revert Channel of one site is most likely not a Revert Channel of another site. Although it is possible to revert while roaming, roaming while reverted is limited.

While in emergency and configured as non-revert the radio does not perform Passive Site Search. If Active Site Search is enabled, the radio performs an automatic Active Site Search when the RSSI of the repeater drops below the programmed threshold or if it no longer monitors the repeater beacons (normal triggers for passive roam). This is considered as a more aggressive method to site search as compared to passively searching. The radio also supports the ability to trigger an automatic Active Site Search on transmit request by the user or automatically by the radio (GPS). Standard Manual Site Roam is also supported. Active Site Search can be enabled or disabled through the CPS.

While reverted due to emergency, no automatic roaming occurs. This is primarily due to the fact that the emergency Revert Channels may not be on the same logical channel, and the emergency handlers may not be the same. It is not desirable for a user to automatically leave one emergency handler and switch to another without notification.

A radio performs an Active Site Search (using the selected personality's roam list) when the emergency is first initiated if the Revert Channel is not available. Once on the Revert Channel, only Manual Site Roam is available. In other words, if a user enters emergency, and then roams out of range of the Revert Channel, the radio does not automatically roam even if the user presses the PTT. When a Manual Site Roam is initiated while reverted, the radio performs an Active Site Search using the selected personality's roam list.

When a new site is found due to a roam while in emergency, the emergency process restarts on the new site (similar to manually changing the dial position) if the new home is provisioned for revert. If the new home is not provisioned as revert, the emergency process does not restart since the radio never left the wide area channel. It is assumed that the original target of the emergency is still monitoring since the source never left the wide area channel. The radio also assumes that emergency handling configuration (outside of revert) is the same across the wide area channel. The radio reverts if the new home site is provisioned as such. If a new site is not found, the radio returns and remains on the original site or the site revert channel, if

provisioned. Per normal revert rules, upon clearing the emergency the radio would return to the home site. If the radio roams to a site that has Emergency Disabled (or no Emergency System) then radio remains in emergency but does not process the emergency sequence. The user can then attempt another Manual Site Roam to find a site that does have emergency.

NOTE: In most cases, the passive search while not in emergency should get the radio on the correct site and therefore when it emergency reverts, it should still be at the same site. If in Silent Emergency mode, no ergonomics associated with Manual Site Roam are displayed.

When a GPS/Data Revert occurs, no automatic roaming is supported. If the GPS/Data Revert Channel is out of range, the data message is dropped. On return to the home channel after a failed GPS/Data Revert, the radio continues the Site Search using the selected personality's roam list.

While in emergency (initiator, not receiver) and GPS/Data Revert occurs, no automatic roaming is supported while reverted. If GPS/Data Revert Channel is out of range, the data message is dropped. On return to an emergency Revert Channel in an IP Site Connect system, after a failed GPS revert, the radio is NOT initiated an Active Site Search since this is not supported while in emergency.

For more information on how Emergency Revert and GPS/Data Revert operate together, see Emergency Revert and GPS/Data Revert Considerations on page 523 in *Installation and Configuration* manual.

Table 40: Roaming Interaction Summary

Feature	Passive Site Search	Automatic Active Site Search on TX Request	Automatic Active Site Search on Loss of Site	Manual Site Roam
Tactical Emergency (Non-Revert)	Not Available	Available	Available	Available
Emergency Revert	Not Available	Only Available on Emergency Initiation	Not Available	Available
GPS/Data Revert	Not Available while Reverted	Performed After Dropping the Data Message	Not Available	Available

2.15.3.6
Performance while Roaming

It is important to note that roaming (not just enabled, but in the act of searching) may cause some minor degradations in performance. Therefore, it is important that the Roaming RSSI Threshold and the radio's Site Lock be set appropriately when not mobile.

These degradations are similar to what a scanning radio would experience. Degradation may be experienced in the following areas:

- Late Entry to Voice Transmissions (Voice Truncation)
- Longer Preambles required for Control Messages and Data
- Increased setup time for Confirmed Private Calls
- Group Call Time to Talk Permit may increase if Site Search Required

While roaming the radio temporarily leaves the current home channel and inspects other sites to decide if a better site is available (similar to scan). This means that radio may not be present on the home site when a call starts. The home site is inspected between every other site to minimize the time away. This is similar to the scan ordering of a priority scan member.

One issue that arises from this situation is that if a Group Call or unconfirmed Private Call starts while the target is inspecting another site, the may be a short delay before joining the call. This equates to voice truncation for the target radio.

Another issue faced is the need for longer preambles in order for command and control messages, and data to be received by a radio that is currently roaming. Without an extended preamble, roaming radios miss the message.

The need for preambles also affects the setup time for confirmed Private Calls. Confirmed Private Calls utilize command and control messaging to setup the call. In addition, the first setup attempt does not utilize any preambles. This increases the setup time between radios that are not roaming. This means that the first setup attempt of a Private Call is not successful if the target radio is roaming. The radio then attempts a second time with a preamble. This second attempt is likely to be successful and the Private Call continues.

If the current home site cannot be awoken, the radio attempts to locate another site using an automatic Active Site Search. As the radio attempts to wake-up other sites, the user must wait. This increase in time is recognized as an increase in the time from PTT to receiving the Talk Permit Tone. This is not expected to occur often if the beacon interval is set appropriately.

It is expected that the value that the roaming feature adds is worth these performance degradations. The Beacon Interval and the Roaming RSSI Threshold should be set appropriately to minimize the amount of time a radio is searching for a site.

2.15.3.7
ARS Registration on Roaming

When a radio roams in data capable mode with the Presence Service enabled, the radio can be configured to automatically send ARS registration messages to the Presence Notifier application. This ARS registration on roaming capability can be enabled or disabled through CPS configuration, and is applicable in both Passive Site Search and Active Site Search.

During Passive Site Search roaming, when ARS registration on roaming is disabled, the radio roams when the RSSI of the repeater roamed into is greater than the RSSI of the current Home channel by 0 dB. However, when ARS registration on roaming is enabled, the radio roams only when the RSSI of the repeater roamed into is greater than the RSSI of the current Home channel by 6 dB. As a result, this reduces frequent registrations on roaming.

During Active Site Search roaming, when ARS registration on roaming is enabled, the radio automatically sends an ARS message to the Presence Notifier application if it roams into a site successfully.

This ARS registration on roaming capability can be used by user applications to monitor which repeater site a radio is currently in.

2.16
Voice and Data Privacy

Over a digital channel, MOTOTRBO supports a way to keep communication (both voice and data) private. Privacy protects the information, where “protection” means that the MOTOTRBO resists reading of data payload or listening of voice by anybody other than the intended receivers.

MOTOTRBO does not provide any mechanism to authenticate the radios or radio users and it does not protect the integrity of the messages.

2.16.1
Types of Privacy

MOTOTRBO offers the following types of privacy mechanisms – Basic, Enhanced, and Advanced Encryption Standard (AES). Basic privacy utilizes Motorola Solutions proprietary mechanisms and algorithms and therefore is not interoperable with privacy offerings from other vendors.

Both Enhanced and AES privacy are licensed to the subscriber. They can be utilized in all MOTOTRBO architectures.

The main differences between Basic, Enhanced privacy, and AES privacy are that Enhanced and AES privacy provide a higher level of protection and support multiple keys in a radio, compared with one key in the case of Basic privacy.

The main differences between Enhanced and AES privacy are the algorithm utilized and their key size. Enhanced privacy utilizes the ARC4 algorithm with 40-bit keys, and AES privacy utilizes the AES algorithm with 256 bit keys. The AES privacy has a higher level of protection in terms of algorithm than Enhanced privacy.

The privacy types are not interoperable. Only one type can operate in each radio at any time. This implies that all digital private channels support either Basic or Enhanced privacy, and that all radios on a repeater must use the same mode, even if they are in different groups. In direct mode, all radios that communicate with each other must use the same privacy mechanism.

Enhanced and AES privacy are interoperable with privacy offerings from other vendors.

2.16.1.1
AES Configuration in MOTOTRBO

The Symmetric keys (AES privacy) options are visible in the CPS only if the AES feature is purchased. The radio, repeater, and MNIS of a system require configuration for AES. In CPS, the radio codeplug lists all **Symmetric** keys on the **Symmetric** section of the Security tab. Privacy types **None** or **Enhanced** are independent from the Symmetric keys configuration. Basic privacy does not work with AES. If Basic privacy is configured, the radio bypasses AES for the transmission even if Symmetric keys are configured in the radio. The radio allows the **Privacy Type** selection of **None** or **Enhanced** in the section **Privacy** from the **Security** tab with or without Symmetric Keys. Only one privacy type is allowed on each radio channel. The radio allows up to 16 different Symmetric keys to be configured. Each Symmetric key can be up to 256 bits in length.

To support AES, the repeater codeplug must be configured with Enhanced Privacy Type since the repeater does not encrypt or decrypt any AES payload. The Enhanced privacy option allows the repeater to repeat the AES and Enhanced privacy encrypted audio and data bursts. For proper functioning of the repeater in a system with AES encrypted transmissions, the repeater must be running on firmware version R02.30.00 or later.

A radio can be configured with both Enhanced privacy keys and Symmetric keys. The radio can receive audio and data calls encrypted with AES or Enhanced Privacy keys, from any talkgroup in the RX Talkgroup list that is tied to a personality, as long as the same key and privacy type of the transmitting radio is selected in the personality.

The RM feature of the CPS can be used to pre-configure and manage the Symmetric Keys. The AES uses the Symmetric Keys as encryption keys.

The MNIS requires a Symmetric Keys configuration for the AES encryption. The MNIS allows up to 255 Symmetric Keys.

2.16.2
Strength of the Protection Mechanism

The Basic, Enhanced, and AES privacy types protect the confidentiality of the payload. The protection mechanisms described in this section require a key that is shared only among the intended parties.

The resistance provided by Basic privacy is minimal for the following reasons:

- Basic privacy uses a non-cryptographic algorithm to transform plain voice/data into protected voice/data. It is possible for an adversary to obtain the key by storing a few Over-the-Air voice or data packets and performing a few simple mathematical operations.
- Basic privacy uses 16-bit keys. A user selects a key from 255 predefined keys stored in the CPS. The limited number of possible keys makes it easy for an adversary to guess the key in use.

NOTICE: The intended use of the Basic privacy is to stop casual eavesdropping only.

The resistance provided by the Enhanced privacy is significantly more extensive than the resistance provided by the Basic privacy for the following reasons:

- Enhanced privacy uses a cryptographic algorithm to transform plain voice/data into protected voice/data. The algorithm is the well-known Alleged RC4 (ARC4) and is the same as RC4. A cryptographic algorithm makes it very difficult for an adversary to obtain the key from over-the-air protected messages.
- **NOTICE:** The name “RC4” is trademarked by RSA Security. Although “unofficial” implementations are legal, the RC4 name cannot be used.
- The Enhanced privacy uses 40-bit long keys. A radio can store up to 16 keys and the Enhanced privacy allows using different keys for different channels. A large number of possible keys (approximately 1 trillion) makes it difficult for an adversary to guess the value of a key. Note that a 40-bit long key may not provide the protection needed to transmit valuable data such as credit card numbers.
- Using the same key, the Enhanced privacy protects each superframe of voice or each data packet in a different and unrelated way. This increases the resistance further.

The resistance provided by the AES privacy is significantly better than the resistance provided by Enhanced privacy for the following reasons:

- A cryptographic algorithm is used to transform plain voice/data into protected voice/data. The AES has been adopted by the United States government and is now used worldwide.
- The AES uses 256-bit long keys. A radio can store up to 16 Symmetric Keys for AES privacy, and the radio configuration allows using different keys for different channels. A large number of possible keys makes it difficult for even sophisticated hackers to guess the key from the OTA interface.
- Using the same key, the AES privacy protects each superframe of voice or each data packet in a different and unrelated method, which further increases the resistance.

2.16.3
Effects of Privacy Protection on Performance

Basic privacy uses only one key, which is known to both the sender and the receiver. This eliminates the need to transport cryptographic parameters (for example, Key Identifier) with the voice or data payload. A voice message, in case of Basic privacy, neither requires any modification in the payload nor any additional headers. Therefore, the System Access Time and the audio quality of a Basic privacy protected voice are the same as that of an unprotected voice.

Enhanced and AES privacy use multiple keys and a random number to ensure that the encryption data is different for each data message and each super frame of a voice message. This requires transporting cryptographic parameters (for example, Key Identifier, Initialization Vector) with the voice or data payload. A voice message, in the case of Enhanced and AES privacy, requires an additional header and replaces some

of the least important bits of the voice payload with the Initialization Vector. The additional header increases the System Access Time except when Talk Permit Tone is enabled (in repeater mode) where the additional header replaces one of the normal voice headers. The replacement of payload bits reduces the voice quality. Note that the reduction in voice quality is barely noticeable.

In the case of Basic , Enhanced privacy, and AES privacy, a data message requires an additional header to distinguish between an unprotected data message and a protected data message. In the case of Enhanced and AES privacy, the additional header is also used to transport cryptographic parameter. This reduces the data throughput. For example, a typical protected confirmed location response takes 600 milliseconds compared to 540 milliseconds for an unprotected one (approximately 10% loss in throughput).

2.16.4
User Control Over Privacy

Customer Programming Software (CPS) allows a System Installer to select the type of privacy (that is, Basic or Enhanced privacy or AES privacy). CPS also allows the enabling or disabling of the privacy service of a channel. When **Enhanced** privacy is selected in the **Security** tab, it is possible to choose whether the Enhanced or AES privacy key will be used in the channel configuration. The option to toggle the privacy capability per channel can additionally be given to the radio user by providing a menu entry or programmable button. Without the menu entry or programmable button, the radio user is essentially “locked” to the channel’s privacy setting. It is important to note that a user can set or reset privacy for a channel, and not for the radio. If the user is provided with the menu entry or programmable button, and the user toggles the privacy setting, only the selected channel’s privacy setting is toggled and remains toggled even after the user changes channels or zones. Toggling the privacy setting on a channel will not affect the privacy setting on other channels.

The privacy setting of a channel controls the transmitting privacy setting, not the receiving privacy setting. A radio on a privacy-enabled channel always transmits protected, while a radio on a privacy-disabled channel always transmits unprotected.

However it is different for the privacy reception. It depends on whether **Ignore Rx Clear Voice/Packet Data** and **Fixed Privacy Key Decryption** options are selected in the **General** section of the **Zone/Channel Assignment** tab. See When Ignore Rx Clear Voice/Packet Data and Fixed Privacy Key Decryption Options are not Enabled on page 184.

2.16.4.1
When Ignore Rx Clear Voice/Packet Data and Fixed Privacy Key Decryption Options are not Enabled

In general, the radio receives and decodes both unprotected and protected message, regardless of the channel’s privacy setting. Also, when the radio receives a protected message, regardless of the channel's privacy setting, the radio always tries to unscramble or decrypt the message.

If a radio is never required to receive protected messages, then it should not be provisioned with keys or should be provisioned with a key that is different from the key(s) used by the rest of the system. Simply setting a channel to be privacy-disabled does not stop the radio from receiving protected messages. A radio receives a protected message correctly as long as it has the right key.

Therefore, when one radio user on a privacy-enabled channel transmits, every radio, regardless of its channel’s privacy-enabled or privacy-disabled status hears the transmission clearly if their provisioned Privacy Key is identical to that of the transmitting radio. A radio user receiving a protected transmission sees the green LED blinking rapidly. The receiving radio user should consider changing the privacy setting to match that of the call initiator when replying.

In Basic Privacy, a system utilizes only one key and if all radios are privacy capable, it is recommended that all radios are set to privacy enabled and equipped without the option to toggle the privacy settings by a radio user. Since Basic Privacy does not cause any degradation in audio quality, or decrease in performance, there

is no reason for the normal user to switch between non-privacy and privacy. Removing the option to toggle the setting from the radio user safeguards against any complicated privacy mismatch scenarios.

The following configurable options for reception are available within CPS and the Radio Management (RM) application.

2.16.4.2
Ignore Rx Clear Voice or Packet Data Option

The **Ignore Rx Clear Voice or Packet Data** option determines how the radio handles the reception of unprotected (clear) calls while configured for privacy.

If a radio receives an unprotected (clear) call while configured for no privacy, then it decodes the call normally. If a radio receives an unprotected call while configured for Basic, Enhanced, or AES privacy, and the **Ignore Rx Clear Voice or Packet Data** option is unchecked on the selected personality, then it decodes the call normally. If a radio receives an unprotected call while configured for Basic, Enhanced, or AES privacy, and the **Ignore Rx Clear Voice or Packet Data** option is checked on the selected personality, then it does not decode the call.

The **Ignore Rx Clear Voice or Packet Data** option per personality is not available if a radio is configured for **Privacy Type**selected as **None**. When the **Ignore Rx Clear Voice or Packet Data** option is enabled and the radio user disables privacy from the radio menu or a programmable button, the **Ignore Rx Clear Voice or Packet Data** option does not apply, and the radio decodes unprotected (clear) calls normally.

Table 41: Reception of Unprotected Calls While Privacy Configuration

Source Configuration	Target Configuration		Result
Privacy Type	Privacy Type	Ignore Rx Clear	
No Privacy	No Privacy	N/A	Decodes
No Privacy	Privacy	No	Decodes
No Privacy	Privacy	Yes	Does Not Decode

The **Ignore Rx Clear Voice or Packet Data** option is useful if there is a concern that non-secure individuals may disrupt communication within a talkgroup.

While the **Ignore Rx Clear Voice or Packet Data** option is checked, none of the voice/data calls are decoded if they do not utilize privacy.

The **Ignore Rx Clear Voice or Packet Data** can also be configured at a radio-wide level in the **General** section of the **General/Security** tab in Radio Management. If selected in the radio's security configuration, all personalities in the radio have **Ignore Rx Clear Voice or Packet Data** enabled.

If the **Ignore Rx Clear Voice or Packet Data** is not selected, then a **Clear Call Received** tone in the **Alerts** section of the **General/General Settings** tab can be enabled. When this tone is enabled, the radio sounds a tone every five seconds when the radio is decoding an unprotected (clear) voice call.

2.16.4.3
Fixed Privacy Key Decryption Option

The **Fixed Privacy Key Decryption** option determines how the radio handles the reception of protected (encrypted) calls while configured for privacy.

If a radio receives a protected (encrypted) call, and the **Fixed Privacy Key Decryption** option is unchecked on the selected personality, and there is a matching key (with the same **Key ID** and **Privacy Type**) in its key lists, then it decodes the call. If there is no matching key, then it cannot decode the call.

If a radio receives a protected (encrypted) call, and the **Fixed Privacy Key Decryption** option is checked on the selected personality, and the received key (as indicated by **Key ID** and **Privacy Type**) matches the key of the configured transmit key for the selected personality, then it decodes the call. If the received key does not match the configured transmit key for the selected personality, then it does not decode the call, even if there is a matching key in the key list. This feature has no effect on Basic privacy since only one key is used for both transmitting and receiving.

If the receiving radio is configured with **Privacy Type** selected as **None** or the radio user disables privacy from the radio menu or a programmable button, and the **Fixed Privacy Key Decryption** is checked, then the radio transmits and receives unprotected (clear) calls and decodes protected calls if the received key matches any key in the key list.

Table 42: Reception of Protected Calls While Privacy Configuration

Source Configuration	Target Configuration	Received Key Match	Result
Privacy Type	Fixed Privacy Key De-cryption		
Enhanced or AES Privacy	No	Matches a Key in Key List	Decodes
Enhanced or AES Privacy	Yes	Matches the Configured Key	Decodes
Enhanced or AES Privacy	Yes	Matches a Key in Key List	Does Not Decode
Enhanced or AES Privacy	N/A	Does Not Match a Key in Key List	Does Not Decode

The **Fixed Privacy Key Decryption** option is useful if there is a need that a radio user, once on the selected personality, does not want to be disrupted by other communications. For example, if a group of radio users wants to have the capability of focusing on the protected communication among them when some event occurs, a dedicated personality can be configured with the same transmit key and with this option turned on. When such an event occurs, they could move to that configured personality and focus on the communication among themselves and not be disrupted.

When the **Fixed Privacy Key Decryption** option is checked, the voice/data calls are not decoded if the received key does not match the selected personality's transmit key. The ramifications of this could result in missed communications in some configurations.

If numerous radio configurations are utilizing the **Fixed Privacy Key Decryption** option, it implies that not all radio configurations share a common receive key. If radios do not share a common receive key, call types that utilize a single transmit key and are targeted towards many users, such as All Call or Talkgroup Call may not be decoded by everyone. Similarly, since the MNIS Data Gateway utilizes a single transmit key, data calls from a data application to the radios may not be decoded by everyone.

In addition, if utilizing a talkgroup receive list, only talkgroup calls that utilize the same key as the selected personality's Transmit Key are decoded. Only individual calls that utilize the same key as the selected personality's Transmit Key are decoded. All this should be considered when utilizing the **Fixed Privacy Key Decryption** option.

The **Fixed Privacy Key Decryption** can also be configured at a radio-wide level within the Security folder in Radio Management. If selected in the radio's security configuration, all personalities in the radio have **Fixed Privacy Key Decryption** enabled.

2.16.5
Privacy Indications to User

It is important for a radio user to know the privacy status (that is, enabled or disabled) of the current channel, and also to know if the received voice transmission is unprotected or a protected voice transmission. There is no privacy indication for incoming protected data transmissions.

Prior to transmitting, a radio user should check the privacy setting of the current channel. On privacy-enabled channels, an icon is shown on the front panel display of the radio when the radio is idle.

Table 43: Icons for the Privacy Status/Type

Privacy Status/Type	Icon
Enabled	
Enhanced and Disabled	
None	no icon

Upon receiving a voice transmission, the radio user can know the privacy status of the voice transmission by observing the blinking rate of the receive LED. When receiving a protected voice transmission, the LED blinks green but at a quicker rate than when receiving an unprotected voice transmission.

If radio users in a call have mismatching privacy settings, but the same key, they are able to communicate, but the transmissions are protected in only one direction. In other words, only the transmissions from radios with privacy enabled are protected.

The radio does not automatically negotiate privacy settings, or block transmissions that are not protected. Therefore, it is up to the radio users to monitor the privacy indications to determine if all the users in the call have a matched privacy setting. The radio displays the privacy setting of the received transmission, but blinks if it does not match the transmit mode of the receiving radio. When a privacy setting mismatch occurs, they should request the other members of the call to switch their privacy settings to match. The radio allows users to enable or disable privacy on the channel while on a call.

Radio users with non-display or numeric display radio models are not able to view the icon that is shown on a privacy-enabled channel. Therefore, it is recommended that such users should not have the option to toggle the privacy setting.

If non-display or numeric display radio users must be able to toggle between protected and unprotected, it is recommended that this be done by programming duplicate channels, one with privacy enabled and one without, and the user should use the dial position to toggle between protected channels and unprotected channels. For example, dial position one may be set to communicate with a Group in unprotected mode, and dial position two may be set to communicate with the same group but in protected mode.

2.16.6
Key Mismatch

In the case of Basic Privacy, a receiving radio assumes that the received protected transmission is protected using the same Key that it has, because the key identifier is not sent with the message.

If the receiving radio does not have the same key as the transmitting radio, the receiving radio cannot decode the transmission correctly. For voice transmissions, this results in unintelligible audio - sometimes referred to as digital warbles, being played through the target’s speaker. For data transmissions, this results in an unsuccessful data message transmission. This is because the IP/UDP headers of a data message when

unprotected using a wrong key fail to CRC check. On failure of the checksum, the data message is not delivered to the application.

In the case of Enhanced and AES Privacy, the key identifier is sent with the message and if the receiving radio does not have the key then it either remains muted (in case of voice message) or discards the data message. If the key value associated with the key identifier is different in the sender and receiver, due to a miss-configuration, then the voice transmissions result in unintelligible audio and the data transmissions are unsuccessful.

2.16.7
Keys and Key Management

In the case of Basic Privacy, a radio is capable of holding only one Privacy Key. The same key is used to protect and unprotect voice and data transmissions over all the channels and for all call types: Group Call, Private Call, All Call, or Emergency Call.

In the case of Enhanced Privacy, a radio is capable of holding up to sixteen Privacy Keys, where keys are associated with channels. In the case of AES, a radio is capable of holding up to sixteen Symmetric Keys, where each key is associated with channels.The relationship between keys and channels is 1:0...n. (in other words 1 to 0 or 1 to many) “0” means that keys may be provisioned into the radio but are not associated with any channel. In this case, the keys are used to decode a received message but are not used by the radio to encode a transmission.

A Privacy Key is provisioned in a radio using a CPS. The keys are not readable, editable, or erasable by the radio user. Once a key has been chosen and programmed into a radio, the key cannot be extracted and viewed by CPS. It can only be retained or overwritten.

In the case of Basic Privacy, a CPS user can select one of the 255 prescribed keys. These keys are referenced by a key index from 1 to 255. Each key index references a particular 16-bit key that is used for protecting Over-The-Air. There is no option for a “blank”, “null”, or “zero” key. In the case of Enhanced Privacy, the valid range for the value of a key is 1 to 1,099,511,627,774 (that is, FFFFFFFFFE in hex). The key values 0 and 1,099,511,627,775 (that is, FFFFFFFFFF in hex) are reserved and should not be used. In the case of AES, the valid range for the value of a key is 1 to 1.15x 10^77 (FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF FFFF in hex i.e. a 256-bit binary number except for zeros in all the 256 bits).

NOTE: The following details of this key management section is only applicable when the OTAP feature is not purchased or not available in the system. If OTAP is present, refer to the OTAP sections on updating the privacy type and the keys.

MOTOTRBO does not support remote or Over-The-Air programming of keys into a radio. For a system without the OTAP feature, the encryption keys can be programmed in a radio using only CPS. Keys can be programmed in a radio using only CPS. CPS supports loading of the value and identifier of a key into a radio either manually, or from the RM, or from a protected archive file (in case of Enhanced Privacy only). In case of getting the keys from a protected archive file, the CPS User selects the protected file and provides the password. The file is unreadable without a password. The CPS is capable of copying key(s) from one radio's archive into another radio's archive without the user needing to retype the key for each radio.

A customer may need to change one or more keys (in the case of Enhanced and AES Privacy) with a set of new keys into a set of radios. Some of the reasons for changing keys are:

- Compromise of keys
- Security policy of the customer requires periodic update of keys
- Loss of a radio resulting in a concern that this may lead to compromise of keys or eavesdropping.

The easiest way to implement a key switchover is to gather all radios and re-program them together at the same time. But it may not always be possible to gather all the radios without seriously affecting day-to-day operations.

An alternate method is to create two zones where one zone is set to "unprotected" while the other is set to “protected”. The key can be changed on the "protected" zone and the users shall use the "unprotected" zone until all radios have been updated. Once all radios have been updated, the dispatcher informs the fielded radios to switch zones. This allows users to communicate in clear until the all radios are provisioned, and then all the users switch keys at the same time.

A similar zone strategy can be used to perform periodic key set changeovers. For example, when one zone has January’s keys and another duplicate zone has February’s keys. On the first of February, the users switch to the February zone. Throughout February, the January zone is updated with March’s keys and renamed to “March Keys”. On the first of March, the users switch, and so cycle starts again. This makes sure that only two months of keys are compromised if a radio is stolen or lost.

2.16.8
Multiple Keys in a Basic Privacy System

Although a radio can only use one key in a Basic privacy system at a time, a Basic privacy system may utilize multiple keys to sub-divide a group into a set of groups. Note that this is not a recommended configuration, and some considerations need to taken into account, if the decision is made to utilize multiple keys in a system.

It is not recommended that Groups be sub-divided into smaller groups with the use of keys. This results in one sub-group of users hearing unintelligible audio (or digital warbles) when the other sub-group communicates. It is recommended that the users should be divided into Groups, and provisioned so that a user can not transmit nor receive on another Group. If users with different keys are allowed to communicate with Basic privacy enabled, for example through a protected Private Call, a key mismatch occurs and unintelligible audio is heard. Although these users with different keys are never able to communicate privately, they are able to communicate when privacy is disabled.

For example, two different Groups are isolated by provisioning different privacy keys. When a user in each Group needs to communicate to each other through a Private Call, they must do it with privacy disabled. If a radio user needs to communicate with both Groups through an All Call, the radio user must transmit in clear mode so that both Groups can monitor. If users respond with privacy-enabled, the user who initiated the All Call only monitors the responses protected with a matching key.

If the system is utilizing data applications and must communicate through a Control Station to the Application Server, all radios on a slot must have the same key or they are not all able to properly communicate with the Control Station. For similar reasons, it is not recommended to have radios without privacy capability, like the older software versions, in the same Group as radios with privacy capability. Since older radios are not provisioned with a Privacy Key, the audio is muted. If radios with privacy capability need to communicate to radios without privacy capability, they must disable privacy before transmitting.

As a general rule, it is always recommended that groups with different privacy capabilities and settings be placed in different Groups and on different slots.

2.16.9
Data Gateway Privacy Settings

See MOTOTRBO Network Interface Service on page 315 and MOTOTRBO Device Discovery and Mobility Service on page 327 for details on privacy configuration when the MNIS is acting as the data gateway.

The privacy setting of a Control Station acting as the data gateway to the Application Server is very important for consistent data communications. This may even drive the privacy configuration of the rest of the system.

If a system contains some privacy-capable radios and some privacy-incapable (older software versions), radios then the Control Station must be privacy capable, but configured to transmit in clear mode. This way, outbound messages can be received and processed by the older radios (not privacy capable). Note that the privacy capable radios send their data protected and the Control Station will be able to decode these messages, as long as it has the proper key.

In case of Basic Privacy, there can only be one key per channel (or slot). Since the Control Station can only contain one key, it cannot communicate protected to two different Groups utilizing different keys. If a Basic Privacy system utilizes multiple keys, those users must be divided onto two separate channels (or slots), each with their own Control Station utilizing the proper key. Setting the Control Station to privacy disabled does not solve this problem since incoming messages such as GPS or text messages may be protected using different keys and only one key can be used at the Control Station to decode. Therefore, although outbound messages would be functional, inbound messages would not be.

If users have the ability to toggle their privacy settings, it is acceptable to have the Control Station set to either privacy enabled or privacy disabled, but only if their provisioned keys match. If the Control Station is set to privacy enabled, and the radio is set to privacy disabled, one direction of the data communication is protected and the other is unprotected. Since radios set to privacy disabled receive protected, and radios set to privacy enabled receive unprotected, the communication path works. If important data is being transferred to and from the fixed infrastructure, it is recommended that the Control Station should be set to “protected”. This guarantees that at least half of the data transmission is private. Also, the system is tolerant if fielded radios are set to privacy disabled.

It is recommended that all radios including Control Station should have same privacy settings. If the privacy setting is Enhanced and/or AES Privacy, then the Control Station should have the transmit keys of all the radios and all the radios should have the transmit key of the Control Station.

2.16.10
Protecting One Group’s Message from Another Group

There may be a need for one group’s voice and data to be protected against another group over the same channel (same frequency and same slot). There may be some radio users who are members of one or more of the groups. In this case, if a group not only wants to protect their communication from intruders but also from other groups then each group should use separate keys for protection.

The System Installer should make each group that need to be protected as “TX Group” for a personality. The relationship between a personality and a group is 1:1. The System Installer should associate a key to a personality. The relationship between a key and a personality is 1:1. And therefore the relationship between a key and a group becomes 1:1. If a radio ‘X’ wants to make a protected Private Call to a radio ‘Y’ and if both the radios are member of a group ‘T’ then the radio ‘X’ goes to a personality whose “TX Group” is ‘T’. If there is no group where both the radios are member then it is not possible to send a protected message.

For a protected “All Call”, the transmitting radio should go to a specific personality and the key associated with that personality is present in all the radios. For a protected Private Call, the transmitting radio should go to a specific personality and the key associated with that personality is present in the receiving radio.

2.16.11
Updating the Privacy Type

It may not be possible for a System Installer to update all the radios from Basic Privacy to Enhanced Privacy and/or AES in one session for a system where OTAP is not available. In such cases, the System Installer instructs all the radio users to disable the privacy feature and operate in clear mode. When instructed, the radio users disable the privacy feature using the radio front panel. All the messages are transmitted in clear.

The System Installer updates the software of radios and configures the radios for desired privacy (Enhanced Privacy and/or AES). Once all the radios are upgraded, the System Installer updates the software of repeaters and configures them for Enhanced Privacy. The repeaters require Enhanced Privacy configuration for AES.The Control Stations acting as the data gateway should also be upgraded.

The System Installer instructs all the radio users to enable the desired privacy feature. The radio users enable the desired privacy feature using the radio front panel. The Control Stations also enable the desired privacy. All the messages are transmitted using the desired privacy setting.

2.17
Real-Time Clock Synchronization

The SLR Series Repeaters contain a Real-Time Clock (RTC) which is used by the repeater to keep track of the actual time. This RTC can be used to timestamp data such as alarm and diagnostic logs. Any application showing these logs should be able to show the logs with timestamps that contain the year, month, day, hour, minute, and second. There is a rechargeable battery, which is used to keep the RTC operating when the repeater is turned off or disconnected from power. The RTC can remain operating with power supplied from the rechargeable battery for approximately 23 days. Once the battery is fully discharged, it will take approximately 33 hours to recharge once power is restored.

The RTC must be synchronized to a time source at least once every 24 hours to maintain the most accurate timestamps. The recommended time source is an Network Time Protocol (NTP) Server that all of the repeaters in the system can be configured to synchronize to periodically. If an NTP Server is not specified using CPS, then CPS will sync the repeater's RTC to the current time of the PC running CPS. This should allow the RTC to be somewhat accurate, but it will become less accurate each day that it cannot be synchronized to an NTP Server.

In the event that the network where the repeaters are deployed do not have any local NTP Servers available, then a public NTP Server can be used instead. There are public NTP Servers available on the Internet that be used for this time synchronization. More information about NTP and the addresses for public NTP Servers can be found at the following website: http://support.ntp.org/bin/view/Servers/WebHome%20and%20http://www.pool.ntp.org.

In a Connect Plus system, the repeaters can be configured to synchronize themselves to the NTP Server address on the XRC. If there are more than 100 repeaters in the system, then a separate dedicated NTP Server should be used instead of the NTP Server on the XRC.

RTC synchronization to NTP servers can be configured through CPS by specifying one of the following:

- check the **DHCP** option,
- check the **DNS** option and select the **NTP DNS Address** name of the DNS server from the list,
- configure the IPv4 address of the server using the **NTP Server IP** option.

When the **DNS** option is selected, the **DNS Address List Items** need to be configured in the DNS **Addresses** section.

When the **DHCP** option is selected, other options are unavailable. The DHCP server can send the IPv4 address of the NTP server during repeater IPv4 address assignment, but not all DHCP servers support assigning the NTP server IPv4 address to devices.

It should be noted that the RTC based timestamps will only be available on SLR Series repeaters. All other repeaters will continue to report diagnostic and alarm logs with timestamps that equate to the number of seconds since the repeater last powered up.

2.18
Repeater Diagnostics and Control

Repeater Diagnostics and Control (RDAC) allows a system administrator the ability to monitor and control repeaters within the system.

The following services are provided:

Repeater Diagnostics

- Read Enabled/Disabled Status
- Read Analog/Digital Status
- Read Wide or Local Area Status

- Read Transmit Power (High or Low) Status
- Read Available Channels (including Currently Selected)
- Read Inbound RSSI
- Read IPv4 Address and UDP Port (required for connectivity)
- Read FRU status, for example the AC Voltage, DC Current, and Modem Board Temperature (only on the SLR 5000 and SLR 8000 series).

Repeater Alarm Reporting

- Detect and Report Receiver Lock Detect Failure
- Detect and Report Transmitter Lock Detect Failure
- Detect and Report AC Power Failure
- Detect and Report RF PA/System Overheating
- Detect and Report RF Power Out
- Detect and Report High VSWR Detection
- Detect and Report RF PA Fan Failure Alarm (only on the MTR3000, SLR 5000 and SLR 8000 series)
- Detect and Report EEPROM Corruption (only on the MTR3000)
- Detect and Report Low and High RF PA Voltage (only on the MTR3000, SLR 5000 and SLR 8000 series)
- Detect and Report SCM Reference Incompatibility Alarm, for example, SCM with TCXO in 800/900MHz band (only on the MTR3000, SLR 5000 and SLR 8000 series)
- Detect and Report FRU Incompatibility Alarms, for example, PA and exciter are incompatible (only on the MTR3000, SLR 5000 and SLR 8000 series)
- Detect and Report Main Fan Failure (only on the SLR 5000 and SLR 8000 , DR 3000 not applicable for the MTR3000)
- Detect and Report FRU Module ID Failure (only on the SLR 5000 and SLR 8000 series)
- Detect and Report FRU Communication Failure (only on the SLR 5000 and SLR 8000 series)
- Detect and Report Power Supply Status alarm, for example, over voltage and over current (only on the SLR 5000 and SLR 8000 series)
- Detect and Report Battery Status alarm, for example, low and bad battery (only on the SLR 5000 and SLR 8000 series)

Repeater Control

- Change Enabled or Disabled Status
- Change Channels
- Change Transmit Power Level (High or Low)
- Reset Repeater
- Knockdown Repeater

The RDAC application can be configured to work over the network through an IP or locally through a USB.

When working over the IP network, the application communicates with all repeaters within an IP Site Connect or Capacity Plus Single Site system using the same link establishment process that the repeaters utilize. Therefore, it benefits from the existing link establishment and authentication utilized between repeaters. All services in the list above are available through the RDAC application.

When working locally, the RDAC application connects to a single repeater through a USB. All services in the previous list are available through the RDAC application. The repeater control services are not available through the USB interface through the RDAC application.

The user also has access to the repeaters external GPIO pins. External equipment (or existing remote adapters and desk-sets) can be configured to set or read the GPIO pins to allow access to the repeater control services as well as access to indications that a minor or major alarm has occurred. The access to these GPIO pins further allows the radio installer to utilize the alarm pin and enable/disable pin to create a redundant switch over configuration. Alarm Reporting and Control is available using the GPIO pins.

NOTE: Any combination of RDAC connected over the Network, RDAC connected via USB, or connections via GPIO are supported.

The ability to change the repeater channel can be utilized to toggle channel parameters between predetermined settings. For example, if the repeater contains one channel that is in analog mode and another channel that is in digital mode, changing the channel between these channels essentially changes the mode from analog to digital. The same strategy can be used to toggle the wide area and local setting of a timeslot. One personality could be provisioned for two wide area channels, while the next has one wide and one local channel. Other channel parameters can be changed using the same strategy.

NOTE: When a repeater in Capacity Plus Single Site or Capacity Plus Multi Site mode changes to an analog mode via RDAC, the repeater can no longer be accessed via RDAC.

It is important to note that many control operations require the repeater to perform a reset before processing the control operation. During the reset the repeater is not able to service inbound transmission from fielded radios. Also note that the repeater takes no consideration to the ongoing traffic when instructed to perform a control operation. In other words if a call is in progress (Group Call, Private Call, All Call, Emergency Call, data call, and other), the repeaters perform the control operation and drop the call in progress. In addition, the IP connection between the repeater and the RDAC will be temporarily severed while the repeater is rebooting. The connection must be
re-established before additional operations can be performed. This should be taken into consideration before performing any control functions on an active repeater.

In addition to the repeater reporting alarms to RDAC application and setting the GPIO alarm pins accordingly, it is important to note that it also takes action when major alarms are received. The repeater performs a reset after a major alarm is reported as an attempt to clear the alarm. If the alarm is not clear after reset it resets again. This continues until the alarm is cleared or the repeater is locked.

NOTE: For XPR 8300/8380/8400 and MTR3000, the repeater enters the "Locked" state and set the Major Alarm Pin after three major alarms have been reported.
For SLR 5000 and SLR 8000 series, for the alarms that do not impact transmitter performance, repeater enters the "Locked" state and sets the Major Alarm Pin after three major alarms have been reported.

For other alarms which impact transmitter performance, repeater will enter the "Locked" state and set the Major Alarm Pin after one major alarm has been reported. At this time, all the LEDs on the Repeater front panel are solid. While in the "locked" state, the repeater does not service any calls Over-The-Air. The RDAC application displays the "locked" state and has the ability to retrieve logs.

NOTE: In order to exit the "locked" state for XPR 8300/8380/8400 and MTR3000, the repeater must be read and written to with the CPS to reset the major alarm counter. This is automatically done when CPS writes a codeplug to the repeater.
For SLR 5000 and SLR 8000 series, the repeater can also be unlocked by power cycle repeater.

NOTE: Three major alarms mean that there is a hardware problem that should be addressed prior to clearing the "locked" state.

All MOTOTRBO repeaters support the following alarms:

- Rx Alarm
- Tx Alarm
- Fan Alarm
- Power System Alarm
- Temp Alarm

The following alarms are additionally supported by the MTR3000 , SLR 5000 and SLR 8000 series repeaters:

- Tx Power Alarm
- VSWR Alarm

The following alarms are additionally supported by the MTR3000, SLR 5000 and SLR 8000 series repeaters only:

- PA Voltage Alarm
- Tx Gain Alarm

The following alarms are additionally supported by the MTR3000 repeater only:

- Backplane Supply Alarm

The following alarm is additionally supported by the MTR3000 and SLR 8000 series repeaters only:

- External Circulator Temp Alarm

The following alarms are additionally supported by the SLR 5000 and SLR 8000 series repeaters only:

- Frequency Reference Alarm
- PSU HardwareVer Alarm
- Chassis Hardware Ver Alarm
- Front Panel HardwareVer Alarm
- PA HardwareVer Alarm
- Illegal Carrier Alarm
- PSU Program Fail Alarm

The following alarms are additionally supported by the SLR 8000 series repeaters only:

- Wireline Board Module ID Alarm
- Front Panel Communication Fail Alarm
- Front Panel Program Fail Alarm
- Wireline HardwareVer Alarm
- Incompatible DC Supply Alarm

NOTE: Revision A UHF B1 and VHF repeaters do not support any RDAC alarms. These alarms were only supported on Revision B and later, hardware.

Alarms are categorized as shown below:

Major Alarms
Major alarms indicate hardware failures that prevent the repeater from functioning normally.

Minor Alarms
Minor alarms are warning alarms, which impacts the repeater performance, but still responds to GPIO controls such as channel steering, alarms and diagnostics.

Informational Alarms
Informational alarms are prompting user about repeater status change, repeater performance may be impacted.

Mixed Alarms
This alarm type could be major, minor or informational, depending on the availability of a backup repeater and the type of the system configuration

The list of major, minor, informational and mixed alarms varies for different repeaters and repeater models.

NOTE: For SLR 5000 and SLR 8000 series, the alarm type of some alarms can be configured in CPS. Refer to the RDAC application and CPS Online Help for further details.

2.18.1
Connecting Remotely Through the Network

Connecting RDAC via the network allows access to all repeaters in an IP Site Connect or CPSS system. If the customer system has more than one system (more than one Master repeater) then the RDAC application is required to know the static IPv4 or DNS address, and UDP port for each of the Master repeaters.

A single RDAC application supports up to 8 systems (8 Master repeaters). It will learn the addresses of the other repeaters through communication with each Master. Depending on the topology used by the systems, the RDAC application may require some specific firewall or NAT configuration. RDAC requires the appropriate authentication to be entered that is being utilized by the repeaters in the system.

When connecting to multiple systems, RDAC **must be** configured with a different RDAC UDP port for each Master.

System	Description
IPSC IP Site Connect	Connecting RDAC via the network allows access to all repeaters in an IP Site Connect system.
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	Connecting RDAC via the network allows access to all repeaters in CPSS and CPMS systems.

Although the network connection is designed for “connecting remotely”, a local network connection in close proximity to the repeater is supported.

The RDAC-IP application can communicate with enabled and disabled repeaters, knock-downed repeaters, digital and analog repeaters, and wide and local area repeaters. As long as they are on the network and communicating with the same Master repeater that the RDAC application is communicating with, they are controllable through the application.

Note that over-use (or misuse) of RDAC diagnostics could cause strain to the network link and therefore, cause voice degradation. For example, numerous requests for status or error logs could cause excess traffic on a network link which could delay voice through the network. Please review the network bandwidth considerations in later chapters.

2.18.2
Connecting Locally Through the USB

Connecting RDAC locally through the USB provides the user with all the services of RDAC but only allows access to the local repeater.

This connection is very useful if the repeater is in close proximity to the dispatch center or while performing service or troubleshooting locally.

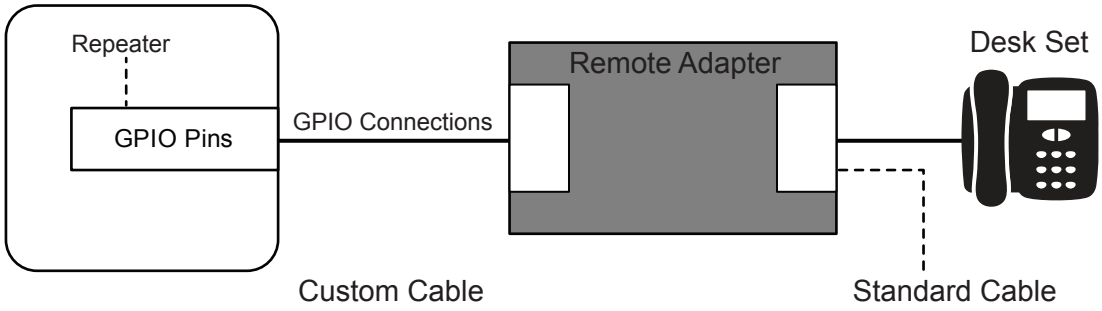
2.18.3
Connecting Locally Through GPIO Lines

Connecting locally through GPIO lines only allows access to the local repeater. The user has access to the repeater control services as well as access to indications that a minor or major alarm has occurred from the

GPIO lines. The GPIO lines can be configured in various ways and can be integrated to communicate with a variety of external equipment.

A custom cable is needed to connect the repeater accessory port to the outside control device. Below is an example of one configuration. Note that the pin out of the cable is dependent on how the GPIO lines are provisioned through CPS.

Figure 34: Local Connection Using GPIO Lines



2.18.3.1

RDAC Local Settings Rear Accessory Port CPS Programmable Pins

The rear accessory also has some pins that can be programmed to specific input/output functions. These pins can be programmed to either active high or low.

The following table shows the description of these functions available for each GPIO pin.

Table 44: CPS Programmable Pins

CPS Programmable Pins	Description
Major Alarm (Locked State)	This output pin is used to report a major alarm has happened for certain times (three times for XPR 8300/8380/8400 and MTR3000, 1 time for transmitter related alarms on SLR 5000 and SLR 8000 series), and the repeater is in now locked state.
Minor Alarm	This output pin is used to report minor alarm(s) is happening on the repeater.
Repeater Disable	Asserting this input pin triggers the repeater to enter disabled state. In this state, the repeater cannot execute repeat functions. Releasing this input pin reverts the repeater back to enabled state where the repeaters can start repeating calls.
Tx Power Level High	Asserting this input pin triggers the repeater to change the TX power level to be high. Releasing this input pin reverts the repeater back to TX low level low.
Repeater Knockdown	Asserting this input pin triggers the repeater to temporarily enter Repeat Path Disable Mode. In this mode, the repeater's transmitter is only enabled by the external PTT and the audio source is the Tx Audio Input pin.

CPS Programmable Pins	Description
	Releasing this input pin reverts the repeater back to Normal Mode where the repeaters transmitter can be activated by a qualified RF signal on the receive frequency. **NOTE:** Repeater knockdown is not supported in digital mode. In Dynamic Mixed Mode system, this feature is not supported during an ongoing digital transmission.
Channel Change	**For XPR 8300/8380/8400 and MTR3000**, there are up to four pins that can be configured and used for channel change. The repeater can support up to 16 channels. Asserting this input pin represents 1. Releasing this input pin represents 0. 0000 represents first channel, 1111 represent the last channel. **For SLR 5000 and SLR 8000 series**, there are up to six pins that can be configured and used for channel change. The repeater can support up to 64 channels. 000000 represents first channel, and 111111 represent the last channel.

2.18.4
Redundant Repeater Setup

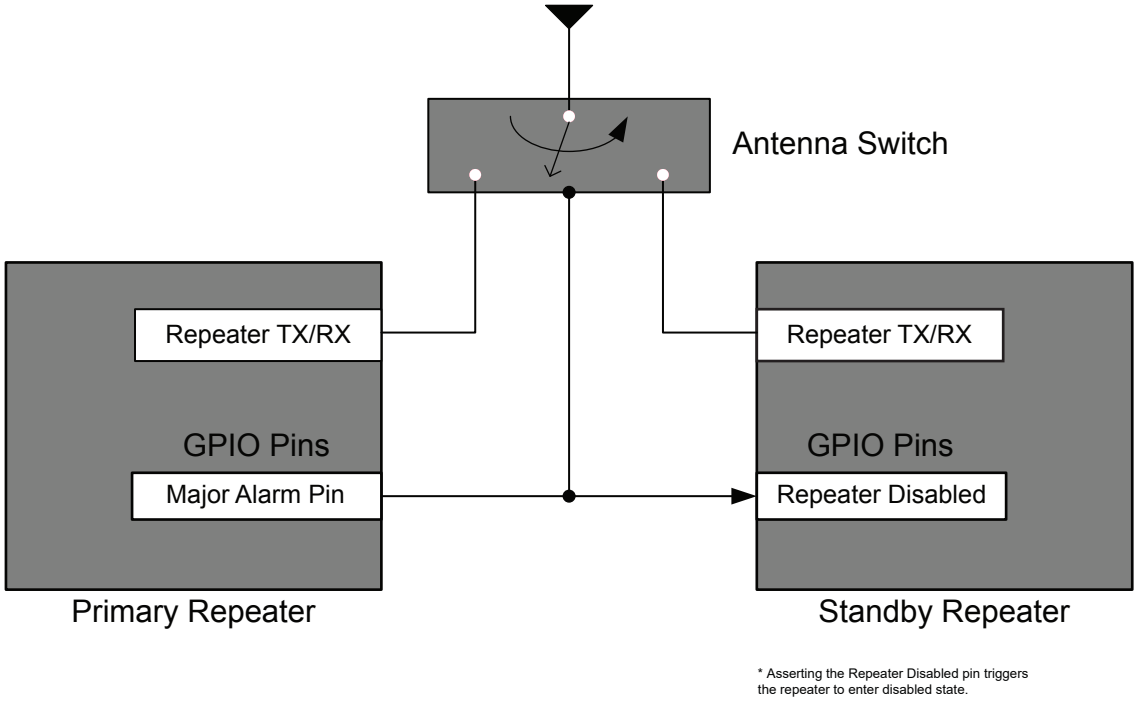
By using the alarm feature and control feature together, it is possible to setup redundant repeaters. So that when one repeater fails, the standby repeater can take over the repeat function.

Before installation, both repeaters are programmed with the same channel information. The installer configures one repeater as primary repeater and the other one as standby repeater. For the primary repeater, the installer configures one GPIO pin for major alarm reporting and configures the pin's polarity. Additionally, it configures through CPS in the primary repeater to indicate the availability of a standby repeater. For the standby repeater, the installer configures one of its GPIO pins as repeater disabled control input pin and its polarity opposite of the primary repeater's alarm pin polarity. When the primary repeater's alarm pin becomes active it deactivates the disabled pin and the standby repeater becomes enabled. The antenna system is connected to the primary repeater and also connected to an antenna switch. The antenna switch is external to the repeater hardware. The installer connects the primary repeater's alarm pin (output pin) and standby repeater's repeater disable pin (input pin) and the antenna switch all together. The installer powers on the primary repeater first and verifies it is working with no major alarm reported. Then the installer powers on the standby repeater.

When a major alarm happens for certain times in the primary repeater and the repeater enters the locked state, the primary repeater sets the major alarm GPIO pin to active level. The standby repeater detects the disable pin is changed to inactive level and it becomes enabled. The antenna switch is also triggered which changes the antenna to the now active repeater.

Once the fault in the primary repeater is addressed, the repeater is removed from the locked state and reset, the primary repeater is enabled and again becomes the primary repeater. The standby repeater then becomes disabled.

Figure 35: Redundant Repeater Setup



System	Description
IPSC IP Site Connect	If repeaters are operating in IP site Connect mode, they must both have existing IP network connections and be communicating with the Master. Since they are both on the network, they must have different IP Addresses. Although the system will not send voice to a disabled repeater, it will require link management. In IP Site Connect, ensure taking this into consideration when planning for network bandwidth.

System	Description
	See Required Bandwidth Calculations on page 428 for details on calculating the bandwidth for IP Site Connect. **NOTE:** A redundant repeater connected to the IP Site Connect system counts in the total number of supported peers. It is also important to note that when setting up the Master repeater of an IP Site Connect system into a redundant configuration, the network link must also be switched with external hardware similar to that of an RF Antenna. In this case, the IP Address of both the Primary and the Standby repeaters must be the same since all the Peers communicate with it using this IP address. As they have the same IP Address, they cannot be connected to the network at the same time. This also means that the standby repeater cannot be contacted via a network RDAC application while not in the primary repeater role since it is not connected to the network. Because the two devices have the same IP address but different MAC addresses, Peers may not be able to contact the Master repeater until the router and repeater ARP tables are updated. Depending on router configuration this could take up to 15 to 20 minutes. It is recommended to consult the Network Administrator for details on setting the ARP interval within the customer's network.
CPMS Capacity Plus Multi Site	Similar configuration as IP Site Connect System for Redundant Repeater Setup applies to Capacity Plus Multi Site.

2.18.5
Dual Control Considerations

It is possible to have RDAC connected locally, over the network, and connected through GPIO lines simultaneously to a single repeater.

In this case, the repeater can be controlled through GPIO as well as through the network. The user should be aware that it is not recommend using both methods to control the repeater at the same time. Note that after a control command has being executed from RDAC application, the control console connected through GPIO may no longer indicate the state of the repeater correctly since it reads the state of the hardware pin rather than the internal repeater state. In other words if the external application has pulled a pin low or high, the repeater cannot change the level of that pin after RDAC has made a change.

2.18.6
Digital Voting Control and Monitor

RDAC can be used to control digital voting such as enabling or disabling the feature, force vote, and display voting status. See Digital Voting on page 454 section for more details.

2.18.7

General Considerations When Utilizing the RDAC Application to Set Up the Network Connection

Connecting a single RDAC application to numerous systems that were previously residing on the same LAN, VPN, or WAN requires minimal configuration change. The RDAC application needs to be configured with each Master repeater's IPv4/UDP address and a unique RDAC UDP port for each system. This is because the IPv4 address of the Master repeater that can be reached at a wide or local area IPv4 address does not change.

When connecting a single RDAC application to systems that were previously residing on independent LANs or VPNs, the following configuration options can be considered:

- Combine both networks into one LAN or VPN, which most likely requires changing repeater IPv4 addresses in one of the networks.
- Connect to each LAN over a WAN. As it is now a wide area configuration, in the case of NAT topology this requires some changes because all peers (including the RDAC application) are now required to utilize the Master repeater's wide-area IPv4 address, instead of the local IPv4 address.
- Place the RDAC on the LAN of one of the sites. This requires correctly configuring the Master repeater IPv4 address for each system. Depending on the topology of each system, it can use the local IPv4 addresses for one system, and the wide-area IPv4 address for the others.

In all of the options previously mentioned, each **System** settings of the RDAC application must utilize a unique **RDAC UDP Port**.

If a channel is changed to a channel not supported by the system, the channel's repeater does not reconnect to the system, and the repeater will not be visible in RDAC. Therefore, it is strongly not recommended to change a channel's mode to an unsupported mode of the system.

When utilizing the RDAC application to communicate with multiple IP Site Connect or Capacity Plus Single Site systems, each system's network topology has to be considered independently. This is important because some connections may utilize a LAN configuration (see: LAN Configuration on page 366), while others utilize a WAN configuration (see: WAN Configuration on page 367). The main difference is that local area configurations utilize the Master repeater's local IPv4 address, while wide-area configurations utilize the wide-area IPv4 address.

System	Description
IPSC IP Site Connect	An IP Site Connect system supports analog and digital conventional channels.
CPSS Capacity Plus Single Site	A CPSS system supports only CPSS channels.
CPMS Capacity Plus Multi Site	A CPMS system supports only CPMS channels.

2.19
Repeater Diagnostics System Enhancement

Repeater Diagnostics, Alarm and Control (RDAC), described in Repeater Diagnostics and Control on page 191, is for monitoring of hardware alarms, diagnosis of RSSI, power level, repeater state, and repeater control of enable/disable, channel change and so on. In contrast, Repeater Diagnostics System (RDS) feature focuses more on software alarm detection which provides more troubleshooting capability in the field. The RDS feature uses RDAC to control and retrieve the diagnostic information from the repeaters.

The following services are provided:

- Enable and disable RDS
- Repeater software alarm control
- Configure automatic polling interval
- Detect and report software alarms
- Retrieve and clear software alarms
- Log file management

Software alarms detected in RDS are as follows:

OTA Layer
FCC interference type I and II; Color code failure; MFID failure and others.

IP Layer
Link status between repeaters; Call streaming failure.

Network Layer
Network cable error; Gateway error; DHCP error and others.

All the services in the list above are available in both analog and digital mode. The connection between repeater and RDAC application can be network either through IP or locally through a USB.

When working over the IP network, the application communicates with all repeaters within the system; when working locally, the RDAC application connects to a single repeater through a USB. All services in the list above are available through the RDAC application.

The alarm information of multiple repeaters in the same system will be stored in the same log file by RDAC application. PC time stamp and repeater peer ID are added to each alarms in the log file. Different log folders are used for different system configurations.

NOTE: RDS feature are applied in MOTOTRBO 32 MB Repeaters.

2.20
IP Repeater Programming

NOTE: This feature is supported on repeaters equipped with a 32 MB memory running on firmware version R01.07.00 or later.

IP Repeater Programming (IRP) allows a system administrator to provision and to upgrade repeaters within the system that uses the IP network. The Master repeater of a system configuration must be running on the same firmware version.

The following services are provided:

1. Repeater Configuration
   - Reading the current repeater configuration
   - Writing a modified repeater configuration

2. Repeater Upgrade
   - Upgrading repeater firmware and/or codeplug version
3. Repeater Feature Enable
   - Activating a purchased feature on the repeater

2.20.1
System Configuration for IRP Support

Connecting the Radio Management (RM) to an IP network allows the RM to access all repeaters in an IP Site Connect, Capacity Plus Single Site and Capacity Plus Multi Site systems, by using their backend network connections. The RM can also leverage IP-based access to Dynamic Mixed Mode (DMM) or Single Site repeaters by connecting the repeaters to an IP network and configuring each one to act as a single site Master.

To enable IRP, the feature must be configured with the repeater locally connected through a USB to the RM application. The RM can communicate with repeaters of multiple modes; enabled, disabled, knockdown, digital, and analog. The primary requirement is that the repeater must be on an IP network and it must communicate with a Master repeater or act like one. However, the RM can only connect to one Master at a time and can only program a single repeater at a time.

When the repeater is properly configured and installed, the user must direct the RM application to the IPv4 address of a Master repeater as defined by the repeater configuration. If the customer system has more than one system (more than one Master repeater), then the static IPv4 or DNS address, and UDP port for each of the Master repeaters must be configured in RM. When the application connects to the Master repeater, the addresses of other repeaters connected to the Master are saved in RM.

IRP operation consists of two steps:

- RM-to-repeater communication over IPv4/UDP: when RM informs the repeater on which TCP port it will be waiting for communication from the repeater.
- Repeater-to-RM communication over IPv4/TCP: the entire read from or write to repeater process happens.

If the PC with RM resides behind a firewall, the firewall must be configured to allow inbound traffic (repeater-to-RM) on a specific RM TCP port range that is configurable in the RMDP application. If multiple RM applications (different PCs) are behind a single firewall, each RMDP application must use a unique TCP port range, and the firewall must be configured to correctly route TCP traffic to the corresponding application.

To authorize access to the repeater, there is an optional codeplug password authentication on a per-repeater basis. It is configurable through RM. The codeplug password can be provisioned in the repeater before using this feature.

NOTE: Using the RM to provision or to upgrade a repeater disables the repeater temporarily until the operation is completed. The duration of the operation depends on the network bandwidth and the amount of transferred data.

2.20.2
Configuring IRP in RM

Follow these steps to enable IP Repeater Programming (IRP) on your repeater.

Procedure:

1. Launch the RM Device Monitor program.
2. Select **Settings**.
3. In the **Device Communication Method** section, select **IP Program** check box.

4. Configure **IP Program Settings** depending on your requirements and click **OK**.
5. Restart the RM Device Monitor to enable the applied changes.
6. Launch the Radio Management (RM).
7. In Radio View, right-click the repeater for which you want to enable IRP feature and select **Edit Configuration**.
8. From the **Set Categories** navigation tree, select **General** → **Network**.
9. In the **IP Repeater Programming** section, select **Enable** check box.

2.21 Over-The-Air Battery Management

System	Description
 IP Site Connect	IP Site Connect supports Over-The-Air Battery Management
 Capacity Plus Single Site	Capacity Plus Single Site supports Over-The-Air Battery Management
 Capacity Plus Multi Site	Capacity Plus Multi Site supports Over-The-Air Battery Management

When a battery fails and communication is lost, it impacts every aspect of an organization from serving customers to saving lives. But monitoring and maintaining the status of a large fleet of batteries can be time-consuming, inefficient and potentially overwhelming.

That is why the proprietary IMPRES™ Battery Fleet Management technology was created. It saves the guesswork, complexity and costs of managing hundreds even thousands of radio batteries and chargers wherever they're located, and makes it easier for users to do their work safely and successfully.

IMPRES Battery Fleet Management already supports collection of battery information each time an IMPRES battery is inserted into an IMPRES charger. And now IMPRES Battery Fleet Management supports automatic collection of battery information over the air while the radios are in use. This removes the need for wired network connections, Charger Interface Units, and remote clients at charger locations.

With IMPRES Battery Fleet Management, existing or customizable reports can be utilized to see the most relevant information. Data is stored in a database and can be exported to an Excel file or printed. IMPRES Battery Fleet Management software records and organizes a variety of data so the user can:

- Evaluate whether batteries are meeting their performance criteria
- Determine when batteries are nearing their end-of-life
- Eliminate unexpected downtime and work interruptions
- Avoid the expense of throwing batteries away prematurely
- Identify batteries that are missing, misplaced or inactive

- Identify radios that are not using IMPRES batteries
- Decide exactly when to buy new batteries
- Optimize charger utilization

NOTE: Over-The-Air battery management focuses on managing the long term health of the batteries. It is not meant to acquire the current real-time energy levels of all radios within the system.

Automatic collection of battery information over the air is supported in the following system architectures:

- Direct Mode (including Dual Capacity)
- Single Site Repeater
- IP Site Connect
- Capacity Plus Single Site
- Capacity Plus Multi Site

Collection of battery information over the air is supported in the following radios when they are utilizing IMPRES batteries:

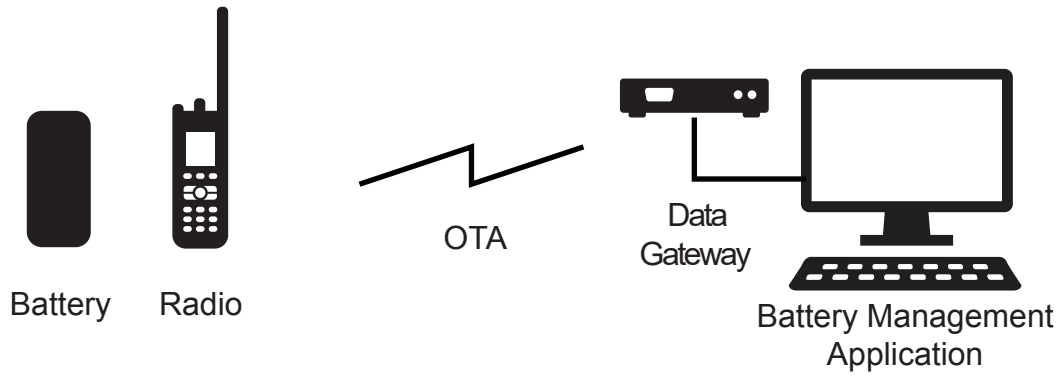
- DP2000 and DP4000 Series

2.21.1
Over-The-Air Battery Management Process

The Battery Fleet Management application (BFM) communicates with the radio system through an IP data gateway. The IP data gateway can be either the Motorola Solutions Network Interface Service (MNIS), which communicates through IP to the repeaters in the system, or a mobile radio configured as a Control Station.

To support AES privacy, the repeater codeplug must be configured with Enhanced privacy type since the repeater does not encrypt or decrypt any AES payload. The Enhanced privacy option allows the repeater to repeat the AES and Enhanced privacy encrypted audio and data bursts. For proper functioning of the repeater in a system with AES encrypted transmissions, the repeater must be running on firmware version R02.08.00 or later.

Figure 36: Battery Fleet Management Application (BFM) set up



BFM starts empty. Within a few hours after radio power-up, it registers its current battery Over-the-Air with the BFM. If the battery has never been registered with the BFM before, the BFM creates a new record for the battery and reads its battery data Over-the-Air. If the battery has been registered with the BFM before, the BFM checks the last time the battery's data was read. If it has not been recently read, the BFM reads the

battery data Over-the-Air. If it has been recently read, no action is taken. Radios register their battery about once a day, and a battery's data is read once every few weeks.

2.21.2
Automatic Over-the-Air Battery Data Collection Configuration

The radios must be programmed with the Radio ID of the IP data gateway that the Battery Fleet Management application is utilizing. Over-the-Air battery management must also be enabled on the channel that the IP data gateway is monitoring.

The Battery Management Server ID can be found in the network section of the radio CPS, under **Services**. Digital capable channels have a check box to enable Over-The-Air Battery Management. The radio only sends automatic battery registrations on channels that are enabled for Over-The-Air battery management.

Per standard data system configuration, the IP data gateway, either MNIS or a Control Station, must have a unique Radio ID on the system. The IP data gateway utilized by the BFM must be configured for confirmed data calls otherwise the success rate of the Over-the-Air battery management messaging is noticeably low.

If there is a UDP port conflict on the PC, the IP data gateway, either MNIS or a Control Station, and the BFM application can be configured with a different UDP port. The setting can be found in the **General** / **Network** section of CPS for the Control Station, and the **Configuration** menu of the Battery Fleet Management application.

Over-the-Air battery management messaging does not revert; therefore the BFM IP data gateways need not be monitoring Revert Channels.

Since the Over-the-Air messaging utilizes the MOTOTRBO IP data service, all prerequisites and limitations of the standard IP data service apply to battery management.

2.21.3
System Level Optimizations

Two timers may require adjustments for optimal performance such as the **Battery Data Refresh Timer**, and the **Radio Hold Off Timer**.

The default values should be acceptable for most scenarios.

2.21.3.1
Battery Data Refresh Timer

The **Battery Data Refresh Timer** controls how frequently the battery data is read.

Its default value is 21 days (3 weeks). Battery data changes fairly slowly, therefore it is unnecessary to read it Over-the-Air very often. The more often the battery data is read, the larger the load on the system. This is especially true if the system contains a very large number of radios. The **Battery Data Refresh Timer** can be found in the **Preferences** of the Battery Fleet Management application.

2.21.3.2
Radio Hold Off Timer

The **Radio Hold Off Timer** controls how long after power-up the radio waits before registering its current battery with the Battery Fleet Management application. Its default value is two hours. The radio waits for a random time between 30 minutes and the configured **Radio Hold Off Timer**.

If a system contains a very large number of radios, the **Radio Hold Off Timer** should be increased to minimize the Over-the-Air message collisions and congestion during shift changes or other scenarios where

many radios power cycle within a short period of time. Because battery data is normally only read once every three weeks, delaying a battery registration a few hours after power-up does not impact the long-term automatic battery data collection process.

The **Radio Hold Off Timer** can be found in the **Preferences** of the Battery Fleet Management application. It can also be configured per radio within the **Radio Information** dialog. The Battery Fleet Management application informs the radio of the new **Radio Hold Off Timer** the next time it registers.

The radio utilizes the new **Radio Hold Off Timer** starting after the next power cycle, which usually occurs the next day.

After the CPS configuration, the radio registers within minutes after power-up before its first successful registration with the Battery Fleet Management application.

2.21.3.3
Manual Battery Data Read Performance

The automatic Over-The-Air battery data collection process maintains the battery data in the Battery Fleet Management application (BFM) up to date, within the duration of **Battery Data Refresh Timer**.

If an immediate battery data refresh is required, the Battery Fleet Management application allows the user to request a manual read of the radio and battery.

If the requested radio is not available (turned off, out of range, busy in a call, in a charger, and others), the BFM marks the radio and battery to be read the next time either registers with the BFM. If the requested radio is available, but the attached battery does not match the requested battery, the BFM reads the attached battery and then marks the requested battery to be read the next time it is registered with the BFM.

NOTE: It is not recommended to perform rapid manual requests. The resulting data transfers may cause disruption to other services.

2.21.3.4
Radio Battery Utilization While Charging

When a radio is placed in a charger while powered on, its battery data cannot be collected Over-The-Air. The radio does not register an IMPRES battery while in the charger. The automatic collection process pauses, and then continues when removed from the charger. A radio does not respond to a manual battery data read request Over-The-Air while in a charger.

It is expected that a radio spends at least the duration of the Radio Hold Off Timer powered up and not in a charger per day. If a radio is always in a charger, a wired solution utilizing Charger Interface Unit is the best solution.

If a radio is powered up (turned on) while already in the charger, it will not recognize the IMPRES battery and registers as a non-IMPRES battery with the Battery Fleet Management application. When the radio is removed from the charger the first time after power up, the radio registers its battery as an IMPRES within the duration of the Radio Hold Off Timer.

2.21.4
Advanced System Deployments

There are generally two types of Over-the-Air battery management deployments for the IMPRES Battery Fleet Management application: those that connect to the radio system through an IP link through the Motorola Solutions Network Interface Service (MNIS), and those that connect to the radio system through the Over-the-Air link through Control Stations.

It is important to note that the BFM sends IPv4 data messages targeted towards the radios and is agnostic to the underlying radio system architecture.

2.21.4.1

MOTOTRBO Network Interface Service Deployments

The following parameters within the MOTOTRBO Network Interface Service (MNIS) software must be set:

- Confirmed Layer 2 Data Enabled
- A Radio ID (**MNIS Application ID**) that matches the **Battery Management Server ID** configured in the fielded radios.

The Battery Fleet Management application itself does not require Presence via the Device Discovery and Mobility Service (DDMS), but the MNIS requires the DDMS to route the data to the appropriate channel and site. The Battery Fleet Management application and MNIS can reside on the same PC or different ones. When BFM is deployed on its own PC, then a static IPv4 route is required to be manually entered in the BFM PC that routes all radio data through the MNIS. On the MNIS the UDP port for battery management messages (default is 4012) must be forwarded to the BFM PC IPv4 address. The MNIS and BFM PCs should be in the same subnet. For more information about this kind of deployment, see Data Applications and MNIS Deployment on Separate PCs on page 500. Radios in the field always send Over-the-Air battery management messages confirmed regardless of the radio's configuration.

NOTE: The Battery Fleet Management (BFM) is supported in Windows-based MNIS and DDMS deployments only. It is not supported in Edge Node-based MNIS and DDMS deployments.

2.21.4.1.1

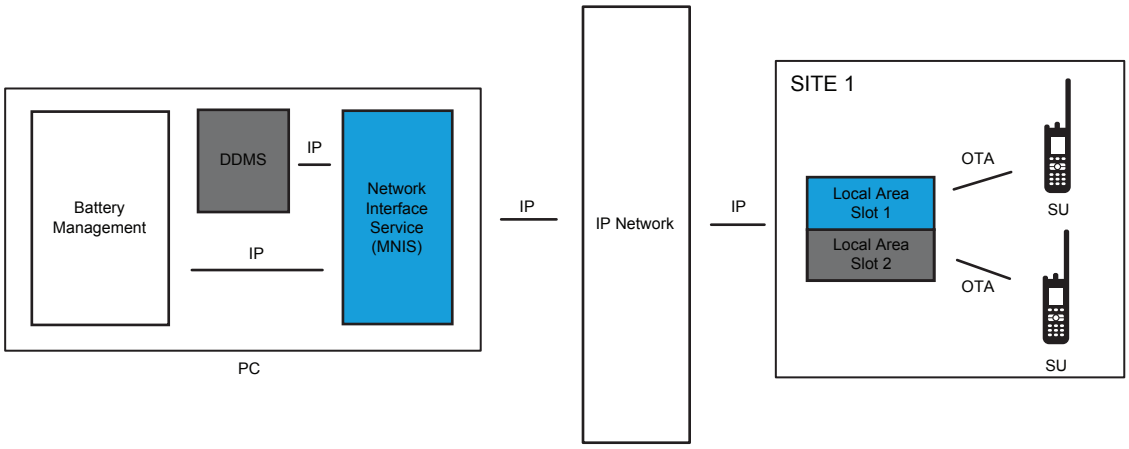
Single Site

Over-The-Air battery management is supported through MOTOTRBO Network Interface Service (MNIS) to single site repeaters.

MNIS can connect to eight single site repeaters at a time. In order for MNIS to perform mobility, DDMS must be installed, and ARS must be enabled in the radios.

NOTE: The Battery Fleet Management (BFM) is supported in Windows-based MNIS and DDMS deployments only. It is not supported in Edge Node-based MNIS and DDMS deployments.

Figure 37: BMA Deployment in Single Site with MNIS



2.21.4.1.2
IP Site Connect

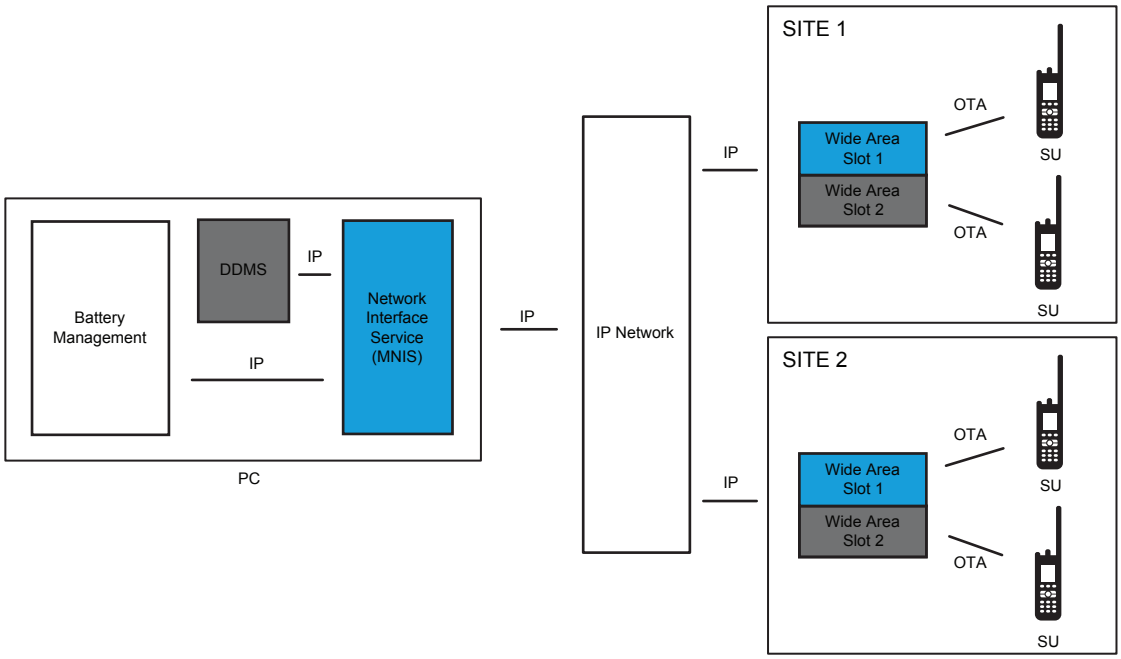
IPSC

Over the air battery management is supported through MNIS to IP Site Connect systems.

MNIS can connect to eight IPSC systems at a time. Each system can have 15 sites and eight systems can have 16 wide area channels. If utilizing local channels, one MNIS supports 32 wide and local channels overall. In order for MNIS to perform routing, DDMS must be installed, and ARS must be enabled in the radios.

NOTE: The Battery Fleet Management (BFM) is supported in Windows-based MNIS and DDMS deployments only. It is not supported in Edge Node-based MNIS and DDMS deployments.

Figure 38: BMA Deployment in IP Site Connect with MNIS



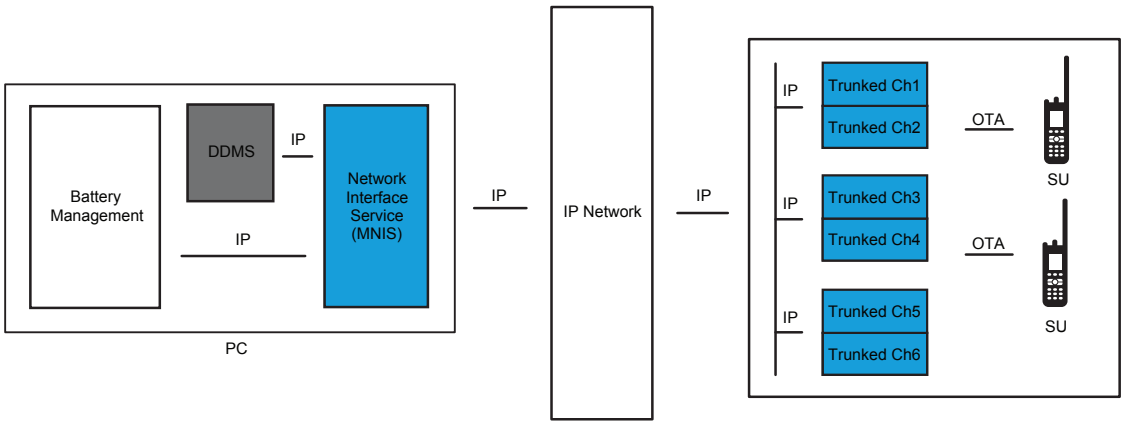
2.21.4.1.3
Capacity Plus Single Site

CPSS

Over-The-Air battery management is supported through MNIS to a CPSS system. MNIS can connect to one Capacity Plus system. In order for MNIS to perform routing, DDMS must be installed, and ARS must be enabled in the radios.

NOTE: The Battery Fleet Management (BFM) is supported in Windows-based MNIS and DDMS deployments only. It is not supported in Edge Node-based MNIS and DDMS deployments.

Figure 39: BMA Deployment in Capacity Plus Single Site with MNIS



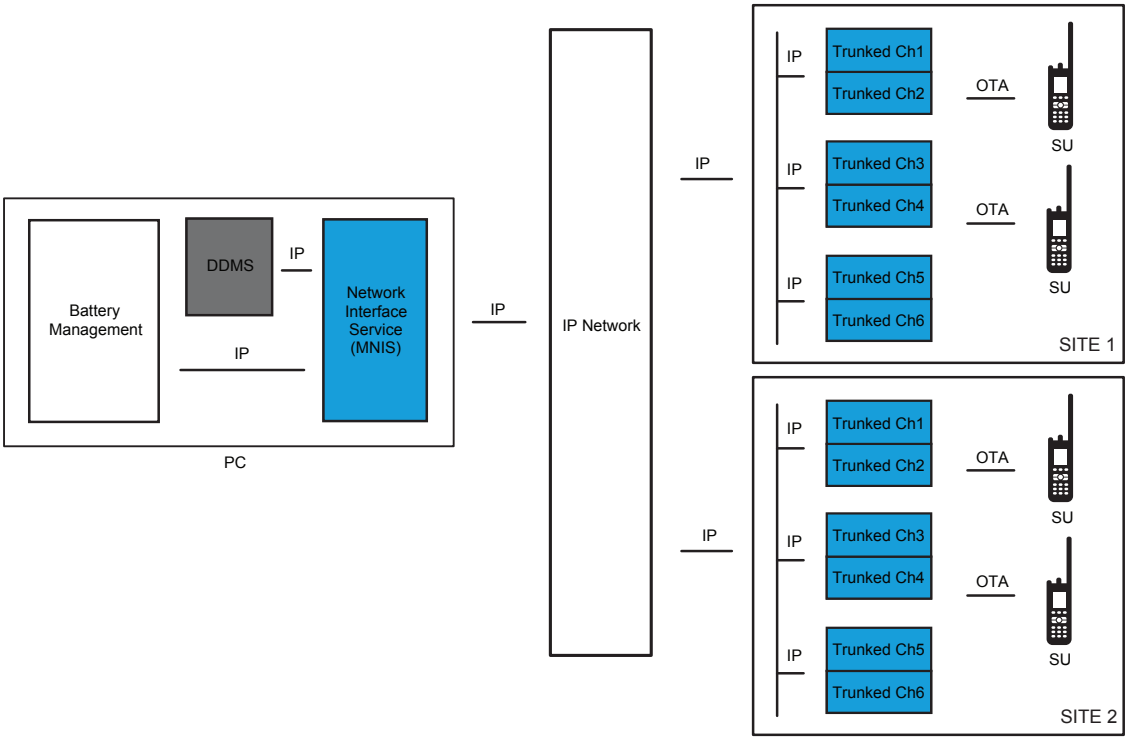
2.21.4.1.4
Capacity Plus Multi Site

CPMS

Over-The-Air battery management is supported through MNIS to a Capacity Plus Multi Site system. MNIS can connect to one Capacity Plus Multi Site system. In order for MNIS to perform routing, DDMS must be installed, and ARS must be enabled in the radios.

NOTE: The Battery Fleet Management (BFM) is supported in Windows-based MNIS and DDMS deployments only. It is not supported in Edge Node-based MNIS and DDMS deployments.

Figure 40: BMA Deployment in Capacity Plus Multi Site with MNIS



2.21.4.2

Control Station Configurations

The following parameters must be set within the Control Stations:

- Confirmed Layer 2 Data Enabled
- A Radio ID (**MNIS Application ID**) that matches the **Battery Management Server ID** configured in the fielded radios.

The Battery Fleet Management application itself does not require Presence through the Device Discovery and Mobility Service (DDMS). The Battery Fleet Management application and DDMS must reside on the same PC.

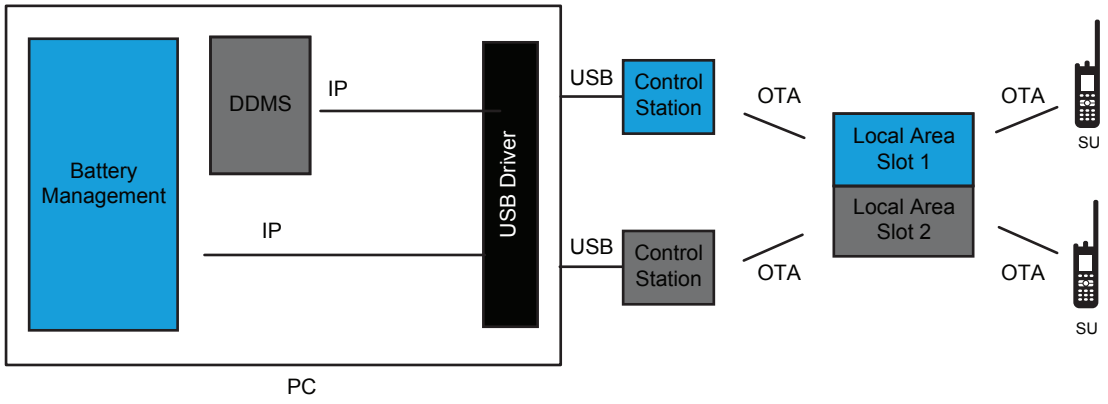
A static IPv4 route may be required to be manually entered in the PC that routes all radio data through the Control Station's network interface. Radios in the field always send Over-the-Air battery management messages confirmed regardless of the radio's configuration.

NOTE: The Battery Fleet Management (BFM) is supported in Windows-based MNIS and DDMS deployments only. It is not supported in Edge Node-based MNIS and DDMS deployments.

2.21.4.2.1
Direct Mode

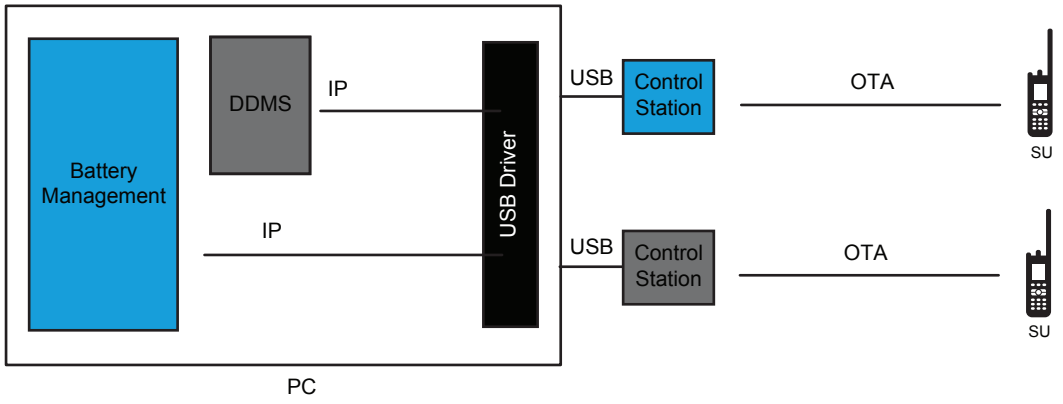
Over-The-Air battery management is supported through a Control Station in direct mode (including dual capacity). The USB Driver is required in all Control Station configurations in order for the Battery Fleet Management Application to send IP data grams through the Control Station.

Figure 41: BMA Deployment in Single Channel Direct Mode with Control Stations



Over-The-Air battery management is supported through up to 16 control stations in direct mode (including dual capacity). When using multiple Control Stations, a static IPv4 route configuration and the Device Discovery and Mobility Service (DDMS) are required. ARS must be enabled in the radios.

Figure 42: BMA Deployment in Multi-Channel Direct Mode with Control Stations

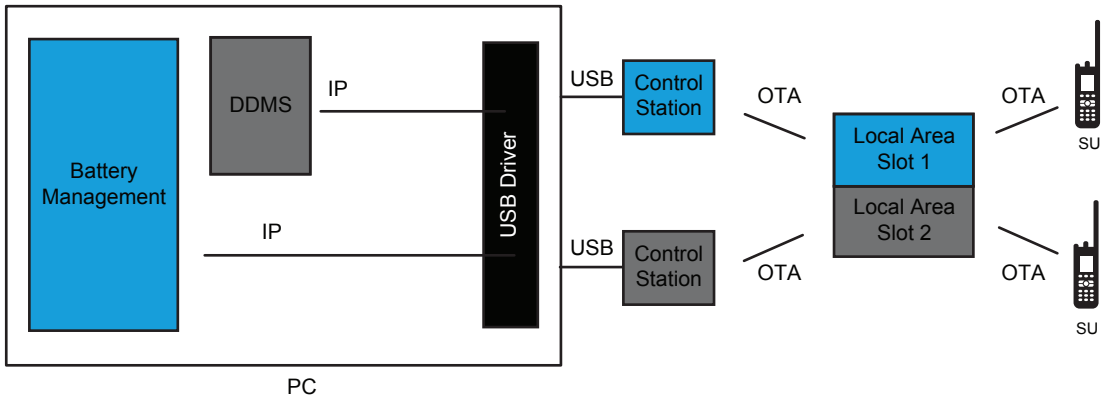


2.21.4.2.2
Single Site

Over-The-Air battery management is supported through up to 16 Control Stations in single site repeater mode.

When using multiple Control Stations, a static IPv4 route configuration and the Device Discovery and Mobility Service (DDMS) are required. ARS must be enabled in the radios.

Figure 43: BMA Deployment in Single Site with Control Stations



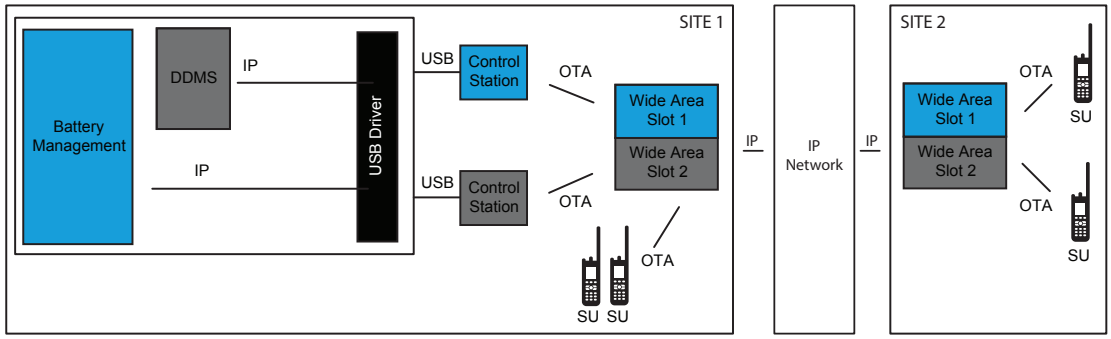
2.21.4.2.3
IP Site Connect

IPSC

Over the air battery management is supported through up to 16 Control Stations in IP Site Connect mode.

When using multiple Control Stations, a static IPv4 route configuration and the Device Discovery and Mobility Service (DDMS) are required. ARS must be enabled in the radios. Local channels may require an additional proxy and Control Stations in order to communicate over the air to the local channel.

Figure 44: BMA Deployment in IP Site Connect with Control Stations



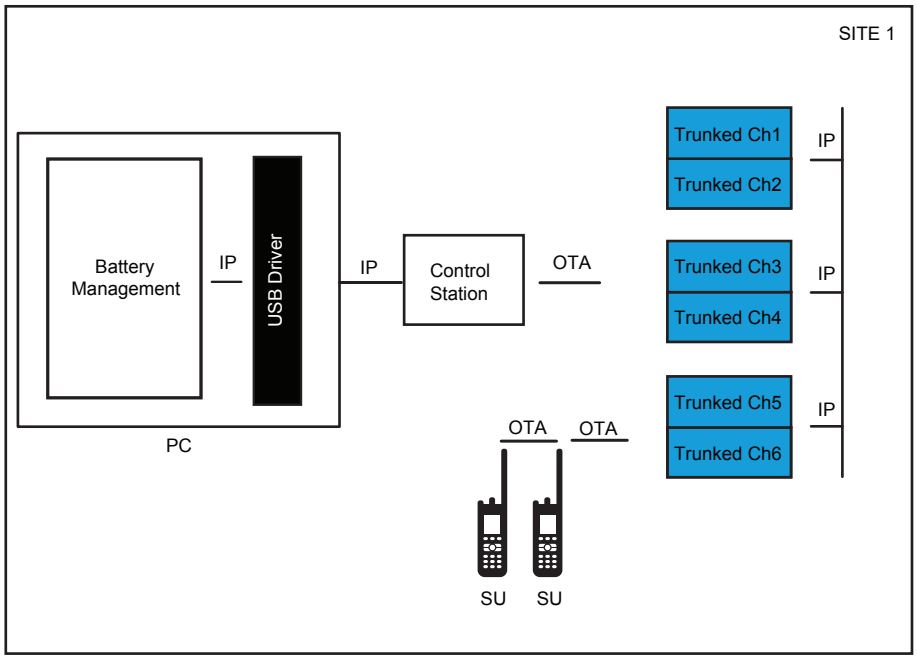
2.21.4.2.4
Capacity Plus Single Site

CPSS

Over-The-Air battery management is supported through Control Stations in Capacity Plus Single Site mode.

Only one trunking Control Station is required. The Device Discovery and Mobility Service (DDMS) isnot required in Capacity Plus Single Site. Over-The-Air battery management messages are sent on the trunking channels. They are not sent on data Revert Channels.

Figure 45: BMA Deployment in Capacity Plus with a Control Station



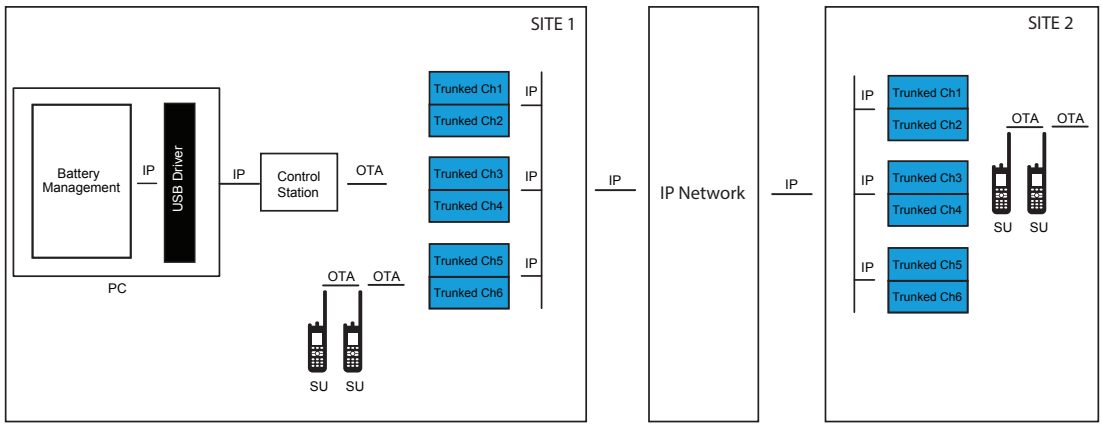
2.21.4.2.5
Capacity Plus Multi Site

CPMS

Over-The-Air battery management is supported through Control Stations in Capacity Plus Multi Site mode.

Only one trunking Control Station is required. The Device Discovery and Mobility Service (DDMS) is not required in Capacity Plus Multi Site. Over-The-Air battery management messages are sent on the trunking channels. They are not sent on data Revert Channels.

Figure 46: BMA Deployment in Capacity Plus Multi Site with a Control Station



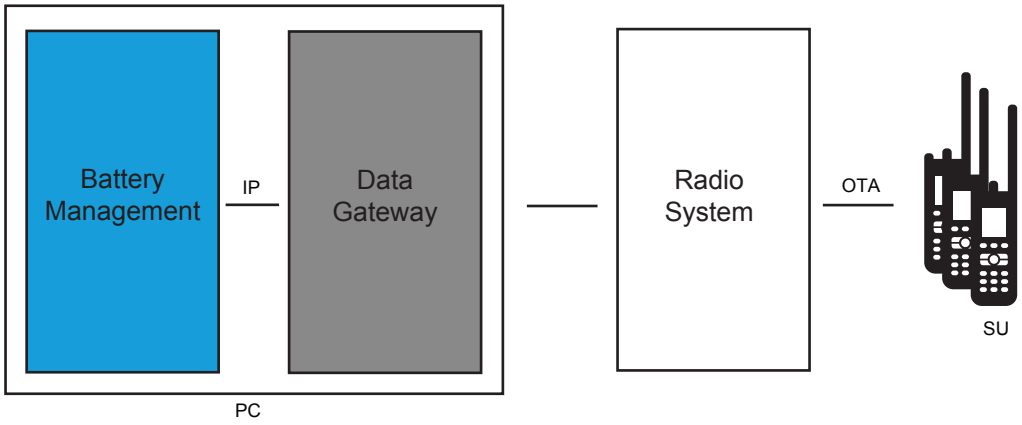
2.21.4.3
Battery Management Application Deployment

As shown in the previous section, the Battery Fleet Management application sends IP data messages targeted towards the radios and is agnostic to the underlying radio system architecture or the type of data gateway utilized, MNIS or Control Stations.

This section provides basic information on the ‘data gateway’ which represents the DDMS and MNIS, or the DDMS, USB Driver, and Control Stations. The radio system can be any of the architectures.

NOTE: The Battery Fleet Management (BFM) is supported in Windows-based MNIS and DDMS deployments only. It is not supported in Edge Node-based MNIS and DDMS deployments.

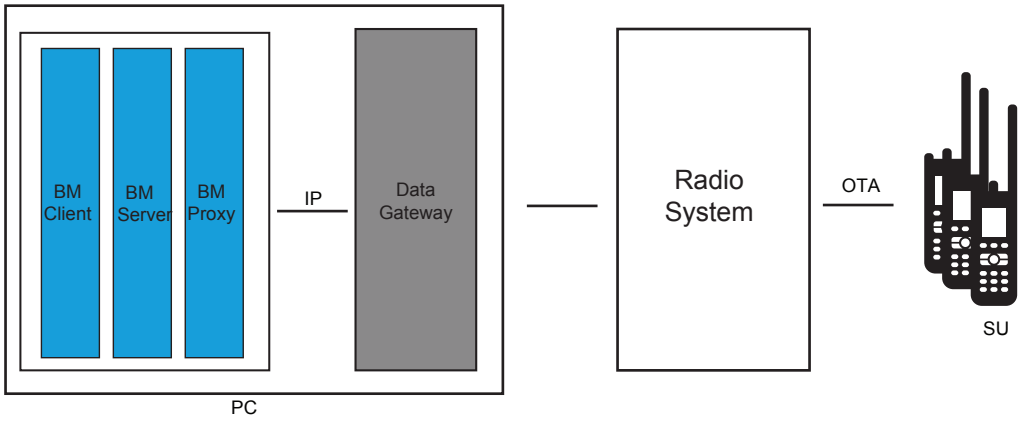
Figure 47: Simplified BMA Deployment Diagram



2.21.4.3.1
Battery Fleet Management Application

The Battery Fleet Management Application is made up from a Client, a Server and a Proxy.

Figure 48: BMA Deployment with Client, Server and Proxy on the Same PC



The Battery Fleet Management Client is the main user interface for the application. The Battery Fleet Management Server is where all the battery data is stored. The Battery Fleet Management Proxy communicates with the radio system. The Battery Fleet Management Proxy resides on the same PC as

the Data Gateway (MNIS or Control Stations). The other components may reside on other PCs, as long as there is a direct IP connection between all components.

NOTE: The Battery Fleet Management (BFM) is supported in Windows-based MNIS and DDMS deployments only. It is not supported in Edge Node-based MNIS and DDMS deployments.

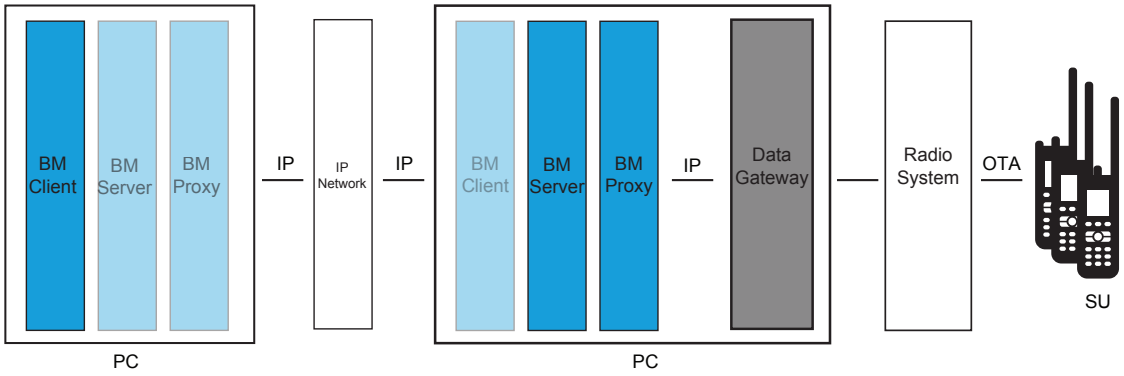
2.21.4.3.2

Remote Battery Management Client

The Battery Fleet Management Application Client can be remotely located away from the Battery Fleet Management Server and Proxy, and useful when the dealer site is not co-located with the customer's site.

NOTE: The Battery Fleet Management (BFM) is supported in Windows-based MNIS and DDMS deployments only. It is not supported in Edge Node-based MNIS and DDMS deployments.

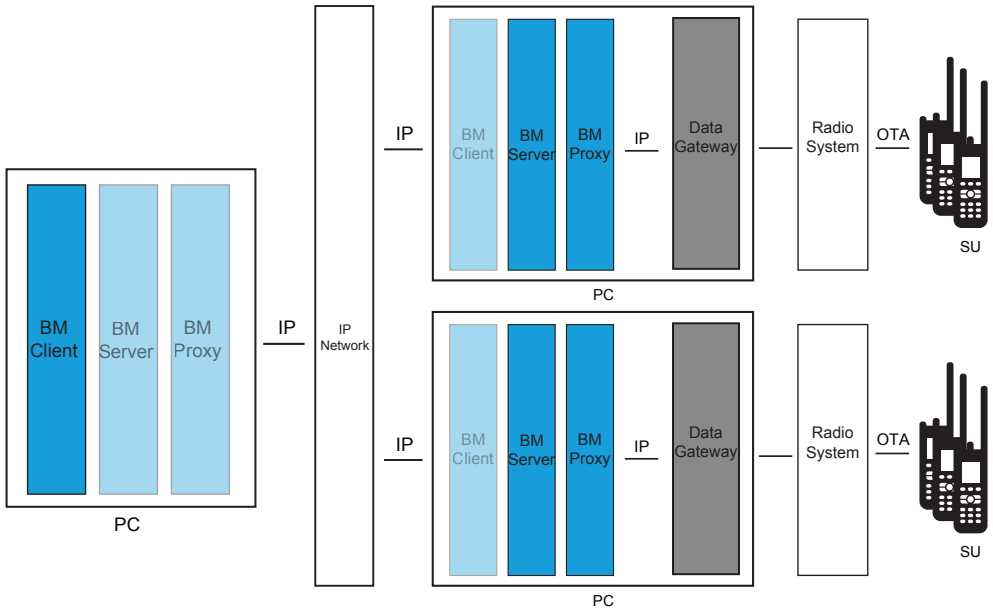
Figure 49: BMA Deployment with Client Remote from Server and Proxy



It is helpful when one battery management user needs to manage multiple systems that cannot be accessed with one data gateway. For example, if using control stations to monitor systems that are not within RF coverage of each other, multiple sets of Control Stations and proxies must be utilized. Since an MNIS has limitations on how many systems it can connect to, multiple sets of MNIS and proxies must be utilized.

In the case of remote client, each data gateway has its own Battery Fleet Management Proxy and Server. This means that each system's batteries have their own database and the database is often located at the customer's site.

Figure 50: BMA Deployment with Client Remote from Multiple Server and Proxies



2.21.4.3.3

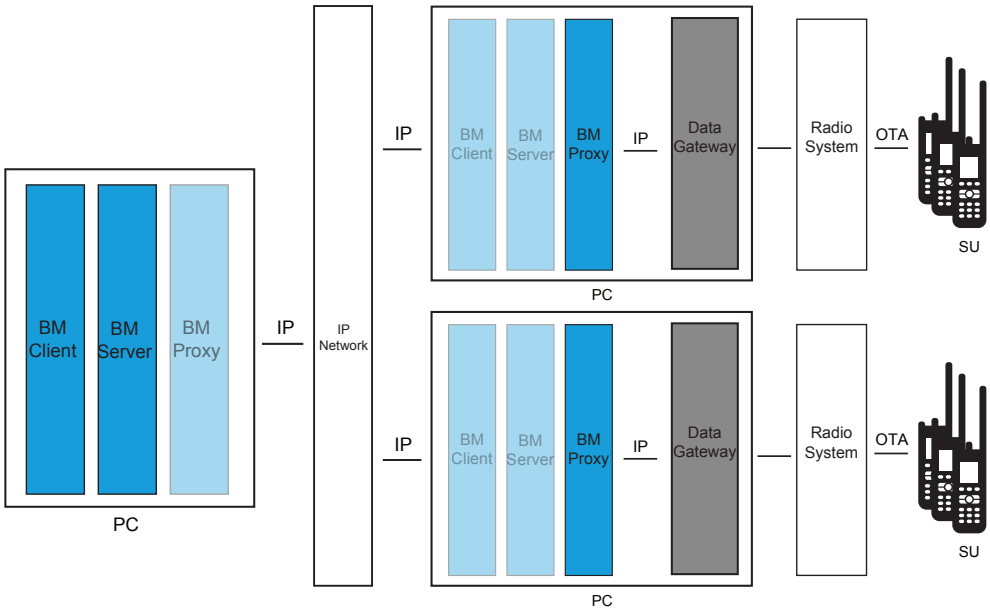
Remote Battery Management Proxy

A remote battery management proxy is similar to the remote client use cases explained earlier; however this allows the battery management user to maintain one server for all of their batteries and systems. Rather than the servers being located at the customer sites, only the proxy is located at the customer sites. This is convenient for the battery management user, but requires the connection between the server site and the proxy site to be available all the time since there is communication between those components occurring all the time. In contrast, the client only communicates to the server when the user is present and reviewing battery data.

The Battery Fleet Management application handles the mobility between the server and the proxies. When a radio registers its battery, the proxy from which it registered is saved in the Battery Fleet Management Server in order to route outbound messages. There is only one MNIS on one PC at a time.

NOTE: The Battery Fleet Management (BFM) is supported in Windows-based MNIS and DDMS deployments only. It is not supported in Edge Node-based MNIS and DDMS deployments.

Figure 51: BMA Deployment with Multiple Proxies Remote from Server



2.21.4.4

Coexistence with Other Data Applications

The Battery Fleet Management application is supported in system configurations with the Radio Management application. Battery Fleet Management and Radio Management may be installed on the same computer.

NOTE: The Battery Fleet Management (BFM) is supported in Windows-based MNIS and DDMS deployments only. It is not supported in Edge Node-based MNIS and DDMS deployments. Therefore, the below information is applicable for Windows-based MNIS and DDMS deployments only.

The Battery Fleet Management application is supported in system configurations with third-party applications, but there may be some special considerations and configurations required.

In general, it is recommended that the Battery Fleet Management application be installed on a different computer than any other third-party application. There may be various conflicts present, message routing being the most common, which may cause issues. Interoperability testing with every third-party application in the market is not possible; therefore we only support installations on different computers. If installation on the same computer as a third-party application is a must, it is recommended you pre-test all functionality before deployment.

Third-party applications have a wide array of methods to implement presence notification. In some cases, their implementations conflict with our implementation. As described in earlier sections, although the Battery Fleet Management application itself does not require presence, some system architectures may require it for data routing.

Radios can be configured to send automatic registration service (ARS) messages through the system to the Device Discovery and Mobility Service (DDMS). These messages are utilized by the system for presence and mobility. The radios are configured to send these messages to one target. If the radios are already configured to send these messages to a third-party application’s presence service, steps must be taken so that the DDMS can also receive them.

If installing the Battery Fleet Management application on a system with a third-party application that utilizes a non-ARS based method of implementing presence, then the Device Discovery and Mobility Service (DDMS) can be installed and utilize the automatic registration service (ARS) over the air without any further issues. An example of a non-ARS based method would be monitoring for traffic of any kind instead of utilizing the

actual presence notification service over the air. This allows the radios to send their presence to Motorola Solutions's DDMS.

If installing the Battery Fleet Management application on a system with a third-party application that utilizes a Non-Motorola Solutions based presence service, then the Device Discovery and Mobility Service (DDMS) and Data Gateways must be installed on the system in a passive presence configuration.

Simply stated, a passive presence configuration means the DDMS and Data Gateways (MNIS or Control Stations) are configured to not acknowledge incoming ARS messages, where they act passively to incoming messages. This allows the reception of messages by both the third-party applications and Motorola Solutions applications without creating duplicate acknowledgements that might collide or conflict in the system.

2.21.5
Battery Fleet Management Computer Specifications

There are four computer specifications that a user needs to know in battery fleet management.

2.21.5.1
Operating System Requirement

- Windows 8 x86 and x64
- Windows Server 2003 x86 and x64
- Windows Server 2008 x86 and x64
- Windows Server 2008 R2 x64

2.21.5.2
Hardware Minimum Requirement

The IMPRES Battery Fleet Management application can either be installed on a client/proxy computer or a server computer.

Although the installation package is the same for client and server computers, the hardware installation requirements are different for each.

2.21.5.3
Server Hardware Minimum Requirement

- DVD drive
- 1 GB of hard disk space
- 2 GB RAM

2.21.5.4
Client or Proxy Hardware Minimum Requirement

- 1 USB (Universal Serial Bus) Port
- DVD drive
- 200 MB of hard disk space
- 1 GB RAM

2.22

Over-The-Air Radio Programming

System	Description
 IP Site Connect	IP Site Connect supports Over-The-Air Radio Programming
 Capacity Plus Single Site	Capacity Plus Single Site supports Over-The-Air Radio Programming
 Capacity Plus Multi Site	Capacity Plus Multi Site supports Over-The-Air Radio Programming

When the need to program a radio or a fleet of radios occurs, the process can take place at the customer location or the dealer's shop. However, the process of programming radio parameters, features, contact lists, and others can be troublesome.

Some issues encountered include – difficulty to locate all radios, delays waiting for radios to be brought in for programming, radios mounted in vehicles, operation and downtime during programming, wasted time traveling to/from customer location, only a limited number of radios can be programmed simultaneously. It is often difficult for dealers to extract value for this. Therefore, radio programming is viewed as a hassle, time consuming, and inefficient.

To support this need, the MOTOTRBO Radio Management (RM) now offers the following services with software version R02.10.00 or later:

- Writes and reads radio configurations Over-The-Air
- Manages up to 5000 radio configurations
- Group and individual archive management
- Application and radio mutual authentication
- Synchronized configuration switchover
- Radio user receives one time option to accept or delay
- Scheduling of Over-The-Air operations
- Unmanned batch processing of numerous Over-The-Air operations
- Remote client capability
- Multi-customer and system capable
- Optimized performance using Presence Services
- Compressed and differential configuration transfer
- Designed to allow voice traffic priority while transferring
- Utilizes existing Over-The-Air encryption
- Session logging

- Historical reporting

The above features are available in all digital architectures including:

- Direct Mode (12.5e and 6.25e)
- Single Site Repeater
- IP Site Connect
- Capacity Plus Single Site
- Capacity Plus Multi Site

The services that are supported are not available to the ADP developers.

The following features and services are specifically not supported by OTAP:

- radio software upgrades
- language packet updates
- radio tuning parameter updates
- device recovery
- update or download voice announcement files
- radios prior to software version R02.10.00
- Over-The-Air repeater programming (only IP Repeater Programming is available)
- programming while in Connect Plus or Passport Mode
- programming while in Analog Mode
- "welcome screen" icon updates

2.22.1
Basic Deployments of OTAP Software

There are six basic deployments of Radio Management for OTAP. These are used as the building blocks for more complicated configurations.

The configurations are:

- Local Single Channel Configuration
- Local Single Channel Configuration with Presence
- Remote Client Configuration
- Remote Client Configuration with Multiple RM Servers
- Remote Device Programmer Configuration
- Multi-Channel Configuration

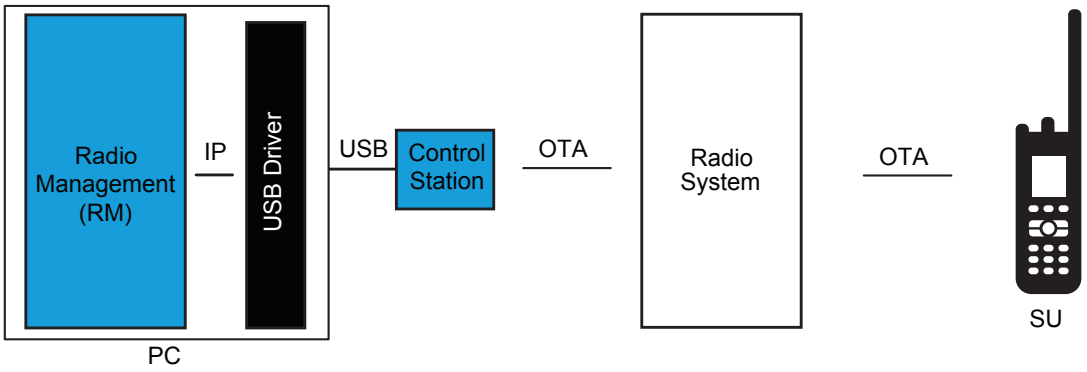
NOTE: Over-the-Air Programming (OTAP) is not supported in Edge Node-based MNIS deployments. It is supported in Windows-based MNIS deployments only. Therefore, configurations described in this section and its subsections are applicable for Windows-based MNIS deployments only.

2.22.1.1
Local Single Channel Configuration

The RM application utilizes the existing MOTOTRBO IP data service to communicate with the field radios Over-the-Air. Connectivity with the system can be achieved Over-the-Air through Control Stations or over the IP network utilizing the MOTOTRBO Network Interface Service (MNIS). No other Over-the-Air data application is supported on the same PC as the RM.

This Control Station setup requires a radio to be configured as a Control Station, connected to the RM PC via a USB cable, and utilized as the data gateway into the radio system. The standard radio USB driver is also required.

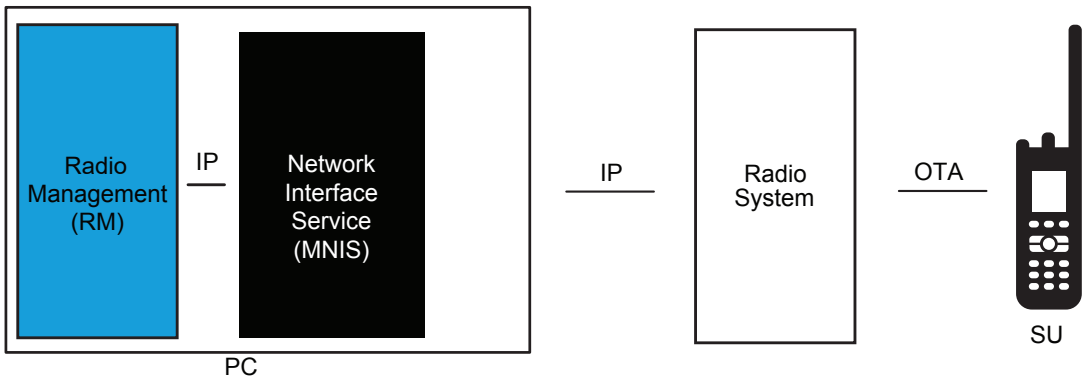
Figure 52: Single Channel Non-Remote RM Configuration Through Control Station



The setup with MNIS requires the RM software to be installed on the MNIS PC or a separate PC but in this case, the extra configuration is required. For more information about this kind of deployment, see; Data Applications and MNIS Deployment on Separate PCs on page 500. The RM with MNIS setup requires the Network Application Interface (NAI) to be enabled in the repeaters.

MNIS deployments are not available in Direct Mode since the MNIS interfaces directly with the repeaters, and there are no repeaters used in Direct Mode.

Figure 53: Single Channel Non-Remote RM Application Configuration Through MNIS



2.22.1.2

Local Single Channel Configuration with Presence

The RM can use the ARS and the presence service of the DDMS software to optimize Over-The-Air operations. When used, radios are only contacted if they are present. The ARS must be configured in the radios.

Without presence and the DDMS, the RM attempts to contact each radio one by one, regardless if they are present on the system or not. For optimal performance, it is recommended to use the presence service.

If used, the DDMS is installed on the same computer as the control stations or the MNIS.

Figure 54: Single Channel Non-Remote RM Application with Presence and Control Station

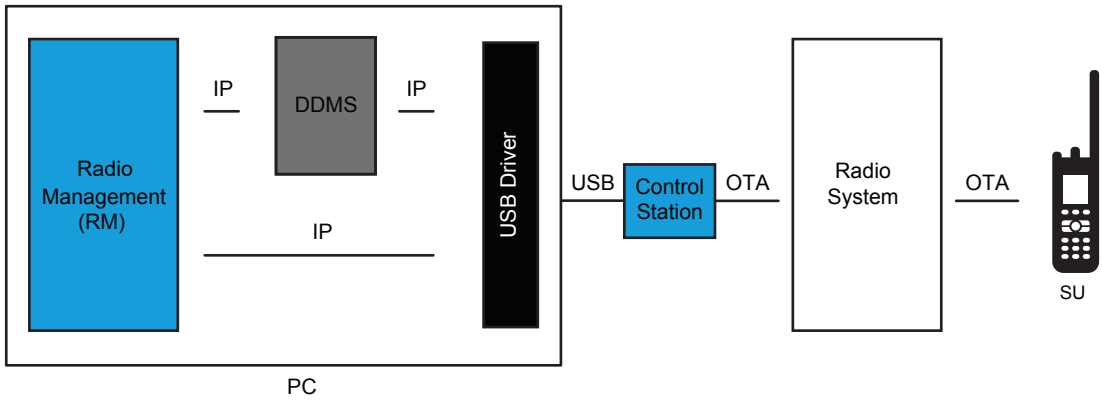
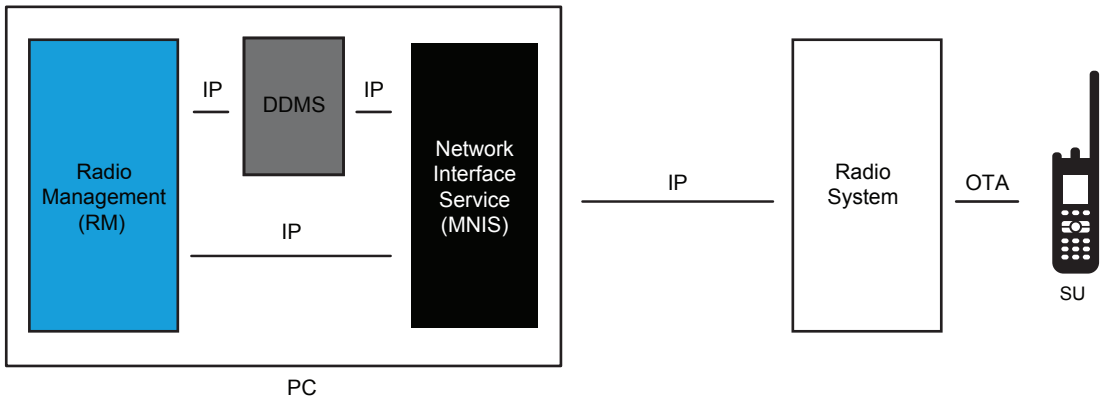


Figure 55: Single Channel Non-Remote RM Application with Presence and MNIS



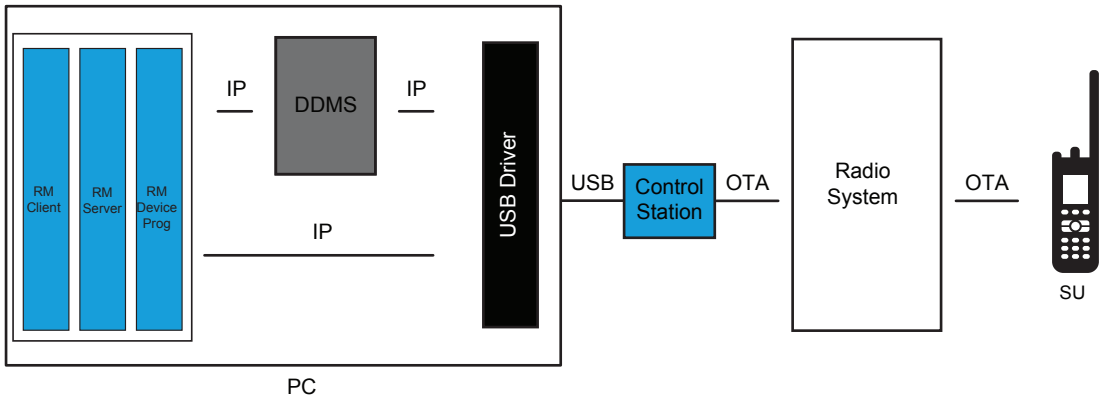
The RM consists of three major components:

- RM Client: Main User Interface
- RM Server: Storage of Configurations
- RM Device Programmer: Communication to Radio System

NOTE: The RM Device Programmer is also known as the “RM Proxy”.

In local deployments, all three components can be installed at the same time on the same computer. This is most useful when the system administrator is within RF coverage of the radio system. The following diagram shows the individual components. It is the same when using the MNIS.

Figure 56: Single Channel Non-Remote RM Application with Presence



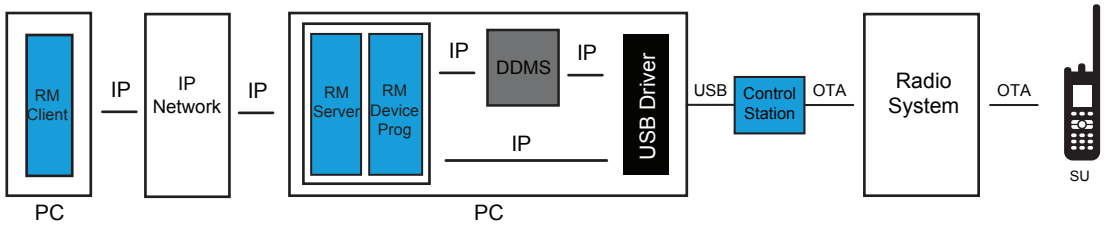
2.22.1.3

Remote Client Configuration

If the system administrator is not within RF coverage of the system, it is possible for the RM Client to be installed on a different PC and remotely access the RM Server and Device Programmer over an IP network.

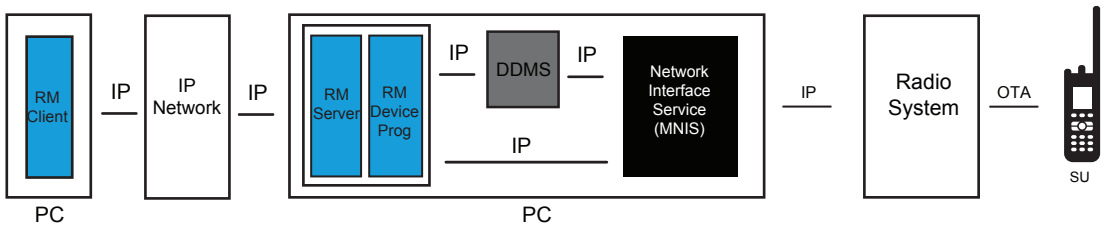
Direct network connectivity is required between the RM Client and the RM Server, therefore a VPN must be used or they must reside on a private network. The RM Server, RM Device Programmer, and Control Stations are located on the same PC.

Figure 57: Remote RM Client from RM Server with Control Station



When utilizing the MNIS, the RM Client can also be installed on a different PC from the RM Server. This allows the RM Server and RM Device Programmer to remain centrally located while the RM Client is located at another location on the IP network. The RM Device Programmer can be installed on the same PC as the MNIS or on a separate PC but in this case, the extra configuration is required. For more information about this kind of deployment see: Data Applications and MNIS Deployment on Separate PCs on page 500.

Figure 58: Remote RM Client from RM Server with MNIS



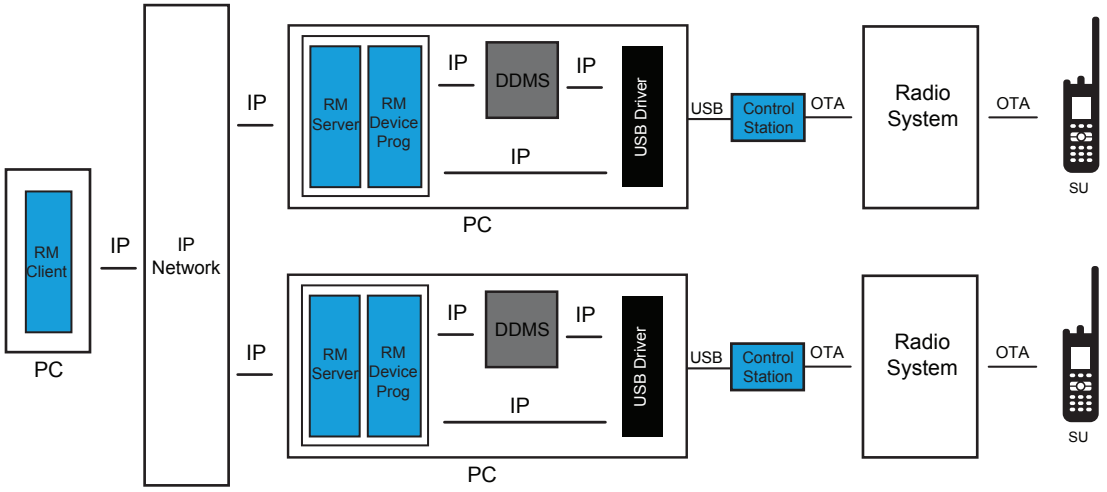
2.22.1.4

Remote Client Configuration with Multiple RM Servers

The RM Client can connect to any RM Server, but only one at a time. This allows the system administrator access to different customers with non-overlapping RF coverage from one location.

Although the RM Server, RM Device Programmer, and Control Stations must be within RF coverage, the RM Client does not. Each RM Server manages its own set of radios. Direct network connectivity is required between the RM Client and the RM Server; hence a VPN must be used or they must reside on a private network. However, the network connection between the RM Client and the RM Server doesn't need to be up all the time. The system administrator can set up a job with one RM Server, and then disconnect. The RM Server continues to execute.

Figure 59: Remote RM Client with Multiple RM Servers with Control Station

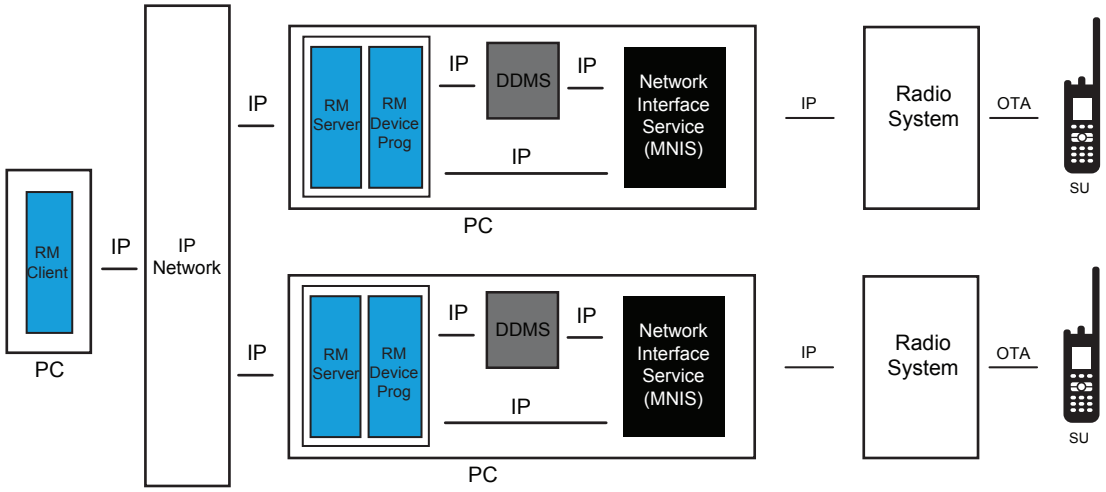


NOTE: One MNIS can connect to multiple remote single site systems over an IP network.

The RM deployment with MNIS does not require the RM Server and RM Device Programmer to be within RF coverage, because MNIS communicates with repeaters over the IP network.

System	Description
IPSC IP Site Connect	One MNIS can connect to multiple remote IP Site Connect systems over an IP network.
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	One MNIS can connect only to one CPSS or CPMS system at a time. Therefore, for multiple systems, multiple MNISs should be deployed. A remote RM Server, RM Device Programmer, and MNIS can be located at each CPSS system or one of the sites of a CPMS system. They can share one central RM Server which can be accessed with an RM Client.

Figure 60: Remote RM Client with Multiple RM Servers with MNIS



NOTE: One MNIS can connect to multiple remote single site systems over an IP network.

2.22.1.5

Remote Device Programmer Configuration

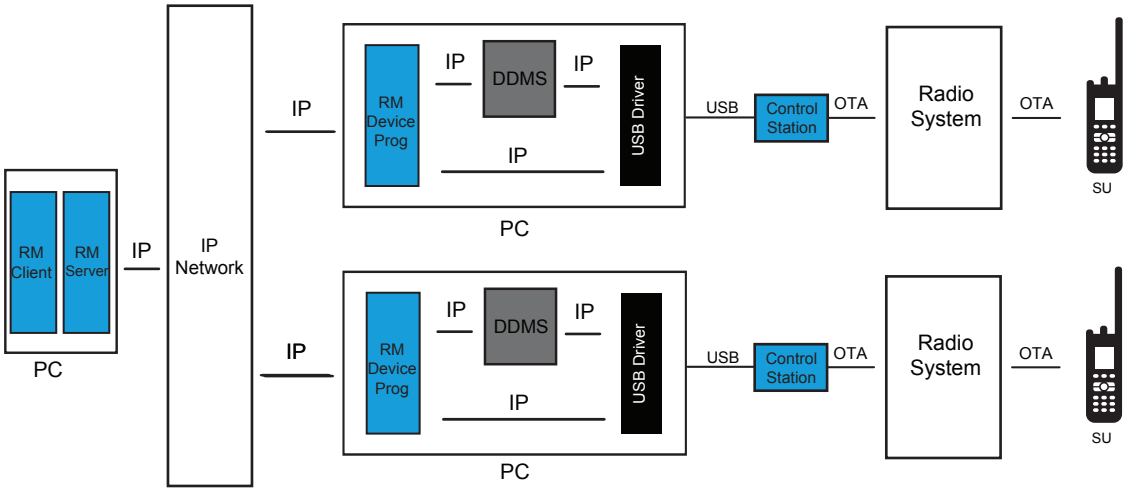
The RM Server can support up to 128 RM Device Programmers. This allows the system administrator to have all radios in one RM Server and have access to different sites with non-overlapping RF coverage.

The Device Programmer and Control Stations must be within RF coverage of their corresponding systems, which is unnecessary for the RM Server.

NOTE: If necessary, the RM Client can be remote from the RM Server as well.

Stable and direct network connectivity is required between the RM Server and RM Device Programmers. Therefore a VPN must be used, or they must reside on a private network. If stable, direct network connectivity is not possible, a Remote RM Client configuration with multiple RM Servers and the RM Device Programmers may be required.

Figure 61: RM Server with Remote Device Programmers and Control Stations



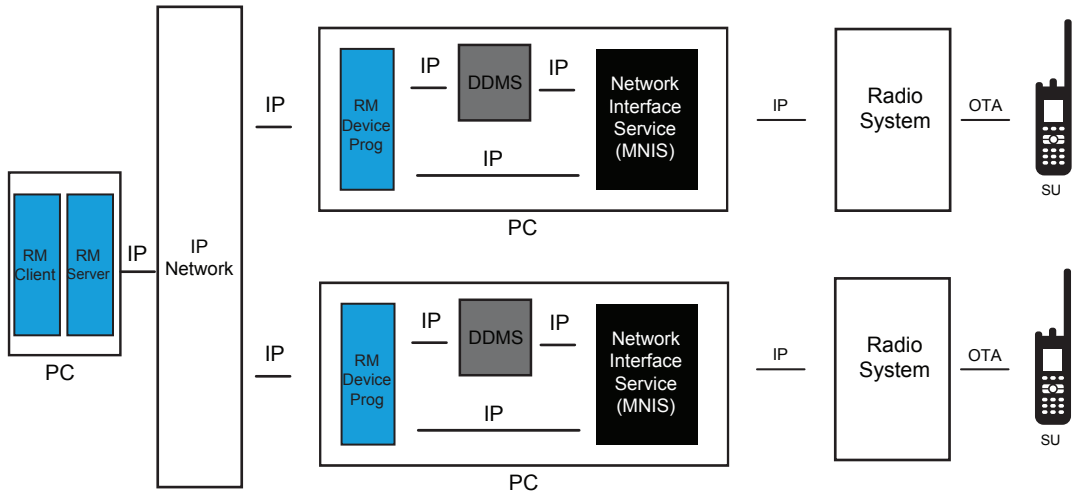
If utilizing Presence, the RM Device Programmer in the system where the target radio has registered can service jobs for that radio. An RM Device Programmer can also be configured to only service a specified set of radios. This is accomplished by setting the radios to a group within the RM Server and then configuring the RM Device Programmer to service this group.

NOTE: One MNIS can connect to multiple remote single site systems over an IP network.

System	Description
IPSC IP Site Connect	One MNIS can connect to multiple remote IP Site Connect systems over an IP network.
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	One MNIS can connect only to one CPSS or CPMS system at a time. Therefore, for multiple systems, multiple MNISs should be deployed. A remote RM Server, RM Device Programmer, and MNIS can be located at each CPSS system or one of the sites of a CPMS system. They can share one central RM Server which can be accessed with an RM Client.

The RM Device Programmer can be installed on the same PC as the MNIS or on a separate PC but in this case, the extra configuration is required. For more information about this kind of deployment, see Data Applications and MNIS Deployment on Separate PCs on page 500.

Figure 62: RM Server with Remote RM Device Programmers and MNIS



NOTE: One MNIS can connect to multiple remote single site systems over an IP network.

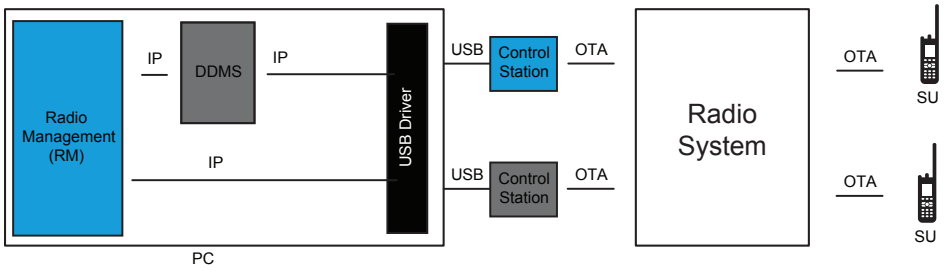
2.22.1.6

Multi-Channel Configuration

Multiple conventional channels are supported per RM Device Programmer in both local and remote configurations.

This requires a Control Station per channel; up to 16 Control Stations are allowed. Because radios can move from channel to channel, this configuration requires the DDMS to be installed and a static IPv4 route configured on the same PC.

Figure 63: Multi-Channel Non-Remote RM Application Configuration with Control Stations

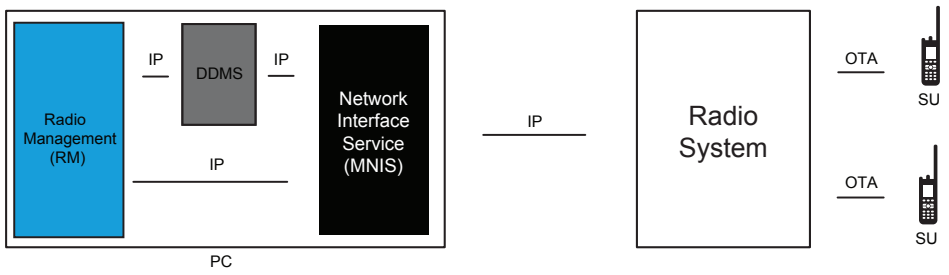


It is not recommended to utilize multiple Control Stations without DDMS. Without it, there is no method for RM messages to be properly routed on the appropriate channel. Specific routing can be added to the PC, but in this case radios can only be contacted on a specific channel. Another option is to configure the PC to broadcast on all channels; however, this uses up bandwidth.

NOTE: A multiple channel configuration can be deployed with remote RM Device Programmers, remote RM Servers, or a remote RM client. The RM works the same regardless of whether the Control Stations are communicating in direct mode, single site repeater mode, dynamic mixed mode, IP Site Connect mode, Capacity Plus Single Site mode, or Capacity Plus Multi Site mode.

When utilizing MNIS with DDMS. DDMS handles the mobility in a single site and IPSC systems. DDMS requires ARS to be enabled in the fielded radios. The MNIS can connect to up to 8 conventional systems.

Figure 64: Multi-Channel Non-Remote RM Application Configuration with MNIS



2.22.2
Process Flow for Over-The-Air Programming

There are five high-level steps for Over-The-Air Programming (OTAP), as follows:

- Initial programming of the essential communication parameters into the radio via wired CPS
- Populating the RM Server with the current radio configurations
- Modifying the radio configuration within the RM Server
- Delivering the modified radio configurations to the radios
- Applying (or switching over) the delivered radio configurations

2.22.2.1
Essential Communication Parameters Initial Programming

Prior to the first time a radio is programmed Over-The-Air, it must be provisioned with CPS through a wired connection. All the essential communication parameters required for the radio and the RM to communicate with each other on the system must be programmed.

The following are they essential communication parameters:

- Radio software upgrades
- System and channel parameters
- Data parameters
- Radio ID
- OTAP authentication key

2.22.2.1.1
Radio Software Upgrades

Any radio software upgrades required for Over-The-Air operation must be updated through configuration software in a wired operation.

Radio software upgrades are not supported Over-The-Air.

2.22.2.1.2
System and Channel Parameters

All system and channel parameters required for the radio to communicate with the system must be configured prior to the first operation Over-The-Air.

This includes the standard communication parameters such as frequencies, color codes, channels, talkgroups, voice privacy keys, and so on. If the radio cannot communicate on the system properly, the RM will not be able to contact it.

2.22.2.1.3
Data Parameters

RM utilizes the MOTOTRBO data service to communicate with the radios.

This means that all communication parameters required for data capability must be provisioned prior to the first operation Over-The-Air. This includes the ARS parameters.

2.22.2.1.4
Radio ID

In conventional configurations, the data service requires every radio on a logical channel to have a unique Radio ID.

If a data application is communicating on multiple channels, and DDMS are present, every radio communicating through the DDMS must have a unique Radio ID, even if they are on different logical channels.

If the RM communicates through a DDMS to multiple channels, every radio across those channels must have a unique Radio ID.

If utilizing a centralized RM Server to communicate with multiple systems using remote RM Device Programmers, every radio across those systems must have unique Radio IDs. If this is not achievable, then OTAP sessions to systems with duplicate IDs have to be executed sequentially – only one at a time or a separate RM Server must be utilized for each system. Ultimately, end-user fleets should be reconfigured to unique Radio IDs so that multiple OTAP sessions to multiple customer fleets can be processed simultaneously.

NOTE: The Radio ID must be programmed before the first Over-the-Air operation. There are rules about the data service and the uniqueness of the radio's Radio ID that must be followed.

System	Description
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	In Capacity Plus Single Site and Capacity Plus Multi Site, every radio must have a unique radio ID. If one customer contains multiple Capacity Plus Single Site systems, then every radio across those systems must have unique radio IDs. If this is not achievable, then one customer must have multiple RM Servers, one for each Capacity Plus Single Site system. This only limits the ability to connect to both systems at the same time.

2.22.2.1.5
Over-The-Air Programming Authentication Key

The only new OTAP parameter required to be programmed in the radio is the OTAP authentication key and key ID.

It must be present in both the radio and in the RM prior to the first Over-The-Air operation. The OTAP authentication key can be changed Over-The-Air if the current key in the radio matches the previous key entered in RM.

2.22.2.2
Populating the RM Server with Current Radio Configurations

After the radios have been initially programmed with wired CPS, their configurations must be populated into the RM Server.

There are three different ways to populate the RM Server with the current radio configurations:

- Archive importing
- Entering radio identity information
- Radio identity file importing

2.22.2.2.1
Archive Importing

Radios can be populated into the RM Server by importing the saved archive as each radio is programmed with its initial programming. This requires the CPS to have IP network connectivity to the RM Server during the initial programming.

If IP network connectivity is not available while initially programming the radios, each radio archive can be saved and imported into the RM Server when connection is available. One archive must be saved and imported for each radio since their specific identity information must be available in order to properly identify them in the RM Server.

The saved archive to be imported should contain the Over-The-Air authentication key, Enhanced Privacy keys, and Symmetric Keys that were entered in CPS prior to programming the radio via the wire. These are not available if a radio is only read with wired CPS since these cannot be retrieved from a radio. If not within the imported archive, the keys have to be entered into the RM prior to first Over-The-Air delivery.

NOTE: The initial retrieval or delivery Over-The-Air is not differential after importing an archive. For large codeplugs, it is recommended to perform a scheduled wired retrieval or delivery prior to the first Over-The-Air operation to minimize transfer time.

2.22.2.2.2
Entering Radio Identity Information

Radios can also be entered one at a time into the RM Server.

This requires the system administrator to know all identification information of the radio including the serial number, Radio ID, CAI Network, OTAP Authentication Key ID, and OTAP Authentication Key value.

2.22.2.2.3
Radio Identity File Importing

If populating numerous radios at one time, a Radio Identity File may be used.

The Radio Identity File is a Comma Separated Value (CSV) file that contains a list of radios each containing the serial number, Radio ID, CAI Network, OTAP Authentication Key ID, and OTAP Authentication Key value. An example file can be found in the RM install directory.

2.22.2.2.4
Configuration Retrieval Operation

The RM allows scheduling of multiple radio configurations to be retrieved unattended. The RM starts the retrieval at the scheduled time and continues until all selected radios are either complete, errored, or canceled.

It is recommended that Over-The-Air operations are scheduled during times of low traffic in order to minimize the impact on system performance.

NOTE: After importing a radio into the RM Server, a scheduled Over-The-Air or wired retrieval operation is required. For large codeplugs, it is recommended to perform a scheduled wired retrieval or delivery prior to the first Over-The-Air operation to minimize transfer time.

The retrieval mechanism Over-The-Air supports RM data and voice to coexist, although system performance may be degraded slightly. The mechanism can also handle radios that enter and leave RF coverage. The retrieval operation utilizes presence to optimize the delivery.

2.22.2.2.5
Populating the RM Server

There are numerous methods to initially populate the RM Server. Most dealers can quickly determine which method aligns the best with their standard practices. The following steps are considered the most optimal RM Server population method:

Procedure:

1. Add a new radio with a serial number.
2. Schedule a wired read.
3. Assign the proper **Radio ID**, **CAI Network**, **Radio IP**, **OTAP Authentication Key**, and value.
4. Select the appropriate radio template.
5. Upgrade the template firmware if necessary.
6. Schedule a wired delivery.

Result:
After a successful wired delivery, the radio should be completely synchronized and ready for use on the system, and for its next Over-the-Air Programming. These steps should be followed for each radio.

If the RM Client, Server, and Device Programmer are all on the same computer, these steps can all be performed without disconnecting the radio from the computer. The RM Device Programmer should be configured via a wired connection during these steps. If the selected template has Enhanced privacy and/or Symmetric Keys (AES privacy) enabled, the key values must be populated for the delivery to be successful.

2.22.2.3

Modification of the Radio Configurations within the RM Server

Once populated in the RM Server, the radio configurations are modified using the classic CPS interface. A radio entry in the RM Server references a configuration. The referenced configuration, referred to as a template, can be unique to the specified radio, or can be a configuration referenced by numerous radios. Radio identity information is specific to the radio, while other parameters in the template are shared.

When a radio's configuration is updated, the status gets updated to "Codeplug Modified". This means that the configuration needs to be delivered to the radio Over-The-Air.

If the radio user is allowed to make changes via the radio front panel, it is important to understand that these updates are not retained after a delivery. The configuration in the RM Server overwrites what is in the radio when delivered. Similar to how wired CPS functions today, the system administrator must read radios Over-The-Air first, make individual updates to each, and then deliver the new configurations in order for the previous changes to be retained. If using a single configuration (a template) for numerous radios, there is no way to retain any individual changes the radio users may have made. All radios are updated to match what is in the template, with the exception of the radio identity information.

NOTE: Programming radios that are managed within the RM Server with an unmanaged wired CPS causes the radio to be out of sync with the RM Server. This causes the next Over-The-Air operation to take a longer time since the entire configuration must be retrieved or delivered.

It is important to take special care when changing parameters that may break communication between the radio and the Control Stations used by the RM Server. For example, accidentally changing the frequencies of the channel used for OTAP communication results in the RM no longer being able to communicate with that radio. The radio must be programmed via the wire in order to recover.

If changing parameters such as radio ID and OTAP authentication key ID and value Over-The-Air, the previous known values are used to deliver the new values. If these values become out of sync (possibly due to an unmanaged wired write of a radio), the Reset Identifiers feature should be utilized. Reset Identifiers allows the values used to communicate with the radio (in contrast to the new values) to be set within the RM Server. If these values are unknown, the radio must be programmed via the wire in order to recover.

2.22.2.4

Delivering the Modified Radio Configurations to the Radios

Once the updates have been made to the radio configurations within the RM Server, their status gets updated to "Codeplug Modified". This means that the configuration needs to be delivered to the radio Over-The-Air.

The RM allows scheduling of multiple radio configurations to be delivered Over-The-Air unattended. The RM starts the delivery at the scheduled time and continues until all selected radios are either complete, errored, or canceled. It is recommended that Over-The-Air operations are scheduled during low traffic in order to minimize the impact on the system performance. The delivery mechanism Over-The-Air allows for voice to coexist with the RM data, although system performance may be degraded slightly. The mechanism can also handle radios that enter and leave RF coverage. It utilizes presence to optimize the delivery.

The time it takes to deliver a configuration to a set of radios is dependent on the number of radios and the amount of changes to the configuration currently in the radio.

A pacing option is available to add additional delay to the delivery process. This is useful when delivery time is not important and it is desirable to minimize impact on the system performance. The pacing option is set to zero unless manually changed in the RM Device Programmer.

2.22.2.5
Delivered Radio Configurations Switchover

A delivery has an option to simply deliver the new configuration without applying it, or to apply it immediately after delivery. Applying the configuration is known as a “switchover”.

NOTE: When changing critical communication parameters, it is recommended that the new configuration is delivered to all the radios first, and then a separate switchover is delivered to the same set of radios.

This minimizes the downtime by applying all configurations at the same time. If making minor changes to the configuration, for example address book entries or button configurations, it is acceptable for each radio to apply the changes immediately as they are delivered.

Although the first radio may end up receiving the address book before the last radio, there would be little impact on the system operation. In contrast, if updating a critical communication parameter like transmit or receive frequency, the first radio is out of communication with the last radio until the last radio receives its programming.

2.22.2.5.1
Delay Option and Switchover Timer

A configuration switchover has the option for a max delay timer, also known as the switchover timer. The switchover timer is the maximum duration the radio waits after receiving the switchover message before performing the switchover.

NOTE: Because radio users have the option to accept or delay, it is not recommended to have a large switchover timer when changing critical communication parameters. Otherwise the first radio applies its changes well before the last and results in possible communication disruption.

If the switchover timer is set to zero, there is no prompt at the radio, and the switchover occurs immediately upon receiving the switchover message. If the value is greater than zero, the radio user receives a prompt to accept or delay the switchover.

If accept is selected, the radio immediately resets and applies the changes. If there is no selection or a delay is selected, the radio continues to operate on the old configuration until the switchover timer expires, at which time the radio resets and applies the changes.

If in an emergency or in a voice call when the switchover timer expires, the radio delays the switchover until the emergency is cleared or the voice call is over. If at any time while the switchover timer is running and the radio user cycles power, the configuration is applied on power up.

2.22.2.5.2
Presence Registration Suppression

If switching over many radios independent of the delivery and utilizing a zero value switchover timer, the radios may be reset within a short duration of each other.

This may result in radios sending their presence registration, also known as their automatic registration service (ARS) message, within a short duration of each other, which may result in channel blocking. There is an option available in the RM to enable or disable the radio from sending a presence registration immediately after a switchover.

If making changes to the radio configuration that does not affect the channel assignments, like address book entries or button layout, it is not necessary to re-register with the DDMS. Therefore presence registration can be suppressed after a switchover.

If making changes to the radio configuration that affects the channel assignments, like adding, changing or removing channels, it is necessary to re-register with the DDMS. Therefore presence registration should not be suppressed after a switchover.

If making changes to the presence server address, the presence should not be suppressed.

2.22.2.5.3
Access to the Last Modified Date and Time via the Radio Menu

The radio user can access the radio menu to see the date and time the configuration was modified.

This represents the date and time the codeplug package was compiled by the device programmer just prior to delivery.

2.23
Voice Operated Transmission

MOTOTRBO provides the ability for hands-free radio transmissions with selected radio accessories.

2.23.1
Voice Operated Transmission Operation

Voice Operated Transmission (VOX) monitors the accessory microphone for voice activity.

When voice is detected, the radio is keyed-up and the voice is transmitted. When voice is no longer detected at the accessory microphone, the radio is de-keyed.

2.23.2
Voice Operated Transmission Usage

There are several considerations that should be made when Voice Operated Transmission (VOX) is used. First, VOX is designed to key-up and transmit whenever voice is detected. This means that every time the operator speaks the radio will transmit. If the radio operator is in close proximity to another person, the radio may detect the other person's voice and begin transmitting. The successful use of VOX requires the radio operator to be aware of any possible audio sources that may inadvertently cause the radio to transmit at an undesirable time.

Second, the use position of the VOX accessory is an important factor in using VOX successfully. The radio operator should position the accessory so that it can pickup the operators voice with a minimal amount of ambient noise.

Additional consideration is needed as outlined in the following sections.

2.23.2.1
Suspending Voice Operated Transmission

In situation when Voice Operated Transmission (VOX) may not be desired, the radio operator can temporarily suspend VOX by pressing PTT. The radio will immediately suspend VOX and key-up the transmitter. Traditional (non-VOX) radio behavior will be used for any following transmissions. VOX operation will be resumed if the channel is changed (and changed back), the radio is power cycled, or the user re-enables VOX using the menu or a designated programmable button.

To disable VOX on a channel so that VOX behavior does not resume after a power-cycle or channel change, the menu or the designated programmable button must be used.

2.23.2.2
Talk Permit Tone

When VOX is used in conjunction with the Talk-Permit-Tone (TPT), some expected behaviors of the radio can be noticed.

When TPTs are disabled, the radio operator may begin speaking and the radio will immediately key-up and transmit the entire phrase uttered by the radio operator. However, when TPTs are enabled the radio operator must use a trigger word to key-up the radio. The trigger word will not, in most cases, be transmitted. After uttering the trigger word, the radio operator should wait until after the TPT is heard to begin speaking.

2.23.2.3
Emergency Calls

When a radio operator presses the Emergency Alarm button on a VOX-enabled channel, VOX is temporarily suspended so that the radio operator can handle the emergency situation.

VOX operation will automatically resume once the emergency has been cleared. If at any time during the emergency the radio operator presses PTT, VOX operation will not automatically resume after the emergency is cleared. Suspending Voice Operated Transmission on page 234 for instructions on how to resume VOX.

2.23.2.4
Transmit Interrupt

Because of the long delay involved with interrupting a voice transmission that translates to large amounts of audio truncation in a radio configured for VOX operation, VOX is not compatible with the Transmit Interrupt features (specifically, Voice Interrupt and Emergency Voice Interrupt).

Accordingly, for a radio that is provisioned to transmit interruptible voice, VOX is prevented from operating. Radios should not be provisioned with VOX and either Voice Interrupt or Emergency Voice Interrupt features on the same channel.

2.24
Lone Worker

The Lone Worker feature is available for both the portable and mobile radios, and in analog and digital modes.

For a radio user who is operating machinery, carrying out a security patrol or working in a plant alone, the Lone Worker feature provides a way to remotely monitor, if a user has stopped activity.

The Lone Worker feature is a predefined timer reset with user activity. For example, if the activity timer is set for 10 minutes and the user has no interaction with the radio during this time, the inactivity timer expires and a pre-warning tone sounds immediately after 10 minutes. If the user fails to reset the timer by an interaction with the radio (such as a button press, PTT, volume knob turn, and others), the radio initiates Emergency. For more information, see section Digital Emergency on page 95.

2.25
Bluetooth Support

The MOTOTRBO radio subscriber supports the Bluetooth Headset Profile (HSP), Bluetooth Personal Area Networking (PAN) profile for Bluetooth IP networking to a PC, and Serial Port Profile (SPP) for communication with Commercial Off-the-Shelf (COTS) Bluetooth Headset, Bluetooth Barcode Scanner, Motorola Solutions Bluetooth Headset with remote PTT, and Motorola Solutions Bluetooth PTT Only Device (POD).

The radio subscriber supports up to four simultaneous Bluetooth device connections, one of each type. The types include HSP, SPP, PAN and Fast PTT.

NOTE: The radio subscriber can connect to a Bluetooth headset, a Bluetooth scanner, a Bluetooth PAN PC and a Motorola Solutions Bluetooth POD simultaneously.

2.25.1
Bluetooth Pairing and Connection

Bluetooth operates within a range of 10 meters line-of-sight. This is an unobstructed path between the radio and the Bluetooth device. It is not recommended to leave the radio behind and expect the headset to work with a high degree of reliability when they are separated. At the fringe areas of reception, both voice and tone quality may start to sound “garbled” or “broken”. To correct this problem, simply position the radio and headset closer to each other to re-establish clear audio reception.

For pairing with multiple Bluetooth devices, it is recommended to pair with data devices such as the scanner and/or Motorola Solutions POD, before the headset. If the headset is paired first and activates the audio link, the audio link delays and/or interferes with subsequent pairings between the radio and additional Bluetooth devices. In some scenarios, pairing to additional devices may time out and fail due to audio link interferences, requiring attempts for reconnection. Hence pairing with data devices prior to the headset provides a better pairing experience.

In order to allow other Bluetooth devices such as the PC to discover and pair with the radio, place the radio in Bluetooth “Find Me” mode. The radio can enter this mode through the user menu in the display model, or via a programmable button on the non-display model.

2.25.1.1
Bluetooth Device Pairing with Display Radios

Pairing a device with a display radio is a user-initiated action. Basically, turn on the Bluetooth device and place it in pairing mode.

Use the “Find Devices” option under the Bluetooth menu to locate available devices. Some devices may require additional steps to complete the pairing. Refer to the respective devices’ user manuals. Upon successful pairing, the radio display and tone indicators will alert the user of an established connection.

NOTE: If the Bluetooth device requires pin authentication, the user will be prompted to enter the pin code via the keypad, to establish a connection.

2.25.1.2
Bluetooth Device Pairing with Non-Display Radios

Pairing a device with a non-display radio is also a user-initiated action.

Turn on the Bluetooth device and place it in pairing mode. Use the preprogrammed Bluetooth button on the radio to connect to the device. The LED blinks yellow and a tone sounds when a connection is being established. Upon successful pairing, a positive tone will alert the user of an established connection.

NOTE: If pin authentication is required for pairing, the pin codes should be preprogrammed into the non-display radios via CPS.

2.25.2
Bluetooth Headset, PTT and Radio Operation

2.25.2.1
Radio Operation with COTS Headsets

When the radio and the COTS headset are paired and connected via user selection through the display radio user interface, the radio sends ring indications to the headset to indicate the start of an incoming audio call setup.

The incoming call can be accepted by pressing the multi-function button on the headset; the audio link is set up between the radio and headset for communication. Once the Bluetooth audio link is connected, the Bluetooth microphone/speaker is used as the active audio path for voice communication. When the radio receives an incoming voice transmission, the incoming audio is routed to the Bluetooth headset speaker. When the radio PTT is pressed, the radio initiates an outgoing voice transmission with the headset microphone audio. The radio treats the headset microphone audio similar to the internal radio microphone audio for outgoing call transmissions.

For portable radios, the active Bluetooth audio path can be switched on/off from the radio user interface via menu, or programmable button. For mobile radios, the active Bluetooth audio path can be switched on/off via the on/off hook.

The audio path automatically switches from the Bluetooth headset to the radio when the headset disconnects either intentionally or accidentally, or when the headset battery is dead. Otherwise, the user can manually press the multi-function key of the COTS headset to switch to the radio audio path.

2.25.2.2
Radio Operation with Motorola Solutions Headsets with PTT

For Motorola Solutions Bluetooth headsets equipped with a remote PTT, the remote PTT can be used to initiate outgoing voice transmissions.

The audio path will be set up to the headset audio path after the connection to the headset/PTT is established.

2.25.2.3
Radio Operation with Motorola Solutions PTT Only Devices

Additionally, the radio supports the Motorola Solutions Bluetooth PTT Only Device (POD) for initiating voice communication.

This device can be connected and used independently with the radio, or could also be used in conjunction with a Bluetooth headset connected to the radio. The remote POD is used to initiate outgoing voice transmissions. The behavior of pressing the POD has an identical operation to pressing the radio PTT button – with respect to audio transmission and routing.

This device is not equipped with a local microphone or speaker; the Bluetooth headset or radio microphone/speaker will be used for audio communication.

2.25.3
Bluetooth Barcode Scanner Operation

When a radio and a Bluetooth Barcode Scanner are paired, the radio must initiate the SPP Bluetooth connection through user selection in the radio user interface. It is not recommended that the Bluetooth Barcode Scanner initiates the SPP Bluetooth connection to the radio. After the connection, the scanned

data sent from the scanner to the radio can be routed to the option board, or to a remote radio through the Over-The-Air interface.

The routing of the data to the option board or to the remote radio is configurable in CPS. Sending the data from the radio through the Over-The-Air interface to the remote radio is supported in digital mode only. The security support for Over-The-Air interface transmission is limited to the radio's Enhanced Privacy and/or AES support. The routing of data from the radio to the option board is supported in both analog and digital mode.

2.25.4
Bluetooth Personal Area Networking Operation

The radio supports the Bluetooth Personal Area Networking (PAN) as an access point.

The remote Bluetooth PAN device, for example a PC should be connected to the radio as a PAN client. After the radio and the remote Bluetooth PC client are paired and connected with the PAN profile, an IP network connection will be established for IP datagram communication. All data communication between the radio and Bluetooth PC client should be addressable with IP address and application port number over the Bluetooth PAN connection.

If a large amount of data needs to be communicated between the radio and the PC application, it is recommended to disconnect any Bluetooth headset and other Bluetooth devices from the radio. The PAN connection data communication can slow down greatly if any devices of other Bluetooth profiles are connected.

2.25.5
Recommended Bluetooth Devices

For the latest update on supported Bluetooth accessories, please refer to MOTOTRBO Professional Tier Accessory Catalog.

The following are key considerations when selecting a COTS device:

- A Bluetooth device that has been certified from Bluetooth SIG.
- A Bluetooth device with enhanced audio processing.
- A headset that supports disconnecting/reconnecting the active audio link to the radio by pressing/releasing the multi-function button. This maximizes headset battery life.

2.25.6
Avoiding Accidental Connection

The Bluetooth headset is usually assigned to one person. However, the two-way radio may not be assigned to a person; it could be shared by different people such as retail sales associates, housekeeping, security and others. If a Bluetooth headset was paired with a radio, the headset automatically reconnects to the same radio the next time it powers on.

Scenario: If the same radio has been assigned to a different user, the headset can accidentally reconnect to the wrong radio belonging to a different user. Automatically, the previous user still receives a positive pairing indication from the headset.

To avoid accidental connection as described in the above mentioned scenario, follow the instructions below:

- On MOTOTRBO radio, erase previous Bluetooth headset/PTT/POD information via Bluetooth device list menu. (applies for display model radio).
- On Motorola Solutions Headset/PTT and POD: Erase all pairing information from the device by pressing and holding the PTT button followed by turning on the headset. When this procedure is performed, the headset or POD does not initiate connection to any radio automatically.

2.26
One Touch Home Revert Button

This feature is available for mobile radios in both analog and digital modes.

The customer can program a button as the “Home Revert” button via the CPS. This button allows the user to jump to a pre-assigned “Home” channel. The CPS does not allow a customer to select a channel in the "Channel Pool" to be the Home Revert Channel.

NOTE: The “Channel Pool” is a zone for keeping all the trunked and Data Revert Channels.

2.27
Password and Lock Feature

MOTOTRBO provides a password-based locking mechanism (Radio Authentication) to protect radios from unauthorized users.

This feature can be enabled and the password can be changed both via the CPS or the radio menu.

With this feature enabled, a radio prompts the user to enter a four-digit password on powering up. After three incorrect password attempts, the radio enters a locked state for 15 minutes. No calls (including Emergency Calls) can be placed or received, when a portable radio is in locked state. Upon correct password entry, the radio enters normal operation mode.

The password input method varies according to the radio display models. For example:

- On a non-keypad portable, a user inputs the password via a combination of the Channel Switch and Side Button(s).
- On a non-keypad mobile, a user inputs the password via a combination of the Channel Knob and Front Button 2.
- On a keypad mobile, a user inputs the password either with the Accessory Keypad or via a combination of the Channel Rocker button and the <OK_Button>.

If a Foot Switch is configured to initiate an emergency and the radio is powered up using the Foot Switch, the radio skips the password input procedure. Upon completion of an emergency, the radio then initiates the password authentication if this feature is enabled.

If a user presses the test mode series button when the radio is locked or in password input state, the radio skips the password authentication and enters test mode.

2.28
Digital Telephone Patch

System	Description
IPSC IP Site Connect	IP Site Connect supports Digital Telephone Patch
CPSS	Capacity Plus Single Site supports Digital Telephone Patch

System	Description
Capacity Plus Single Site	
CPMS	Capacity Plus Multi Site supports Digital Telephone Patch
Capacity Plus Multi Site	

The MOTOTRBO Digital Telephone Patch is a Motorola Solutions proprietary feature introduced in software version R01.08.00 supporting two types of phone patch calls:

Individual Phone Patch Call
This allows a half-duplex voice communication between a radio user and a phone user. This communication can be initiated from either party.

Talkgroup Phone Patch Call
This allows a half-duplex voice communication between a phone user and a group of radio users. This type of communication can be initiated only by the phone user.

This feature is supported in Single Site, IPSC LACs, IPSC WACs, and Capacity Plus Single Site configurations. This feature is supported in display and non-display radios. However, for non-display models, phone numbers, over dial or access/de-access codes need to be configured manually to the programmable buttons because the radios do not have a keypad.

The DTP feature utilizes Commercial Off-the-Shelf (COTS) Analog Phone Patch (APP) boxes, and is compatible with any DTMF-based APP box that supports the 4-wire interface and can communicate in half-duplex mode. The Zetron 30 (Worldpatch) and PL 1877A (MRTI2000) are two examples. Most APP boxes in the market support the following telephony services:

- Access and De-access Codes
  - The access code is used to wake up the APP box, and prevent the radio user or phone user from making unauthorized phone patch calls.
  - The de-access code is used to terminate the phone patch call if an access code is required when setting up the call.
  - Different access code/de-access codes may be configured to have different privileges, so the codes can be used to block/allow radio from performing a call type.
- Phone Usage Time-Out Timer (TOT) – The APP box ends the call once the timer expires.
- A go-ahead tone is emitted to the phone user when the radio user de-keys. This provides an indication to the phone user to begin talking.
- Direct connection to the PBX or PSTN line
- Type Approvals for Supported Countries

Instead of recreating such services in the radio system, this feature relies on the APP box to provide these services. The APP Box is connected to the MOTOTRBO repeater via the 4-wire interface. The phone patch feature utilizes APP boxes that are connected to the repeater, hence this feature is only available in repeater mode, but not direct mode.

2.28.1
Phone Call Initiation

It can be configured via CPS to allow a radio to initiate or receive phone calls on per digital personality basis.

Only phone-enabled radios can initiate and receive a phone call.

2.28.1.1
Call Initiation by a Radio User

When a radio user initiates a phone call, the channel access is always polite (even if configured as impolite), regardless of the radio's programmed admit criteria. This is analogous to sending CSBK or data signaling, which is sent politely.

When a radio enters a phone call, a phone call text string and icon shows up on the display screen to alert the radio user.

Buffer dial is supported for access/de-access code, phone number, and over dial digits. "Buffer Dial" means that the radio user enters the digits from the radio keypad, then presses the "OK" button to send out the digits as in-band audio. The phone number can be 22 digits long or shorter. Before calling a phone user, the radio user switches to the channel that is capable of a phone patch call, and uses one of the following dialing methods:

- Manual Dial – Enter the phone number from the radio keypad manually. This option can be enabled or disabled on the radio via CPS.
- Phone Address Book – Select a phone number from the radio's Phone Address Book.
- One Touch Button – Push a programmable button of the radio. The one touch button is associated with a phone number from the Phone Address Book.

If an access code is required for phone calls, it could be configured in the radio or entered by the radio user manually. When the access code is not configured in the radio, the radio user is prompted to manually enter the access code after dialing the phone number. If access code is not required, the radio user can skip this step by not keying anything. After the radio user sends out the phone number and access code, the phone rings and the user can answer the call.

If there is an Interactive Voice Response (IVR) device at the phone user's end and over dial is required, the radio user can enter the over dial digits via the radio keypad or a programmable button.

NOTE: The IVR device at a bank may prompt the user to enter the account number to access account information.

2.28.1.2
Call Initiation by a Phone User

When a phone user initiates the call, the phone user dials the phone number of the APP box, or the PBX box, if a PBX is used. The PBX then connects the call to the APP box.

If access code is required, the phone user enters the access code following the audible prompt from the APP box. After the APP box validates the access code, the box connects the call to the repeater. The repeater sounds a tone and prompts the phone user for the target ID. Then, the phone user enters the Target ID to reach the radio user/group.

NOTE: If a Go-Ahead tone is configured in the APP box, the phone user hears the tone for the Target ID, followed by the Go-Ahead tone.

The length of the Target ID is configurable via CPS, and the format varies according to different system configurations.

System	Description
IPSC IP Site Connect	The Target ID includes the call type, channel slot number, and the radio/talkgroup identifier.

System	Description
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	The Target ID only includes the call type and the radio/talkgroup identifier; the channel slot number is not required.

When keying in the Target ID, the phone user may try up to three times maximum, after which the system terminates the call automatically if no valid Target ID is received. After the repeater validates the Target ID, if the channel is busy, the repeater sounds a busy-waiting tone to the phone user and waits for the channel to become idle, before resuming the call setup. While waiting for the channel to become idle, the phone user hears the busy-waiting tone, and can choose to wait or end the call. If the channel does not become idle for a configurable period of time, the repeater ends the call setup. In this scenario, the phone user stops hearing the busy-waiting tone and hangs up the call. If the channel is idle or becomes idle before the timer expires, the repeater alerts the called radio user/group by ringing tones.

A radio user can join a phone call from a phone user while scanning for activities on the phone channel.

System	Description
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	Scanning is NOT supported in Capacity Plus Single Site and Capacity Plus Multi Site

For individual phone calls, the target radio user answers by pushing the PTT before the call can be set up completely. For talkgroup phone calls, it is configurable in the repeater via CPS to allow a target radio user to answer the call by pushing the PTT before the call can be set up completely. When answering is not required, the phone user can talk immediately after the first ring. When answering is required, the phone user is not permitted to talk until one of the target radio users answers the call by pushing the PTT. Otherwise, the phone user is not heard by the radio users. When answering is required but the call is unanswered during the configured response period, the repeater sends a de-access code to the APP box, and the call ends automatically.

Phone All Call, an exclusive phone talkgroup call, is supported in the DTP feature as well. The phone user can follow the same phone talkgroup call setup procedure to set up the phone call by using the All Call ID or 0s as the Target ID. In a Phone All Call, the phone user can start to talk after the first ring, before any radio user answers the call. During a Phone All Call, not all radio users are able to respond to the phone user. Only radio users with radios configured with All Call announcement capability are able to respond to the landline phone user and heard by all the other radio users. These users are able to end the Phone All Call by sending the de-access code. Hence, when a phone user makes a Phone All Call, it is recommended to provide contact information so that the receiving radio users have means to contact the phone user if needed. Phone All Call can be enabled/disabled in the repeater via CPS.

Pre-Configured Target ID: For any system configuration (Conventional Single Site, IPSC, Capacity Plus Single Site and Capacity Plus Multi Site), a default Target ID may be preconfigured in the phone gateway repeater. This is an optional configuration and can be enabled/disabled via CPS. When enabled, if the phone user does not enter the first digit of the Target ID within 3 seconds (3-second rule) after hearing the Target ID prompt tone, the preconfigured Target ID will be used for the phone call automatically and the system will start to ring the target user or user group. If the Target ID entered by the phone user is invalid and a re-try is needed, the same 3-second rule will be applied in each retry. The preconfigured Target ID can be an individual radio user, or a user group, or an All Call.

2.28.2

Access Priority During Phone Calls

During a phone patch call, the radio user in the phone call has higher channel access priority than the phone user, allowing the radio user to key up and talk impolitely over a phone user regardless of the radio's in-call permit criteria configuration.

However, if a phone user needs to talk, the phone user has to wait until the radio user dekeys. Otherwise, the phone user will not be heard by the radio users.

When another radio user is talking in a phone talkgroup call, the radio user follows the radio's In Call Criteria configuration with the exception of using the Follow Admit Criteria when the In Call Criteria is provisioned with Transmit Interrupt.

NOTE: This is because Transmit Interrupt is not supported in the phone call.

When detecting an impolite takeover from a radio that is not partied to the phone call or an emergency on the phone patch channel during a phone call, the repeater automatically ends the phone call by sending a de-access code to the APP box.

During a phone call, if a radio drops out of the call due to various reasons (for example; out-of-range), the radio can make a late entry back into the call if it is a talkgroup call. If it is an Private Call, the radio can make a late entry back to the call in Conventional Single Site or IPSC. However, late entry is not supported in a Capacity Plus Single Site system configuration if a radio fades out of an Private Call completely.

There are three switches that happen during a call:

Radio-to-Phone switch
The radio user finishes talking and dekeys, then the phone user starts to talk.

Phone-to-Radio switch
The phone user talks while a radio user keys up and starts to talk.

Radio-to-Radio switch
The radio user finishes talking and dekeys, while another radio user keys up immediately and starts talking. This switch only takes place in talkgroup calls only.

To ensure a smooth switch and avoid voice truncation, the Enhanced Channel Access feature is introduced to minimize the switching impact and to achieve the best overall user experience in all system configurations. As a result, only minimum additional Voice Access Time is introduced for the switches. The performance parameters are summarized in the following table.

Table 45: Summarized Performance Parameters

Additional Voice Access Time (ms)	Single Site			IP Site Connect			Capacity Plus Single Site		
	Min	Mean	Max	Min	Mean	Max	Min	Mean	Max
Radio-to-Radio / Phone	60	210	360	60	210	360	60	210	360

NOTE: All time figures increases to existing Voice Access Time

A phone call is clear regardless of whether privacy/Enhanced Privacy/AES is enabled in the radio or not. Transmit Interrupt is also automatically disabled for the phone call.

When a radio is in a phone call, there are visual ergonomic indications to show that the radio is currently in a phone call. A text string and icon appearing on the radio display indicates that it is currently in a phone call.

2.28.3
Ending Phone Calls

A phone patch call can be ended by either the radio user, phone user, or the APP box, with the following methods:

- The radio user may push the back button, or a programmable exit button to end/reject the call. Alternatively, the de-access code can be sent manually from the keypad.
- The phone user ends the call simply by hanging up, or by sending the de-access code from the keypad. Sending the de-access code is recommended, because this method allows the radio system to end the call immediately, thus letting the radio users know that the call is ended in the correct manner. However, if the phone user ends the call by hanging up, this depends on when the APP box responds to the PSTN disconnecting signaling. Some APP boxes may not be able to detect PSTN signals and therefore waits for the TOT to expire. Hence, ending the call in this manner normally takes a longer time.
- Additionally, if a phone TOT is configured in the APP box, the call is ended by the APP box automatically when the call duration exceeds the timer. Some APP boxes provide configurable 30-second warning/alert tones before the timer expires.

When the phone call ends, the text string and icon on the radio screen disappear. This is followed by a “phone exit” tone from the radio, to alert the user that the radio has been disconnected from a phone call.

The phone patch feature works similarly in all MOTOTRBO system configurations, except some minor differences in specific system configurations. The following subsections describe the minor differences in each particular system configuration.

2.28.4
Digital Telephone Patch System Configuration

2.28.4.1
Phone Patch in Single Site and IP Site Connect Local Area Channels

In Single Site, the system can support only one phone call per repeater because a repeater can only be connected to one APP box.

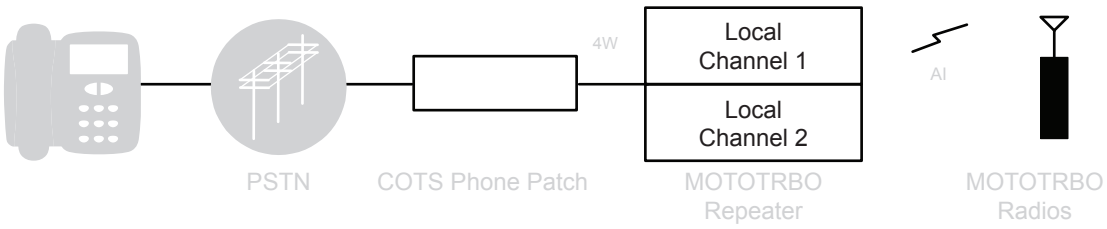
The phone call utilizes either channel of the repeater one at a time, and the selection of the channel, is the choice of the party initiating the phone call. This could be the radio user or the phone user. The other unused channel can be used for other voice or data services. Legacy or third-party radios are not able to join in the phone call because this is a new Motorola Solutions proprietary feature.

The phone patch call on an IPSC Local Area Channels (LAC) works similarly as the phone patch call in a Single Site channel. The Target ID includes the call type (Talkgroup “8” or Individual “7”), the channel (slot 1 or 2), and the radio or talkgroup identifier.

The phone user is instructed to dial the phone number associated with the Phone Patch box, and then prompted to provide the Target ID to reach a radio user. The phone user dials extension 710020 after the beep, which initializes an Private Call on channel 1 to radio 20. To contact an entire talkgroup, the phone user dials extension 820100, which initializes a talkgroup call on slot 2 to talkgroup 100.

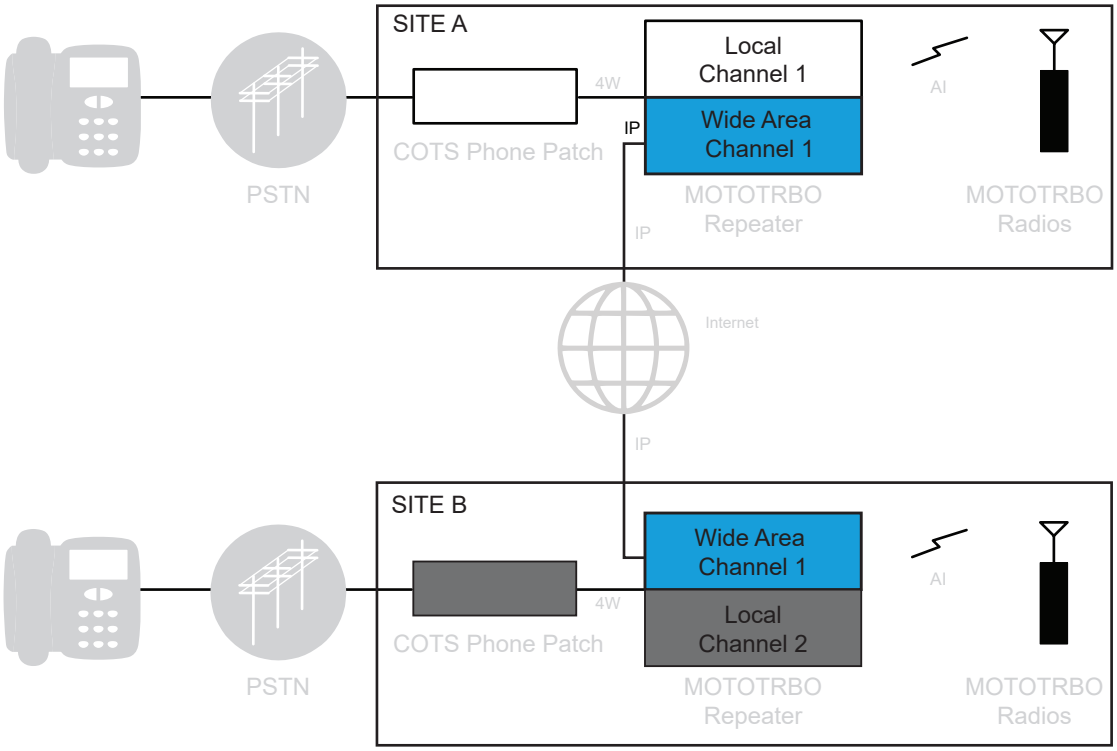
The following figure describes the typical phone patch topologies in Single Site configuration.

Figure 65: Phone Patch Topology in Single Site Configuration



The following figure describes the typical phone patch topologies in IPSC LACs

Figure 66: Phone Patch Topology in IP Site Connect Local Area Channel Configuration



2.28.4.2
Phone Patch in IP Site Connect Wide Area Channels

IPSC

In IP Site Connect (IPSC), Wide Area Channels (WAC) include channels from multiple repeaters.

However, since a WAC can host only one call at a time, it is designed that a WAC can support only one APP box that can be connected to any repeater on the WAC. The phone patch call can be initiated from any site, but it always goes through the only APP box supported on the WAC.

NOTE: The Target ID includes the call type, the channel, and the radio or talkgroup identifier.

Legacy or third-party radios are not able to join in the phone call because this is a new Motorola Solutions proprietary feature.

The following figures describe the typical phone patch topologies in IPSC.

Figure 67: One APP Box Supporting Two Wide Area Channels in IP Site Connect

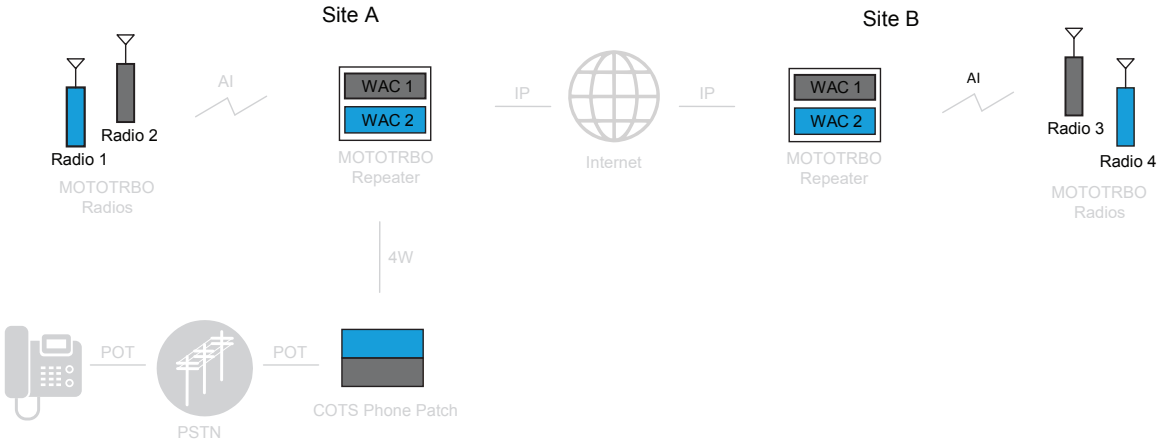


Figure 68: Two APP Boxes Supporting Two Wide Area Channels in IP Site Connect

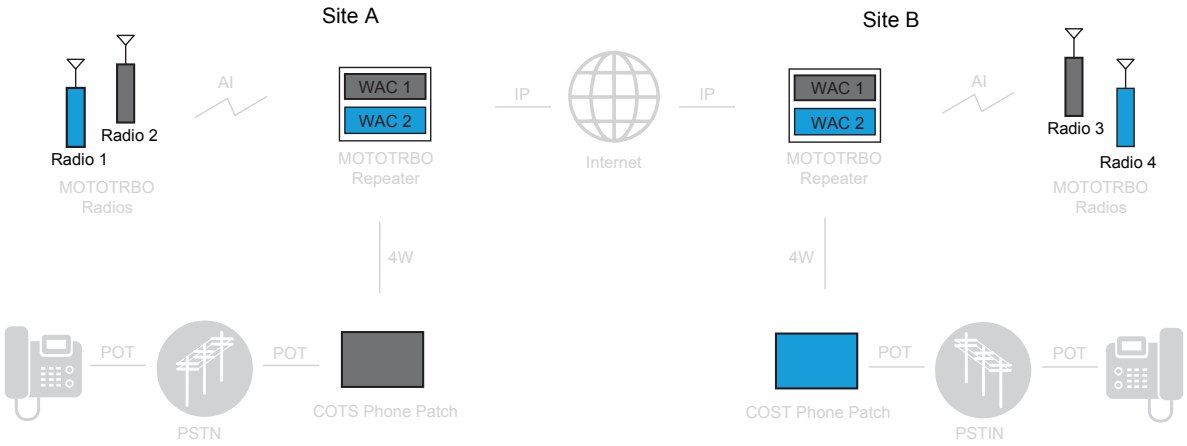
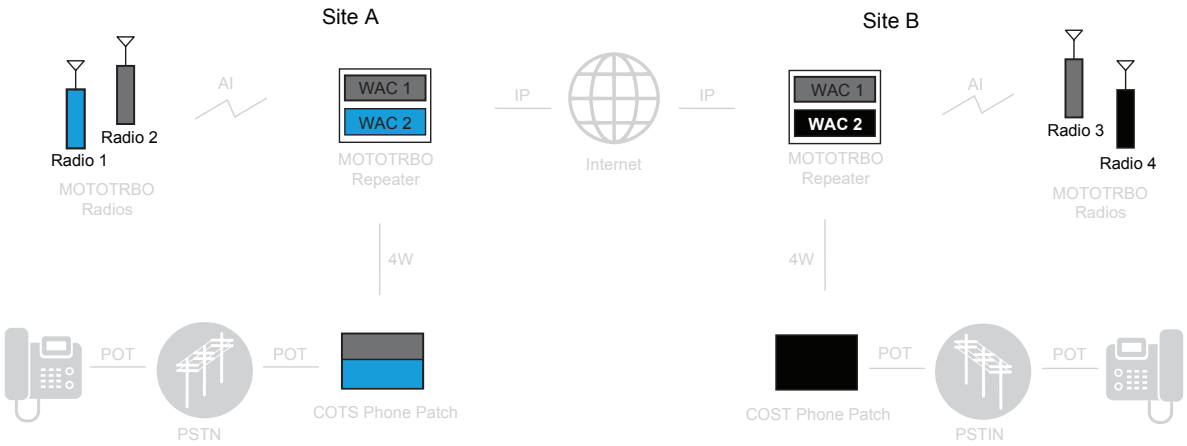


Figure 69: APP Boxes Supporting Wide Area Channels and Local Area Channels in IP Site Connect



2.28.4.3
Phone Patch in Capacity Plus Single Site

CPSS

In Capacity Plus Single Site, because a repeater can only be connected to one APP box, the system can support one phone call per repeater.

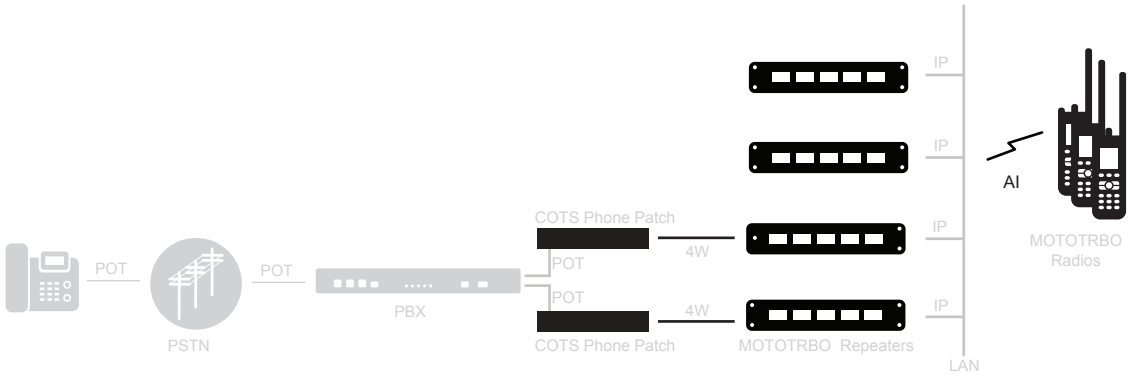
The phone call only uses one channel; the other channel can be used for other voice or data services. Any voice repeater can be used for phone calls, hence the maximum number of APP boxes that can be supported in a Capacity Plus Single Site system is equal to the number of voice repeaters in the system.

The Target ID includes the call type, and the radio or talkgroup identifier. The channel ID is not required because the system automatically selects the channel for the phone call. When the radio user initiates a phone call, if the rest channel is idle and phone capable for this radio, the phone call starts on the rest channel. If the rest channel is not phone capable for the radio, the phone call starts on an idle channel that is phone capable.

When a phone user calls a radio user/group, the user dials the telephone number of the APP box. The phone call can start on either idle channel of the repeater that the APP box is connected to. Then the following rule is in order - If a channel is the rest channel, the phone call starts on this channel; if neither channel is the rest channel, channel 1 has a higher priority than channel 2. Legacy or third-party radios are not able to join in the phone call because this is a new Motorola Solutions proprietary feature.

The following figure describes the typical phone patch topology in Capacity Plus Single Site.

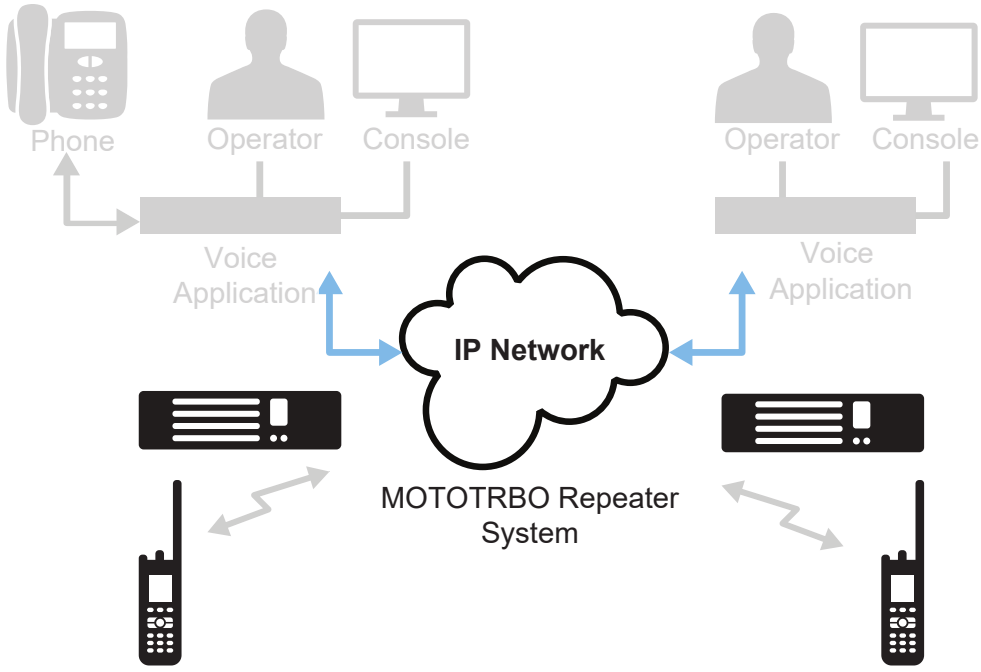
Figure 70: Phone Patch Topology in a Capacity Plus Single Site Configuration



2.28.5
Wireline Telephony

A wireline telephony solution is available in all MOTOTRBO system configurations (Conventional Single Site, IPSC, Capacity Plus Single Site and Capacity Plus Multi Site) through Network Application Interface (for voice), and also supported by third-party telephony applications. The wireline telephony is illustrated in Figure 71: Wireline Telephony with Third-party Telephony Application on page 248.

Figure 71: Wireline Telephony with Third-party Telephony Application



The wireline telephony solution provides the same set of functionalities and similar user experience as the DTP solution that uses the APP box. The only difference is that the wire line solution does not use the APP box, instead, it uses a third-party telephony application.

2.29
Voice Announcement Feature

MOTOTRBO 2.0 radio products support the voice announcement feature suite to audibly convey information to the radio user.

An example of when this feature is helpful is when the MOTOTRBO radio display or indicators are not easily accessible (for example, located under protective clothing) or when radio operator cannot be distracted from their task to look at the display or indicators.

The voice announcement feature is supported in both analog and digital operation. The voice announcement feature includes a standard feature set and a premium feature set. The standard feature set and premium feature set are mutually exclusive (only one may be enabled). The voice announcement priority configuration determines whether radio traffic and alert tones may interrupt a voice announcement. The MOTOTRBO radio operator can enable or disable the voice announcement feature as appropriate for their work environment.

The standard feature set uses pre-recorded voice announcement files that are loaded into the MOTOTRBO radio. A selection of professionally recorded voice announcement files is included with the MOTOTRBO Customer Programming Software (CPS). In addition, users may record their own voice announcement files[1] and load them into the MOTOTRBO radio. For example, to create a meaningful channel announcement (for example, Maintenance Channel instead of Channel 4) or when the available voice announcement files do not match the language or dialect of the end users.

NOTE: [1] The MOTOTRBO CPS software supports importing WAV files with the following audio formats:

- 16 Bits, 8K, mono sample, pulse-code modulation (PCM) audio
- 8 Bits, 8K, mono sample, Mu-law encoding.

The premium feature set generates the voice announcement using a speech synthesis algorithm in the MOTOTRBO radio. The MOTOTRBO CPS supports configuration of a custom dictionary to ensure accurate readout of abbreviations and industry specific terminology. The MOTOTRBO CPS loads the selected voice file [2] into the MOTOTRBO radio. The premium feature set supports read out of received text messages and job tickets. The radio management integration is seamless because the audio is generated in the MOTOTRBO radio. The following table shows the comparison between the Standard and Premium Voice Announcement Features.

NOTE: [2] A voice file consists of a language (for example, English), regional dialect (for example, American), and gender (for example, male) that describe the generated voice.

Table 46: Standard and Premium Voice Announcement Feature

Feature Name	Standard Feature Set	Premium Feature Set
Channel Alias Announcement	Yes (128 Channels Maximum)	Yes (Unlimited)
Zone Alias Announcement	Yes (20 Zones Maximum)	Yes (Unlimited)
Configurable Voice Announcement Priority	Yes	Yes
Programmable Button Feature Announcement	Yes	Yes
Programmable Button Feature State	Yes	Yes
Multiple Language Support	Yes	Yes
Text Message Readout Support	No	Yes
Job Ticket Readout Support	No	Yes
Voice Announcement Updates via Radio Management OTAP	No	Yes

2.30 Wi-Fi Support

Wi-Fi® support, 802.11 b/g/n (2.4 GHz), for MOTOTRBO is a premium feature that is available on selected devices.

Wi-Fi client operation, that is, the MOTOTRBO device connecting to a Wi-Fi access point, is supported. MOTOTRBO devices do not currently support ad-hoc operation or access point operation (the MOTOTRBO device performing as an access point for other devices).

2.30.1 Wi-Fi Network Name

The Service Set Identifier (SSID) or network name, needs to match the SSID configured in the access point.

The SSID is case sensitive and supports internationalization per the IEEE 802.11-2012 standard.

NOTE: Hidden networks do not broadcast their SSID over Wi-Fi. Hidden networks are supported, but not recommended, because it increases the connection time and doesn't increase security since the SSID is still available through other means.

2.30.2
Wi-Fi Security Support

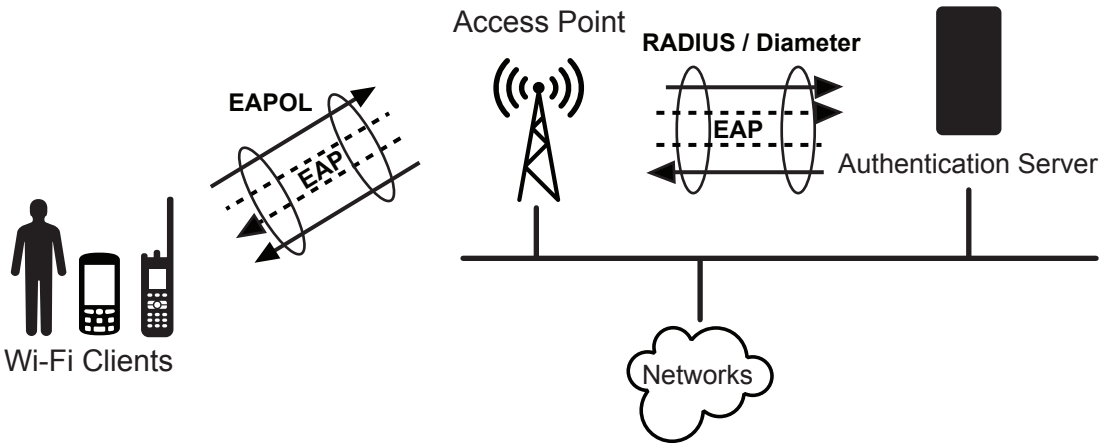
The security setting should match the type of authentication and encryption used by your Wi-Fi router. The security setting controls the access to the wireless network and the level of privacy between the MOTOTRBO device and the access point. WPA2 with AES encryption provides the strongest security offered by the Wi-Fi product and is recommended.

The following security modes are supported:

- “None” provides no authentication or encryption. This security mode is supported but not recommended.
- “WEP” is insecure and obsolete. This security mode is supported but not recommended.
- "WPA/WPA2 Personal" is supported with both AES and TKIP encryption.
- “WPA/WPA2 Enterprise” is supported with both AES and TKIP encryption.
  - Support EAP TLS
  - Support PEAP with Phase 2 authentication as TLS and MSCHAPV2
  - Support EAP TTLS with Phase 2 authentication as PAP, CHAP, MSCHAP, and MSCHAPV2

NOTE:
WPS is not supported due to security flaws discovered in the protocol.

If validation of the server certificate is required, the certificate of the subscriber and the certificate of the authentication server must be issued by the same Certificate Authority (CA).



2.30.3
Wi-Fi Default Profile

MOTOTRBO devices that support Wi-Fi without an additional premium feature purchase include the following default network.

This supports an “out of box” configuration of the MOTOTRBO device via Wi-Fi without requiring an initial programming of the Wi-Fi network parameters using a programming cable. It is recommended to remove this network once the initial provisioning is completed.

Table 47: Wi-Fi Default Profile

SSID	Security Type	Network Passphrase
MOTOTRBO	WPA/WPA2 Personal (AES)	Radio Management

2.30.4
Wi-Fi Channel Usage

The MOTOTRBO device supports the configuration of the regulatory region to meet the regulatory requirements for frequency usage and power level for the Wi-Fi feature.

The MOTOTRBO device also supports configuration of the 802.11d protocol. If support for 802.11d protocol is enabled but no 802.11d broadcast is received, the MOTOTRBO device will use the regulatory region specified in the MOTOTRBO device configuration.

NOTE: As of January 1, 2015, the U.S. Federal Communications Commission (FCC) banned the use of 802.11d within the U.S.

2.30.5
Wi-Fi Network Settings

The MOTOTRBO device supports Dynamic Host Configuration Protocol (DHCP) to obtain the network settings from the Wi-Fi access point.

The MOTOTRBO device also supports static IP address assignment. The use of DHCP is recommended in most cases because the IP network configuration typically varies across different wireless networks.

2.30.6
Wi-Fi Network Protocols

The MOTOTRBO device supports configuration of Domain Name System Service Discovery (DNS-SD) protocol using Multicast Domain Name System (mDNS).

The MOTOTRBO device requires this feature to be enabled to support some features on Wi-Fi and this information is detailed in the Wi-Fi feature description. This protocol uses User Datagram Protocol (UDP) port 5353.

NOTE: The use of Domain Name System Service Discovery (DNS-SD) protocol using Multicast Domain Name System (mDNS) is also configurable for the Bluetooth and USB network connections.

The average network bandwidth requirement, per device, is less than 50 bytes/second.

2.30.7
Wi-Fi Features

The following features can be supported over the Wi-Fi interface on MOTOTRBO devices.

2.30.7.1
Radio Management in Wi-Fi

The MOTOTRBO radio management application supports all device configuration operations via the Wi-Fi interface.

The following are the supported operations:

- Configuration of Device Settings

- Update of Device Firmware
- Activation of Premium Features
- Updates of Device Resources (that is, Language Packs and Voice Packs)

NOTE: Please refer to the MOTOTRBO radio management application release notes to determine the release that supports some or all the following functionalities

The MOTOTRBO radio management device programmer component must be present on the same local area network (LAN) as the MOTOTRBO device. This is required because the MOTOTRBO radio management device programmer identifies MOTOTRBO devices using the DNS-SD protocol. The deployment of a virtual local area network (VLAN) is beyond the scope of this system planner but does provide additional deployment options when physically deploying a MOTOTRBO radio management device programmer on the same LAN is not feasible.

2.31 Enterprise Wi-Fi Roaming Enhancement

The Enterprise Wi-Fi Roaming Enhancement feature allows the radio to roam between Access Points (AP) without the necessity to perform full authentication.

The subscriber performs full authentication only on the first connection. At that moment, the Pairwise Master Key (PMK) is cached. The PMK is used for all the subsequent authentications, whenever the radio roams to another AP.

Enabling the feature provides faster roaming that reduces audio holes in the transmission. Additionally, subscribers are less prone to authentication failures in case of any dropped frames during the full authentication process.

The feature is available for the following Wi-Fi supporting radio models:

- DP 4000e series
- DM 4000e series
- DP 3000e series
- SL 4000e series
- SL 2600

2.31.1 Configuring Enterprise Wi-Fi Roaming Enhancement in RM

Perform the following steps in Radio Management (RM) to enable Enterprise Wi-Fi Roaming Enhancement on your subscriber.

Procedure:

1. In Radio View, right-click the subscriber on which you want to enable the feature, and select **Edit Configuration**.
2. From the **Set Categories** navigation tree, select **General** → **Wi-Fi Network**.
3. To enable the feature, in the **Network Profile Table** select the **Opportunistic Key Caching** check box.

   NOTE: The feature operates only when **Security Type** is set to `WPA/WPA2 Enterprise`.
4. At the top of the tab, click **Save**.

5. Return to Radio View.

Postrequisites: Schedule a Write job for the subscribers with the configuration that uses the edited set.

2.32 Certificate Management

Certificate management provides a solution for managing certificates in the MOTORBO system.

2.32.1 Certificate Management Feature Overview

The MOTOTRBO device supports Certificate Management through the Simple Certificate Enrollment Protocol (SCEP).

The following certificate management operations are supported:

- Supports RSA based X.509 V3 certificate.
- Supports downloading Certificate Authority (CA) certificate.
- Supports client certificate enrollment and auto-renewal.
- Uses Challenge Password to authenticate the radio as the valid SCEP client.
- Uses MD5 Fingerprint to validate the CA certificate.
- Supports RSA key size as 1024, 2048 and 4096 bits.
- Supports Signature Hash Algorithm as MD5, SHA-1, SHA-256, SHA-384 and SHA-512.

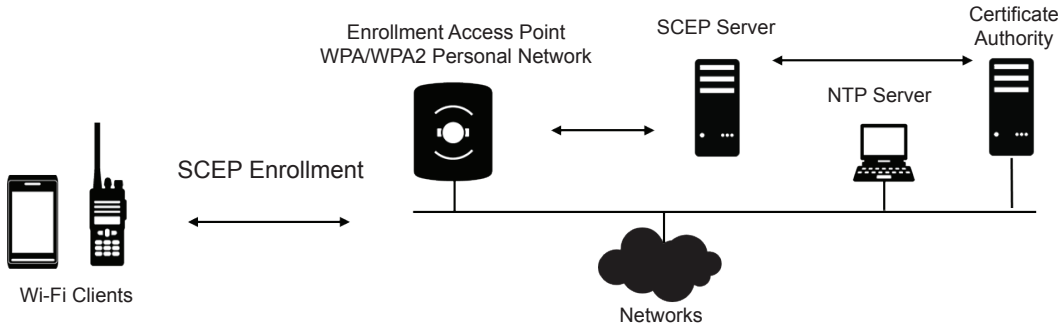
NOTE: Certificates are used for Wi-Fi Enterprise.

2.32.2 Certificate Enrollment

The certificate enrollment process consists of the following parts:

1. Network Administrator receives a challenge password from the Simple Certificate Enrollment Protocol (SCEP) server.
2. Network Administrator passes the challenge password and other enrollment data to a Fleet Manager.
3. Fleet Manager loads the challenge password and other enrollment data to radio through RM and associates it with the Enterprise SSID.
4. Fleet Manager programs an enrollment access point and SCEP server location into the radio.
5. The radio initiates enrollment through enrollment access point (WPA/WPA2 Personal).

Figure 72: Certificate Enrollment



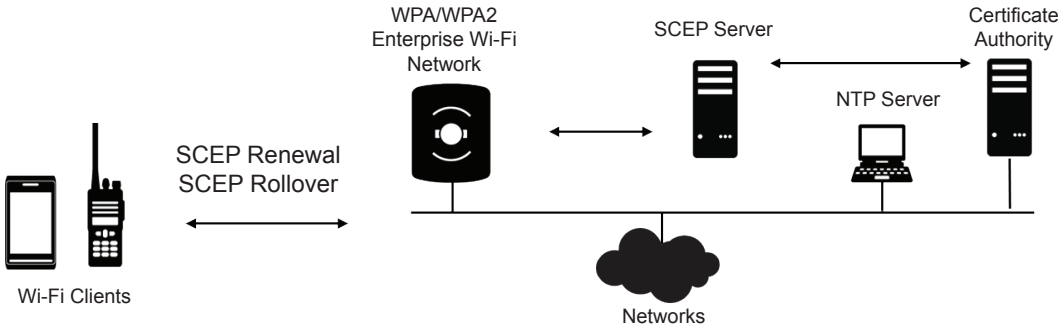
2.32.3

Certificate Renewal and Rollover

The radio initiates the renewal process based on a configurable timer called the Renewal Period. The Renewal Period shows the period that triggers a renewal. For example, the value of 30 days means that the radio triggers the certificate renewal 30 days before the certificate expires.

The radio must be on a network with access to Network Time Protocol (NTP) and Simple Certificate Enrollment Protocol (SCEP) to renew the certificate. Rollover or Certificate Authority (CA) Renewal is also supported.

Figure 73: Certificate Renewal and Rollover



2.32.4

Design Considerations

When designing your certificate management system, you must follow these general guidelines.

- The certificate enrollment, renewal, and rollover processes take one to five minutes to complete each. The duration of these processes depend on the key size and network conditions.
- Configure the renewal period of the Certificate Authority (CA) certificate longer than that of the client certificate, so that the renewed CA certificate is available for the client certificate renewal.
- You can leverage the key usage extension for the following two purposes:
  - To single out the Registration Authority (RA) certificate. The key usage of the RA certificate must contain at least a `digitalSignature` and must not contain `keyCertSign & cRLSign`.
  - To single out the encryption certificate. If a separate certificate is deployed at the Public Key Infrastructure (PKI) to decrypt the Simple Certificate Enrollment Protocol (SCEP) data from the radio,

the key usage of the certificate must contain `keyEncipherment` only. Certificate Enrollment Protocol (CEP) encryption certificate by Microsoft Network Device Enrollment Service (NDES) is an example.

- Ensure that the subscriber has good coverage in the Wi-Fi network so that the PKI can be accessed during the renewal and rollover period. You must re-enroll the certificate if the renewal or rollover process cannot be completed before the certificate expires.

2.33 Radio Transmit Inhibit

Radio Transmit Inhibit behaves similar to “Airplane Mode” on a cellular phone.

Once the radio user turns the radio into the Radio Transmit Inhibit mode, the radio will continue to receive LMR (Land Mobile Radio) voice/data/CSBK calls, but will neither respond to received transmissions nor initiate any transmissions. The radio user can turn the radio into or out of this mode via programmable button, radio menu or GPIO.

NOTE: This Radio Transmit Inhibit only applies to the LMR calls, but not to Bluetooth operations. Bluetooth operations can be enabled or disabled separately on the radio via CPS, radio menu or programmable button.

2.34 Radio Response Inhibit

Radio Response Inhibit is an extension from the Radio Transmit Inhibit feature. This feature may be used when the radio user wants to minimize the risk of being located (for example, via GPS) or remote monitored etc.

When the radio user activates Radio Response Inhibit mode, the radio continues to allow only user initiated transmissions, which include all types of Voice Call, CSBK calls, and data calls (for example, text message, job ticket and telemetry). All other transmissions (including all ACKs, ARS, GPS, and the like, including third-party requested transmissions, that are not initiated by user action) are blocked.

The radio user can activate or deactivate this mode via programmable button or GPIO.

This feature only applies to Land Mobile Radio (LMR) related calls, not to Bluetooth or Wi-Fi operations, which can be enabled or disabled separately.

This feature is applicable in the following digital system configurations including:

- Direct Mode
- Dual Capacity Direct Mode
- Extended Range Direct Mode
- Conventional Single Site and IPSC
- Capacity Plus

2.35 Analog Features

For customers that are migrating from Analog systems to Digital systems, MOTOTRBO supports both analog and digital modes of operation.

MOTOTRBO mobile and portable radios support both analog and digital modes (the user can select which mode to use, and change modes dynamically), while MOTOTRBO repeaters are configured to operate in digital mode or in analog mode. When in Analog mode, MOTOTRBO utilizes traditional FM technology, supports both 12.5and 25 kHz channel spacing, and can operate in repeater and direct modes.

2.35.1
Analog Voice Features

The following traditional Analog features are supported by the MOTOTRBO system:

Table 48: MOTOTRBO Analog Voice Features

Feature Name	Description
Time-Out Timer	Sets the amount of time that the radio can continuously transmit before the transmission is automatically terminated.
Squelch	Special electronic circuitry added to the receiver of a radio which reduces or squelches, unwanted signals before they are heard through the speaker.
Monitor/Permanent Monitor	The user can check channel activity by pressing the Monitor button. If the channel is clear, the user hears static. If the channel is in use, the user hears the conversation. It also serves as a way to check the volume level of the radio, as while pressing the monitor button, the user can adjust the volume according to the volume of the static/conversation heard.
Talkaround	This feature allows a user to talk directly to another unit for easy local unit-to-unit communications and bypass the repeater.
12.5/20/25 kHz Configurable Bandwidth	Channels on the radio can be programmed through the CPS to operate at either 12.5 kHz or 20/25 kHz.
PL/DPL	Transmitted when the receiving radio is to only receive calls from radios with specific PL/DPL codes, this creates communications groups while operating in Conventional Dispatch mode. PL/DPL allows for more privacy on a frequency. PL/DPL is transmitted as a sub-audible frequency or a digital code.
Channel Access Control	This feature dictates what conditions a radio is allowed to initiate a transmission on a channel. There are three possible values which are Always, Channel Free, and Correct PL. Refer to MOTOTRBO Channel Access on page 83 for more details.

2.35.2
MDC Analog Signaling Features

MOTOTRBO contains a limited set of built-in MDC signaling features.

Table 49: MOTOTRBO MDC Analog Signaling Features

Feature Name	Description
Emergency Signaling	Sends a help signal to a pre-defined person or group of people. The emergency feature also allows a user to sound an alarm or alert the dispatcher in an emergency situation. The user is also able to acknowledge an emergency.
PTT-ID	PTT-ID identifies the user's outgoing calls on other users' radios.
Call Alert	Call Alert notifies the radio user of incoming calls if they are a short distance away from their radio. Call Alert also informs unavailable users that someone is trying to reach them.

2.35.3
Quik-Call II Signaling Features

The Quik-Call II signaling is used during analog mode of operation and encodes either single tone or a sequence of two tones within the audible frequency range (approximately 300 – 3000Hz). Encoding/Decoding is particularly used for the Call Alert and Voice Selective Call features.

Table 50: Quik-Call II Signaling Features

Feature Name	Description
Voice Selective Call	This feature allows announcement type messages to take place during a call to an individual or group of radios. This feature is used in systems whereby the majority of transmissions are between a dispatcher and a single radio. Voice Selective Call can be used to eliminate the need to listen to traffic that is irrelevant to the users. There are two distinct types of voice selective call – basic voice selective call and automatic voice selective call.
Call Alert	Call Alert notifies the radio user of incoming calls. This feature also informs the radio users when another radio user is trying to reach them. No voice communication is involved in this feature.
Call Alert with Voice	This feature is a combination of the Call Alert and Voice Selective Call features. Call Alert with Voice allows a receiving radio to receive voice messages and call alert signals. This feature is useful when a dispatcher needs to transmit a voice message and leave a Call Alert to the targeted radio.

2.35.4
Analog Scan Features

Table 51: Analog Scan Features

Feature Name	Description
Nuisance Channel Delete	A channel with unwanted activity is called a Nuisance Channel. The user can remove a Nuisance Channel from the Scan List temporarily by using the Nuisance Channel Delete feature.
Priority/Dual Priority Scan	Priority Scan allows a user to program the radio to scan more frequently transmissions on the most important channel, and ensure they do not miss critical calls. Dual Priority Scan allows a user to program a radio to frequently scan transmissions on the two most important channels, and ensure they do not miss critical calls.
Tone Private Line Lockout	During scan, if activity is detected on a channel, but does not match the un-muting condition, lockout occurs. Once lockout occurs, the radio ignores activity on that channel for the next nine scan cycles. However, if scan finds that activity has ceased on that channel, the counter is reset and is no longer ignored.
Talkback Scan with Home Channel Revert	Talkback scan allows activity on different communications channels to be monitored and answered. Home channel revert allows a user to automatically access a preferred channel.

2.35.5

Analog Repeater Interface

To facilitate the migration from analog to digital, the MOTOTRBO repeater offers an analog repeater interface that allows the repeater to operate with legacy analog accessories.

The interface is configurable via the CPS and can support the following applications:

- Tone panels
- Phone Patches
- Console Desksets connected via a local interface
- Console Dispatcher in base station configuration
- Trunking controllers such as LTR, PassPort and MPT1327

2.35.5.1

Analog Repeater Interface Settings

The analog repeater interface is configurable via the CPS. The CPS offers repeater-wide settings as well as programmable input and output pins on the rear accessory connector.

2.35.5.1.1

CPS Repeater Wide Settings

Table 52: CPS Repeater Wide Settings

CPS Repeater Control Name	Description
Audio Type	“Filtered Squelch” configures the repeater so that only the audible frequency spectrum (300 Hz – 3 kHz) is sent to the rear receive audio pin/speakers as well as transmitted Over-The-Air. The user in deskset controller applications is interested in this audible frequency spectrum. “Flat Unsquelch” should be used in applications such as trunking controllers or community repeaters where there is sub-audible signaling that needs to be passed. In this configuration, the repeater will pass the audio unfiltered Over-The-Air as well as to the rear receive audio pin and speakers. The filtering is performed in the external device, not in the repeater.
Analog Accessory Emphasis	Pre-emphasis is configurable on transmitting subscribers. In order to match the emphasis settings on the wireline, de-emphasis on the receive path and pre-emphasis on the transmit path of the analog repeater interface can be enabled or disabled. This setting is in addition to the repeater’s Emphasis setting. Furthermore, when Audio Type is set to “Flat Unsquelch”, there is no emphasis in the audio.
Audio Priority **NOTE:** This feature only applies to certain radio model. MTR3000	This setting determines if “External PTT” or “Repeat Path” has priority over the transmitter when Disable Repeat Path is disabled. A priority of None implies the transmitter will be granted on a first come first served basis. *This feature is not supported for digital transmissions in Dynamic Mixed Mode; priority is on a first come, first served basis.

CPS Repeater Control Name	Description
Tx Audio Priority **NOTE:** This feature only applies to certain radio model. (SLR 5000 and SLR 8000)	It allows the user to configure the preempt priority for OTA transmitting between Tx audio and all other transmission requests. Available values are 0 and 1 for SLR 5000; and 0, 1, 2, and 3 for SLR 8000. The higher value means the higher the priority. If both audios have the same priority, the OTA transmission will be granted on a first come first served basis. *This feature is not supported for digital transmissions in Dynamic Mixed Mode.
Repeat Audio Priority **NOTE:** This feature only applies to certain radio model. (SLR 5000 and SLR 8000)	It allows the user to configure the preempt priority of OTA transmitting between repeat audio and all other transmission requests. Available values are 0 and 1 for SLR 5000; and 0, 1, 2, and 3 for SLR 8000. The higher value means the higher the priority. If both audios have the same priority, the OTA transmission will be granted on a first come first served basis. *This feature is not supported for digital transmissions in Dynamic Mixed Mode.
Wireline Tx1 Audio Priority **NOTE:** This feature only applies to certain radio model. (SLR 8000)	It allows the user to configure the preempt priority for OTA transmitting between Wireline Tx1 audio and all other transmission requests. Available values are 0,1, 2 and 3. The higher value means the higher the priority. If both audios have the same priority, the OTA transmission will be granted on a first come first served basis. *This feature is not supported for digital transmissions in Dynamic Mixed Mode.
FP Tx Audio Priority **NOTE:** This feature only applies to certain radio model. (SLR 8000)	It allows the user to configure the preempt priority for OTA transmitting between Front Panel microphone audio and all other transmission requests. Available values are 0, 1, 2 and 3. The higher value means the higher the priority. If both audios have the same priority, the OTA transmission will be granted on a first come first served basis. *This feature is not supported for digital transmissions in Dynamic Mixed Mode.
Disable Repeat Path	Some applications do not want the repeater to perform in-cabinet repeat; they warrant that the external PTT be the only input that can trigger the repeater to transmit. This setting configures the repeater to only transmit when the PTT is asserted. *This feature is not supported for digital transmissions in Dynamic Mixed Mode; digital transmissions from the radio are repeated regardless of Disable Repeat Path configuration.

2.35.5.1.2
Rear Accessory Port CPS Programmable Pins

The rear accessory also has some pins that can be programmed to specific input/output functions. These pins can be programmed to either active high or low.

Table 53: Rear Accessory Port CPS Programmable Pins

CPS Programmable Pins	Description
PTT	PTT can be programmed to any programmable pin on the rear accessory connector.

CPS Programmable Pins	Description
	In Dynamic Mixed Mode, if channel is busy when PTT is asserted on the repeater accessory port, then an audible channel busy alert tone is generated on speaker and Rx audio accessory pins.
RSSI Output (SLR 8000)	The RSSI Output can only be programmed to GPIO#7 on the rear accessory connector.
CSQ Detect	Squelch detect will toggle this output pin on. Loss of squelch will toggle this output pin off. In Dynamic Mixed Mode, this pin is asserted ON, on the repeater accessory port when: • Squelch is detected • The repeater is transmitting digital call (includes call transmission, call hang and channel hang time) • The repeater is transmitting exclusive CWID This pin is asserted OFF, on the repeater accessory port when all of the above mentioned conditions are false.
PL Detect	A signal meeting the PL rules programmed in the channel toggles this output pin to its active state. Loss of the PL signal toggles the output pin to its inactive state. In Dynamic Mixed Mode, this pin is asserted ON, on the repeater accessory port when: • PL detected • The repeater is transmitting digital call (includes call transmission, call hang and channel hang time) • The repeater is transmitting exclusive CWID This pin is asserted OFF on the repeater accessory port when all of the above mentioned conditions are false.
Monitor	Asserting this input pin reverts the receiver to carrier squelch operation. Upon detection of RF signal, the repeater enables the Rx Audio lines and unmutes the speaker. In a Dynamic Mixed Mode repeater, the user is able to listen to the analog channel activity. However, for digital channel activity, the repeater will emit audible channel busy alert tone on speaker and Rx audio accessory pins, but it will not unmute to the actual digital channel activity.
Repeater Knockdown	Asserting this input pin triggers the repeater to temporarily enter Repeat Path Disable Mode. In this mode, the repeater's transmitter will only be enabled by the external PTT and the audio source will be the Tx Audio Input pin. Releasing this input pin will revert the repeater back to Normal Mode where the repeaters transmitter can be activated by a qualified RF signal on the receive frequency. In Dynamic Mixed Mode, this feature is not supported during an ongoing digital transmission.
Antenna Relay	This output pin is used to drive an antenna relay switch for applications where the repeater acts as a dispatch station that will only re-

CPS Programmable Pins	Description
	ceive or transmit at a time. This allows the use of a single antenna without the need of expensive combining equipment. The pin toggles active when the repeater enters a transmit state, and reverts to inactive when the repeater drops back to idle/receive. This feature is not supported in Digital and Dynamic Mixed modes.

2.35.5.1.3

Rear Accessory Port Fixed Audio Pins

The following table provides a description of the fixed audio pins on the rear accessory connector for the DR 3000 which can be used in Digital Telephone Patch or Analog modes only.

Table 54: Rear Accessory Port Fixed Audio Pins for DR 3000

Fixed Pins	Description
Speaker+/Speaker-	Act as a differential pair and should be connected at opposite ends of an audio speaker or equivalent load. Under rated conditions, the output voltage will be 7.75V RMS and the radio supports impedances down to 4 ohms with distortion typically less than 3%. Under no conditions should either of these two outputs be connected to ground.
Rx Audio	Provides a line level audio output at 330 mVrms under rated conditions. The frequency response of this output has been extended below 300 Hz to support data transfer for specific applications (Flat Unsquelch).
Tx Audio	Accepts transmit audio at 80 mVrms through a 560 Ω load. Care must be taken when choosing an audio source as the output impedance of the source can affect the audio level which may need to be adjusted accordingly.

The following table provides a description of the fixed audio pins on the rear panel ports for the MTR 3000 which can be used in Digital Telephone Patch or Analog modes only.

Table 55: Rear Panel Port Fixed Audio Pins for MTR 3000

Fixed Pins	Description
Rx Audio	An RF input signal with 60% RSD provides an Rx Audio output of 330 mVrms into 50 kΩ. Also a microphone input of 56 mVrms provides an Rx Audio output of 330 mVrms into 50 kΩ. The Rx Audio output has DC bias of 2.5 VDC.
Aux Rx Audio	An RF input signal with 60% RSD provides an Aux Rx Audio output of 330 mVrms into 50 kΩ. The Aux Rx Audio output has a DC bias of 2.5 VDC.
Tx Audio	The Tx Audio input provides no pre-emphasis. The nominal level of 80 mVrms (226 mVpp) produces 60% Relative Standard Deviation (RSD).
Tx Audio with Pre-Emphasis	The Tx Audio-Pre input provides a pre-emphasis network. The nominal level of 80 mVrms (226 mVpp) produces 60% RSD.
Tx Data	Transmit data, PL or DPL signaling. The nominal level of 80 mVrms (226 mVpp) produces 12% RSD.

The following table provides a description of the fixed audio pins on the rear panel DB25 ports for the SLR 5000 and SLR 8000, which can be used in Digital Telephone Patch or Analog modes only.

Table 56: Rear Panel DB25 Port Fixed Audio Pins for SLR 5000 and SLR 8000

Fixed Pins	Description
Rx Audio	An RF input signal level of -77dBm with a 1KHz tone at 60% RSD provides an Rx Audio output of 330 mVrms into 50 kΩ. The Rx Audio output has DC bias of 2.5 VDC.
Discriminator Audio	An RF input signal level of -77dBm with a 1KHz tone at 60% RSD provides an Rx Audio output of 330 mVrms into 50 kΩ. The Rx Audio output has DC bias of 2.5 VDC. Discriminator Audio is only available when the MPT 1327 box is checked and it is always flat.
Tx Audio	The nominal level of 80 mVrms (226 mVpp) produces 60% RSD with a 1KHz tone.
Tx Data	Transmit data, PL or DPL signaling. The nominal level of 80 mVrms (226 mVpp) produces 12% RSD.

2.35.5.1.4

Front Panel Audio Ports on the MTR3000

Front Panel Audio Ports on the MTR3000

The following table provides a description of the front panel ports for the MTR3000.

Front Panel Ports	Description
Speaker	Output to Powered Voice speaker. Adjustable between 0 to 500 mVrms [1.4 Vpp] across 2.4 kΩ @ 60% system deviation. Audio signal appears between Pins 3 and 4 on the connector. Must use speaker type HSN1000 (older model) or HSN1006 via adapter cable Part.No. 0185180U01. **NOTE:** The Speaker port is only supported in analog mode regardless of the speaker used.
Microphone	Local microphone Input. Use microphone type GMN6147 (older model) or GMMN4063. Modulation sensitivity for 60% system deviation is typically 56 mVrms (158 mVpp). **NOTE:** The Mic port is only supported in analog mode regardless of the Mic used. For older model of microphone (GMN6147), the 3 control buttons for speaker volume control, Rx monitor and Intercom control functions are not supported.

2.35.5.1.5

Front Panel Audio Ports on the SLR 8000

The following table provides a description of the front panel ports for the SLR 8000.

Table 57: Front Panel Audio Ports on the SLR 8000

Front Panel Ports	Description
Speaker	The front panel assembly contains an integrated speaker which is controlled via the two front panel speaker volume adjust buttons. The "Volume Increase Button" raises the volume level of the integrated front panel speaker, while the "Volume Decrease/Mute Button" lowers the volume level, with the lowest volume level muting the speaker altogether.
Microphone	Local microphone Input. Use microphone type GMMN4063. Modulation sensitivity for 60% system deviation is typically 56 mVrms (158 mVpp).

NOTE: Operation of the Front Panel Speaker and Microphone in digital modes of operation requires an optionally purchased software license. The optional software license allows Front Panel Speaker Audio support in all digital system types, with the Front Panel Microphone Audio support limited to single site digital conventional operations (that is, non-IP Site Connect conventional).

2.35.5.2
Configuration Summary Table

The following table gives a high level view of which features of the analog repeater interface are needed to support specific types of accessories. This table is meant to act only as a guideline.

Table 58: Configuration Summary Table

Acc Type	Trunking	Phone Patch	Tone Panel	Local Desk-set	Console Base Station
RX Audio	Y	Y	Y	Y	Y
Discriminator Audio (SLR 5000/SLR 8000)	Y	N	N	N	N
TX Audio (MTR3000)	N	Y	N	Y	Y
TX Audio (DR 3000)	Y	Y	Y	Y	Y
TX Audio with Pre-Emphasis (MTR3000)	Y	N	Y	N	N
Tx Audio (SLR 5000 / SLR8000)	Y	Y	Y	Y	Y
TX Data (MTR3000 / SLR 5000 / SLR 8000)	Y	N	Y	N	N
Ext PTT	Y	Y	Y	Y	Y

Acc Type	Trunking	Phone Patch	Tone Panel	Local Desk-set	Console Base Station
Disable Re-peat Path	Y	N	Y	N	Y
Repeater Knockdown	NA	Y	NA	Y	NA
Monitor	N	Y	N	Y	Y
PL Detect	N	O	O	O	O
CSQ Detect	O	O	O	O	O
Audio Type	FLAT	FILTERED	FLAT	FILTERED	FILTERED
Analog Acces-sory Emphasis	NA	O	NA	O	O
Antenna Relay	NA	NA	NA	O	O

Y = This feature is necessary for the application
N = This feature is not necessary for the application

O = This is an optional parameter for the application

NA = Not Applicable

2.35.5.3
Configuration Considerations

2.35.5.3.1
Analog Trunking Controllers and Community Repeaters

Most analog trunking controllers and community repeaters will have two outputs that are to be modulated by the repeater: voice audio, signaling data.

NOTE: The MOTOTRBO DR 3000 repeater only accepts one audio input. Thus the two outputs must first be mixed into a single input and dropped down to the audio level the MOTOTRBO repeater expects on the microphone port.

The microphone port is designed to transmit audio at 80mV RMS (220 mVp-p) through a 560 ohm load. Care must be taken when choosing an audio source as the output impedance of the source can affect the audio level which may need to be adjusted accordingly.

When mixing the audio and signaling, care must also be taken to determine the expected deviation of the signaling. For example, in LTR controllers, the expected deviation of the LTR data is ~800Hz. Please refer to your controller's user manual which gives guidance on how to tune the data signal output to achieve adequate data deviation.

Similar to existing cables, resistors can be placed on the cable to drop the level coming out from the controller (on the order of 1-2 Vp-p) to the level expected by the transmit audio pin. Once the resistor value is determined, the audio and signaling signals can be mixed into a single wire that can be crimped onto the MOTOTRBO accessory connector (Motorola Solutions Part Number PMLN5072_).

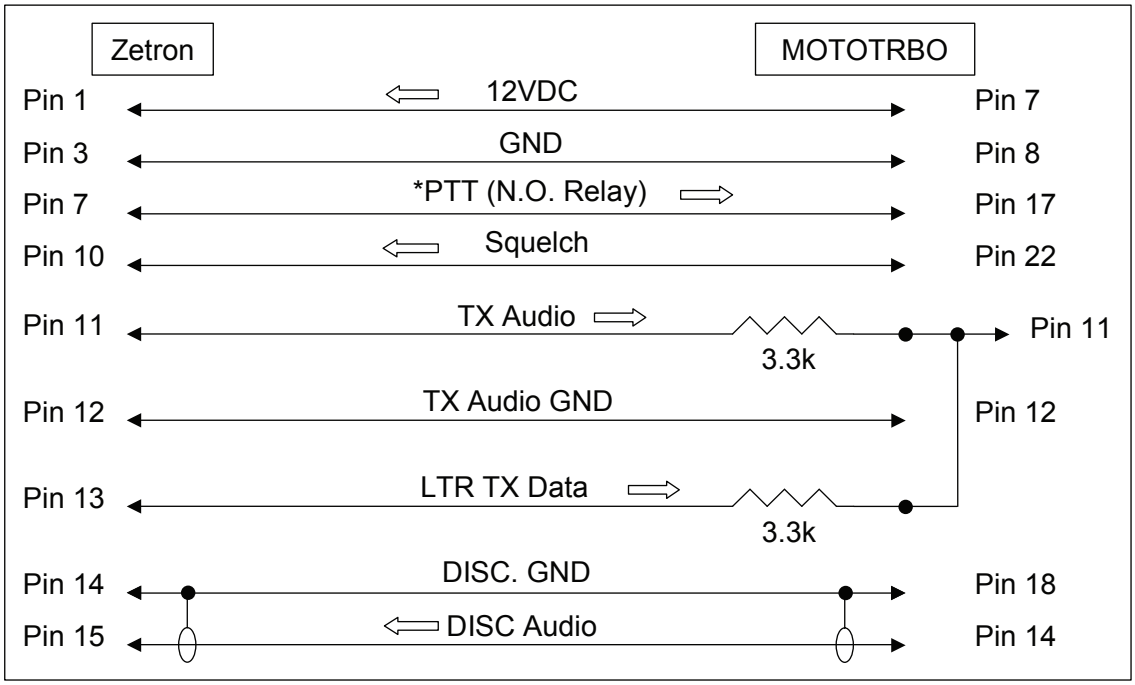
NOTE: The MTR3000/SLR 5000/SLR8000 repeater has an audio transmit input and a data transmit input that can be used with the two outputs on the analog trunking controllers and community repeater panels (tone panel).

2.35.5.3.2

Zetron Controllers

The following are the Zetron configurations needed that will enable Zetron controllers to interface with the MOTOTRBO repeater.

Figure 74: DR 3000 Cable Schematic for Zetron Controllers



Schematic Notes:

- On the Zetron connector, pin 6 is PTT Common, this must be jumpered to one of the grounds. This is the common pin of the PTT relay. Without this, the unit will not key-up.
- Use a shielded cable for Discriminator Audio.
- The two 3.3k ohm resistors need to be mounted at the MOTOTRBO end of the cable.
- Large arrows indicate signal/function flow.
- Please note that Pin 17 (PTT) and Pin 22 (Squelch/CSQ Detect) need to be provisioned in the CPS.

NOTE: To set up the MTR3000 with Zetron controllers, see the *MTR3000 Repeater Basic Service Manual (68007024096) - Appendix D* for more information.

NOTE: The pin configuration at SLR 5000/SLR 8000 DB 25 connector is backwards compatible to MTR3000. The cable manufactured for MTR3000 can be used for SLR 5000/SLR 8000. On the controller side, the jumper settings for MTR3000 can also be applied to SLR 5000/SLR 8000.

The following table lists the jumper/switch settings for trunking/tone panel controllers.

Table 59: Zetron Model 42 Trunking Controller Jumper Settings

Zetron Model 42 Trunking Controller Jumper Settings
JP1 set to ‘B’ (Flat)
JP2 set to ‘A’ (Tone Flat)
JP3 set to ‘A’ (Sub Out High)

Zetron Model 42 Trunking Controller Jumper Settings
JP4 set to ‘A’ (+20dB Receive Audio Gain)
JP6 set to ‘A’ (TX Audio Level High)
JP7 set to ‘Ext Sq +’ (pins 5-7 and 6-8 jumpered)

NOTE: If you have an older Zetron controller that will be used in a 12.5 kHz system for the first time, make sure it has first been modified for 12.5 kHz operation. See Zetron’s supplemental publication: 011-0509 for instructions on making this modification.

Table 60: Zetron Model 42 Trunking Controller Jumper Settings

Zetron Model 49 Trunking Controller Jumper Settings
JP1 set to ‘A’ (Flat Audio)
JP2 set to ‘A’ (Tone Flat)
JP7 set to ‘A’ (COR as input)
JP9 set to ‘A’ (+20dB Receive Audio Gain)
JP10 set to ‘A’ (TX Audio Level High)
JP12 set to ‘Ext Sq +’ (pins 5-7 and 6-8 jumpered)
JP13 set to ‘B’ (HP Filter IN)
JP23 set to ‘A’ (Sub In from Disc: pins 1-2 and 3-4 jumpered (grounds pin 4 on rear connector))
JP24 set to ‘A’ (Sub Out DC coupling)
JP25 set to ‘A’ (Sub Out High)
JP26 set to ‘A’ (Sub Out analog)

NOTE:
Pin 4 of the rear connector is listed as a ground. But it will not be grounded unless JP23 is set for it. This pin also acts as an input for the receive LTR data path.

The jumpers do not follow standard positioning. Some may be vertical, some may have position ‘A’ on the left, some may have position ‘B’ on the left. Take extra care when making these settings. If you have an older Zetron controller that will be used in a 12.5 kHz system for the first time, make sure it has first been modified for 12.5 kHz operation. See Zetron’s supplemental publication: 011-0509 for instructions on making this modification. For transmit audio alignment, the Zetron Model 49 manual calls for setting the Tone Generator at TP4 for 1.4Vp-p/495mv RMS, then adjusting the TX audio for 2 kHz deviation (40% of full system deviation). This is for a 25 kHz BW system. For 12.5 kHz BW, this adjustment is 1 kHz deviation.

Table 61: Zetron Model 38 Tone Panel Switch Settings

Zetron Model 38 Tone Panel Switch Settings
SW2 set to off (up) Audio Output Gain (high)
SW3 set to off (up) PL/DPL output Gain (high)
SW4 set to off (up) Flat/De-emphasis (Flat)
SW6 set to off (up) Internal/External Squelch (External)

Zetron Model 38 Tone Panel Switch Settings
SW7 set to on (Down) COR Positive/Negative (Negative)

NOTE: Tone Panel Programming Note - It may be necessary to set the generated DPL (DCS) signal to “Invert” from the tone panel to be recognized by the user radios. These DTMF commands are 3750 for normal and 3751 for inverted signal generation.

Once the above cable and jumper/switch settings have been achieved, you should now be able to refer to the specific controller product manual to complete installation.

2.35.5.3.3
Trident Controllers

Trident MicroSystems manufactures a cable that interfaces Trident Controllers with MOTOTRBO repeaters and provides jumper settings for Trident Controllers.

NOTE: The pin configuration at SLR 5000/SLR 8000 DB 25 connector is backwards compatible to MTR3000. The Trident cable manufactured for MTR3000 can be used for SLR 5000/SLR 8000. On the Trident controller side, the jumper settings for MTR3000 can also be applied to SLR 5000/SLR 8000.

2.35.5.3.4
Zetron M827/M807 Controllers

In addition to the Zetron controllers mentioned in the previous section, SLR 5000/SLR 8000 supports Zetron M827/M807 for the MPT 1327 analog trunking application.

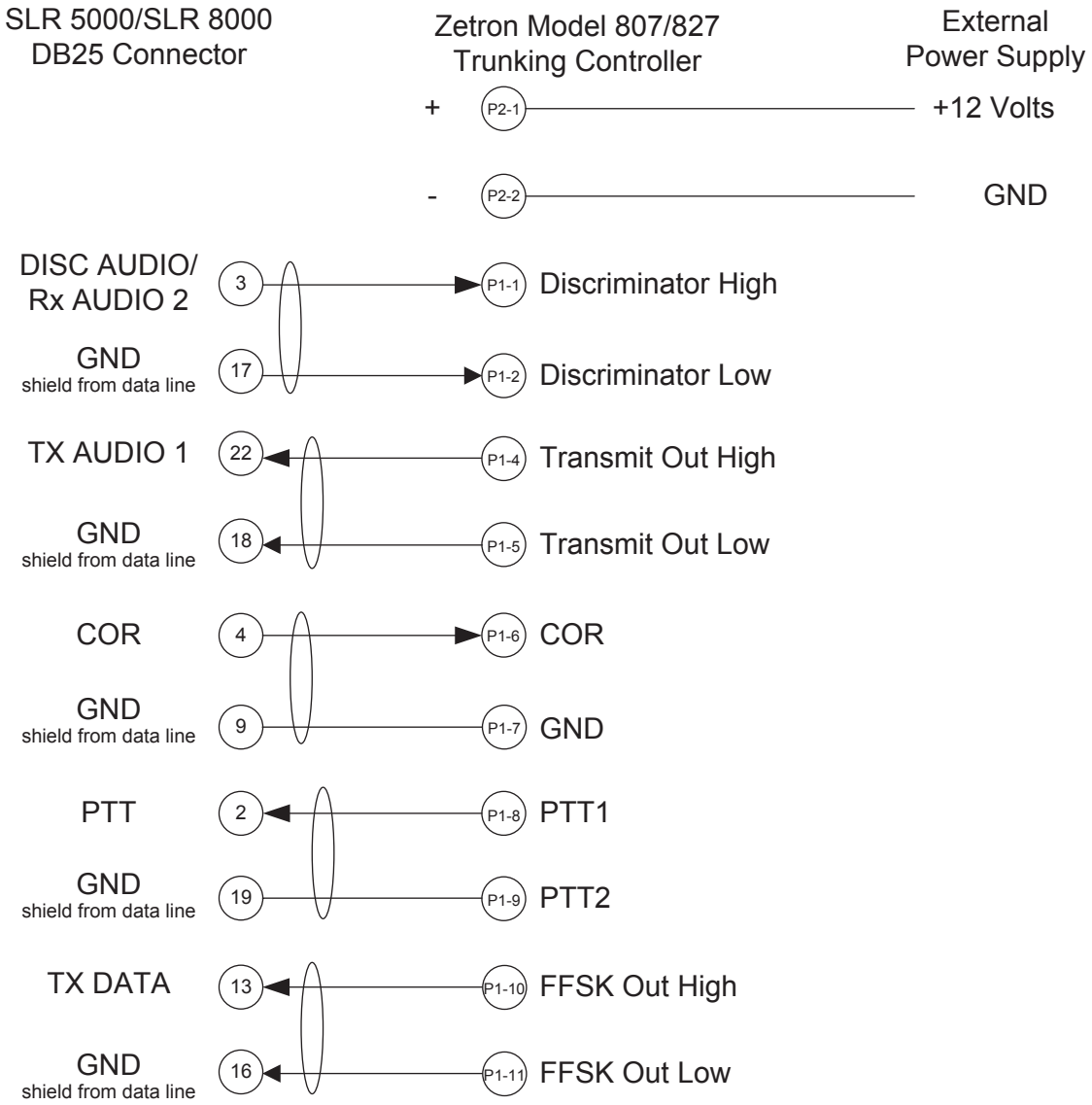
Hardware Connection

The connections between the SLR Base Station/Repeater and the M827/M807 controller are facilitated with cable connected between the SLR 5000/SLR 8000 DB25 connector and that of the M827/M807 controller. The connection cable provides the following signals:

- Transmit Data
- Transmit Audio
- Discriminator audio
- Push-to-talk (PTT)
- Carrier Operated Relay (COR)
- Ground

The connection diagram is illustrated in Figure 75: Hardware Connections between SLR 5000/SLR 8000 and M827/M807 Controller on page 268.

Figure 75: Hardware Connections between SLR 5000/SLR 8000 and M827/M807 Controller



CPS Configuration

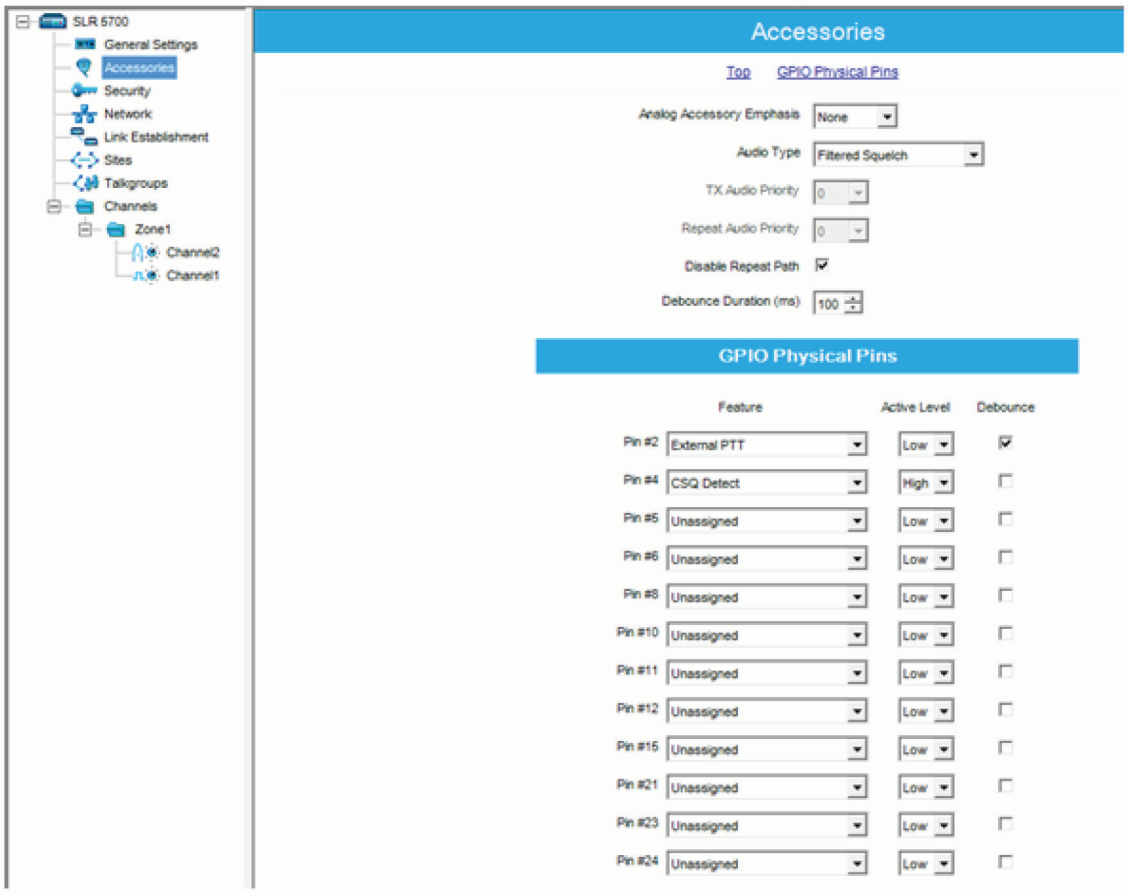
The SLR 5000/SLR 8000 Base Station/Repeater will need to be configured via the CPS application as shown in Figure 76: CPS Configuration for M827/M807 Controller (1 of 2) on page 269 and Figure 77: CPS Configuration for M827/M807 Controller (2 of 2) on page 270. The configurations include the Accessories and OTA Channel.

The specific configurations at accessories are:

- Audio Type
  - Rx and Tx Flat
- Disable Repeat Path
  - Checked
- GPIO Pin number 2
  - Ext Mic PTT
  - Active Low

- GPIO Pin number 4
  - Carrier Squelch (CSQ) Detect
  - Active High

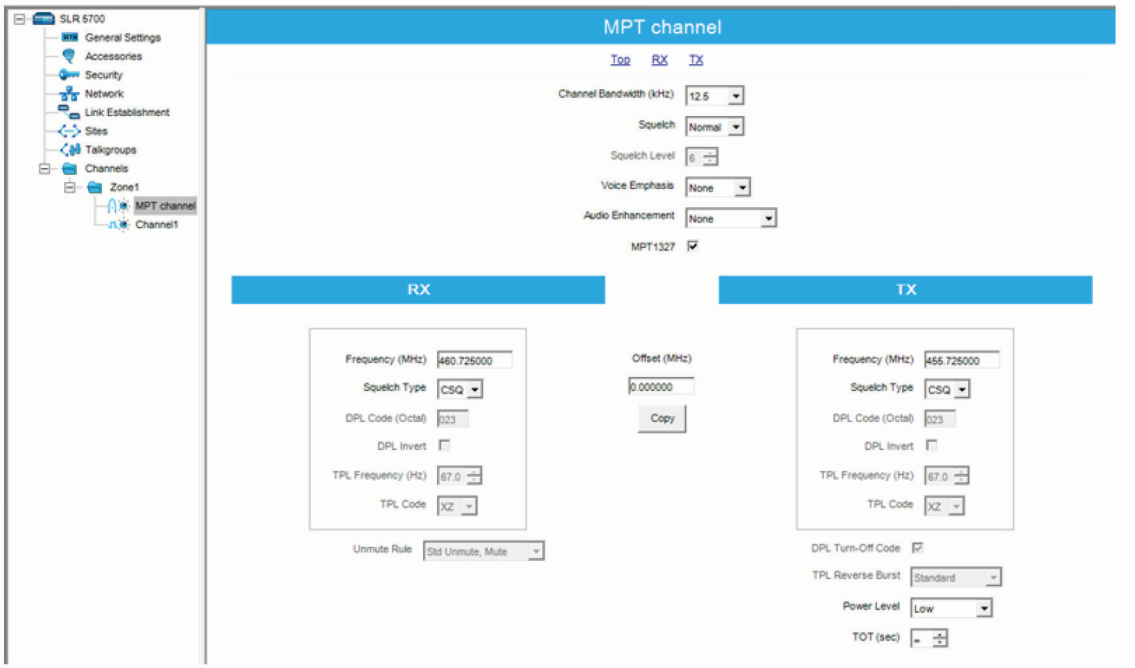
Figure 76: CPS Configuration for M827/M807 Controller (1 of 2)



The specific configurations at (OTA) channel are:

- MPT 1327
  - Checked
- Squelch Type (Rx)
  - CSQ
- Squelch Type (Tx)
  - CSQ
- Time Out Timer (sec)
  - ∞

Figure 77: CPS Configuration for M827/M807 Controller (2 of 2)



M827 Controller Configuration

The hardware jumpers on Zetron M827/M807 shall be set to the following positions:

- JP3 = position A, PTT1 normally Open
- JP6 = position B, external COR source
- JP13 = position B, COR positive polarity
- JP7 = A; JP10 = A, pre-emphasized audio and flat data
- JP5 = position A, Pre-Emphasized Tx audio signal
- JP11 = position A, flat Tx data signal

Follow “Model 807–Model 827 MPT1327 Trunking Controller Operation and Installation” from Zetron for the controller configuration and alignment. To configure the repeater interface for SLR 5000/SLR 8000, set the parameters in Site Configuration -> Repeater Editor to the followings:

- Keyup delay = 40
- Receive Delay = 7
- Transmit Delay = 4
- Enable Delay= 10

2.35.5.3.5
Fylde Micro Controllers

NOTE: SLR 5000/SLR 8000 supports TSCC03 channel controller from Fylde Micro for the MPT1327 analog trunking application.

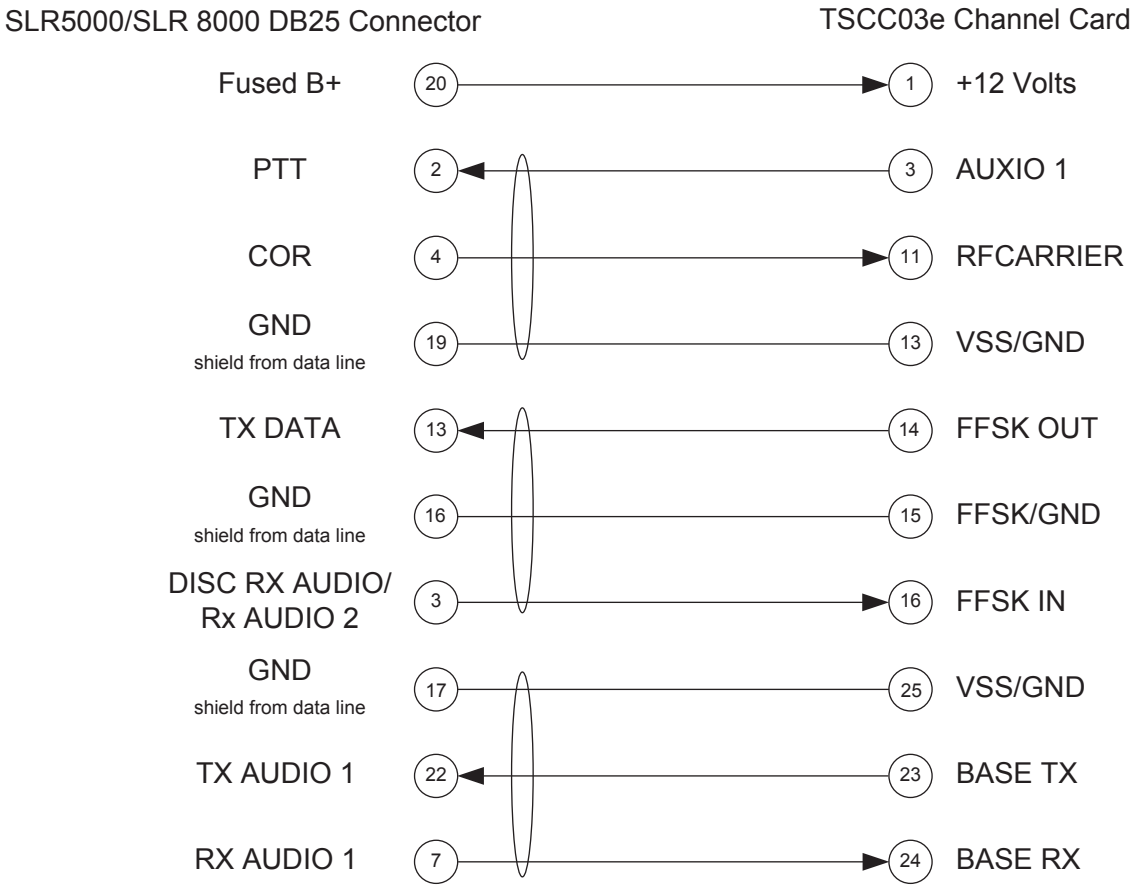
Hardware Connection

The connections between the SLR Base Station/Repeater and the TSCC03 channel controller are facilitated with cable connected between the SLR 5000/SLR 8000 DB25 connector and that of the TSCC03 channel

controller. The connection diagram is illustrated in Figure 78: Hardware Connections between SLR 5000/SLR 8000 and TSCC03 Channel Controller on page 271. The connection cable provides the following signals:

- Transmit Audio
- Transmit Data
- Discriminator Audio
- Receiver Audio
- Push-to-talk (PTT)
- Carrier Operated Relay (COR)
- 14.2 VDC (The DC current draw from TSCC03 is less than 1 amp)
- Ground

Figure 78: Hardware Connections between SLR 5000/SLR 8000 and TSCC03 Channel Controller



CPS Configuration

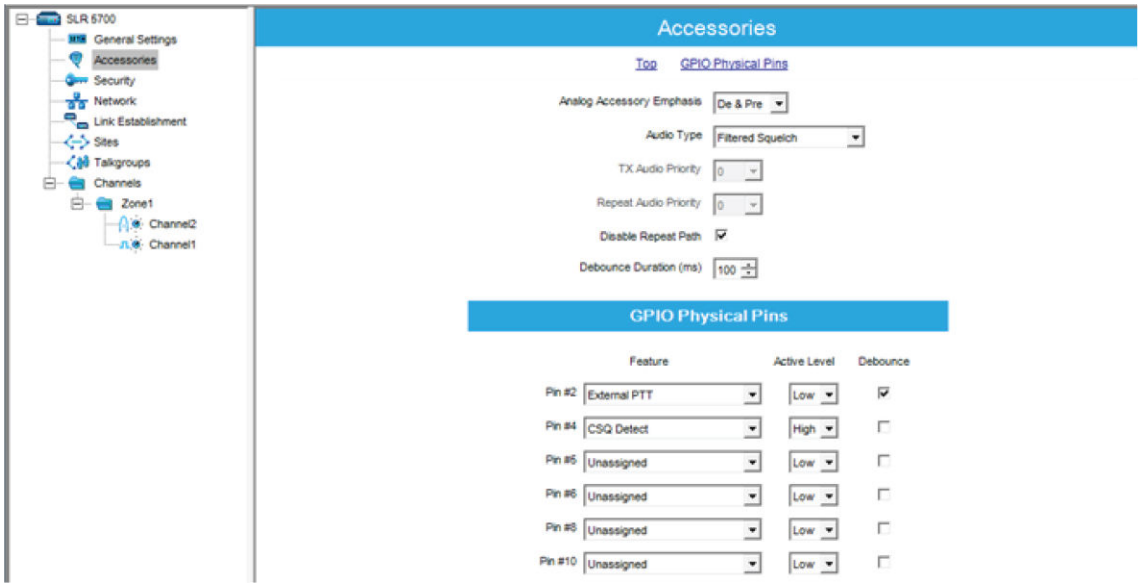
The SLR 5000/SLR 8000 Base Station/Repeater will need to be configured via the CPS application as shown in and . The configuration includes the Accessories and OTA Channel.

The specific configurations at accessories are:

- Audio Type
  - De-emphasis and pre-emphasis
- Disable Repeat Path
  - Checked

- GPIO Pin number 2
  - Ext Mic PTT
  - Active Low
- GPIO Pin number 4
  - Carrier Squelch (CSQ) Detect
  - Active High

Figure 79: CPS Configuration for TSCC03 Channel Controller (1 of 2)



The specific configurations at (OTA) channel are:

- MPT 1327
  - Checked
- Squelch Type (Rx)
  - CSQ
- Squelch Type (Tx)
  - CSQ
- Time Out Timer (sec)
  - ∞

Figure 80: CPS Configuration for TSCC03 Channel Controller (2 of 2)

TSCC03 Channel Controller Configuration

For more information, see the *Service and Operation Manual* from Fylde for the channel controller configuration and alignment.

NOTE: To configure the repeater interface for SLR 5000/SLR 8000, the “override settings for MTR2000 base station” box must be checked in the field programmer menu.

2.35.6

Auto-Range Transponder System

Auto-Range Transponder System (ARTS) is now available in analog mode (direct or repeater) in software version R02.10.00. This feature informs radio users when their radio is out of range from other ARTS-equipped radios.

ARTS uses automatic polling whereby the radio automatically transmits once every 25 or 55 seconds in an attempt to “shake hands” with another ARTS-equipped radio. When a radio receives an incoming ARTS signal, a short in range tone sounds and an “In Range” message is shown on the radio. If a radio is out of range for more than two minutes, a short out of range tone sounds and an “Out of Range” message is shown on the radio. When radios return in range from out of range, a short in range tone sounds and an “In Range” message appears again on the radio to notify the user.

The Auto-Range Transponder System (ARTS) feature has three operating modes:

- **Transmit Mode**
  The radio only transmits polling signals to connect with other radios. The radio does not receive signals and therefore does not notify the radio user of its own range status.
- **Receive Mode**
  The radio only receives polling signals to be notified when in range or out of range. The radio does not transmit polling signals to connect with other radios.

- **Transmit and Receive Mode**
  The radio transmits and receives polling signals. The radio can connect with other radios and notifies the radio user of its own range status.

ARTS can only be active on analog channels with a TPL/DPL squelch type. A radio is considered to be in range if carrier and matching TPL/DPL is detected, regardless of which radio transmitted it.

It is important to note that a radio with ARTS enabled only notifies the range status by receiving transmissions from other radios. This does not mean that the receiving radio can transmit or talk back to the transmitting radio. A good example of this is when a mobile radio with high power transmits its ARTS polling signal to a portable radio with low power. Although the portable can receive the high power signal from the mobile and notify the radio user that it is in range, it may not be able to reach the mobile since it is transmitting using low power.

Another very important item to note is that if there are many radios with ARTS enabled operating in Transmit and Receive (TRX) Mode in the same area, some of them may not be able to transmit successfully because of the excess loading on the channel. This should be considered when distributing radios across channels and when setting the ARTS TX Period.

Because radios with ARTS enabled are required to transmit often, battery life may be impacted. This should be considered when setting the ARTS TX Period.

The table below summarizes the programmable options for ARTS.

Table 62: Programmable Options for ARTS

Name	Value	Wide	Description
ARTS Mode	Off / TX / RX / TRX	Channel	ARTS operating mode
ARTS TX Period	25 / 55 (seconds)	Channel	ARTS TX period for polling transmission
ARTS Audible Indication	Off / Once / Always	Radio	Indicates whether radio sounds audible indications when valid transmission is received
ARTS Visual Indication	Off / On	Radio	Indicates whether radio shows visual indications

2.35.7
TX Inhibit Quick Key Override

This feature gives the radio user the ability to override the selected Busy Channel Lockout rule, thus allowing a transmission to be sent on a busy channel. The radio user accomplishes this by quick-keying the PTT button. This means pressing the PTT, then releasing, and quickly re-pressing within one second. This feature can be enabled or disabled via CPS.

This feature is available for internal PTT, external PTT via accessory or Bluetooth, and XCMP PTT, but not applicable for VOX PTT via accessory or Bluetooth. This feature applies only when the radio is operating in analog conventional dispatch mode. This feature is only available in portables.

2.35.8
Alert Tone Fixed Volume

When the Alert Tone Fixed Volume feature is enabled via CPS, all alert tones remain at a constant volume level. This constant volume level is equal to the radio's Midpoint Volume Setting, plus or minus the Alert Tone

Volume Offset setting. The volume level for alert tones then remains constant, even when the radio's volume knob is adjusted.

This does not affect tone volumes that are automatically adjusted by the radio, for example, when Quik-Call II Call Alert, Escalate, and Intelligent Audio features are enabled. This feature is only available in portables, and both analog and digital modes.

2.35.9
Alert Tone Auto Reset

The Call Alert tone is normally a repetitive alert tone.

This feature enables the radio to generate only one sequence of the Call Alert tone when the radio decodes a Digital, MDC, or Quik-Call II Call Alert. The Call Alert tone duration can be configured via CPS from 0 (∞) second to 1200 seconds by a 5-second increment. If the Infinity (∞) option is selected, the Call Alert tone continuously sounds until the user cancels the Call Alert indication.

This is a radio-wide feature available in analog and digital modes. This feature is only applicable if the Disable All Tones feature is disabled.

2.35.10
Emergency Permanent Sticky Revert

This feature enables the radio to remain permanently on the Emergency Revert Personality after the emergency transmission has been sent and acknowledged. The radio must be powered off for it to return to the selected channel on the Channel Selector.

Any mode change – analog vote scan, scan and auto scan will not work while the radio is operating on the Emergency Sticky Revert Channel. The radio can still receive MDC and Quik-Call II Call Alerts or Selective Calls, but cannot initiate them.

This feature can be enabled or disabled via CPS and is only available in portable radios.

.

2.36
Software Update Management

Software Update Management (SUM) is the feature that enables MOTOTRBO systems to continue to accept new software updates.

Applicable to all MOTOTRBO subscribers, repeaters, and Capacity Max System Servers (CMSS), this feature provides products with built-in intelligence to define if they are eligible to accept a software update. Products on prior software releases must be upgraded to R2.10 before being upgraded to any future releases.

Feature availability

New products

Products sold with R2.10 or any future releases accept major and minor software releases while the product is under warranty, or covered with a MOTOTRBO service package that includes MOTOTRBO Software Updates.

Existing products

Products deployed before R2.10 require a SUM license to be upgraded beyond R2.10. SUM licenses are issued for products that have purchased a MOTOTRBO service package that includes Software Updates. Once a service package is purchased, a license is issued and pre-registered for that product serial number in Motorola Solutions' licensing database. The license is available then retrieved by using

Radio Management (RM) or Customer Programming Software 2.0 (CPS). Once the license is retrieved, the product accepts new software updates for the duration of the MOTOTRBO Service Package.

License Status

Available for registration
License is available and ready to be activated.

Available for purchase
A contact with a Motorola Solutions representative is required.

2.36.1
Activating SUM License

Use this procedure to activate Software Upgrade Management (SUM) license in Radio Management (RM) software.

Procedure:

1. In RM, perform one the following actions:

If…	Then…
If you want activate a SUM license for a radio,	perform the following actions: **a.** Click , and navigate to **Manage** → **Licenses** → **Radio Licenses**. **b.** Ensure that in the target desired radio row, **Status** section displays the **Available for registration** text.
If you want activate a SUM license for a Capacity Max System Server (CMSS),	perform the following actions: **a.** Click , and navigate to **Manage** → **Licenses** → **Capacity Max System Server Licenses**. **b.** Ensure that in the target CMSS row, **Status** section displays the **Available for registration** text.

2. In RM, click , and navigate to **Settings**.
3. In the **Settings** window, click **Licenses**.
4. In the **Recover Licenses** section, perform one of the following actions:
   - To activate the license for a radio, in the target **Radio Licenses** row, click **Recover**.
   - To activate the license for a CMSS, in a desired **Capacity Max System Server** row, click **Recover**.

2.37
Repeater Webserver Functions

The following section describes the main functions of the webserver of the repeater.

2.37.1
Accessing the Webpage of the Repeater

Use this procedure to access the webpage of the repeater.

NOTE: DR 3000 repeaters do not support multiple connections to the webpage.

Prerequisites: The webpage of the repeater is accessible through a web browser on any personal computer that meets the following computer specifications.

Table 63: Computer Specifications for Access to the Webpage of the Repeater

Parameters	Recommendations
Operating System Requirements	• Windows 10 (32–bit or 64–bit) • Windows 11 (32–bit or 64–bit)
Hardware Minimum Requirements	2 GB RAM
Software Requirements	Recent versions of web browsers. **NOTE:** As of the release of this document, the following browser versions have been tested with the current repeater firmware release: Google Chrome 119, Mozilla Firefox 120, Microsoft Edge 119.

Procedure:

1. Perform one of the following actions:
   - For the SLR 1000/5000/8000 Series repeater, in the address field of the browser, enter `https://<repeater_ip_address>`
   - For the DR 3000 repeater, in the address field of the browser, enter `https://<repeater_ip_address>/cgi-bin/index.htm`
2. Provide your username and password, and click **OK**.

   NOTE:
   The default username is `motorola`
   The default password is the serial number of the repeater, printed on the back panel of the repeater.

Logging on the webpage for the fist time:

3. If you are logging on for the first time, you are redirected to the **Config** page. In the **Change credentials** section, change the user name and password.

   See Configuration on page 280 for password limitations.
4. Optional: In the **Change certificate** section, add new key and certificate.

   To improve the overall security, it is recommended to perform this step.

2.37.2
Repeater Alarms

The **Repeater Alarm** page displays the Alarm Log stored in the repeater codeplug.

The Alarm Log contains the Alarm Name, Opcode, State, Severity, and Time stamp. Repeaters alarms are presented in the same way that in Repeater Diagnostics and Control (RDAC). Alarm states show all alarms history. They can be cleared from RDAC only.

NOTE: The maximum number of displayed alarms is 50.

2.37.3
RDS Logs

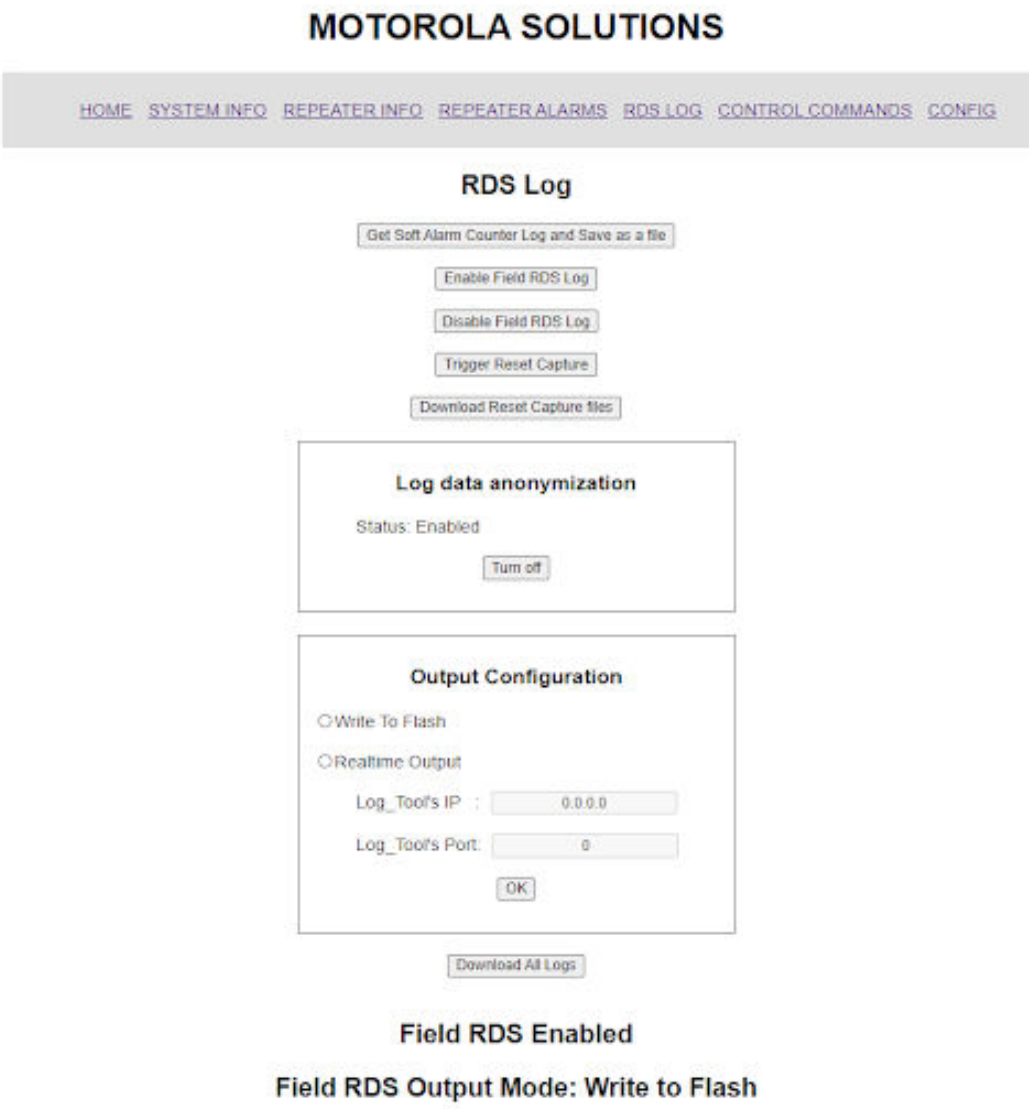
You can enable or disable the RDS function on the Repeater Diagnostic System (RDS) Log page.

After the RDS is enabled, Repeater records internal logs into the flash memory (preferred method) or sends directly to the logging tool depending on Output Configuration settings. The key logs include:

- Repeater field running logs.
- Repeater Air tracer logs.

You can do the manual reset capture through the browser. In SLR family repeaters, you can download the log files through the browser. See Downloading SLR Repeater Logs on page 279.

Figure 81: RDS Log for SLR Repeaters



2.37.3.1

Downloading SLR Repeater Logs

You can use this procedure to download all the SLR Repeater logs.

Procedure:

1. In the web page of the repeater, click **RDS LOG**.
2. In the RDS Log page, click **Download All Logs**.

   NOTE: The log files are usually large (about 700 Mb). Depending on the file size, download might take up to 20 minutes. Repeater logs will be automatically disable during the downloading procedure. Enable repeater logs again if needed.

2.37.3.2
Enabling Repeater Logs

Repeater Field RDS logs are disabled, and voice and data payload are anonymized by default. For SLR Repeaters there is a possibility to turn off anonymization of user data for specific diagnostics purposes.

Procedure:

1. In the web page of the repeater, click **RDS Log**.
2. In the **RDS Log** page, click **Enable Field RDS Log**.

2.37.4
Control Commands

The **Control Commands** page allows you to clear the RDS log stored in the Repeater Codeplug. Clearing the RDS Log does not clear the alarm state of the repeater, just the RDS log history.

2.37.5
Configuration

The **Configuration** page allows you to modify certain setting of the web server.

You can modify the following functions:

- Change the user name and password.
- Change the certificate and private key.
- Change the session login time.

NOTE: The following limitations apply:

- User name cannot be longer than 9 characters.
- Password cannot be longer than 63 characters.
- Certificate cannot be longer than 2000 characters.
- Key cannot be longer that 2000 characters.

If the certificate key for DR 3000 repeater is longer than 1024 bits, the initial connection is slowed down.

2.37.6
Resetting Login Credentials/Certificate

Follow this procedure to reset webserver login credentials, or authentication certificate.

NOTE: To perform this procedure, a repeater must be connected to a PC by using a USB cable.

Procedure:

1. Open the AT debug console by performing the following actions:
   a. By using a USB cable, connect your PC to the repeater.
   b. In Radio Management (RM), Locate **Radio IP** address field of the preferred repeater.
   c. By using a ***<Radio IP address>*** and a 8501 port, establish a telnet connection to the repeater.

      NOTE: The Radio IP address can be established only if repeater drivers are installed.
2. Perform one of the following actions:

- To restore the default login credentials, certificate, and codeplug for SLR 1000/5000/8000 Series, type `reset_web_credentials`

  WARNING: For SLR 1000/5000/8000 Series, this command resets whole repeater configuration.

- To restore the default login credentials, certificate and delete sensitive data for DR 3000/ MTR3000, type `factory_reset`

  NOTE: The default key is 1024 bits long.

NOTICE: If **`reset_web_credentials`** or **`factory_reset`** command failed, send the error code to the support team.

2.38 MOTOTRBO 2-4-1 Feature Overview

MOTOTRBO 2-4-1 is an RF Site configuration that doubles the capacity of a MOTOTRBO digital 800 MHz 25 kHz channel.

FCC allows 800 MHz band non-NPSPAC channels to apply the unused capacity as a second MOTOTRBO channel. Mostly, 25 kHz channel licenses at 800 MHz have unused capacity within the channel, this utilization doubles the capacity of the licensed channel.

Until now, one 12.5 kHz wide RF carrier was transmitted on the center frequency of the licensed channel. If the channel was configured for MOTOTRBO operation, the one carrier provided two talkpaths of voice or data capacity.

Now, the allowable emission on the channel for the 800 MHz non-NPSPAC channels is widened. This allows having multiple carriers in an exclusive channel, and enables the original MOTOTRBO RF carrier to be shifted by 6.25 kHz off of the center frequency of the licensed channel. A second MOTOTRBO RF carrier is then added with a center frequency shifted by 6.25 kHz the other way from the center frequency of a licensed channel, creating a 12.5 kHz separation between the two sub-channels.

The combination of the two MOTOTRBO RF carriers fits within the FCC revised emission limits for the 800 MHz band non-NPSPAC channels. With the new carrier and the original carrier configured for TDMA, the licensed channel now transports four talkpaths.

MOTOTRBO 2-4-1 is implemented using one MTR 3000 or SLR 8000 base radio for each sub-channel, so a two carrier 2-4-1 channel requires two MTR 3000 or SLR 8000.

MOTOTRBO 2-4-1 system configuration has small effect on a system wide operation beyond increasing the number of channels available for the system. Its primary impact is at the RF Site and channel level. The MOTOTRBO system treats a two carrier 2-4-1 channel as two typical channels at the site. The primary difference with MOTOTRBO 2-4-1 is the RF considerations associated with having two co-located channels within 12.5 kHz of each other. MOTOTRBO 2-4-1 is implemented by using existing infrastructure and subscribers, but requires extra base radios.

2.38.1 MOTOTRBO 2-4-1 Benefits

MOTOTRBO 2-4-1 allows you to use more channels at the RF Sites without requiring additional licenses.

A license modification application must be approved by a frequency coordinator, such as EWA, and filed with the FCC regarding the use of the license for two carriers instead of one.

More channels supports more talkgroups, which allow the system operator to structure more specialized talkgroups. This ensures that all communication is relevant to the participants, and minimizes the risk of ignoring the call.

It is also possible to use additional talkgroups to support an increase in the number of system users. Personnel can be brought onto the system, but kept separate from the existing groups with new talkgroups made available by the additional 2-4-1 channels.

MOTOTRBO 2-4-1 provides benefits even if no additional talkgroups are required. By adding 2-4-1 channels, the system can be expanded to include data applications such as GPS.

More channels at a given site can increase surge capacity. Surge capacity allows more talkgroups to be supported simultaneously on a site during an event in the vicinity. With personnel from various groups responding to the event, they can retain their talkgroup affiliation while on site to focus attention on their portion of the response.

2.38.2
Regulatory Requirements

When a license with non-NPSPAC 800 MHz band channels is operational, to implement MOTOTRBO 2-4-1, it is required to file an application to modify the licenses, obtain approval of a frequency coordinator, and subsequent filing with and approval by the FCC.

The application is required to obtain approvals form the frequency coordinator and and FCC to deploy multiple carriers as allowed under FCC rule 90.645(f), while meeting the emission limits in Section 90.209. The license holder, who is usually the system operator, or its regulatory legal counsel can prepare the application. However, given that this is a new approach, it is advised that the licensee and/or its regulatory legal counsel work with the Motorola Solutions Government Affairs Spectrum Team.

2.38.2.1
Application Process

The application for conducting 2-4-1 operation is submitted to the frequency coordinator for approval, who then forwards the application to the FCC.

All applications are submitted online. For 2-4-1 implementation, the critical element is a supplementary attachment to the license modification application. The supplementary attachment must explain the intention to transmit two carriers offset by ± 6.25 kHz at the site. The attachment must also include a table summarizing measured emissions with the MOTOTRBO 2-4-1 operation, comparing them to the maximum emissions allowed under the FCC rules. The filing should satisfy the frequency coordinator that the 2-4-1 emissions do not exceed the originally licensed Effective Radiated Power (ERP) for the channel.

IMPORTANT: Increasing ERP can result in frequency coordinator rejection of the request for license modification.

The application for conducting 2-4-1 operations on a channel licensed for 25 kHz analog operation is similar. A normal application to change from analog operation to MOTOTRBO digital operation must be filed. A supplementary attachment similar to the example in the following subsection explaining the intention to operate 2-4-1 emissions should accompany the license application. The emissions and the Adjacent Channel Protection (ACP) values in the table may be different.

2.38.2.2
Sample Attachment to MOTOTRBO 2-4-1 License Application

Sample attachment for MOTOTRBO 2-4-1 must be customized for each applicant.

Supplemental Statement to Application for Modification

<Licensee's Name> submits this modification application for station ***<Call Sign>*** so that its license provides for operations on channels offset by 6.25 kHz within the authorized 25 kHz licensed channel on frequency pair ***<Insert specific frequency pair>*** MHz (the 800 MHz pair).

Under § 90.645(f) of the FCC's rules, licensees are authorized to operate multiple emissions on a channel that has been licensed on an exclusive basis so long as the out-of-band emission (OOBE) limits of § 90.209 are met. Section 90.209(b)(5) currently permits use of up to a 22 kHz bandwidth per 25 kHz channel, provided the equipment meets the Adjacent Channel Power (ACP) limitations of § 90.221. ***<Insert licensee name>*** seeks to operate within the permitted 22 kHz bandwidth of this 800 MHz pair.

The 800 MHz pair is authorized on an exclusive basis. ***<Insert licensee name>*** proposes to operate on channels offset by 6.25 kHz, for example, ***<Insert lower offset base transmit center frequency>*** MHz and ***<Insert upper offset base transmit center frequency>*** MHz, with a 7.6 kHz bandwidth emissions for FB2 station. ***<Insert licensee name>*** would also operate on ***<Insert corresponding lower offset mobile transmit frequency>*** MHz and ***<Insert corresponding upper offset mobile transmit frequency>*** MHz, with an 7.6 kHz bandwidth emission for MO and FX1 stations. These emissions are the same as currently licensed. ***<Insert licensee name>*** equipment supplier has confirmed that the proposed channel configuration satisfies the ACP limitations of § 90.209. The chart below summarizes the equipment manufacturers' calculations confirming the proposed operations comply with the ACP limitations. Depending on the adjacent frequency offset being measured, the anticipated ACP is 8 to 20 dB better than what is required by the FCC rules.

Table 64: Sample Attachment to MOTOTRBO 2-4-1 License Application

Frequency offset	§ 90.221 required ACP (dBc) for devices less than 15 W	§ 90.221 required ACP (dBc) for devices 15 W and above	Measured ACP for Proposed Operation (Worst Case)
25 kHz	-55 dBc	-55 dBc	-63 dBc
50 kHz	-65 dBc	-65 dBc	-85 dBc
75 kHz	-65 dBc	-70 dBc	-85 dBc

The proposed license modification does not impact any co-channel licensee because there is no increase in effective radiated power for the 800 MHz pair and no increase in coverage area for station ***<Insert call sign>***. Moreover, the proposed modification promotes spectrum efficiency.

Accordingly, ***<Insert Licensee Name>*** requests the FCC grant the modification to station ***<Insert call sign>***. To document the modification to the licensed operations and to provide the necessary coordination protection for operations consistent with the permitted 22 kHz bandwidth, ***<Insert Licensee Name>*** requests that the license for station ***<Insert call sign>*** be modified by adding the following condition:

Per § 90.645 of the rules, licensee is authorized to implement multiple 7.6 kHz emissions on the frequency *<insert base station frequency>* and multiple 7.6 kHz emissions on the frequency *<insert corresponding mobile station frequency>* that in aggregate comply with the 22 kHz bandwidth Adjacent Channel Power (ACP) limitations of § 90.221.

Should the FCC have questions, it is requested to contact ***<list name, email, phone of appropriate contact in the licensee's organization or its outside regulatory counsel.>***

2.38.2.3 FCC Coordinators

First, the FCC coordinators evaluate the license filing.

The EWA, an FCC certified frequency coordinator involved with the energy and other industrial markets, is on 2-4-1 and pocessed an application for a license that is pending at the FCC as of December 2013. Other regional coordinating bodies are not briefed on 2-4-1. The initial filing with a regional body other than

EWA requires participation of the Motorola Solutions Government Affairs Spectrum Team, who can brief the frequency coordinator on 2-4-1 and its benefits.

NOTE: It is recommended that the initial contact with frequency coordinating bodies is made through the Motorola Solutions Government Affairs Spectrum Team.

Briefing and working with the FCC certified frequency coordinators is important in getting authorization to operate 2-4-1.

2.38.3
MOTOTRBO 2-4-1 Site Configurations

MOTOTRBO 2-4-1 is a feature that impacts the RF Site at a channel level.

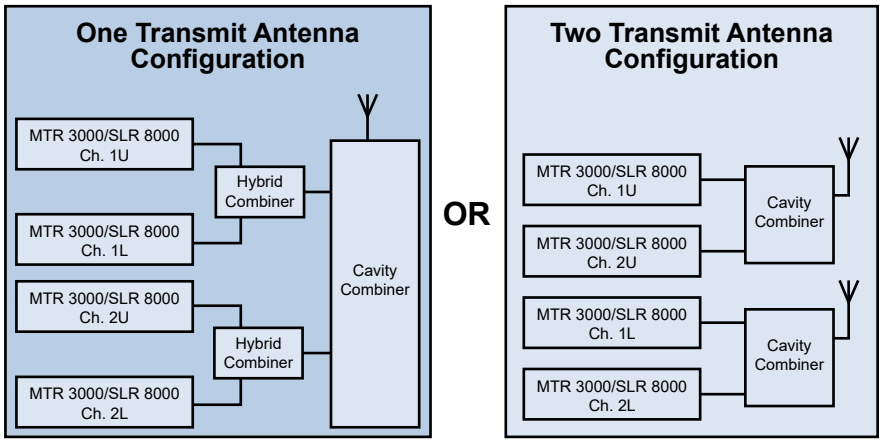
It provides a way to add a channel using an existing 25 kHz licensed channel at 800 MHz. MOTOTRBO 2-4-1 is an extra channel at the RF Site, except for regulatory and the conditions associated with a co-located adjacent channel offset by 12.5 kHz.

MOTOTRBO 2-4-1 is available in two configurations:

- Configuration for sites that have only one transmit antenna
- Configuration for sites that have two transmit antennas

The major differences between the two configurations are related to radiated power levels, and heat generated by hybrid combiners. The following figure is a summary of both configurations.

Figure 82: RF Site Configurations for MOTOTRBO 2-4-1 Channels



2.38.3.1
One Transmit Antenna Site Configuration

For sites with one transmit antenna, MOTOTRBO 2-4-1 uses two MTR 3000/SLR 8000 repeaters with frequencies offset +6.25 kHz (for a total of 12.5 kHz separation) coupled together through an 800 MHz Hybrid Combiner and then coupled to the transmitter antenna.

The hybrid combiner has a 3.5 dB to 3.8 dB insertion loss, which dissipates as heat. That insertion loss reduces the radiated power of the transmitted signal by 3.5 dB to 3.8 dB below the radiated signal from a non-2-4-1 configuration. If more channels are used, an appropriate cavity combiner is typically used post hybrid combiner to add the additional channels.

2.38.3.2
Two Transmit Antenna Site Configuration

An RF Site with two transmit antennas can use the Two Transmit Antenna Configuration to add extra channels.

This solution prevents the signal loss and heat generated by hybrid combiners. The MTR 3000/SLR 8000 base radios servicing the low side of each 2-4-1 channel are connected into a cavity combiner and then coupled to one transmit antenna. The MTR 3000/SLR 8000 base radios servicing the high side of each 2-4-1 channel are connected to a second cavity combiner and then coupled to a second transmit antenna.

In this configuration, all normal RF restrictions apply. RF isolation provided by transmit antennas that are mounted in an industry-acceptable geometry combined with the isolation from the cavity combiners provides sufficient isolation between the two antenna systems.

2.38.4
MOTOTRBO 2-4-1 System Configurations

MOTOTRBO 2-4-1 is a system configuration that increases the number of channels available for the system to use at a site. Apart from that, it has little effect on system-wide operation.

Its primary impact is at the RF Site and channel levels where it doubles the capacity of a 25 kHz licensed channel in the 800 MHz band.

2.38.4.1
Impact to MOTOTRBO System and Network Management

A system detecs MOTOTRBO 2-4-1 channel as two channels available for use.

The system does not recognize whether a channel is a part of a 2-4-1 superchannel, or if it is just another typical channel at the site. The system and network tools report on the 2-4-1 sub-channels as if they were two separate channels at the site. As the system treats a 2-4-1 channel as two individual channels, all the MOTOTRBO digital system topologies are supported. These configurations include:

- Trunked Repeaters
- Voting Repeaters
- Satellite Receivers

MOTOTRBO 2-4-1 operation is also possible when using MOTOTRBO digital conventional operation.

2.38.4.2
Recommendation when Using 2-4-1 for Control Channel

It is recommended to avoid carrying the control channel on a 2-4-1 sub-channel.

It is technically possible to use a 2-4-1 channel for a control channel, but the potential for near-far interference can cause weak inbound signals to not be detected by the control channel base radio receiver. Although the techniques described later can minimize or virtually eliminate the near-far interference, its impact to the user is greatest if it occurs on the control channel.

2.38.4.3
MOTOTRBO System Retrofit with 2-4-1 Channels

It is possible to retrofit existing MOTOTRBO systems with 2-4-1 channels.

One scenario is to add an MTR3000/SLR 8000 repeater, assuming that the current repeater is also an MTR3000/SLR 8000, and a hybrid combiner in the One Transmit Antenna Configuration.

Another retrofit scenario is to use the Two Transmit Antenna configuration. If an existing channel is converted to a 2-4-1 channel, the existing MTR 3000/SLR 8000 is tuned to a frequency of 6.25 kHz above or below the channel center frequency. Then a new MTR3000/SLR 8000 which is connected to the second transmit antenna is added. The current MTR3000/SLR 8000 is then tuned to a frequency offset by 6.25 kHz in the opposite direction to the original and the antenna spacing and must have appropriate isolation.

2.38.5
RF Coverage and Near-Far Interference

Coverage Area is the region of useable received signals, either from the uplink or downlink that is present when the subscriber or the base radio is transmitting.

The definition of useable signal can be described at various received signal levels. Useable sensitivity exists at levels as low as -118 dBm to -121 dBm while coverage is often stated at the kTb+18 dB point, - 110 dBm for instance, where kTB noise is the thermal noise present due to bandwidth and temperature. A value of -174 dBm/√Hz is assumed for “k”. For some users, useable sensitivity may occur as high as -100 dBm. Motorola Solutions typically defines useable signal quality by means of DAQ or PESQ, and occasionally expresses those results in terms of BER or signal strength.

In this section, Baseline Coverage Area is the physical service outline of a single transmission offset by 6.25 kHz within a 2-4-1 split channel when there is no interference present from the other, opposite offset side of the 2-4-1 channel. Coverage Area is determined after the acceptable, specified signal strength contour is defined and established.

Near-far interference occurs when both sides of the 2-4-1 channel are in base radio receive mode, and the signal strength into the base radio on one side of the 2-4-1 channel is greater than the signal strength into the base radio on the other side of the 2-4-1 channel. When the difference between the two signals becomes great enough, the weaker signal is not be properly detected, even though it is the only signal on the 2-4-1 opposite offset sub-channel. The RF blocking that occurs can also be referred to as the Undesired / Desired Ratio (U/D) of the pair of signals occupying the 2-4-1 split channel. Near-far interference is passively prevented in one of two ways:

- Limit the strength of the strong interfering signal into the base radio site receiver.
- Limit the weakness of the weak desired signal into the base radio site receiver.

2.38.5.1
Baseline RF Coverage

The baseline coverage area of a MOTOTRBO 2-4-1 split, offset channel is the same as the normal coverage area of a typical channel at the same center frequency.

Baseline coverage occurs when one side of the MOTOTRBO 2-4-1 channel is active. Baseline coverage also occurs when one side of the 2-4-1 channel is in base radio transmit mode and the other side is in base radio receive mode, if the typical transmitter to receiver isolation techniques are employed for both sides of the 2-4-1 channel.

Baseline coverage is also present when both sides of the 2-4-1 channel are in base radio transmit mode, as long as both transmit antennas are located within a few hundred feet of each other, and the power output from both sides of the 2-4-1 channel is essentially the same. This occurs because the interfering signal from the interfering side of the 2-4-1 channel is the same strength as the desired signal from the desired side of the channel, the U/D ratio at the subscriber radio does not exceed 20 dB to 30 dB, even with deep, selective fading. When that is the case, the subscriber receiver filtering and the robust nature of the MOTOTRBO modulation is sufficient to prevent near-far interference.

2.38.5.2
RF Channel Coverage Balance

An RF Site can host 2-4-1 channels alongside channels that are typical non-2-4-1 channels.

It is important to balance the transmit power of the 2-4-1 channels with the typical channels in installations that employ the one antenna configuration using the hybrid combiners for the 2-4-1 channels. The hybrid combiners introduce an extra 3.5 dB to 3.8 dB of insertion loss into the transmit path of the 2-4-1 channels. To balance the coverage area for all channels on the site, the non-2-4-1 typical channels must be set to radiate at a power level equal to the 2-4-1 channels. That requires the power levels of the typical non-2-4-1 channel transmitters to be set 3.5 dB to 3.8 dB lower than the transmit power of the 2-4-1 channel transmitters.

2.38.5.3
Near-Far Interference

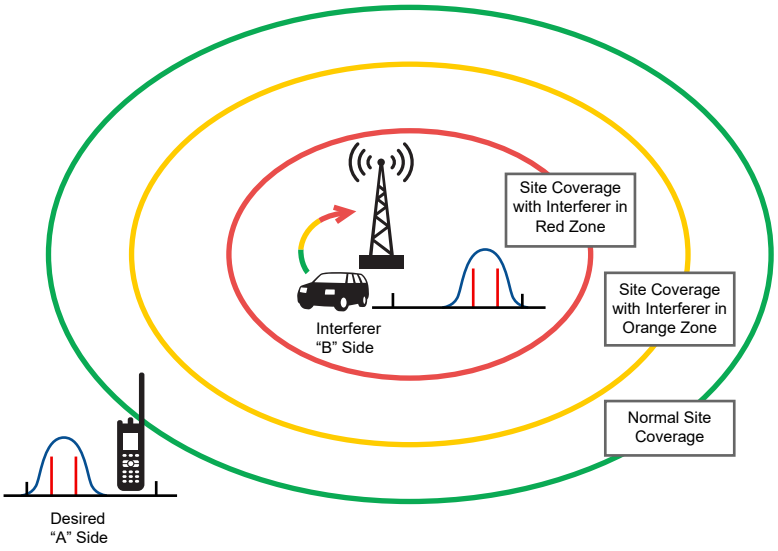
Near-far interference occurs when both sides of the 2-4-1 channel are in base radio receive mode, and the signal strength into the base radio on one side of the 2-4-1 channel is greater than the signal strength into the base radio on other side of the 2-4-1 channel.

When the difference between the two signals becomes great enough, the weaker signal is either not detected, or degraded. This results in two parameters governing the coverage area of a 2-4-1 channel which is experiencing near-far interference. One governing parameter is the weakest signal that is usable for the system. In the absence of near-far interference, this parameter is the same as the weakest useable signal that is used in typical coverage predictions.

The other governing parameter is the strength of the interfering signal on the other side of the 2-4-1 channel. The strength of this signal determines the weakest signal that is useable on the other side of the 2-4-1 channel.

This relationship between the strong interfering signal and the weak desired signal creates a variable coverage area for the weak signal side of the 2-4-1 channel. With a weak or moderate adjacent channel interfering signal, the coverage area of the desired weak side of the 2-4-1 channel is unaffected. As the interfering signal on the interfering side of the 2-4-1 channel grows stronger, the effective coverage area of the weak side of the 2-4-1 channel is reduced. This is illustrated in the following figure.

Figure 83: Coverage Area Depends on the Strength of an Interfering Signal



When the interferer on the “B” side of the 2-4-1 channel is sufficiently far away from the base site tower to be on the green portion of the interfering line, the corresponding signal strength area for the “A” side of the 2-4-1 channel is within the area represented by the green circle. The green circle corresponds to the baseline coverage area for the channel.

As the interferer moves closer to the base site tower and enters the orange portion of the interfering arrow, the coverage area for the “A” side of the 2-4-1 channel is reduced to the signal strength area represented by the orange circle. When the interferer moves very close to the base radio tower and enters the red portion of the interfering line, the coverage area for the “A” side of the channel is reduced to the signal strength area represented by the red circle.

2.38.5.4
Tools and Techniques Determining the Magnitude of Near-Far Interference

The magnitude of the near-far interference effect depends on the ratio of the signal strength from the interfering 2-4-1 sub-channel to the signal strength on the desired 2-4-1 sub-channel.

The Hydra coverage prediction tool models this effect to some extent, if the coverage model were constructed for an adjacent channel at fc +12.5 kHz occurring at varying signal levels. The Hydra techniques which are used to predict coverage degradations for near-far interference at 900 MHz also apply for MOTOTRBO 2-4-1 in the 800 MHz band.

2.38.6
Near-Far Interference Mitigation Techniques

2.38.6.1
Utilization of the Narrow Filter Option

The Customer Programming Software gives the user the option to utilize a narrow intermediate frequency (IF) filter. The narrow filter improves the acceptable U/D ratio by reducing the amount of adjacent channel noise coupling into the receiver.

2.38.6.2
Multi-Site Implementation – Voting and Simulcast

Near-far interference occurs when the signal strength of a weak signal into the base radio is overwhelmed by a strong signal into the base radio on the adjacent 2-4-1 sub-channel.

The interference occurs only when the base radios on both of the 2-4-1 sub-channels are receiving, and the difference between the two received signals is too great.

A radio frequency (RF) subsystem in a voting configuration mitigates near-far interference. If a weaker desired signal on a 2-4-1 sub-channel is subject to near-far interference at an RF site, then another voting receiver at another site can successfully detect the desired signal. This is because the interferer subscriber must be very close to the base radio site receiving antenna to produce a signal strength great enough to cause near-far interference, resulting in the fact that the interferer is not close enough to the other voting site to also cause interference to it. Since near-far interference is a phenomenon of the inbound channel, receiver voting mitigates near-far interference. In addition, the desired signal is likely to be stronger at another voting site than it is at the site experiencing the interference.

It is possible, that the adjacent 2-4-1 sub-channel at the voting site is assigned to a third talkgroup and it also receives a strong signal from another interferer near its tower. However, the probability of all these events occurring at the same time is low.

2.38.6.3
Single Site Implementations

In situations where voting is not an option, take steps to minimize the effect of near-far interference.

Prevent near-far interference in one of the following ways:

- Limit the strength of the strong interfering signal into the base radio site receiver.
- Limit the weakness of the weak desired signal into the base radio site receiver.

2.38.6.3.1
Recommended Site Antenna Height Increase

According to Radio frequency (RF) modeling and testing, an RF site receiving antenna placed at a height of 31 meters nearly eliminates near-far interference, and an antenna height of 50 meters eliminates it completely.

Increase of the height of the receiving antenna raises the main lobe of the antenna sufficiently above the surrounding terrain. In this configuration, the main lobe does not cross the ground level at a point where an interferer is close enough to trigger near-far interference. In such a configuration, as the interferer approaches the site tower, it moves outside the main RF antenna lobe, and prevents sufficient signal strength from the interferer to trigger near-far interference. As the interferer moves away from the tower and into the main lobe of a site receiver antenna, the distance weakens the signal sufficiently to prevent near-far interference despite the gain from the main lobe.

2.38.6.3.2
Selection of a Receiver Antenna with Higher Gain

The increase in gain from a high gain antenna is a result of a narrower main lobe providing greater sensitivity over a smaller elevation and azimuth.

A main lobe that is narrower in elevation intersects the surrounding terrain further away from the tower than an antenna with a wider main lobe and less gain. A sufficiently narrow main lobe does not intersect ground level at a point where an interferer is close enough to trigger near-far interference, particularly when the receiving antenna is mounted at a higher elevation on the tower. In such configuration, as the interferer approaches closer to the site tower, it moves outside the main RF antenna lobe and prevents sufficient signal strength from the interferer to trigger near-far interference. As the interferer moves away from the tower and into the site receiver main lobe of the antenna, the distance weakens the signal sufficiently to prevent near-far interference despite the gain from the main lobe.

2.38.6.3.3
Reduction of Excess Gain in the Receive Path

Typical RF sites are designed with excessive gain in the receiver path to offer additional protection from signal fluctuation and increasing noise.

In typical installations, this provides a benefit with few consequences for inbound signal recovery. With 2-4-1 channels, however, the excess gain in the receive path strengthens the interferer signal, which causes the base radio receive path to saturate. This creates additional harmonic interference on the weak channel, making the near-far problem worse.

To avoid creating additional interference due to base radio receiver saturation, the subscriber inbound power at the base radio receiver must be limited to -44 dBm or below. Reducing the excess gain helps maintain the base radio receive RF input level below -44 dBm.

For example, maximum power at the antenna drop of -48 dBm, plus an excess gain in the receive path of 4 dB, provides a -44 dBm maximum at the base radio receive input, triggering the near-far interference.

If excess gain is removed from the receive path for the 2-4-1 sub-channels, then the receive path gain must be matched for all channels at the site in order to balance the receive sensitivity of all channels at the site.

2.38.6.3.4
Reduction of Site Coverage Area

Limiting the weakness of the target signal is another approach to reducing near-far interference.

The further a subscriber moves from the receiving antenna, the weaker its inbound signal. If the advertised coverage area of the channel is reduced, then the very weak inbound signals are eliminated. This reduces the near-far interference.

Another solution is to predict an expected worst case strength of an interfering signal. Advertise the coverage area of the 2-4-1 channel to coincide with the coverage area predicted by Hydra when the interfering signal is at the predicted worst case level.

2.38.6.3.5
Reduction of Mobile Radios

Both portable and mobile radios can cause near-far interference.

Mobiles are more likely to create near-far interference since they have a higher transmit power and more efficient antennas than portables. Reduction of mobile use close to the RF Site receiving antenna would decrease their near-far interference impact. Reducing the mobile transmitter power also minimizes the chance of a near-far problem. Carefully balance the power level to the applicable coverage area.

2.38.6.3.6
Additional Frequency Offset

An additional frequency offset of 1 kHz can be programmed into the equipment.

The additional offset causes subscriber inbound signals to be separated by 14.5 kHz with respect to each other. As a result, less noise falls into less noise falling onto the receiver of a base radio from a subscriber on the adjacent channel. The offset should be programmed into transmit frequency of the subscriber, and not the receive frequency of the subscriber. The receive frequency of a base radio must have the added offset, while the transmit frequency of a base radio need not have the additional offset programmed.

For more information on applying for additional frequency offset license, see Application Process on page 282.

2.38.7
MOTOTRBO 2-4-1 Deployment

2.38.7.1
Deployment – New Systems

A new system identifies each 2-4-1 sub-channel as a typical channel.

It is recommended not to use a 2-4-1 channel as a control channel, due to the potential near-far interference.

Although steps can be taken to mitigate and virtually eliminate near-far interference, when it occurs on a control channel, a user with a weak signal cannot access the system until the interferer signal is reduced or eliminated.

2.38.7.2
Deployment – 2-4-1 Retrofit Systems

A retrofitted system regards each added 2-4-1 sub-channel as a typical channel.

A system deployed on typical 25 kHz channels which were retrofitted to two 2-4-1 channels has four operational channels. Because of possible near-far interference, you should not use a 2-4-1 channel as a control channel. Although steps can be taken to mitigate and virtually eliminate near-far interference, when it occurs on a control channel, a user with a weak signal cannot access the system until the interfering signal is reduced or eliminated.

2.38.7.3
Deployment – Transmit Power Verification and Balancing Channels

After installation, the power levels of the two sub-channel base radios must be checked to ensure that the total radiated power on the channel conforms to the power output permitted by the FCC license.

There are no software routines in a base radio to detect a 2-4-1 application and adjust power levels accordingly.

It is important to verify radiated power levels for all channels at the site. In order to balance the coverage area of all channels at the site, the radiated power for each channel must be the same. If this is not done, coverage is worse on the lower powered channels occurs. This phenomenon is difficult to diagnose when the system becomes operational, because users operate in talkgroups that are constantly being reassigned to random channels on a site.

It is also important to balance the gains on the receive paths at the site. One of the primary mitigation techniques for near-far interference is to reduce excess gain in the receive path. If excess gain is removed from the receive path for the 2-4-1 sub-channels, the receive path gain must be matched for all channels at the site.

2.39
Radio Features

2.39.1
Configuring Channel Lock Feature

Channel lock allows to select a button or a menu to lock radio on currently selected channel.

Procedure:

1. In Radio Management, click .
2. Select a preferred radio, and click .
3. Navigate to **Configuration:** ***<Name of a radio>*** → **General** → **Control Buttons**.
4. In the **General** section, in the **Controls Lock** drop-down list, select the preferred lock option.
5. From a drop-down list of a preferred button, select **Keypad Lock**.
6. Click **Save**.
7. Schedule a writing job.

2.39.2
Configuring Wi-Fi Roaming Feature

Wi-Fi Roaming allows to set the roaming aggressiveness for each Wi-Fi Network Security Item. The default value is set to Medium.

Procedure:

1. In Radio Management, click .
2. Select a preferred radio, and click .
3. Navigate to **Configuration:** ***<Name of a radio>*** → **General** → **Wi-Fi Network**.
4. In the **General** section, from a **Roaming Aggressiveness** drop-down list, choose aggressiveness of a radio.
5. Optional: Select **Boost Tx Power** check box to increase the Tx power and reliability.
6. Optional: In the left pane, navigate to **Network**, and in the **WAVE 5000** section, set the preferred **Jitter Voice Buffer (ms)** value.
7. Click **Save**.
8. Schedule a writing job.

2.39.3
Configuring Wi-Fi Certificate Feature

This feature allows a radio to authenticate with the WiFi network by using an MSI installed certificate.

NOTE: This setting is applicable only to Enterprise Wi-Fi WPA/WPA2 profiles.

Procedure:

1. In Radio Management, click .
2. Select a preferred radio, and click .
3. Navigate to **Configuration:** ***<Name of a radio>*** → **General** → **Wi-Fi Network**.
4. In the **Network Profile Table**, select the **MSI Wi-Fi Certificate** check box.
5. Click **Save**.
6. Schedule a writing job.

2.40
Fall Alert

Fall Alert is a channel wide feature that triggers emergency procedures when the radio remains still or in a horizontal position for longer than the pre-programmed time.

The feature uses motion sensors in the radio, which detect the alarm conditions pre-programmed in the system. The feature can be configured to trigger emergency procedures in the following circumstances:

- The radio user does not move.
- The radio moves more than what is considered standard.

- The radio is positioned at a different angle than usual.

If the alarm conditions are fulfilled, the Pre Alert timer starts. If it expires after a pre-programmed time, the Alert timer starts. When the Alert timer expires, the radio initiates emergency by alarming the operator.

If the alarm conditions are no longer fulfilled before the Alert timer expires (Fall Alert Trigger is canceled), the radio does not initiate Emergency.

2.40.1
Configuring Fall Alert in RM

Perform the following steps to configure Fall Alert feature on your subscriber in Radio Management (RM).

Procedure:

1. In the RM application in the Radio View, right-click the subscriber on which you want to enable the Fall Alert feature.
2. Select **Edit configuration**.
3. From the **Set Categories** navigation tree, select **Fall Alert** → **Fall Alert Profiles**.
4. In the **General** section, select a type of emergency trigger in **Type** and customize the alarm properties depending on your requirements.
5. From the **Set Categories** navigation tree, select **Zone/Channel Assignment** → **Zone** → **Zone1**.
6. Right-click the channel on which you want to enable the feature and select **Edit**.
7. In the **TX** section, select an item from **Emergency System** depending on your requirements.

   NOTE: This action enables the **Fall Alert Profile** setting in the **General** section.
8. In the **General** section, select an item from the **Fall Alert Profile** list depending on your requirements.
9. At the top of the tab, click **Save**.
10. Return to Radio View.

Postrequisites: Schedule Write jobs for the devices with the edited configuration.

2.41
Inband Data Services

Inband Data Services features let the users inform each other about their location, and manage their User Names (Aliases) established to facilitate the mutual identification during voice calls.

Caller Alias and Caller Location

Features that enable the transmitting unit to send out its User Name (Alias) simultaneously with the voice transmission. The feature is available for any type of voice call. The transmitted alias is received, logged, and displayed by the receiving units.

The transmitting unit can also send out its location (inband location) while on a voice call. The inband location update can be triggered from the location application. There are two types of such triggers:

- every voice transmission
- emergency voice only

The feature is available on all system types, except for Connect Plus and Digital Repeater Backhaul (DRB).

Dynamic Caller Alias

A feature that enables a dynamic assignment of a User Name (Alias) to the radio for the duration of the shift.

2.41.1 Configuring Caller Alias in Radio Management

Perform the following steps in Radio Management (RM) application to enable the Caller Alias feature on a subscriber.

Procedure:

1. In Radio View, select a subscriber on which you want to enable the feature, and click **Edit**.
2. From the **Set Categories** tree, select **General** → **General Settings**.
3. In the **General** section, set **TX Caller Alias** to **With UTF-8** or **With UTF-16BE**, according to your preferences.

   Selecting any of the options other than the default **No** value enables the **Caller Alias** field.
4. From the **Edit Caller Alias** drop-down list, choose the value according to your preferences.
5. Click **Save**.
6. To go to the Radio View screen, click the radio icon.
7. In the **Caller Alias** field, enter the Alias of the subscriber that you want to transmit.

   NOTE: This value cannot be empty. Furthermore, the maximum length of the caller alias is 16 characters for UTF-8 format, and 13 characters for UTF-16BE format.

Postrequisites:
Schedule Write jobs for the subscribers with the edited configuration.

2.42 Data Security Between the RM and the Devices

The following section describes the method for securing the flow of configuration parameters between the Radio Management (RM) and the targeted devices, such as Subscriber Units (SU) and Repeaters.

Securing includes the following features:

- Radio Management delivers parameters only to authenticated devices.
- A secured device receives parameters only from an authenticated RM.
- Reading of parameters from a secured device and writing parameters into a secured device are protected.

Data Security is a configurable option for a device. The RM allows you to select Codeplug transfer mode for a device as either Standard or Enhanced. This is a device-wide parameter. The default value is Standard. Enhanced mode requires attaching the master key to the device.

Standard State

By default, the device is in **Standard** state. The configuration parameters are read from or written into a device without changes in the existing procedures. The existing protection mechanisms, for example Certificate based TLS for Remote Repeater Programming (RRP) or password protection of radios, continue to operate.

Standard to Enhanced State

When the transfer of a codeplug is successful, and the option selected for the **Codeplug Transfer Mode** is set as **Enhanced**, the device enters the **Enhanced** state after the transferred codeplug becomes active. You can use the USB Connection, IP, WiFi, and Over-the-Air Programming (OTAP) to configure the

Pre-shared Key into a device in the **Standard** state. However, the recommended method is through the USB connection in a physically secure environment.

Enhanced State

In the **Enhanced** state, a device allows its codeplug to be read or written only by an application that uses the TLS-PSK protocol, such as RM. The TLS-PSK is described in RFCs 4279 and 5246. A summary of the procedure with the options selected for this implementation is described in the TLS-PSK section. The procedure uses the TLS-PSK for mutual authentication between the application and the device. During mutual authentication, both parties generate session keys which are used for protecting the rest of their messages.

NOTE: TLS-PSK protocol is not used to access DR 3000/MTR3000 codeplug through the USB connection.

2.42.1
Key Management

The TLS-PSK based authentication, which is a key establishment between the Radio Management (RM) and a device, relies on a symmetric key that is shared between the device and the RM. Each device has a unique key, which is obtained from a Master Key (MK) and added to the device through the RM. The main advantage of using the MK is that it is possible to manage authentication for all devices with one key only.

2.42.2
Adding the Pre-shared Key to the Radio Management

The pre-shared key is a unique key derived for the device from the master key associated with the device.

Procedure:

1. In the **Radio Management** window, select → **Manage** → **Pre-shared Keys**.
2. Click .
3. In the **Add Pre-shared Key** dialog box, provide at least one 128-bit Master Key and its unique Key ID. Click **OK**.

2.42.3
Securing Devices

The Radio Management (RM) retrieves a 128-bit key for each device using the specified Master Key (MK) and the ID of the device as per the algorithm described in FIPS PUB 198-1, and delivers the key and the ID of the Master Key to the device. The PSK ID/Alias is a 128-bit field in the codeplug up to 16 ASCII characters, while the PSK data is a 128-bit value.

Prerequisites: Ensure that the pre-shared key is added to the RM. See Adding the Pre-shared Key to the Radio Management on page 295.

Procedure:

1. In the **Radio Management** window, select → **Manage** → **Configurations**.
2. Select a device and click .
3. Select **Configuration:** ***<Device name>*** → **General** → **Security**.
4. Under **TLS-PSK Authentication**, in the **Security Mode** drop-down list, select **Enhanced**.

5. In the **TLS-PSK** drop-down list, select the ***<Pre-shared key>***.

   NOTE: The default value for **TLS-PSK** is **Default Key** and it can be used for the **Standard** Codeplug Transfer Mode. The **Enhanced** mode requires the pre-shared key.

6. Click **Save**.

2.43 Performing Repeater Factory Reset

The Factory Reset functionality enables you to reset the device to its factory default settings, except for licenses. Any user configured data will be cleared including: Pre-shared Key, RAS, HMAC, web server credentials. Each time the factory reset is completed successfully, the repeater restarts immediately, otherwise the default configuration might not be applied and a suitable error code appears.

Follow this procedure to perform the factory reset of the repeater.

NOTE: To perform this procedure, a repeater must be connected to a PC by using a USB cable.

Procedure:

1. Open the AT debug console by performing the following actions:
   a. By using a USB cable, connect your PC to the repeater.
   b. In Radio Management (RM), locate the **Radio IP address** field of the preferred repeater.
   c. By using a ***<Radio IP address>*** and the 8501 port, establish a telnet connection to the repeater.

   NOTE: The Radio IP address can be established only if repeater drivers are installed.

2. Perform one of the following actions:
   - To reset repeater configuration for SLR Series Repeaters, issue the command `reset_web_credentials`
   - To reset the sensitive data for DR 3000/MTR 3000, issue the command `factory_reset` Only the following data are restored to the default values:
     - Web server username and password,
     - Web server private key and certificate,
     - Web server session duration time,
     - TLS-PSK Primary key,
     - HMAC authentication key,
     - RAS key and mode.

   NOTE: Factory Reset for DR 3000/MTR 3000 does not reset whole repeater configuration.

   NOTE: If the `reset_web_credentials` and `factory_reset` commands fail, you can send the error code to the support team.

Chapter 3

System Components and Topologies

Table 65: System Components and Topologies

System	Description
IPSC	Indicates IP Site Connect feature related content.
CPSS	Indicates Capacity Plus Single Site feature related content.
CPMS	Indicates Capacity Plus Multi Site feature related content.
CPSM	Indicates Capacity Plus Single Site AND Capacity Plus Multi Site shared feature related content.

3.1
System Components

MOTOTRBO consists of numerous components and applications that function together in a system. The first step in designing a system that satisfies the customer's needs is identifying the devices and applications within the system, and then choosing a basic system configuration of how these components will be interconnected. This section defines the different components and applications available, their offered services, and their roles in the system. Some of the standard system topologies that MOTOTRBO supports are described.

All data application modules contained in this system planner are depictions of typical third-party data application modules and have been included simply to illustrate certain MOTOTRBO application enabling features.

3.1.1
Fixed End Components

The system contains devices with fixed locations and other devices that are mobile. This subsection covers the devices with fixed locations.

3.1.1.1
Repeater

The MOTOTRBO repeater provides an RF interface to the field subscribers.

The repeater is AC and DC-powered and designed to be discreetly mounted on a standard 19" rack found in most communication tower locations. It offers front panel indicators of its current status including real time transmit and receive indicators for each time slot. Once configured through the Customer Programming Software (CPS), the repeater is designed to operate behind the scenes and without the need for further user interaction.

The repeater can either be configured as a standalone repeater or as a repeater connected to a back-end network, as in the case of IP Site Connect, Capacity Plus Single Site, and Capacity Plus Multi Site modes. As a repeater, it listens on one uplink frequency, and then re-transmits on a downlink frequency. Therefore a pair of RF frequencies is required for each repeater in the system.

A major advantage of using a repeater in the system is that it allows a greater communication range than would be possible talking from subscriber to subscriber. Multiple repeaters can be installed in strategic locations for the users' coverage to be consistent throughout their required range of operation. However, only in IP Site Connect mode, do the radios seamlessly roam between repeaters. In digital repeater mode, the users must know the coverage range provided by each repeater, and manually switch channels when necessary.

The repeater is capable of operating in either digital mode, analog mode, or in Dynamic Mixed Mode. This is determined at the initial configuration, and is not updated dynamically. Therefore at any given time, it either operates as a digital repeater, as an analog repeater, or as a Dynamic Mixed Mode repeater.

When configured for analog operation, the repeater is designed to operate with existing analog systems, therefore making migration to a MOTOTRBO system smoother.

When configured for digital operation, the repeater offers additional services. The digital repeater operates in TDMA mode, which essentially divides one channel into two virtual channels using time slots; therefore the user capacity is doubled. The repeater utilizes embedded signaling to inform the field radios of the busy/idle status of each channel (time slot), the type of traffic, and even the source and destination information.

Another advantage during digital operation is error detection and correction. The further a transmission travels, the more predominant the interference becomes, and inevitably more errors are introduced. The receiving MOTOTRBO radio, operating in digital mode, utilizes built-in error detection and correction algorithms, native to the protocol, to correct these problems. The MOTOTRBO repeater uses the same algorithms to correct the errors prior to retransmission, thus repairing any errors that occur on the uplink; it then transmits the repaired signal on the downlink. This greatly increases the reliability and audio quality in the system, which increases the customer's coverage area.

In digital mode, the repeater only retransmits digital signals from radios configured with the same system identifier. This aids in preventing co-system interference. The repeater does not block transmissions of radios within its own system.

As previously described, the repeater utilizes embedded signaling to announce the current status of each channel. It is up to the radios in the field to interpret these signals, and grant or deny their user's request for transmission. Therefore, when a user or a group of users utilizes a channel (time slot), the repeater announces that the channel is being used and who is using it. Only radios that are part of that group are allowed to transmit. The repeater additionally allows a short duration of reserved time after a transmission. This allows other users in the group to respond to the originator. This reserved hang time greatly improves the continuity of calls, because new calls cannot start until the previous call ends. Without this feature, users may experience delays in responses (that is, between transmissions of calls), due to other calls taking over the channel in-between their transmissions.

After this reserved hang time, the repeater continues to monitor for a short period. If no user transmits on the channel for a duration of time, the repeater stops transmitting. When the next radio transmission occurs, the repeater begins repeating again.

In Dynamic Mixed Mode, the repeater dynamically switches between analog and digital calls. When a repeater repeats a new digital call that starts on one of the logical channels, the repeater does not qualify any analog call including an Emergency Call until the digital call (both the transmission and call hang time) is over and the corresponding channel hang time has expired. Upon the expiry of channel hang time, only then does the repeater start qualifying both analog and digital calls simultaneously. Similarly, if an analog call is being repeated, the repeater does not qualify any digital call including digital data and Emergency Calls on any of the two logical channels until the analog call is over and the corresponding hang time has expired.

The repeater 4-wire interface and Over-The-Air digital calls are polite to each other. If the PTT button or knockdown GPIO pin is asserted on the repeater 4-wire interface while a digital transmission is ongoing, then

an audible channel busy alert tone is generated on the speaker pin of the 4-wire interface. The PTT button press or pin knockdown operation is denied.

System	Description
IPSC IP Site Connect	In IP Site Connect, the repeaters perform the following additional duties: ● Each repeater ensures that their communication links with other repeaters are open all the time. ● They disclose their operating status (for example mode, IPv4/UDP address) to each other. ● In IP Site Connect mode, repeaters ensure that in cases of multiple calls starting within a short period, only one call per destination prevails at all the associated sites and all of them (except those that detect interference) repeat the selected call. ● They inform their alarm conditions and provide diagnostic information to the RDAC application. The RDAC application allows its user to remotely change the mode of a repeater.
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	In CPSS and CPMS, the repeaters perform the following additional duties: ● Each repeater ensures that their communication links with other repeaters are open all the time. ● They inform their operating status (for example mode, IPv4/UDP address) to each other. In CPSS and CPMS, repeaters also inform the status of their logical channels to each other. Based on this status, a repeater selects the next Rest Channel. ● They inform their alarm conditions and provide diagnostic information to the RDAC application. The RDAC application allows its user to remotely change the mode of a repeater.
CPMS Capacity Plus Multi Site	In CPMS mode, repeaters ensure that in cases of multiple calls starting within a short period, only one call per destination prevails at all the associated sites and all of them (except those that detect interference) repeat the selected call.

3.1.1.2
MTR3000 Base Station/Repeater

System	Description
IPSC IP Site Connect	MOTOTRBO MTR3000 Base Station/Repeater supports DMR 2 Tier 2 Conventional –IP Site Connect configurations.
CPSS Capacity Plus Single Site	MOTOTRBO MTR3000 Base Station/Repeater supports Capacity Plus Single Site Trunking configurations.

System	Description
CPMS Capacity Plus Multi Site	MOTOTRBO MTR3000 Base Station/Repeater supports Capacity Plus Multi Site Trunking configurations.

The MOTOTRBO MTR3000 base station/repeater provides a modular, flexible analog and digital station designed for today's communication systems and for the future.

The MTR3000 is an integrated data and voice base station/repeater designed to deliver increased capacity, spectral efficiency, integrated data applications and enhanced voice communications. The base stations are available for use in the following configurations:

- Analog Conventional
- Digital (MOTOTRBO)
  - MOTOTRBO DMR Tier 2 Conventional – Single Site
  - MOTOTRBO DMR Tier 2 Conventional – IP Site Connect
  - MOTOTRBO Capacity Plus Single Site Trunking
  - MOTOTRBO Capacity Plus Multi Site Trunking
  - MOTOTRBO Connect Plus Trunking
  - MOTOTRBO Transmit Interrupt
  - MOTOTRBO Dynamic Mixed Mode (DMM)
  - MOTOTRBO Enhanced GPS
- LTR Trunking
- Passport Trunking

3.1.1.2.1
MTR3000 Key Features

Key features for the UHF and 800/900 MHz release:

- Wireline Card (supports integrated Tone Remote and DC Remote Control)
- Analog RSSI
- Hear clear (800/900 MHz only)
- MTR2000 MOTOTRBO Digital Upgrades for low and high power stations

Standard features for the UHF and 800/900 MHz release:

- Operates in analog or MOTOTRBO digital mode with a LED indicating mode of operation
- Migration path from analog to digital mode
- 12.5 kHz or 25 kHz programmable channel spacing
- Operation down to 8 W
- Reliable 100 W Continuous Duty Cycle Operation
- Analog and digital conventional are all standard in one base station without the cost of additional software or hardware
- Restriction of Hazardous Substances (RoHS) compliant

- Switching power supply functions over a wide range of voltages and frequencies

3.1.1.2.2
MTR3000 Standard Features

The following are standard features for the UHF and 800/900 MHz release:

- Operates in analog or MOTOTRBO digital mode with a LED indicating mode of operation
- Migration path from analog to digital mode
- 12.5 kHz or 25 kHz programmable channel spacing
- Operation down to 8 W
- Reliable 100 W Continuous Duty Cycle Operation
- Analog and digital conventional are all standard in one base station without the cost of additional software or hardware
- Restriction of Hazardous Substances (RoHS) compliant
- Switching power supply functions over a wide range of voltages and frequencies

3.1.1.2.3
MTR3000 Programmed in MOTOTRBO Mode

- Supports two simultaneous voice paths in digital 12.5 kHz TDMA
- Divides an existing channel into two timeslots delivering twice the capacity through a single repeater
-

System	Description
IPSC IP Site Connect	MTR3000 programmed in MOTOTRBO mode supports IP Site Connect for increased wide area coverage.
CPSS Capacity Plus Single Site	MTR3000 programmed in MOTOTRBO mode supports Capacity Plus Single Site Trunking without a separate hardware controller.
CPMS Capacity Plus Multi Site	MTR3000 programmed in MOTOTRBO mode supports Capacity Plus Multi Site Trunking without a separate hardware controller.

- Supports MOTOTRBO Dynamic Mixed Mode to facilitate your analog-to-digital migration in conventional repeater applications
- Supports MOTOTRBO Transmit Interrupt for greater subscriber unit control and flexibility

3.1.1.2.4
MTR3000 Serviceability

- Repeater diagnostic and control software provides remote or local site monitoring
- Easy to replace components with functionally separate Field Replaceable Units (FRU)
- Software-based design simplifies feature upgrades

- Easy access to station ports (no need to remove the front panel) shortening installation and maintenance time
- For ease of installation, minimal station alignment is needed
- Supported by Motorola Solutions 2-year standard warranty

3.1.1.2.5
Total Cost of Ownership

- Analog Conventional, Digital Conventional are standard in one base station without the cost of additional software
- Twice the spectral efficiency; one frequency pair provides two logical voice paths
- Effectively twice the power efficiency as compared to two analog stations when operating in digital mode
- Integrated Components optimizes expensive site space; one physical station provides the capacity of two in digital mode

3.1.1.2.6
Wireline Interface Board

The MTR3000 Wireline board is used to connect an analog audio source and sink (such as a console) to the MTR3000 Base Station/Repeater. The Wireline board supports Tone and DC.

Remote Control modes that allow for channel selection and PTT signaling from compatible consoles. Local PTT operation is also supported. The Wireline can be configured for either 2-wire or 4-wire operation as needed.

The table below provides a description of the impedance supported by the Wireline board.

Table 66: Description of the Impedance Supported by the Wireline Board

Option	Functionality
High Impedance	For use with an external impedance matching
600 Ω	For Argentina, Canada, Chile, Columbia, Ecuador, El Salvador, Guam, Hong Kong, India, Indonesia, Japan, Jordan, Kazakhstan, Kuwait, Macao, Malaysia, Mexico, Oman, Pakistan, Peru, Philippines, Russia, Saudi Arabia, Singapore, South Korea, Taiwan, Thailand, UAE, USA and Yemen
270 Ω + (150 nF || 750 Ω)	For Austria, Belgium, Denmark, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Bahrain, Croatia, Cyprus, Czech Republic, Egypt, Hungary, Israel, Latvia, Lebanon, Malta, Morocco, Nigeria, Poland, Romania, Slovakia and Slovenia
220 Ω + (115 nF || 820 Ω)	For Australia, Bulgaria and South Africa
370 Ω + (310 nF || 620 Ω)	For New Zealand
900 Ω	For Brazil
320 Ω + (230 nF || 1050 Ω)	For United Kingdom
200 Ω + (100 nF || 680 Ω)	For China
900 Ω || 30 nF	For legacy MTR2000

3.1.1.2.7
Repeater Specifications

The MOTOTRBO repeater is currently available in 12.5 kHz or 20/25 kHz operation in analog, or 12.5 kHz in digital. The table below shows the available repeater bands and associated power levels that are currently supported.

Table 67: Repeater Specifications for DR 3000

DR 3000			
Dimensions (h x l x w)		5.25“ x11.75” x19” (133.35mm x 298.45mm x 482.59mm)	
Weight		14 kg (31 lbs)	
Power (watts)	UHF 1	1 – 25	25 – 40
	UHF 2	1 – 40 (up to 512 MHz)	1 – 25 (above 512 MHz)
	VHF	1 – 25	25 – 45
	350 MHz	25 – 40	
	800 MHz	1 – 30	

Table 68: Repeater Specifications for MTR3000

MTR3000			
Dimensions (h x l x w)		5.25"x16.5”x19” (133.35mm x 419.09mm x 482.59mm)	
Weight		19 kg (42 lbs)	
Power		UHF 1/UHF 2	800/900 MHz	VHF
		8 – 100 W	8 – 100 W	8 – 100 W

3.1.1.3
MTR3000 Satellite Receiver

The MTR3000 Satellite Receiver, unlike the base station/repeater, – provides a modular, flexible analog and digital station designed for today's communication systems and for the future. It is designed to eliminate “dead zones” in a communications system by improving the “talk-in” coverage on a particular receive frequency when used in a receiver voting system.

Like the Base Station/Repeater, the Satellite Receiver is divided into functional modules that separate the frequency band specific functions (for example, RF receive) from that of non-frequency specific functions (for example, station control, user audio and GPIO interface, power system, and others).

The satellite receiver is divided into functional modules that separate the frequency band specific and control circuits. These modules are self-contained functional blocks with module-specific alarms. This design facilitates the field replaceable unit (FRU) concept of field repair to maximize system uptime.

The satellite receiver (T7713A) contains the following:

- Receiver Module
- Station Control Module
- Power Supply Module

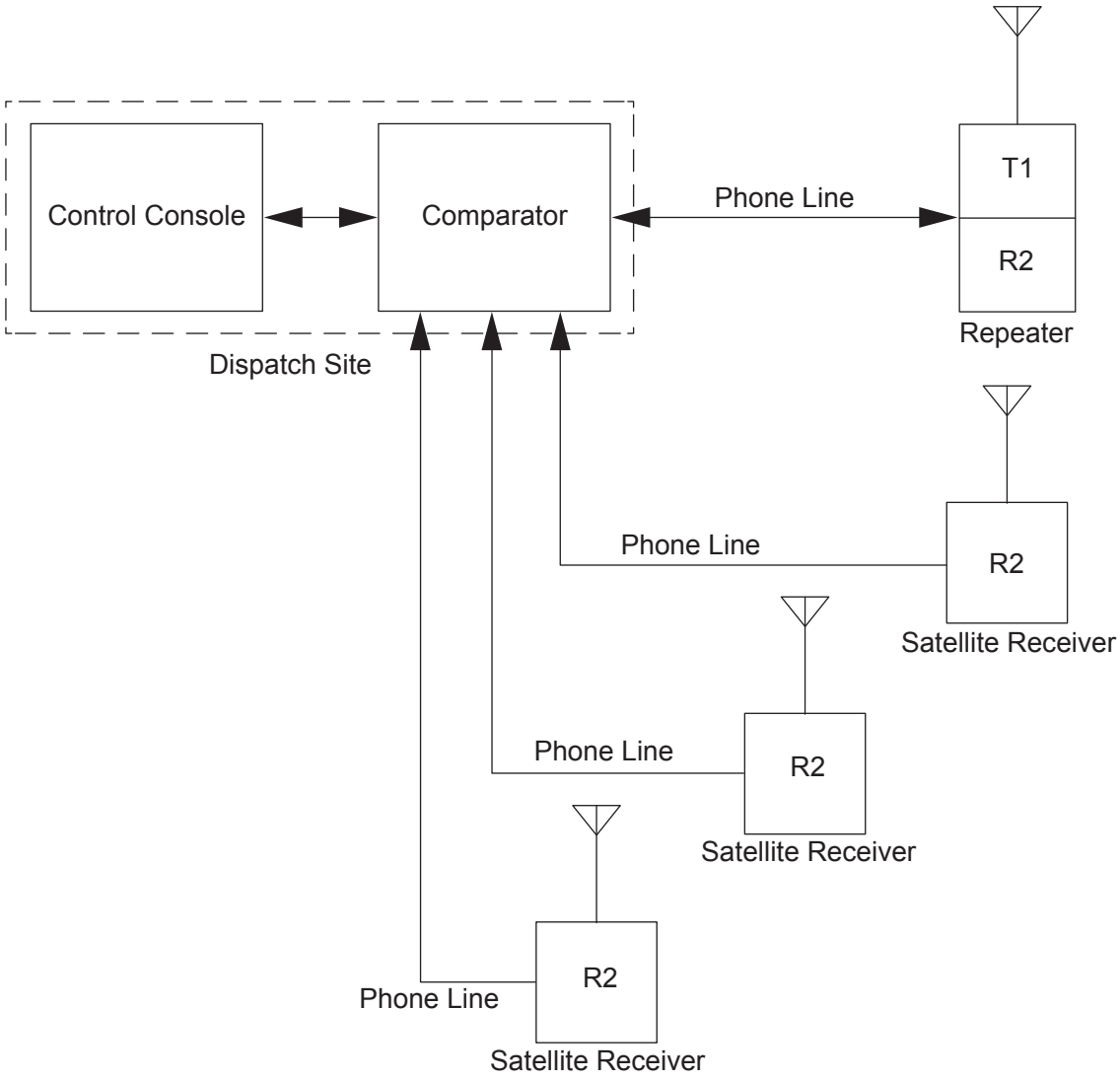
- Backplane Board
- Wireline Board (standard)

NOTE: The MTR3000 Satellite Receiver does not contain a transmitter, however, the RDAC application is supported in local and remote network connections. support any transmitter subsystems or digital communications functionality. However, the RDAC application is supported in local and remote network connections.

3.1.1.3.1
Satellite Receiver System

Typically, the satellite receiver connects to a Spectra-TAC™ or a DigiTAC™ comparator.
Figure 84: Satellite Receiver Connections Within a Voting System on page 304 shows a typical voting system and the connections of the satellite receivers.

Figure 84: Satellite Receiver Connections Within a Voting System



3.1.1.4
SLR 1000 Series Repeater

NOTE: This feature is supported only by specific product model.

System	Description
IPSC IP Site Connect	MOTOTRBO SLR 1000 Series Repeater supports DMR Tier 2 Conventional – IP Site Connect configurations.
CPSS Capacity Plus Single Site	MOTOTRBO SLR 1000 Series Repeater supports Capacity Plus Single Site Trunking configurations
CPMS Capacity Plus Multi Site	MOTOTRBO SLR 1000 Series Repeater supports Capacity Plus Multi Site Trunking configurations.

The SLR 1000 repeater allows for easy expansion of the network and is ideal for addressing areas with little to no coverage. The SLR 1000 is IP65-rated for dust and water protection, and can be deployed indoors and outdoors. The compact size allows for more installation options, and the low power, fanless design takes little space and energy.

Figure 85: SLR 1000 Series Repeater

3.1.1.4.1
Description

The station is available for use in these configurations:

- Analog Conventional
- Digital (MOTOTRBO)

- MOTOTRBO DMR Tier 2 Conventional – Single Site
- MOTOTRBO DMR Tier 2 Conventional – IP Site Connect
- MOTOTRBO Capacity Plus Trunking
- MOTOTRBO Connect Plus Trunking
- MOTOTRBO Capacity Max Trunking
- MOTOTRBO Digital Voting

NOTE: Certain software features enabled through Radio Management can be configured with the Online Help or with a regional representative. See the regional Ordering Guide to determine the features available within the respective regions.

The repeater can either be configured as a stand-alone repeater or as a repeater connected to a network, as in the case of operating in IP Site Connect mode. As a repeater, it listens on one uplink frequency, and then re-transmits on a downlink frequency, thus providing the RF interface to the field subscribers. When configured for analog station operation, the repeater is designed to operate with most existing analog systems, which enables a smooth migration to the MOTOTRBO system.

When configured for digital operation, the repeater offers additional services. The digital repeater operates in TDMA mode, which essentially divides one channel into two virtual channels using time slots; therefore the user capacity is doubled. The repeater utilizes embedded signaling to inform the field radios of the busy/idle status of each channel (time slot), the type of traffic, and even the source and destination information.

3.1.1.4.2
Operating Features

The SLR 1000 Repeater model provides the following features and interfaces.

Standard Features

- MOTOTRBO Conventional Operation (2-Slot TDMA, 4FSK Modulation)
- Analog Conventional Operation (FM)
- Continuous Duty Cycle Operation over -30 °C to +60 °C
- Meets or exceeds the following standards:
  - TIA603E
  - ETSI 086
  - ETSI 113
  - ETSI TS 102 361-1 Part 1: DMR Air Interface Protocol
  - ETSI TS 102 361-2 Part 2: DMR Voice and Generic Services and Facilities
  - ETSI TS 102 361-3 Part 3: DMR Packet Data Protocol
  - ETSI TS 102 361-4 Part 4: DMR Trunking Protocol
- Synthesized Frequency Generation
- Female N-type Antenna Connector (Tx)
- Female N-type Antenna Connector (Rx)
- Ethernet Port (Network)
- USB Port (Service)
- Four configurable GPIO ports (Digital)
- One configurable GPI port (Analog)

- One configurable GPO port (Analog)
- 1.5 PPM Frequency Stability (temperature AND 1-year aging) (VHF and UHF)
- Station Diagnostic Tests – fixed set of tests run upon start-up
- Physical Dimensions: 11" H x 9" W x 4" D (27.94 x 22.86 x 10.16 cm) without brackets or other peripheral equipment
- Weight: 10 pounds (4.56 kg) excluding other peripheral equipment

Motorola Solutions Network Interface

- IP Site Connect
- Repeater Diagnostics and Control (RDAC)
- Capacity Plus
- Connect Plus
- Capacity Max

Third Party Controller Interface

- Tone Remote Adapter

Additional Features

These features are shipped in a preset condition, but may be altered through the use of Radio Management.

- 64 Tx/Rx Frequencies – factory programmed with 1 Tx, 1 Rx
- 12.5 kHz or 25 kHz Operation – factory programmed to 12.5 kHz
- One Tx and one Rx (PL or DPL) Squelch Code per channel – factory programmed to CSQ
- Base Station Identification (BSI) – factory programmed as “BLANK” (“BLANK” disables BSI)
- Push-To-Talk (PTT) Priority – factory programmed to repeat path

3.1.1.5

SLR 5000 Series Repeater

NOTE: This feature is supported only by specific product model.

System	Description
IPSC IP Site Connect	MOTOTRBO SLR 5000 Series Repeater supports DMR Tier 2 Conventional – IP Site Connect configurations.
CPSS Capacity Plus Single Site	MOTOTRBO SLR 5000 Series Repeater supports Capacity Plus Single Site Trunking configurations
CPMS	MOTOTRBO SLR 5000 Series Repeater supports Capacity Plus Multi SiteTrunking configurations.

System	Description
Capacity Plus Multi Site	

The SLR 5000 Series is Motorola Solutions Next-Generation integrated voice and data MOTOTRBO Repeater designed to meet the needs of professional and commercial radio operators. It offers significant improvements in Reliability, Performance and Serviceability in a more Eco-friendly design. The SLR 5000 will reuse much of the MOTOTRBO Suite of tools such as Customer Programming Software (CPS) and Remote Diagnostics and Control (RDAC) that today's customers are already familiar with, and will support all the features and functionality of today's XPR/XiR/DGR/DR products.

Figure 86: SLR 5000 Series Repeater

The Motorola Solutions SLR 5000 Series Repeater provides a modular, flexible analog and digital station designed for today's communication systems and for the future. The station is available for use in the following configurations:

- Analog Conventional
- Digital (MOTOTRBO)
  - MOTOTRBO DMR Tier 2 Conventional – Single Site
  - MOTOTRBO DMR Tier 2 Conventional – IP Site Connect
  - MOTOTRBO Capacity Plus Single Site Trunking
  - MOTOTRBO Capacity Plus Multi Site Trunking
  - MOTOTRBO Connect Plus Trunking
  - MOTOTRBO Capacity Max Trunking
  - MOTOTRBO Digital Voting
- LTR Trunking
- Passport Trunking
- MPT1327 Trunking

The SLR 5000 series can either be configured as a stand-alone repeater or as a repeater connected to a back-end network, as in the case of operating in IP Site Connect mode. As a repeater, it listens on one uplink frequency, and then re-transmits on a downlink frequency, thus providing the RF interface to the field subscribers. When configured for analog station operation, the repeater is designed to operate with most existing analog systems, which enables a smooth migration to the MOTOTRBO system.

When configured for digital operation, the repeater offers additional services. The digital repeater operates in TDMA mode, which essentially divides one channel into two virtual channels using time slots; therefore the

user capacity is doubled. The repeater utilizes embedded signaling to inform the field radios of the busy/idle status of each channel (time slot), the type of traffic, and even the source and destination information.

The SLR 5000 series facilitates the field replaceable unit (FRU) concept of field repair to maximize system uptime. The FRU concept also aids in allowing the end user/ maintainer to lower their inventory costs. The base model SLR 5000 series FRUs are as follows:

- Modem FRU
- Power Amplifier FRU
- Power Supply FRU
- Front Panel FRU

For more details on the FRUs, see the Basic Service and Installation Manual.

3.1.1.5.1
Operating Features

The following are the standard features of an SLR 5000 series model:

- MOTOTRBO Conventional Operation (2-Slot TDMA, 4FSK Modulation)
- Analog Conventional Operation (FM)
- 1 – 50 W Continuous Duty Cycle Operation over -30 °C to +60 °C
- Meets or exceeds the following standards:
  - TIA603D
  - ETSI 086
  - ETSI 113
  - ETSI TS 102 361-1 Part 1: DMR Air Interface Protocol
  - ETSI TS 102 361-2 Part 2: DMR Voice and Generic Services and Facilities
  - ETSI TS 102 361-3 Part 3: DMR Packet Data Protocol
- AMBE +2™ Digital VOCODER
- Synthesized Frequency Generation
- Female N-type Antenna Connector (Tx)
- Female BNC Antenna Connector (Rx)
- Ethernet Port (Network)
- Front mounted USB Port (Service)
- 12 configurable GPIO ports (Digital)
- 4 configurable GPI ports (Analog, Not Supported in Initial Release)
- 2 configurable GPO ports (Analog, Not Supported in Initial Release)
- Power for third-party controllers (1 Amp)
- 1.5 PPM Frequency Stability (Temperature AND 1-Year Aging) (VHF and UHF)
- External Reference Capability
- Real-Time Clock with rechargeable backup battery
- Switching Power Supply operates from 85 – 264 VAC (47 – 63 Hz)
- Multi-Power Source configurable (AC, DC, or AC with Battery Revert)
- Integrated 3 A battery charger

- Station Diagnostic Tests – Fixed Set of Tests run upon Start-up
- Physical Dimensions: 1.75" H x 19" W x 14.6" D (44 x 483 x 370 mm) 1RU
- Weight: 19 pounds (8.62 kg) excluding cabinet or other peripheral equipment

Network Application Interface:

- IP Site Connect
- Repeater Diagnostics and Control (RDAC)
- Capacity Plus Single Site
- Capacity Plus Multi Site
- Connect Plus

Third-Party Controller Interface:

- Phone Patch
- Multi Coded Squelch Interface (Repeater Panel)
- Tone Remote Adapter
- LTR Trunking
- Passport Trunking
- MPT1327 Trunking

In addition, the following features are also included. These features are shipped in a preset condition, but may be altered through the use of the CPS.

- 64 Tx/Rx Frequencies – Factory Programmed with 1 Tx, 1 Rx
- 12.5 kHz or 25 kHz Operation – Factory Programmed to 12.5 kHz
- 1 Tx and 1 Rx (PL or DPL) Squelch Code per channel – Factory Programmed to CSQ
- Base Station Identification (BSI) – Factory Programmed as “BLANK” (“BLANK” disables BSI)
- Push-To-Talk (PTT) Priority – Factory Programmed to Repeat Path

3.1.1.6
SLR 8000 Series Repeater

NOTE: This feature is supported only by specific product model.

System	Description
IPSC IP Site Connect	MOTOTRBO SLR 8000 Series Repeater supports DMR Tier 2 Conventional – IP Site Connect configurations.
CPSS Capacity Plus Single Site	MOTOTRBO SLR 8000 Series Repeater supports Capacity Plus Single Site Trunking configurations.
CPMS	MOTOTRBO SLR 8000 Series Repeater supports Capacity Plus Multi Site Trunking configurations.

System	Description
Capacity Plus Multi Site	

The SLR 8000 Series is Motorola Solutions Next-Generation integrated voice and data MOTOTRBO Repeater designed to meet the needs of professional and commercial radio operators. It offers significant improvements in Reliability, Performance and Serviceability in a more Eco-friendly design. The SLR 8000 will reuse much of the MOTOTRBO Suite of tools such as Customer Programming Software (CPS) and Remote Diagnostics and Control (RDAC), that today's customers are already familiar with, and will support all the features and functionality of today's XPR/XiR/DGR/DR products.

Figure 87: SLR 8000 Series Repeater

The Motorola Solutions SLR 8000 Series Repeater provides a modular, flexible analog and digital station designed for today's communication systems and for the future. The station is available for use in the following configurations:

- Analog Conventional
- Analog Voting
- Digital (MOTOTRBO)
  - MOTOTRBO DMR Tier 2 Conventional – Single Site
  - MOTOTRBO DMR Tier 2 Conventional – IP Site Connect
  - MOTOTRBO Capacity Plus Single Site Trunking
  - MOTOTRBO Capacity Plus Multi Site Trunking
  - MOTOTRBO Connect Plus Trunking
  - MOTOTRBO Digital Voting
  - MOTOTRBO Capacity Max Trunking
- MOTOTRBO Dynamic Mixed Mode (DMM)
- LTR Trunking
- Passport Trunking
- MPT1327 Trunking

The SLR 8000 series can either be configured as a stand-alone repeater or as a repeater connected to a back-end network, as in the case of operating in IP Site Connect mode. As a repeater, it listens on one uplink frequency, and then re-transmits on a downlink frequency, thus providing the RF interface to the field

subscribers. When configured for analog station operation, the repeater is designed to operate with most existing analog systems, which enables a smooth migration to the MOTOTRBO system.

When configured for digital operation, the repeater offers additional services. The digital repeater operates in TDMA mode, which essentially divides one channel into two virtual channels using time slots; therefore the user capacity is doubled. The repeater utilizes embedded signaling to inform the field radios of the busy/idle status of each channel (time slot), the type of traffic, and even the source and destination information.

The SLR 8000 series facilitates the field replaceable unit (FRU) concept of field repair to maximize system uptime. The FRU concept also aids in allowing the end user/ maintainer to lower their inventory costs. The SLR 8000 series repeater supports an optional Wireline Board FRU. The Wireline board supports Tone Remote Control and DC Remote Control, E&M control, and analog voting modes. The base model SLR 8000 series FRUs are as follows:

- Modem FRU
- Power Amplifier FRU
- Power Supply FRU
- Front Panel FRU

For more details on the FRUs, see the Basic Service and Installation Manual.

3.1.1.6.1
Operating Features

The following are the standard features of an SLR 8000 series model:

- MOTOTRBO Conventional Operation (2-Slot TDMA, 4FSK Modulation)
- Analog Conventional Operation (FM)
- 1 – 100 W Continuous Duty Cycle Operation over -30 °C to +60 °C
- Meets or exceeds the following standards:
  - TIA603D
  - ETSI 086
  - ETSI 113
  - ETSI TS 102 361-1 Part 1: DMR Air Interface Protocol
  - ETSI TS 102 361-2 Part 2: DMR Voice and Generic Services and Facilities
  - ETSI TS 102 361-3 Part 3: DMR Packet Data Protocol
- AMBE +2™ Digital VOCODER
- Synthesized Frequency Generation
- Female N-type Antenna Connector (Tx)
- Female BNC Antenna Connector (Rx)
- Ethernet Port (Network)
- Front mounted USB Port (Service)
- 12 configurable GPIO ports (Digital)
- 4 configurable GPI ports (Analog, Not Supported in Initial Release)
- 2 configurable GPO ports (Analog, Not Supported in Initial Release)
- Power for third-party controllers (1 Amp)
- 1.5 PPM Frequency Stability (Temperature AND 1-Year Aging) (VHF and UHF)
- Wireline Capability

- External Reference Capability
- Real-Time Clock with rechargeable backup battery
- Switching Power Supply operates from 100 – 240 VAC (47 – 63 Hz)
- Dual DC Power Supply Systems 12 V or 24 V
- Multi-Power Source configurable (AC, DC, or AC with Battery Revert)
- Integrated 5 A battery charger
- Station Diagnostic Tests – Fixed Set of Tests run upon Start-up
- Physical Dimensions: 3.5" H x 19" W x 17.3" D (89 x 483 x 438 mm) 1RU
- Weight: 31 pounds (14.06 kg) excluding cabinet or other peripheral equipment

Network Application Interface:

- IP Site Connect
- Repeater Diagnostics and Control (RDAC)
- Capacity Plus Single Site
- Capacity Plus Multi Site
- Connect Plus

Third-Party Controller Interface:

- Phone Patch
- Multi Coded Squelch Interface (Repeater Panel)
- Tone Remote Adapter
- LTR Trunking
- Passport Trunking
- MPT1327 Trunking

Optionally, the SLR 8000 repeater may be configured with the following:

- Internal Pre-selector
- Antenna Relay
- Duplexer
- External Dual Circulator Tray
- Integrated Tone Remote Control (with Wireline option)
- Integrated DC Remote Control (with Wireline option)
- Integrated E&M Remote Control (with Wireline option)
- Analog Voting (with Wireline option)
- Simplex operation (Tx=Rx)

In addition, the following features are also included. These features are shipped in a preset condition, but may be altered through the use of the CPS.

- 64 Tx/Rx Frequencies – Factory Programmed with 1 Tx, 1 Rx
- 12.5 kHz or 25 kHz Operation – Factory Programmed to 12.5 kHz
- 1 Tx and 1 Rx (PL or DPL) Squelch Code per channel – Factory Programmed to CSQ
- Base Station Identification (BSI) – Factory Programmed as “BLANK” (“BLANK” disables BSI)
- Push-To-Talk (PTT) Priority – Factory Programmed to Repeat Path

- Local Digital Audio via front panel microphone and speaker

3.1.1.7
Satellite Receiver and Voting Repeater

A satellite receiver is required when digital voting is enabled in the system. The satellite receiver is an RF receiver-only device used to extend the repeaters' inbound range.

The device functions to receive Over-The-Air transmission from the radios, forwards the transmission over an IP link to the voting repeater. The voting repeater then "votes" on all the transmissions received from all its receivers, including its internal receiver and all its satellite receivers, based on the quality of the bursts. The voted result is then repeated over the air, and other sites or applications.

NOTE: The satellite receivers reuse repeater hardware; the following repeaters may be used as satellite receivers:

- MOTOTRBO 32 MB Repeaters (MTR3000 and DR 3000 Series)
- SLR 1000/SLR 5000/SLR 8000 Series
- MTR3000 Receiver only boxes

The regular receive-and-transmit repeater with a built-in voting capability is usually called a voting repeater. Therefore there is no additional voting device in the system. The voting process is a software module built inside the voting repeater. The following repeaters can be used as voting repeaters:

- MOTOTRBO 32 MB Repeaters (MTR3000 and DR 3000 Series)
- SLR 5000/SLR 8000 Series

3.1.1.8
Radio Control Station

The MOTOTRBO Control Station is based on the MOTOTRBO Mobile, except that it is configured to be the RF link from the data Application Server to the repeater and other radios.

The MOTOTRBO Control Station is integrated with an AC power supply and appropriate housing to be placed on a desk. Since it is the radio gateway to the server, it is configured to transmit and receive on a single channel. It is programmed with a known radio ID, so that field radios know how to contact the server. In a MOTOTRBO system, there can be up to 16 Control Stations connected via four USB ports; each control station communicates through a separate logical channel, that is a TDMA slot.

In most cases, the Control Station is externally controlled by the PC. It requires no user interaction once programmed. However, if a situation requires the use of a Control Station to transmit voice, it is capable of transmitting voice as well.

System	Description
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	CPSS or CPMS configurations with Data Revert Channels require two sets of Control Stations. One set of Control Stations operating in conventional mode (called Revert Control Stations) are used for routing data messages from radios to a data application server. The second set of Control Stations operating in CPSS or CPMS modes (called Trunked Control Stations) are used for routing data messages from the data application server to the radios. Unlike Revert Control Stations, idle Trunked Control Stations move with the Rest Channel and

System	Description
	therefore are on the same channel with all the idle radios.

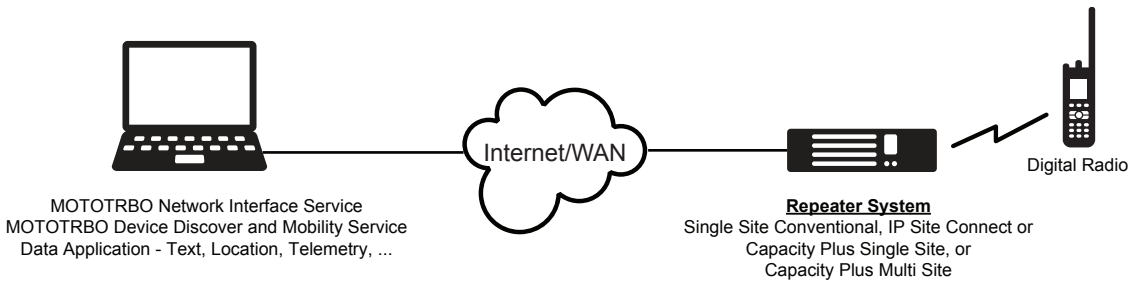
3.1.1.9
MOTOTRBO Network Interface Service

The MOTOTRBO Network Interface Service (MNIS) is a Windows service application which supports data applications such as Text Messaging, Location, Telemetry, and others, without requiring Control Stations.

System	Description
IPSC IP Site Connect	MNIS supports IP Site Connect configurations.
CPSS Capacity Plus Single Site	MNIS supports Capacity Plus Single Site configurations.
CPMS Capacity Plus Multi Site	MNIS supports Capacity Plus Multi Site configurations.

The MNIS connects with the repeater system over an IP network and utilizes the repeaters to transmit and receive data messages between data applications and MOTOTRBO radios. Voice and CSBK calls are currently not supported.

Figure 88: MOTOTRBO Network Interface Service



The following system configurations are supported by the MNIS:

- Single Site Conventional Digital
- IP Site Connect
- Capacity Plus Single Site
- Capacity Plus Multi Site

Data Revert Channels and Enhanced GPS Revert Channels are supported. Data on voice channels are supported too, however, only on selected conventional channels or Trunked Channels.

System	Description
IPSC IP Site Connect	In IP Site Connect, data on voice channels are supported on both wide and local area channel configurations.

The following MOTOTRBO data features are supported by MNIS:

- Layer 2 confirmed and unconfirmed data message delivery
- Individual and Group data messages
- Basic, Enhanced, and AES Privacy
- Data message IP/UDP header compression
- Data Precedence and Data Over Voice Interrupt access priority

The MNIS supports MOTOTRBO data applications, including Text Messaging, Location, Telemetry, Third-Party Raw Data, and OTAP with CPS. The MNIS requires the MOTOTRBO Device Discovery and Mobility Service application (DDMS), formerly called the MOTOTRBO Presence Notifier, for radio ARS.

There are several benefits of selecting MNIS over Control Stations, particularly when the Control Stations are used only by data applications. Some of the benefits include:

- The deployment is simpler compared to using Control Stations, because Control Stations and other associated hardware such as power supplies, antennae, and others are not required.
- Previously, data Revert Channels were required to be wide area in order for the data messages to be routed to the site where the Control Stations are located. Now, MNIS allows a centralized data application to access local Data Revert Channels at all remote sites. The former wide area Data Revert Channel can now be split into multiple local Data Revert Channels, which routes data to the centralized data application via MNIS, thus allowing higher data throughput from each remote site.
- MNIS connectivity with the system can be monitored via RDAC.

However, there are a few considerations to take note of:

- The MNIS does not support Dynamic Mixed Mode system configuration.
- The repeater's "Network Application Interface for Data" feature must be enabled to allow the MNIS to interface with the repeater.
- The MNIS does not support L2 fragmented data. Ensure that the largest data size [Data Message + IP/UDP Header] transmitted from the radio is less than the Max TX PDU Size configured in the radios.
- The MNIS software is available on the MOTOTRBO MOL website.

3.1.1.10
MC1000, MC2000, MC2500 Console

NOTE: This feature is supported only by specific product model.

The MOTOTRBO mobile in analog mode supports the MC Deskset Series of consoles. The MC Deskset Series provides a complete portfolio of products for a small control room. Each unit provides control of the radio(s) via a compact desk unit offering a choice of control methods: Local and Remote. The portfolio ranges from a simple talk and listen unit to a miniature multi-channel console.

The MC1000 can control a single Control Station, and provides a selection of up to four frequencies. This unit requires no software for programming.

The MC2000 can also control a single Control Station, but provides a selection of up to 16 frequencies. Programming this unit is through configuration software installed on a PC.

The MC2500 controls up to four Control Stations, with the ability to patch and multi-select channels. All channels are capable of 16 frequency controls. This unit is programmed through configuration software installed on a PC.

Each unit ships with a power supply and manual. The MC1000 ships with a 110V, 60Hz unit, while the MC2000/MC2500 ship with an 110/220V, 50/60Hz unit.

The MOTOTRBO mobile can be interfaced with the MC1000, MC2000 and MC2500 Desktop Consoles. These consoles allow for remote and local access to the MOTOTRBO Control Station. The interface to the console uses a 26-pin MAP connector. The console interface to the Control Station consists of TX_Audio, RX_Audio, PTT, Monitor and Channel Activity. Additionally, channel steering is provided by the mobile radio through the GPIO pins, which are configurable using the CPS. Advanced MDC commands are only supported in analog mode and a not in digital mode.

See the analog console installation manual for more details on analog console configurations.

3.1.2

Mobile Components

Most users of the MOTOTRBO system utilize mobile devices (non-fixed) to access the system. Below are the devices currently available in the following frequency ranges and power levels.

The MOTOTRBO portable is currently available in the following frequency ranges and power levels:

Table 69: Mobile Components for MOTOTRBO Portable

Frequency Band	Frequency Range	Power Level
UHF 1	403 – 470 MHz	1 – 4 W
UHF 2	450 – 512 MHz	1 – 4 W
VHF	136 – 174 MHz	1 – 5 W
350 MHz	350 – 400 MHz	1 – 4 W
800 MHz	806 – 824 MHz 851 – 869 MHz	1 – 2.5 W
900 MHz	896 – 902 MHz 935 – 941 MHz	1 – 2.5 W

The MOTOTRBO mobile is currently available in the following frequency ranges and power levels:

Table 70: Mobile Components for MOTOTRBO Mobile

Frequency Band	Frequency Range	Power Level
UHF 1	403 – 470 MHz	1 – 25 W 25 – 40 W
UHF 2	450 – 527 MHz	1 – 40 W (for 450 – 512 MHz) 1 – 25 W (for 512 – 527 MHz)
VHF	136 – 174 MHz	1 – 25 W

Frequency Band	Frequency Range	Power Level
		25 – 45 W
350 MHz	350 – 400 MHz	1 – 25 W 1 – 40 W
800 MHz	806 – 824 MHz 851 – 869 MHz	1 – 35 W
900 MHz	896 – 902 MHz 901 – 902 MHz 935 – 941 MHz 940 – 941 MHz	1 – 7 W 1 – 30 W

3.1.2.1
MOTOTRBO Portable

The MOTOTRBO portable is a durable, but lightweight radio that offers many ways to access the system's features. It is designed to allow users to take it with them anywhere, and yet remain connected to the system.

The following table lists the average battery life for conventional operation at 5/5/90 duty cycle with battery saver enabled, GPS options disabled, no option board, no attached accessories, performing with carrier squelch for analog mode, ETSI DMR Tier 2 standard for digital mode, and transmitting at high power. Actual performance may vary by band and usage characteristics.

Table 71: MOTOTRBO Portable Average Battery Life

Battery Type	Battery Life
NiMH 1300 mAh Battery	Analog: 8 Hours Digital: 11.2 Hours
IMPRES FM Li-ion 1400 mAh Battery	Analog: 8.7 Hours Digital: 12.1 Hours
IMPRES Li-ion 1500 mAh Slim Battery	Analog: 9.3 Hours Digital: 13 Hours
IMPRES Li-ion 2200 mAh Battery	Analog: 13.5 Hours Digital: 19 Hours

The portable is available in two tiers:

- A keypad radio with display, and
- A non-keypad radio with no display.

The portable is fully configurable through the Windows-based CPS. It can be programmed to allow access to all MOTOTRBO features and all channels within the system or can be simplified to only allow limited access. The MOTOTRBO portable can truly be configured to cater to your customer's needs.

3.1.2.1.1

User Interface

Figure 89: MOTOTRBO Portable (Display Model)

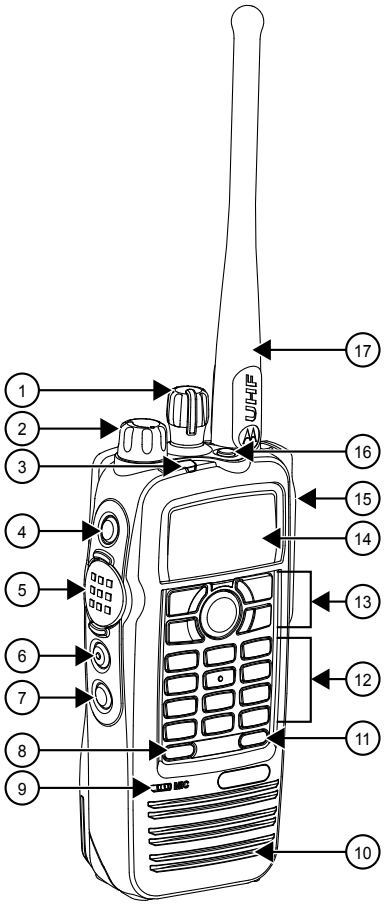
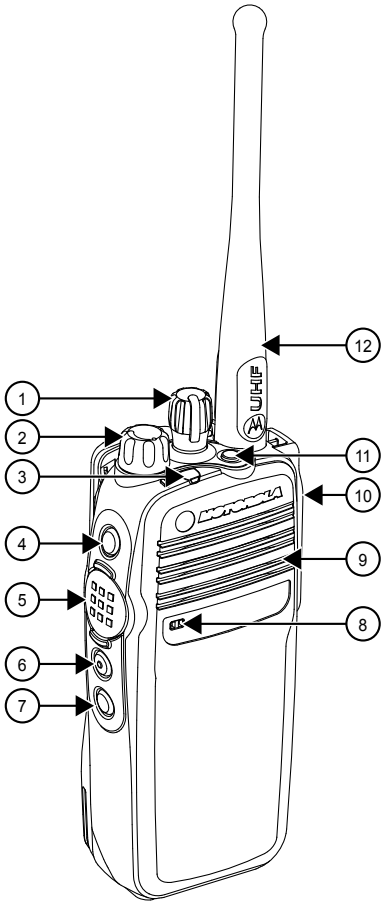


Figure 90: MOTOTRBO Portable (Non-Display Model)



The primary buttons of the MOTOTRBO portable offer the user the ability to initiate most system features. These buttons and switches should be very familiar to radio users.

3.1.2.1.1.1
Push-to-Talk Button

The large round Push-To-Talk button, or PTT button, is the primary button used to initiate voice transmissions. Its location is on the left side of the portable, but is still easy to reach for both right-handed or left-handed users. The button is raised from the side and has a raised pattern, so that it is easily found even under low light conditions. Pressing the PTT button starts a voice transmission on the selected channel. This enables the user to simply push and talk.

3.1.2.1.1.2
Channel Selector Knob

The MOTOTRBO portable user chooses his communication environment by twisting the 16-position channel knob on the top of the portable radio. This Channel Selector Knob is the main way a user uses to access the system. It also has a raised pattern, so it too is easy to find under low light conditions. Although easy to find, it is designed to require some force to turn it, so as not to be accidentally rotated through normal user activities. Each knob position can be programmed to access a different channel within the radio's programming. This allows the user to quickly switch between analog and digital channels and even different groups.

But the user is not limited to 16 channels. Up to 16 channels can be placed into a zone, and then switched between multiple zones. This greatly increases the number of available channels to the user.

3.1.2.1.1.3
Programmable Buttons

There are programmable buttons on the MOTOTRBO portable. The display portable has six programmable buttons, while the non-display portable only has four programmable buttons. Each button can be programmed to perform a particular function. The short press and long press can be programmed to act differently. The orange button located on the top of the radio is commonly used to initiate emergency alarms, although it can be configured to function differently.

3.1.2.1.1.4
Status Indicators

There are a few different ways to provide feedback to the user.

Depending on its color and state, a large tri-colored LED on the top of the radio indicates whether the radio is transmitting or receiving, and whether the selected channel is busy or idle. The LED busy indication represents the presence of RF activity on the selected channel and is not specific to the digital slot currently being monitored. The MOTOTRBO keypad portable with display also has a two-line LCD that displays a wide variety of information including received signal strength, battery power, emergency status, received text message indicator, monitor on/off, and GPS status. This display also allows each channel name to be displayed, so that the user knows the name of the selected channel. The source ID and target group alias are also displayed. User names are kept in an address book. This allows the user to assign user-friendly names as aliases to a radio ID. Various alert tones, talk permit tones and keypad tones are also available to give additional audio feedback to the user.

3.1.2.1.1.5
Menu System

In addition to accessing system features through buttons, the MOTOTRBO keypad portable with display offers a menu shown on its two line LCD display. With use of a menu button, left and right arrow buttons, a back/home button, and an OK button for selection, users can easily navigate through the following additional features.

- Contacts
- Scan
- Messages
- Call Logs
- Utilities

For further details on these menus, see the MOTOTRBO portable user manual.

3.1.2.1.1.6
Full Keypad

The MOTOTRBO keypad portable with display offers a full numeric keypad for users to manually enter target addresses for system features. This keypad is also used as an alphanumeric keyboard for text messaging. The non-display portable does not come with a keypad.

3.1.2.1.2
Voice Feature Support

With use of the MOTOTRBO portable interface, the user has access to all the voice features the MOTOTRBO system has to offer. These features include Group Calls, Private Calls, All Calls, and Emergency Calls.

3.1.2.1.3
Command and Control Feature Support

Command and control system features like Radio Check, Call Alert, Remote Monitor, Radio Enable/Disable are all accessible from the MOTOTRBO portable user interface.

3.1.2.1.4
Analog Compatibility

The radios can be programmed to support many current analog system features. Supported analog features include:

- Analog communications on a 12.5/20/25 kHz channel (as standard),
- Private-Line (PL) and Digital Private-Line (DPL) coded squelch control (as standard),
- MDC signaling.

3.1.2.1.5
Integrated GPS Antenna and Receiver

The MOTOTRBO portable can contain an internal GPS receiver that works with the Location Services / Tracking Data Application. The location application and radio can be configured so that the radio transmits its location to a centralized application. The GPS antenna is integrated into the main antenna of the portable. In the LCD display on the radio, an icon indicates if the radio is in range of the GPS satellites.

3.1.2.1.6
Text Messaging Compatibility

The MOTOTRBO portable can receive and transmit text messages.

These can be Quick Text (pre-defined) messages already stored on the portable. In the case of keypad radio with display, freeform messages also can be created using the keypad. Through the menu, the user can access the Inbox that contains all the messages he has received. The radio allows a user to send a text message to an individual, a dispatcher or a group of radios. He can also reply to and forward text messages to other radios.

Do note that all the features mentioned apply to the radio’s built-in text messaging as well as to “mobile on a PC” text messaging.

3.1.2.1.7
Accessory and Peripherals Interface

The MOTOTRBO portable radio supports an improved accessory and peripherals interface. This new interface is Motorola Solutions platform for future accessory development, and is not compatible with older accessories. It supports the following capabilities:

Enhanced Audio Functionality
This unique technology enables communication between the radio and Motorola Solutions enhanced accessories to optimize audio performance. It enables more consistent audio levels between accessory types. So headsets, remote speaker mics, or the radio's built-in mic and speaker sound more consistent and interoperate more effectively. It also optimizes audio quality performance for a given accessory type, by employing digital signal processing (DSP) technology to best match the radio's audio signals to the capabilities of the accessory.

USB Capability
The MOTOTRBO accessory and peripherals interface incorporates the standard Universal Serial Bus (USB) capability, thus enabling IP connectivity through standard USB ports with personal computers and other peripherals via a Motorola Solutions-supplied cable. This interface supports radio programming capabilities with no Radio-Interface-Box (RIB) required. It also enables the interface to MOTOTRBO data applications such as text messaging and location tracking. This interface also supports third-party applications by enabling interfaces for IP data service, telemetry services, text messaging and location tracking.

Core peripheral
The MOTOTRBO accessory and peripherals interface also includes core functionality for audio input and output, PTT, monitor, receive unsquelch, channel steering, and other general purpose input-output (GPIO) functions. This enables interface with dispatch and telemetry applications and other traditional radio system applications.

RF input/output
The MOTOTRBO accessory and peripherals interface also includes antenna signal (RF input/out) for use with future accessories such as public safety style microphones and vehicular adapters.

Rugged and Submersible
The MOTOTRBO accessory and peripherals interface meets IP57 requirements (submersible to 1 meter for 30 minutes), thus enabling development of rugged and submersible accessories.

3.1.2.2
MOTOTRBO Mobile

The MOTOTRBO Mobile is designed to be located in a vehicle and powered by the vehicle's battery or by AC power. Its durable construction makes it safe to use in most in-vehicle environments. It also can be used on desktops that are not truly mobile. Similar to the portable, the mobile offers numerous ways to access the system's features.

The mobile is available in two tiers:

- A radio with full display, and
- A radio with numeric display.

The mobile is fully configurable through the Windows-based configuration software (CPS). It can be programmed to allow access to all MOTOTRBO features and all channels within the system, or can be simplified to only allow limited access. The MOTOTRBO Mobile can truly be configured to cater to your customer's needs.

3.1.2.2.1

User Interface

Figure 91: MOTOTRBO Mobile Control Head (Full Display Model)

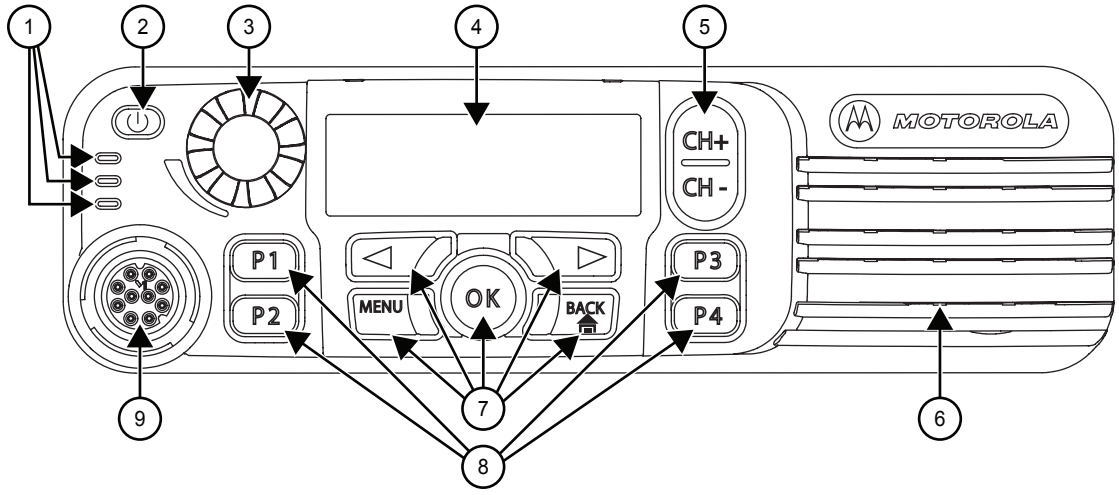
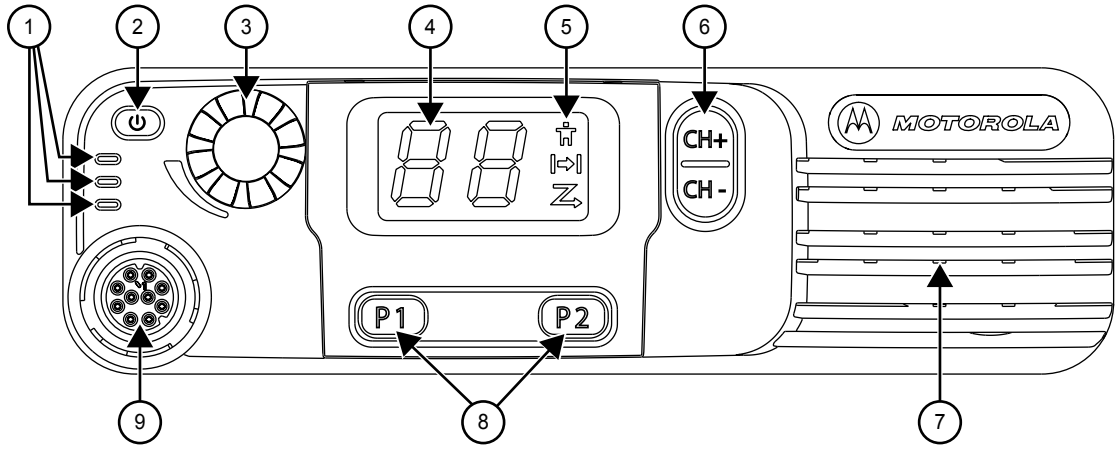


Figure 92: MOTOTRBO Mobile Control Head (Numeric Display Model)



The primary buttons of the MOTOTRBO Mobile offer the user the ability to initiate most system features. These buttons and switches are the corner stone of the radio and should be very familiar to radio users.

3.1.2.2.1.1

Push-to-Talk Button

The Push-To-Talk (PTT) button on the microphone is the primary button used to initiate voice transmissions.

The cable connecting the microphone to the mobile is long enough to be comfortably used by either a right handed or left handed user. The button is raised from the side and has a raised pattern so that it is easily found in the low light conditions. Pressing the PTT starts a voice transmission on the selected channel. This enables the user to simply Push and Talk. The MOTOTRBO mobile can also interface to other accessories such as a Visor Microphone, a Foot Switch and an enhanced full keypad microphone. Motorola Solutions Original™ accessories provide an easy way to turn the MOTOTRBO mobile radio into a custom communication solution to fit your business requirements.

3.1.2.2.1.2
Channel Rocker

The MOTOTRBO Mobile user chooses his communication environment by selecting a channel using the Channel Rocker on the control head.

The Channel Rocker has a raised pattern that is back-lit so it is easy to find in low light conditions. Although easy to find, it requires some force to push it so as not to change channels through accidentally pressing. Each press can be programmed to access a different channel within the radio's programming. This allows the user to quickly switch between analog and digital channels and even different groups. The user can quickly switch to different channels by pushing the up or down sections of the rocker. This greatly increases the number of available channels to the user.

3.1.2.2.1.3
Programmable Buttons

There are programmable buttons on the MOTOTRBO mobile. The full display mobile has four programmable buttons while the numeric display mobile has two programmable buttons.

Each button can be programmed to perform a particular function. The short press and long press can be programmed to act differently. The buttons can be programmed to give quick and easy access to the MOTOTRBO system features, triggering emergency alarms and operating horns or lights.

3.1.2.2.1.4
Status Indicators

The MOTOTRBO mobile provides a multi-colored LED on the front of the radio that informs the user of the busy or idle status of the selected channel. The LED busy indication represents the presence of RF activity on the selected channel and is not specific to the digital slot currently being monitored.

The MOTOTRBO Mobile also provides a two line LCD display that shows a wide variety of information, including received signal strength, battery power, emergency status, monitor on/off, and GPS status. This display allows each channel name to be displayed so that the user knows the name of the selected channel. The source ID and target group alias are also displayed for ease of use. User names are kept in an address book. This allows the user to use familiar names as aliases a radio ID. Various audio alert tones, talk permit tones and keypad tones are available to help the user navigate.

3.1.2.2.1.5
Menu System

In addition to the accessing system features through buttons, the MOTOTRBO Mobile offers a menu shown on its two line LCD display. With use of a menu button, left and right arrow buttons, a back/home button, and an OK button for selection, users can easily navigate through the following additional features. The Menu includes:

- Contacts
- Scan
- Messages
- Call Logs
- Utilities

For further details on these menus, please see the MOTOTRBO mobile user manual.

3.1.2.2.1.6
Full Keypad

As an option, the MOTOTRBO Mobile offers an Enhanced Keypad Microphone so that users can manually enter target addresses for system features. Text messaging from the mobile is available to the end user if the MOTOTRBO mobile is configured with an Enhanced Keypad Microphone. The Enhanced Keypad Microphone has a keypad that also doubles as a keyboard for text messaging.

3.1.2.2.2
Voice Feature Support

With use of the MOTOTRBO Mobile interface, the user has access to all the voice features the MOTOTRBO system as to offer. These features include: Group Calls, Private Calls, All Calls, and Emergency Calls.

3.1.2.2.3
Command and Control Feature Support

Command and control system features like Radio Check, Call Alert, Remote Monitor, and Radio Enable/ Disable are all accessible from the MOTOTRBO Mobile's user interface.

3.1.2.2.4
Analog Compatibility

The radios can be programmed to be backwards compatible and can support many current analog system features. These analog channels can be accessed through the Channel Rocker. Supported analog features include:

- Analog communications on a 12.5/25 kHz channel
- Private-Line (PL) and Digital Private-Line (DPL) coded squelch control
- MDC signaling (Emergency, PTT ID and Call Alert)

3.1.2.2.5
Integrated GPS Antenna and Receiver

The MOTOTRBO Mobile can also be purchased to contain an internal GPS receiver that works with the Location services / tracking data application.

The location application and radio can be configured so that the radio transmits its location to a centralized application. The GPS antenna is an external antenna that will have to be mounted on the vehicle. In the LCD display on the radio, an icon will display whether or not the radio is in range of satellites.

3.1.2.2.6
Text Messaging

The MOTOTRBO Mobile can receive and transmit text messages. An inbox that contains all messages received is accessed through the menu.

When composing a message, the user can generate a free form text message or choose from a list of Quick Text (pre-defined) messages. The MOTOTRBO radio allows a user to send a text message to an individual, a dispatcher or a group of radios, and can reply to and forward text messages to other radios. If the MOTOTRBO mobile is not configured with the Enhanced Keypad Microphone, then text messaging can be accomplished through a mobile computer, running the text messaging client connected to the mobile. Using CPS, the radio can be configured to support text messaging internally or forward data to a mobile computer connected to the radio.

Do note that all the features mentioned apply to the radio's built-in text messaging as well as to "mobile on a PC" text messaging.

3.1.2.2.7
Front Panel Accessory Interface

The MOTOTRBO mobile radio supports an improved front panel accessory interface. This new interface is Motorola Solutions platform for future accessory development and is not backwards compatible with older accessories. This interface supports the following capabilities:

- Enhanced Audio Functionality – This unique technology enables communication between the radio and Motorola Solutions enhanced accessories to optimize audio performance. It enables more consistent audio levels between accessory types, so that users of different microphones sound more consistent and inter-operate more effectively. It also optimizes audio quality performance for a given accessory type, employing DSP (digital signal processing) technology to best match the radio's audio signals to the capabilities of the accessory.
- USB Capability – The MOTOTRBO accessory and peripherals interface incorporates standard Universal Serial Bus (USB) capability, enabling IP connectivity through standard USB ports with Personal Computers and other peripherals through a Motorola Solutions-supplied cable. This interface supports radio programming capabilities with no RIB box required, from the front (microphone port) connection. It also enables the interface to MOTOTRBO data applications such as text messaging and location tracking. This interface also supports third-party applications by enabling interfaces for IP data service, telemetry services, and text messaging and location tracking.
- Improved Connection – The MOTOTRBO microphone connection employs a rugged "twist and lock" mechanism for greater durability and connection strength.

3.1.2.2.8
Rear Accessory and Peripherals Interface

The MOTOTRBO mobile radio also supports an improved rear panel accessory and peripherals interface. It supports the following capabilities:

- USB Capability – The MOTOTRBO accessory and peripherals interface incorporates standard Universal Serial Bus (USB) capability, enabling IP connectivity through standard USB ports with Personal Computers and other peripherals through a Motorola Solutions-supplied cable. This interface supports radio programming capabilities with no RIB box required. It also enables the interface to MOTOTRBO data applications such as text messaging and location tracking. This interface also supports third-party applications by enabling interfaces for IP data service, telemetry services, and text messaging and location tracking.
- Core peripherals – The MOTOTRBO accessory and peripherals interface also includes core functionality for audio input and output, PTT, monitor, receive unsquelch, channel steering, and other general purpose input-output (GPIO) functions. This enables interface with dispatch and telemetry applications and other traditional radio system applications.

3.1.2.3
MOTOTRBO Device Discovery and Mobility Service

The MOTOTRBO Device Discovery and Mobility Service (DDMS) application replaces the MOTOTRBO Presence Notifier in software versions R02.06.10 and later.

The application supports radios presence and radio mobility notification services. It can be deployed with the Control Station or the MNIS. In deployments with a Control Station, the DDMS only supports radio presence notifications. In deployments with the MNIS, it supports presence as well as mobility notifications.

3.1.2.3.1
Mobility Notification Service

When Device Discovery and Mobility Service (DDMS) is deployed with MNIS, both radio presence as well as mobility notification services are supported. The channel and site where a radio transmits its ARS Device Registration message provides the radio's mobility information, which gets recorded in the DDMS. The MNIS subscribes with the DDMS to receive the radio's mobility information, and uses it to route the application data to the radio. Besides MNIS, other watcher applications can also subscribe with DDMS to receive radios' mobility information. The DDMS watcher interface is extended for radio mobility service subscription and notification.

The DDMS is fully backward compatible with the MOTOTRBO Presence Notifier application. Existing applications that interface with the Presence Notifier do not require any changes to receive presence notifications. In the System Planner, the DDMS is assumed where ever the Presence Notifier is mentioned.

3.2
System Topologies

The primary element in the design of any private two-way radio communications system is the networking of a fleet of field radios (portable and mobile radios).

To set up such a system, the following questions should be asked:

- How many system users require a field radio?
- Which system users need to communicate with each other?
- Where are system users transmitting and receiving from when communicating with other system users?

This information becomes the basis in determining the extent of the required system coverage area, and the creation of its topologies. This information and the desired feature set determines decisions on the system's topology.

3.2.1
Direct Mode/Dual Capacity Direct Mode (DCDM)

If, within the customer's required coverage area, any system user can directly communicate with all of the other system users with just the output power of the transmitter in their portable or mobile radio, then a direct mode or dual capacity direct mode system can be used.

Direct mode or dual capacity direct mode is direct radio-to-radio communication for systems that do not use a repeater. When radios operate in direct mode/dual capacity direct mode, the radios always transmit and receive on the same frequency. Direct mode and dual capacity direct mode provide similar services to the end users, with the exception that dual capacity direct mode is only available in digital mode, and supports two simultaneous voice/data paths on a 12.5 kHz bandwidth channel while direct mode supports only one. Additionally, there are some minor differences. For example, dual capacity direct mode channels may not be used as GPS Revert Channels.

The radios are not limited to one direct mode/dual capacity direct mode frequency. They can be programmed to have different frequencies, which are selectable with the channel selector knob.

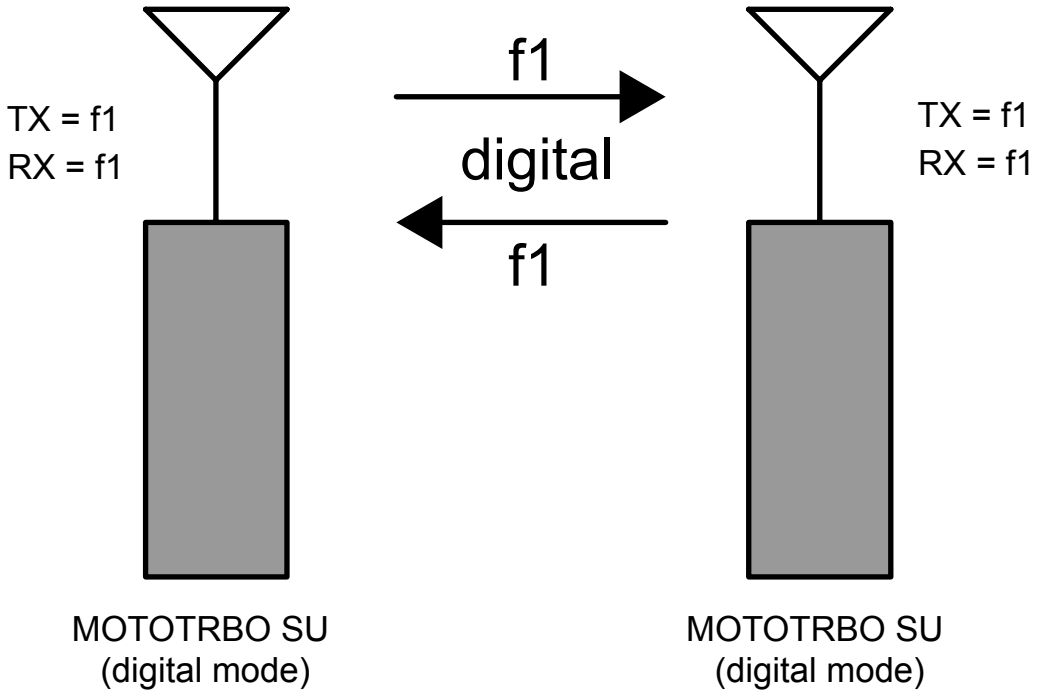
Direct mode/dual capacity direct mode do not need Over-The-Air hang time for voice calls (Repeater on page 297). The radio has an internal call ("talk back") timer. The channel access method used before the call timer expires is impolite, since the radio is still a member of an active call. This is independent of the Channel Access selection for call initiation (polite or impolite).

3.2.1.1

Digital MOTOTRBO Radios in DCDM

In Direct Mode/Dual Capacity Direct Mode (DCDM) configuration, a single frequency is assigned to all radios to communicate with each other. In digital direct mode/dual capacity direct mode, the radios support all three methods of voice transmission: Group Calls, Private Calls and All Calls. They can also support all command and control messaging like Call Alert, Radio Check, Radio Enable/Disable, Remote Monitor and Emergency.

Figure 93: MOTOTRBO Radios (in digital mode) In Direct Mode/Dual Capacity Direct Mode



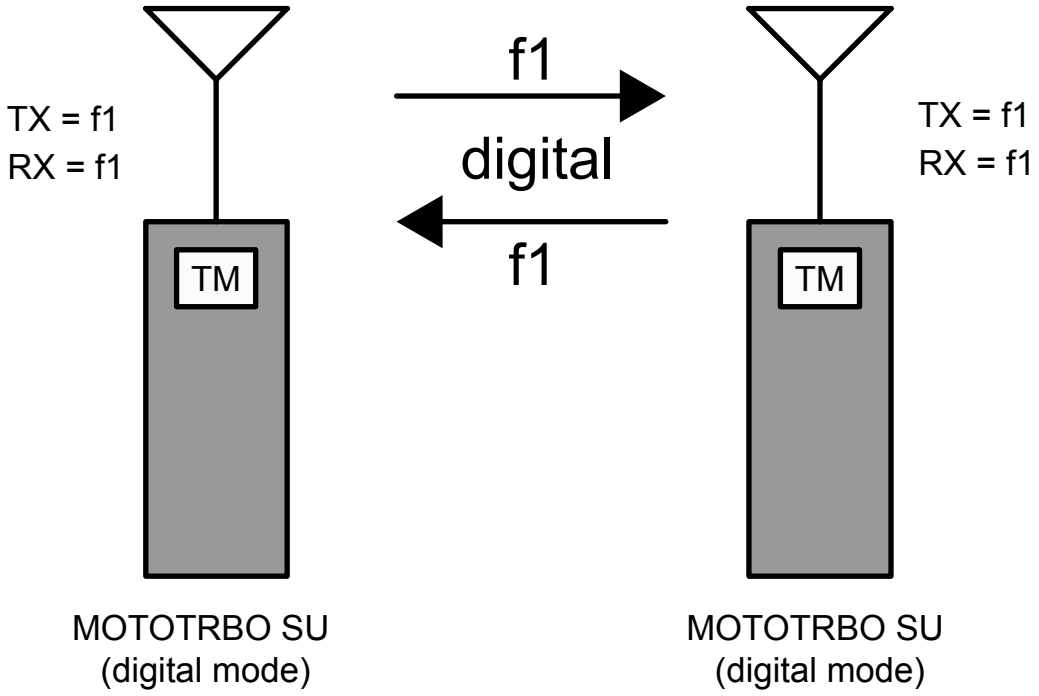
3.2.1.1.1

Text Messaging in DCDM

In Direct Mode/Dual Capacity Direct Mode (DCDM), the MOTOTRBO radios are capable of sending text messages to other radios. Radio to radio text messaging is accomplished by a text messaging application

that is built into the radio. From the front keypad, the radio user can select the target radio, and type a text message.

Figure 94: MOTOTRBO Radios (in digital mode) Text Messaging In Direct Mode/Dual Capacity Direct Mode

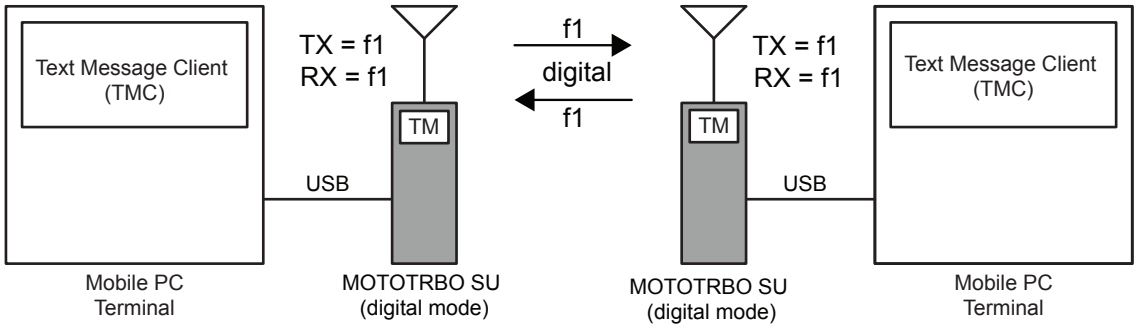


In order for the text message to be sent successfully to the target radio, both radios need to be on the same frequency. Similar to voice, if multiple direct mode/dual capacity direct mode frequencies are being used, the user must choose the channel his target is on before sending his text message. The radios do not have to be on the same group.

Text messaging and the previously discussed voice services operate on the same frequency. Since data operates in a polite manner, the radio avoids transmitting text messages while any voice service is active. If operating with only field radios, text messages are limited to radio to radio communications.

Text messages can also be sent from radio to radio using a PC attached to the radio. A software-based text messaging client will be installed on the PC. These configurations are commonly used in vehicles or on desktops that do not have LAN connections. Since they can run on AC power or off the in-vehicle battery, mobile radios are usually used for these applications, though a portable can also be used. Note that the radio can be configured to route incoming text messages to itself or to the PC, but not both.

Figure 95: MOTOTRBO Radios (in digital mode) Text Messaging In Multiple Direct Mode/Dual Capacity Direct Mode

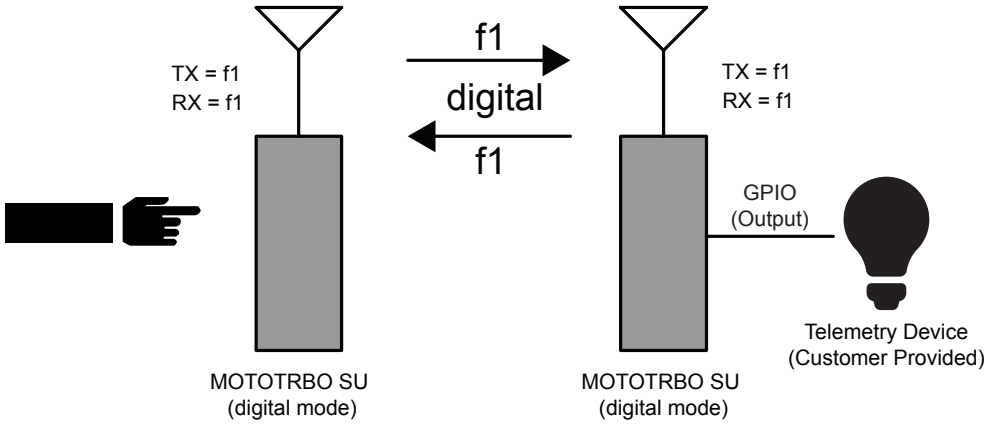


3.2.1.1.2

Telemetry Commands in DCDM

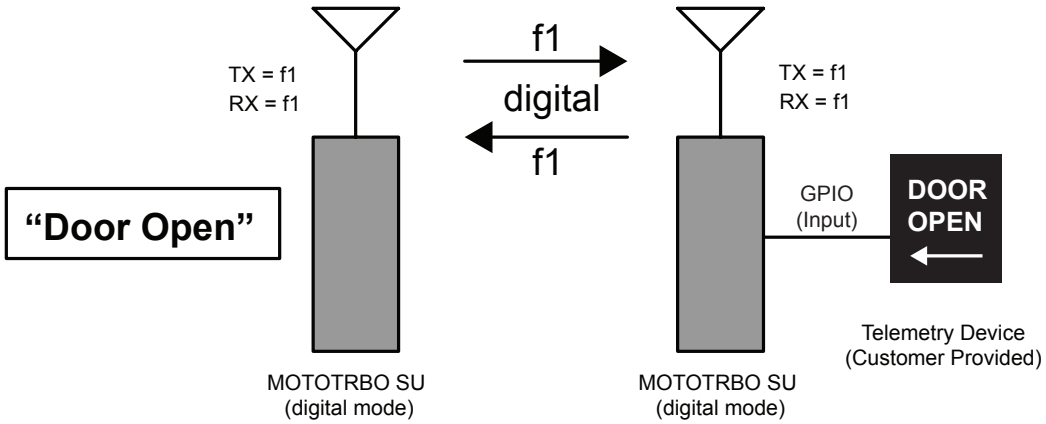
The following are some basic telemetry configurations, each with a quick description.

Figure 96: Send Telemetry Command from MOTOTRBO Radio to Another MOTOTRBO Radio to Toggle an Output Pin



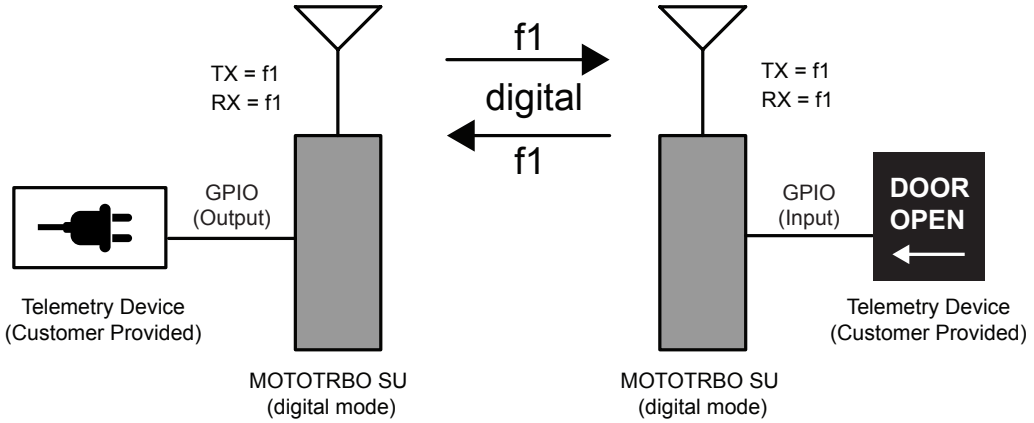
In the first basic configuration, a portable radio is programmed with a button that sends a preconfigured telemetry command Over-The-Air to toggle a mobile radio's output GPIO pin. The GPIO pin is connected to external hardware that detects this change at the GPIO pin, and turns on a light. This configuration can be extended to other applications like remotely opening door locks, turning on pumps, or switching on sprinklers. Another application might be to combine the voice from the radio's external audio lines, a relay closure, and a public announcement system to remotely make announcements over the intercom from your portable radio.

Figure 97: Send Telemetry Message from MOTOTRBO Radio to Another MOTOTRBO Radio when Input Pin State Changes



This second basic configuration is a mobile that is connected to a customer supplied external telemetry hardware, which sends an event to one of the mobile's GPIO pins when it detects that a particular door has been opened. Upon detecting the GPIO pin as active, it sends a preconfigured Text Status Message to a particular portable radio. The portable radio displays "Door Opened" to the user as a pop-up alert. This basic configuration can be used at remote locations to detect a variety of sensors such as water levels, door and window intrusions, or even motion sensors. Combining the first and second configuration, the user can create complex control systems that initiates a large door to close, and then announces when the door physically closes.

Figure 98: Send Telemetry Command to Toggle an Output Pin from MOTOTRBO Radio to Another MOTOTRBO Radio when Input Pin State Changes



The third basic configuration is a mobile that is connected to customer supplied external telemetry hardware, which sends an event to one of the mobile's GPIO pins when it detects that a particular door has been opened. Upon detecting the GPIO pin as active, it sends a telemetry toggle command to another mobile radio. This mobile radio is configured to toggle an output pin, which is connected to telemetry hardware that sounds an alarm. Similar to the other configurations, this method can be extended to a myriad of other solutions such as only opening doors when other doors have been closed, or turning on water pumps when water levels reach a particular level. This configuration can be used automate the environment of two remote locations. The possibilities are only limited by the designer's imagination.

3.2.1.1.3

Server-Based Data Applications in DCDM

MOTOTRBO also supports server based data applications in Direct Mode/Dual Capacity Direct Mode (DCDM). This configuration consists of a PC (referred to as the Application Server) running the server software connected to the radio infrastructure through a mobile radio (or Control Station).

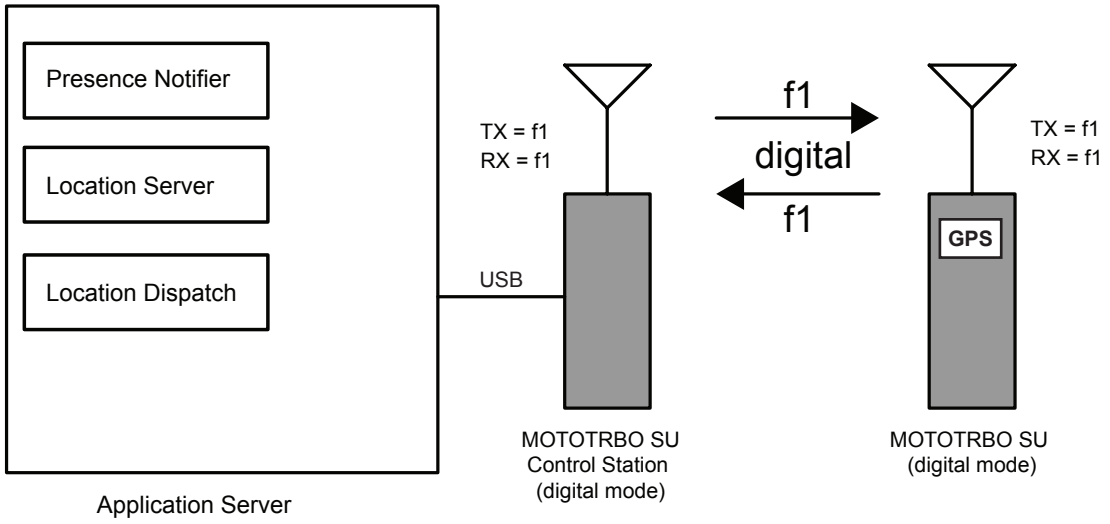
The mobile radio is usually AC powered. The mobile is configured as a Control Station, therefore it routes all data to the Application Server. Since this mobile is the radio gateway to the server, it is configured to transmit and receive on a single channel. The Control Station is programmed with a known radio ID, so the field radios know how to contact the server. The server and the Control Station (connected through a USB) must be located in the center of the customer's coverage area since all field radios are expected to communicate with it. There can only be one Application Server per system.

One key service offered by the server based configuration is radio presence notification. The Presence Notifier is required to reside on the Application Server. The purpose of the Presence Notifier is to track whether field radios are currently present on the system. Upon power-up or channel change, the MOTOTRBO radio transmits a registration message to the Control Station connected to the Application Server, where the Presence Notifier resides. The Presence Notifier then informs other data applications that the radio is available to receive and transmit data messages.

Typically, location applications require a server-based configuration and the Presence Notifier to operate. The Location Server application is installed on the Application Server machine with the Presence Notifier. When a radio registers with the Presence Notifier, it informs the Location Server that this radio is now on the system. The Location Server then sends out a service availability message through the Control Station to the radio informing it how often to send in periodic updates, and what to do if an emergency is initiated.

Location Dispatch applications request a radio's location information from the Location Server application, and display the radio's location on a map. A Location Dispatch application can reside on the Application Server as well. The diagram below depicts this configuration.

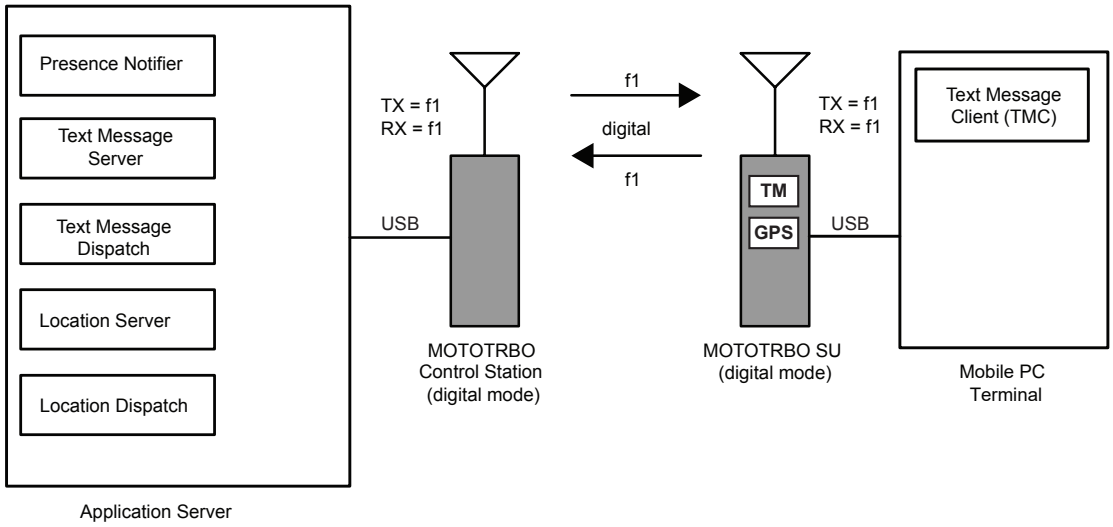
Figure 99: MOTOTRBO Radios In Digital Direct Mode/Dual Capacity Direct Mode with Location Server and Local Location Client



Text Messaging also uses a server based configuration. Similar to the Location Server, the Text Message Server application is installed on the Application Server machine with the Presence Notifier. When a radio registers with the Presence Notifier, it informs the Text Message Server that the radio is now on the system. The Text Message Server then sends out a service availability message through the Control Station to the radio informing it how it can communicate with the Text Message Server. Text Message Dispatch applications communicate with the Text Message Server in order to send and receive messages to and from the radio network via the connected Control Station. A Text Message Dispatch application can reside on the Application Server as well.

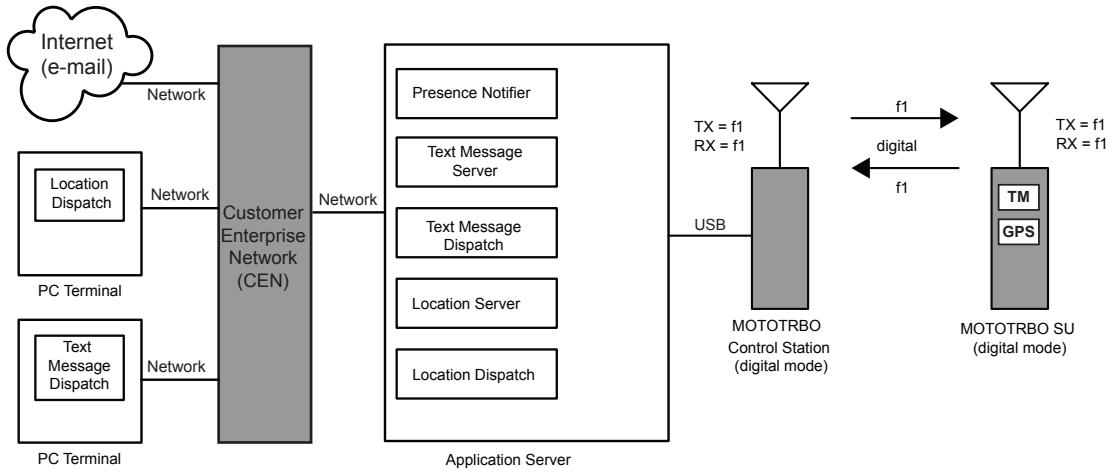
As previously described, radios can send text messages to each other without communicating through the Text Message Server. But in order to send and receive text messages to Text Message Dispatchers, the Text Message Server configuration is required. The diagram below depicts this configuration. This configuration also works with external text message applications connected to the field radios.

Figure 100: MOTOTRBO Radios In Digital Direct Mode with Text Message Server, Location Server and Local Dispatchers



This configuration can be expanded by locating up to four Text Message Dispatchers and four Location Dispatchers throughout the customer's Enterprise Network. Up to four installations of each application can be located anywhere on the customer's LAN, as long as they can communicate with the Application Server. The Dispatcher installation on the Application Server counts as one of the instances of the dispatch software. The diagram below shows two instances of each application. One is on the Application Server and one remote. The applications can reside on the same remote machine, if desired.

Figure 101: MOTOTRBO Radios In Digital Direct Mode/Dual Capacity Direct Mode Server Based Configuration with Remote Dispatchers



Another Text Message service that is only available in a server based configuration is the ability to receive and send text messages to external e-mail addresses. This allows PCs or pagers and cell phones that are text message capable on the system to send e-mail messages. In order for the Text Message Server to communicate with the outside world, the Application Server must have access to the Internet. When a radio sends a text message to a Text Message Dispatcher, and it is identified as an external e-mail address in the Text Message Server, the Text Message Server will forward the text message to the designated e-mail address.

The Text Message Server forwards incoming e-mails in a similar fashion. The source e-mail address must be configured in the Text Message Server for it to forward the text messages to the destination radio. This blocks unknown e-mail traffic from utilizing the bandwidth of the radio system.

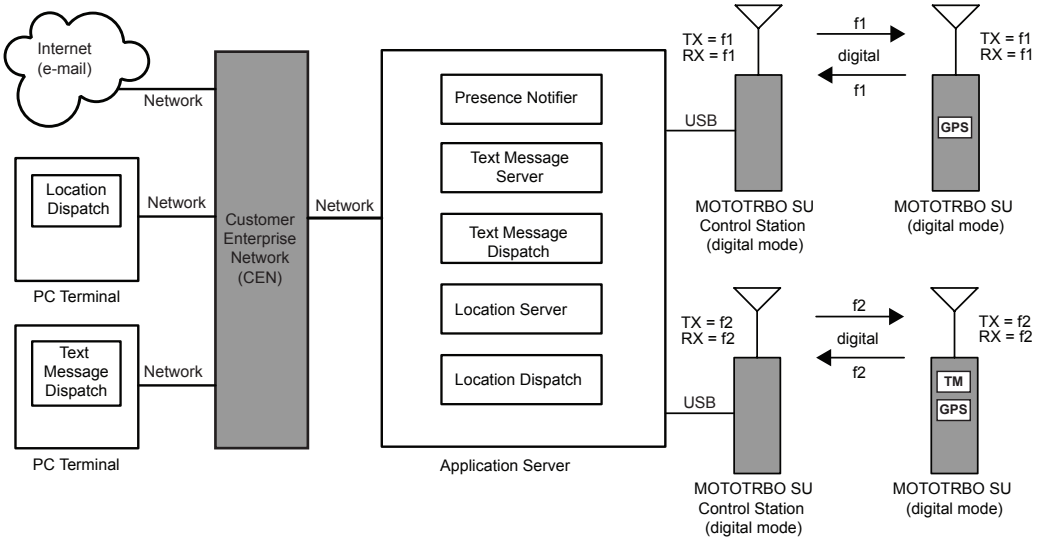
3.2.1.1.4
Multi-Channel Server-Based Data Applications in DCDM

For larger systems that have multiple direct mode/dual capacity direct mode frequencies, the Application Server can be connected to up to 16 Control Stations. Each Control Station is configured to communicate on the specified channel and acts as the data gateway for that channel.

Presence registration works in the same manner with this configuration as it does with the single channel configuration. When a radio powers up or changes channels, it sends in a registration to the Presence Notifier via the Control Station, which then informs the applications of the radio's presence. Each Control Station has the same radio ID, therefore the field radios transmit their messages to this radio ID regardless of which channel they are on.

Any channel, that supports data and needs to communicate to the Application Server, needs a dedicated Control Station.

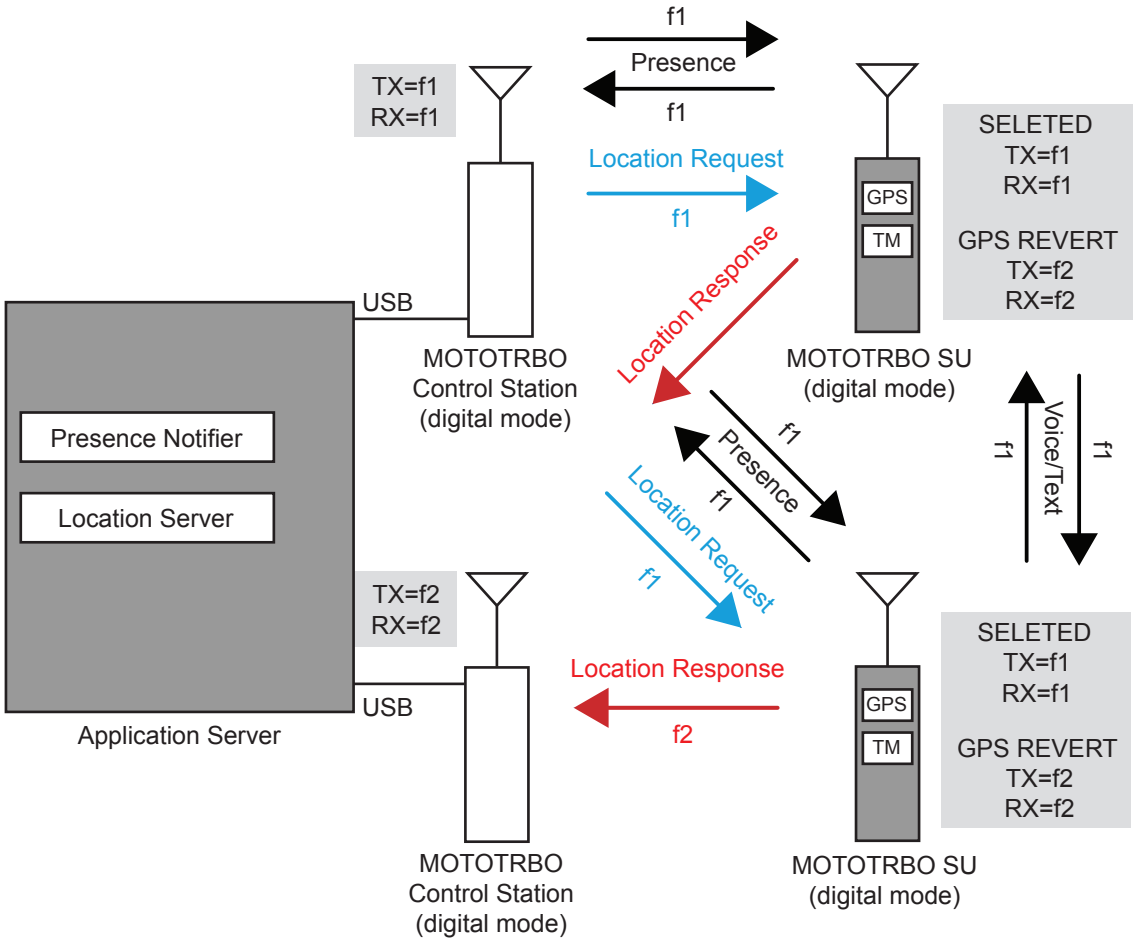
Figure 102: MOTOTRBO Radios in Two Channel Digital Direct Mode Server-Based Configuration with Remote Dispatchers



3.2.1.1.5
GPS Revert in DCDM

With the addition of the GPS Revert feature, it is now possible to transmit Location Update messages on channels other than the Selected Channel (See GPS (GNSS) Revert Channel on page 117 for configuration information). The diagram in Figure 103: MOTOTRBO Radios in Two Channel Direct Mode GPS Revert Configuration on page 336 illustrates this concept in its simplest form while operating in direct mode/dual capacity direct mode. The dual capacity direct mode operation is similar to direct mode in GPS revert scenarios, with the exception that a dual capacity direct mode channel can not be used as a GPS Revert Channel. As a result of that, a radio can revert from a dual capacity direct mode channel, but can not revert to a dual capacity direct mode channel to send the GPS update. In this example, Channel f1 is the Selected Channel and Channel f2 is the GPS Revert Channel. Communications such as presence, location requests (Application Server to radio), text and voice occur on the Selected Channel, while all location responses (radio to Application Server) including location updates occur on the GPS Revert Channel. Therefore, a minimum of two control stations are required to support GPS Revert.

Figure 103: MOTOTRBO Radios in Two Channel Direct Mode GPS Revert Configuration



Under a typical scenario, the radio is powered on, and then registers on the Selected Channel with the Presence Notifier and the Location Server. The radio receives a Periodic Location Request and an Emergency Location Request from the Location Server on the Selected Channel. This Periodic Location Request instructs the radio to send location updates at a specific rate, while the Emergency Location Request instructs the radio to send a single Emergency Location Update when an emergency is initiated.

The radio spends the most time on the Selected Channel. The radio only switches to the GPS Revert Channel when a Location Update needs to be transmitted. Since voice transmissions have priority over data transmissions, when the radio is involved in a call on the Selected Channel, the Location Update is queued until after the call is completed. In order to minimize the amount of time spent away from the Selected Channel while on the GPS Revert Channel, the radio will not attempt to qualify traffic on the GPS Revert Channel. Therefore, all voice, data, and control messages transmitted to a radio should never be transmitted on the GPS Revert Channel, as they will not reach their destination.

The example in Figure 103: MOTOTRBO Radios in Two Channel Direct Mode GPS Revert Configuration on page 336 illustrates only one GPS Revert Channel. However, depending on the GPS data load, more than one GPS Revert Channel may be needed. For example, a single large group that generates significant Location Update traffic must be sub-divided across several GPS Revert Channels. Each GPS Revert Channel requires a Control Station, which must be connected to the Application Server PC. The maximum number of Control Stations that can be connected to the PC is four.

3.2.1.1.6

Summary of Features in DCDM

The following features are supported in digital direct mode/dual capacity direct mode:

Table 72: Digital MOTOTRBO Radios in Direct Mode/Dual Capacity Direct Mode

Voice Features	Signaling Features	Emergency Handling	Data Calls	Other Features
Group Call	PTT ID and Aliasing	Emergency Alarm	Text Messaging	Scan
Private Call	Radio Inhibit	Emergency Alarm with Call	Location Tracking	Priority Scan
All Call	Remote Monitor	Emergency Alarm with Voice to Follow	Telemetry	Time-out Timer
Voice Interrupt	Radio Check	Emergency Revert	Third-Party (ADP) Applications	Polite to All channel access
–	Call Alert	Emergency Voice Interrupt	GPS Revert (DCDM not supported)	Polite to Own System channel access
–	Remote Voice Dekey	–	Data Over Voice Interrupt	Impolite channel access

*See Scan Considerations on page 156 for more information on the different scan modes supported by different topologies.

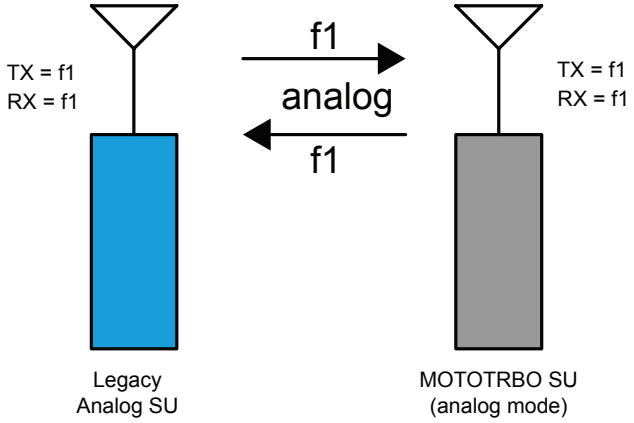
3.2.1.2

Interoperability between Analog MOTOTRBO Radios and Analog Radios in Direct Mode

MOTOTRBO radios support analog mode as well. In order for the MOTOTRBO radio to communicate with an analog radio, it must be programmed for analog mode, as well as programmed with the same frequency and parameters (for example, PL and DPL) as the analog radio.

While in analog mode, the MOTOTRBO radio supports most standard analog features including a subset of MDC signaling features. While in analog direct mode, the MOTOTRBO radios does not support any of the digital features.

Figure 104: Legacy Analog Radios and MOTOTRBO Radios (in analog mode) in Direct Mode



3.2.1.2.1
Summary of Features in Analog Direct Mode

All features listed in Wi-Fi Support on page 249 are supported in analog direct mode.

3.2.1.3
Interoperability Between Digital MOTOTRBO Radios, Mixed Mode MOTOTRBO Radios, and Analog Radios in Direct Mode

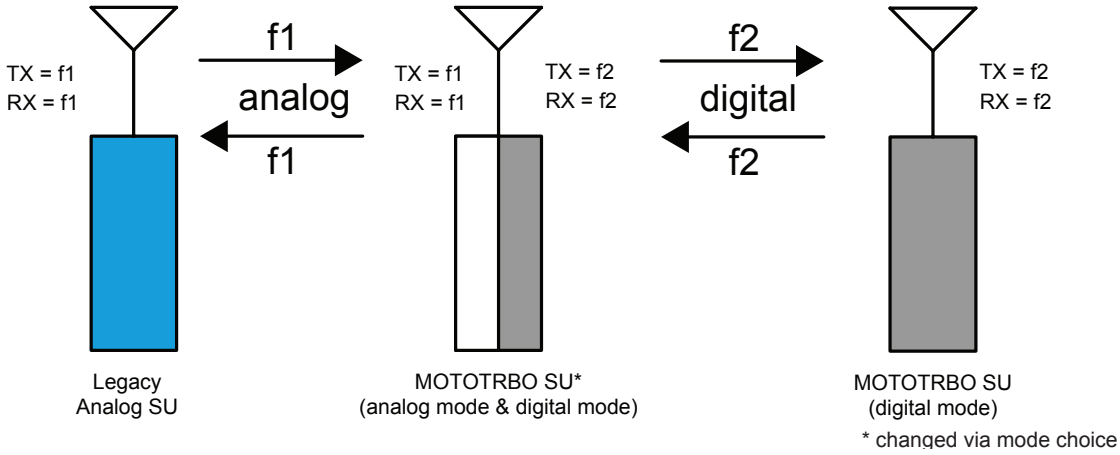
In this configuration, a MOTOTRBO subscriber is programmed to talk to an analog radio as well as a MOTOTRBO radio that is programmed for digital only.

In order for the MOTOTRBO radio to communicate with the analog radio, it must be programmed for analog mode, as well as programmed with the same frequency and parameters (for example PL and DPL) as the analog radio.

When in the digital mode, the MOTOTRBO subscriber has all of the digital features that are available in digital direct mode. However, the MOTOTRBO radio user has to manually switch from digital mode to analog mode to communicate with the two groups.

Alternatively, the MOTOTRBO radio user can program the radio to scan between the analog and digital channels to ensure a call is not missed. This can be done from the keypad of the radio or through the CPS. Please see Scan on page 154 and Scan Considerations on page 156 to learn more about scan.

Figure 105: Legacy Analog and MOTOTRBO Analog and Digital Radios in Direct Mode



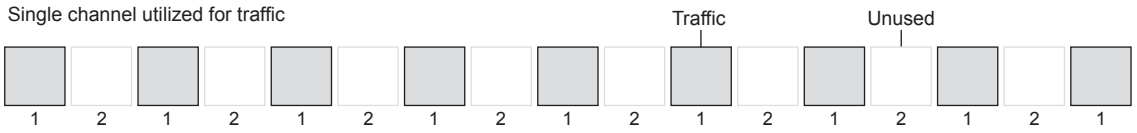
3.2.1.4

Direct Mode Spectrum Efficiency

A radio frequency (RF) channel with 12.5 kHz spectrum allocation can be configured to support direct mode or dual capacity direct mode through CPS.

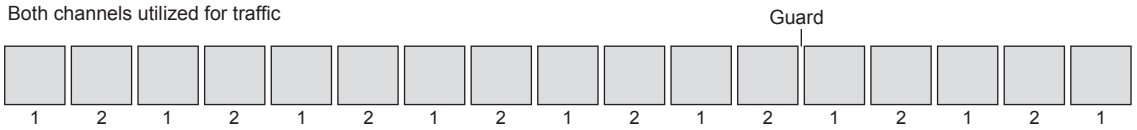
When configured to support direct mode, the radio only utilizes a single timeslot for the traffic, while the other timeslot is unused, as shown in the following figure.

Figure 106: Direct Mode Channels



When configured to support dual capacity direct mode, both timeslots can be used for two different calls. This yields dual capacity (2:1 TDMA) spectrum efficiency, as shown in the following figure. The dual capacity direct mode configuration provides equivalent spectral efficiency when compared with ETSI-DMR repeater solutions and 6.25 kHz FDMA solutions.

Figure 107: Dual Capacity Direct Mode Channels



3.2.2
Dual Capacity Direct Mode

Dual capacity direct mode is a digital feature aimed to benefit end-users who do not have and do not need repeaters, by providing 6.25 kHz spectrum efficiency. When a 12.5 kHz RF channel is configured for dual capacity direct mode, both timeslots are available for independent and simultaneous radio call conversations.

3.2.2.1
Timeslot Synchronization

Since there is no repeater designating a slotting structure and dual capacity direct mode uses both timeslots for the traffic, timeslot synchronization needs to be applied to differentiate timeslot 1 from timeslot 2.

In the absence of a repeater, the radios in dual capacity direct mode automatically and cooperatively select a Channel Timing Leader (CTL) and synchronize to the leader's channel timing. This CTL election process is transparent to the end user. For a 12.5 kHz RF channel, only one CTL is elected, that is, the same radio that provides the channel timing for both timeslots irrespective of radio timeslot provisioning and color code provisioning. The selected CTL periodically announces the channel timeslot structure via beacons, and the other radios synchronize with the leader directly or indirectly (via other radios) by following the synchronization information in these beacons. The dual capacity direct mode beacon transmits for 600 milliseconds every 4.5 minutes. This only uses 0.22% of the channel capacity and should have little impact to other services.

3.2.2.2
Channel Timing Leader Preference

When operating in dual capacity direct mode, a radio's preference to be a Channel Timing Leader (CTL) can be CPS configured on a per channel basis as follows:

Preferred CTL
The radios that are always turned on, always selected to dual capacity direct mode channel, never scans or have large transmit coverage are "good" candidates to be the preferred CTL. Whenever possible, a mobile may act as the preferred CTL since synchronization beaconing may drain more battery capacity.

Normal Preference
The default configuration that allows a radio to act as the CTL, but should yield leadership to higher preference candidates.

Least Preferred
This option is not CPS selectable, but is automatically selected when a scan list is attached to the selected dual capacity direct mode channel.

Ineligible
This option may be selected in radios that are "bad" candidates to be a CTL. For example, radios that change channels often, or roam often, and so on, but at least one radio must not be "Ineligible".

To avoid frequent CTL re-election, it is recommended to assign the same CTL preference to all dual capacity personalities that use the same frequency when configuring a specific radio.

3.2.2.3
Color Code

Similar to direct mode operation, in dual capacity direct mode, color code 0-14 are specified on a per timeslot (channel) basis through CPS provisioning. Color code 15 is reserved for future usage and not available for dual capacity direct mode channels. Different color codes can be used in the two timeslots of an RF channel.

3.2.2.4
Channel Access Rule

Dual capacity direct mode channel access rules are specified on a timeslot (channel) basis through CPS provisioning. The channel access in dual capacity direct mode follows the same rules as defined in MOTOTRBO Channel Access on page 83.

3.2.2.5
Scan

To enable migration and interoperability, a dual capacity direct mode channel can have a scan list that includes a non-dual capacity direct mode channel, and a non-dual capacity direct mode channel can have a scan list that includes a dual capacity direct mode channel.

Therefore, a scan list may include a mixture of dual capacity direct mode and direct mode channels as well as analog and repeater channels. If talkback is enabled and the radio lands on a dual capacity direct mode channel, the radio can talk back in dual capacity direct mode in the proper timeslot.

There may be up to 16 channels in a scan list, among which the radio uses the DTC to track the channel timeslot structure. The choices for the DTC are: selected channel, last active, or other designated channel. In order for the selected DTC to be easily tracked, it is recommended to use the “selected channel” as the DTC and enable “Talkback”, especially when the selected channel is a dual capacity direct mode channel.

3.2.2.6
Interoperability and Backward Compatibility

A radio may be configured in CPS to operate in repeater mode, direct mode, dual capacity direct mode, or talkaround mode on different personalities. Direct mode is not as efficient as dual capacity direct mode in spectrum usage. However, it is still supported so that the radio is interoperable with other ETSI-DMR compatible radio and is backward compatible with software versions R02.00.00 or earlier, which can only support direct mode.

A radio operating in dual capacity direct mode is not interoperable with a radio operating in repeater mode, direct mode, or talkaround mode. The radio treats the other radio’s transmission as interference.

3.2.2.7
Revert Features

A radio does not monitor the GPS Revert Channel hence it does not track the channel timeslot structure on the GPS Revert Channel. Therefore, dual capacity direct mode channels can not be used as GPS Revert Channels.

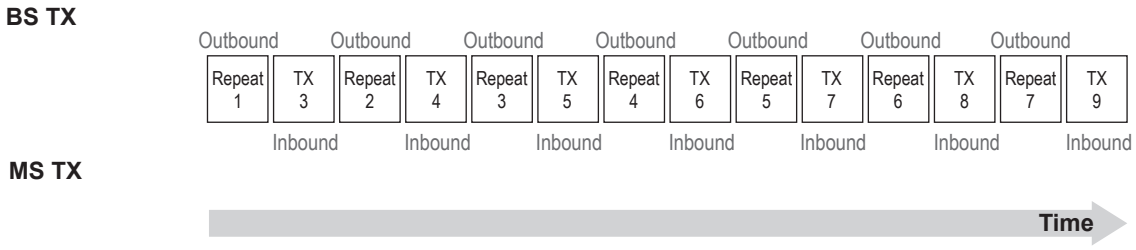
A radio that is selected to a dual capacity direct mode channel may revert to emergency Revert Channels, or GPS Revert Channels, or enhanced GPS Revert Channels.

3.2.3

Extended Range Direct Mode

The Extended Range Direct Mode feature uses a time division duplex repeater that receives a direct mode transmission and repeats it 90 ms later, as shown in the following figure:

Figure 108: Time Division Duplex Repeater



This mode's primary purpose is to extend direct mode range while utilizing a single frequency. (Note, this does not extend the range of Dual Capacity Direct Mode.) A radio initiates a transmission as it does in direct mode and can receive transmissions directly from a radio or from the repeater. At the beginning of reception, the radio selects the signal based on the operational mode. Therefore direct mode operation is still supported in the absence of the repeater without having to change channels.

Extended Range Direct Mode with Compatibility Mode enabled supports First Generation MOTOTRBO Radios and mixed radio fleet.

Extended Range Direct Mode without Compatibility Mode enabled does not support First Generation MOTOTRBO Radios, but supports additional features which are listed in the following table.

Table 73: Extended Range Direct Mode Features Distribution

	Extended Range Direct Mode in Compatibility Mode	Extended Range Direct Mode
Radio Support	First Generation MOTOTRBO and new radios	Radios supporting Extended Range Direct Mode
Operation	Radio locks onto the first signal (typically the direct signal if present).	Radio receives both signals (direct and repeated) and chooses the preferred one.
Transmit Interrupt Support	No **NOTE:** Transmit Interrupt in Direct Mode is still available, but it might be ineffective if an extended signal is present.	Yes
Restricted Access to System (RAS) Support	No	Yes
Wireline Support	Yes	Yes
Enhanced Channel Access (ECA) Support	No	Yes
Other	Radios do not require firmware upgrade.	Extended Range Direct Mode must be enabled on repeater and radios.

In Extended Range Direct Mode without Compatibility Mode enabled at the beginning of reception, the radio selects the preferred signal. When receiving directly from a radio, the receiving radio displays the talkaround icon. When receiving from the repeater, the receiving radio does not display the talkaround icon. Additionally, Enhanced Channel Access (ECA) is supported in this mode to minimize the impacts of transmission collisions.

Extended Range Direct Mode is a single site conventional mode solution that supports the following features:

- Voice Calls (Group, Individual and All)
- IP Data (Unconfirmed Group, Unconfirmed Individual and Confirmed Individual)
- Control (Radio Check, Radio Inhibit and Uninhibit, Remote Monitor and Call Alert)
- Privacy (Basic, Enhanced and AES)
- Restricted Access to System (RAS) (not supported in Compatibility Mode)
- Voice Transmitter Interrupt (not supported in Compatibility Mode)
- Enhanced Channel Access (not supported in Compatibility Mode)
- NAI wireline interface for voice and control for 3rd Party Voice and Control Applications
- MNIS Wireline Data gateway for MSI and 3rd Party Data Applications
- Remote Repeater Programming
- RDAC
- Analog CWID and FCC Level 1 monitoring
- Inband Data Services (Caller Alias and Location)

The solution does not support the following features:

- Repeater Broadcast Hangtime Signaling (same as direct mode)
- Data Revert Channel
- Digital Phone Patch
- Digital Voting
- Digital/Analog Mixed Mode
- RAS Migration Mode

3.2.3.1
Extended Range Direct Mode Feature Licensing

A software license is required in the repeater for this feature to be operational. The license however, is not required in the radio.

3.2.3.2
Repeater Emission Designator

When operating in Extended Range Direct Mode, the repeater should use emission designators 7K60FXD for data and 7K60FXE for voice. These are required to indicate the TDMA (pulsed) nature of the repeater's transmission.

3.2.3.3
Configuration in Repeater

Extended Range Direct Mode or Compatibility Mode for Extended Range Direct Mode is activated in the repeater by selecting **Enable** or **Compatibility Mode** from the drop-down list in Extended Range Direct Mode field within a Digital Channel and entering the same frequency for TX and RX frequency.

If Extended Range Direct Mode was enabled, it allows:

- Enhanced Channel Access (ECA) to be enabled
- The inbound (radio transmission) and outbound (repeater) transmissions to use different color codes. It is not necessary to use different color codes. However, this is recommended when operating on the same frequency as direct mode radios do not support this feature.

In case of an SLR1000 repeater, a high speed RF switch, which is installed internal to the repeater, is available (PMLN7263). If this kit is used, Tx/Rx switch must be configured for GPIO6. The active level is defaulted to the correct state and cannot be changed.

3.2.3.4
Configuration in Radio

Extended Range Direct Mode

This feature is activated in the radio by enabling the Extended Range Direct Mode field within a Digital Channel.

Once enabled, one TX/RX frequency is required to be entered. This feature allows the inbound (radio transmission) and outbound (repeater) transmissions to use different color codes. It is not necessary to use different color codes. However this is recommended when operating on the same frequency as direct mode radios not supporting this feature.

Compatibility Mode for Extended Range Direct Mode

Radios must be configured in Direct Mode to operate with a repeater in Compatibility Mode. No additional activation is required by radio to work with this mode.

3.2.3.5
System Configuration Considerations

Configuring repeater in **Compatibility Mode** and all radios in Direct Mode is required to have an extended range that works with a radio fleet including radios that do not support Extended Range Direct Mode feature. Color codes of a repeater and radios must match.

Both the repeater and all radios must support Extended Range Direct Mode and be configured with Extended Range Direct Mode **Enabled** to benefit from all Extended Range Direct Mode capabilities.

3.2.3.6
Repeater TX/RX Isolation

The Extended Range Direct Mode repeater requires 30 dB of isolation between TX and RX ports for the SLR 5000 and 8000 series. For SLR 1000 series, it requires 40dB of isolation. This can be accomplished by using two different antennas, one for transmit and the other for receive. The following chart can be used for guidance to obtain the required isolation.

Table 74: Horizontal and Vertical Antenna Required Isolation

Dipole Antenna Separation	VHF	UHF
Horizontal	20/65 feet	10/22 feet
Vertical	7.5/15 feet	3/5 feet

A single antenna may be used in conjunction with an RF switch capable of handling the repeaters TX power and deliver a switching delay less than 50 µsec. GPIO output pin T/R Switch is be used to drive the switch.

3.2.4
Repeater Mode

There are a few reasons why a customer may require a repeater in their system. The first is, if the required coverage area is large, they may require strategically located high power repeaters in order to cover all of their operating space. Even if their required coverage area is small, due to geographical limitations such as mountains, valleys or man made obstructions, they may still need multiple high power repeaters to reach all the coverage areas. They also may need the extra bandwidth a repeater offers. One channel may not be able to support a large number of users; therefore additional channels may be required.

In many of these cases, the insertion of a MOTOTRBO repeater can alleviate the problems with minimum additional cost. Such a repeater is transparent to field radio communications. They just select the required channel using their channel selector, and continue their normal communications. However, as in most conventional systems, if the repeater coverage does not overlap, the user needs to know his location, and switch to the other channel when required.

Even just having one MOTOTRBO repeater provides increased user capacity. The digital repeater operates in TDMA which essentially divides one channel into two virtual channels in digital mode; therefore the user capacity doubles. Without the repeater, this TDMA synchronization is not possible. The repeater utilizes embedded signaling to inform the field radios of the status of each channel (time slot). It informs the field radios of each channel's busy/idle status, the type of traffic, and even the source and destination information.

Another advantage during digital operation is error detection and correction. The further a transmission travels, the more interference it encounters, and inevitably more errors are introduced. The receiving MOTOTRBO radio, operating in digital mode, utilizes built-in error detection and correction algorithms, native to the protocol, to correct these problems. The MOTOTRBO repeater uses the same algorithms to correct the errors prior to retransmission, thus repairing any errors that occur on the uplink; it then transmits the repaired signal on the downlink. This greatly increases the reliability and audio quality in the system, which increases the customer's coverage area.

In digital mode, the repeater only retransmits digital signals from radios configured with the same system identifier. This aids in preventing co-system interference. The repeater does not block transmissions of radios within its own system.

As previously described, the repeater utilizes embedded signaling to announce the current status of each channel. It is up to the radios in the field to interpret these signals, and grant or deny their user's request

for transmission. Therefore, when a user or a group of users utilizes a channel (time slot), the repeater announces that the channel is being used and who is using it. Only radios that are part of that group are allowed to transmit. The repeater additionally allows a short duration of reserved time after a transmission. This allows other users in the group to respond to the originator. This reserved hang time greatly increases the continuity of calls, because new calls cannot start until the previous call ends. Without this feature, users may experience delays in responses (that is, between transmissions of calls), due to other calls taking over the channel in-between their transmissions.

After this reserved hang time, the repeater stays active for a short period of time, and offers an opportunity for any user on the system to transmit or start a new call. If no user transmits for a duration of time, the repeater stops transmitting. When the next radio transmission occurs, the repeater starts repeating again.

Most of the basic MOTOTRBO voice and data services work the same in repeater mode as they do in direct mode/dual capacity direct mode. The customer will only notice the increased performance and coverage.

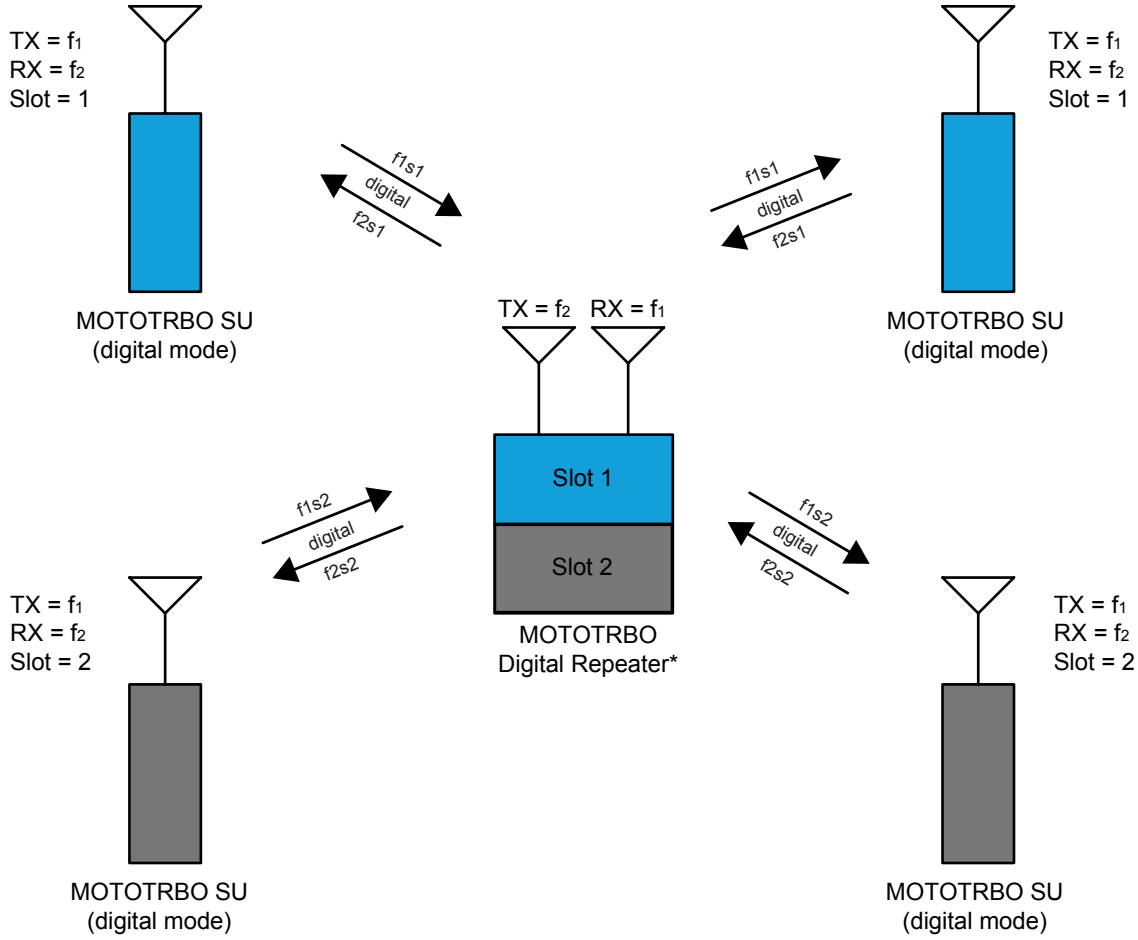
3.2.4.1
Digital MOTOTRBO Radios in Repeater Mode

In digital mode, a repeater uses one frequency pair (1-transmit, 1-receive) to support the two logical channels. As mentioned earlier, this is done by using TDMA technology to divide the physical channel into two time slots. In order to access the repeater, the radio user selects the physical and logical channel using the channel selector. Hence, when operating in repeater mode, the field radios cannot dynamically choose a time slot. Each of the channel selector positions is programmed for a particular digital frequency and time slot.

The end user sees, in effect, each time slot as a different conventional channel. Radio groups can be further segmented within the time slot by assigning different group IDs to each group. Groups on different time slots cannot communicate with each other.

Synchronization is the key to a MOTOTRBO repeater system. It is the role of the repeater to keep this synchronization. When accessed, the repeater begins transmitting idle messages as well as identifying the time slot structure. The radios synchronize to the transmissions from the repeater. When a radio transmits on its time slot, the radio pulses its transmissions in 30ms increments. This allows for simultaneous conversation to occur on the other time slot. While the first radio is pulsed on, the other radio is pulsed off. The repeater receives these two pulsed transmissions, combines them and transmits them in the correct order in one continuous transmission.

Figure 109: MOTOTRBO Digital Radios on MOTOTRBO Two-Slot Digital Repeater



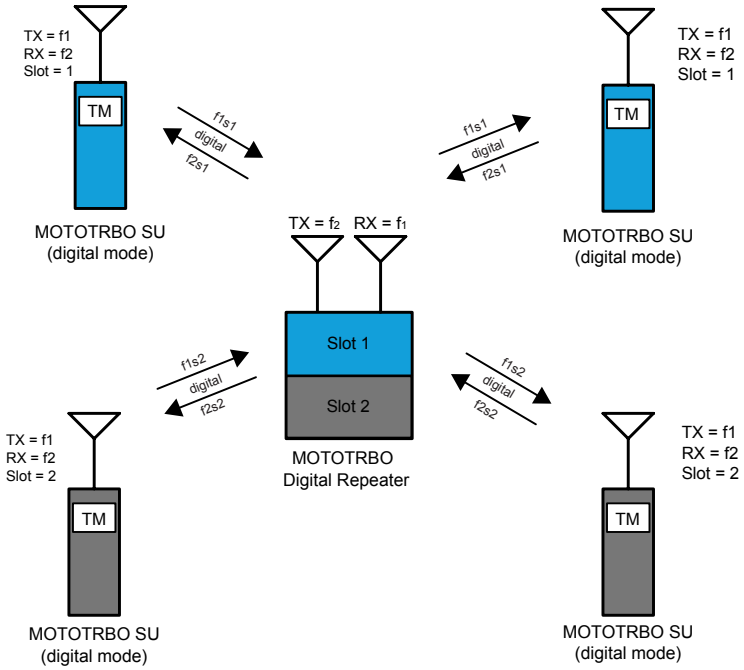
NOTE: Repeater operation supports all three methods of voice transmission: Group Calls, Private Calls and All Calls. They can also fully support all command and control messaging like Call Alert, Radio Check, Radio Enable/Disable, Remote Monitor and Emergency.

3.2.4.1.1

Text Messaging in Repeater Mode

In repeater mode, the MOTOTRBO radios are capable of sending text messages to other radios. Radio to radio text messaging is accomplished by a text messaging application that is built into the radio. From the front keypad, the radio user can select the target radio, and type a text message.

Figure 110: MOTOTRBO Radios in Digital Two-Slot Digital Repeater Mode with Built-In Text Messaging

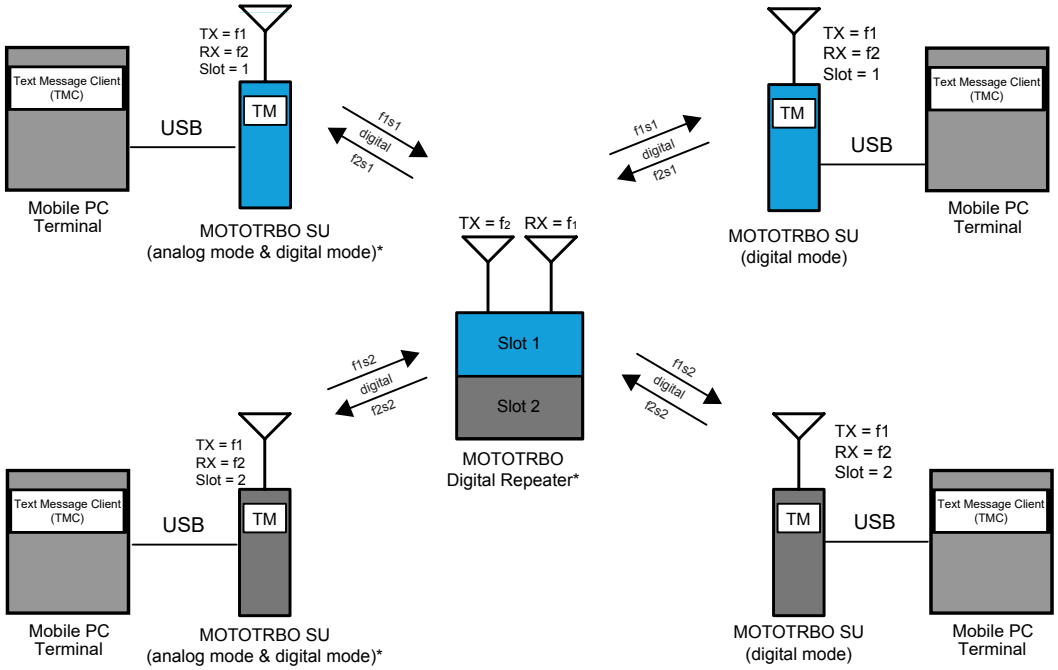


In order for the text message to be sent successfully to the target radio, both radios need to be on the same channel and time slot. Similar to voice, if multiple direct mode/dual capacity direct mode frequencies are being used, the user must choose the channel his target is on before sending his text message. The radios do not have to be on the same group.

Text messaging and the previously discussed voice services operate on the same channel and time slot. Since data operates in a polite manner, the radio avoids transmitting text messages while any voice service is active. If operating with only field radios, text messages are limited to radio to radio communications.

Text messages can also be sent from radio to radio using a PC attached to the radio. A software-based text messaging client will be installed on the PC. These configurations are commonly used in vehicles or on desktops that do not have LAN connections. Since they can run on AC power or off the in-vehicle battery, mobile radios are usually used for these applications, though a portable can also be used. Note that the radio can be configured to route incoming text messages to itself or to the PC, but not both.

Figure 111: MOTOTRBO Radios in Digital Two-Slot Digital Repeater Mode with Text Messaging

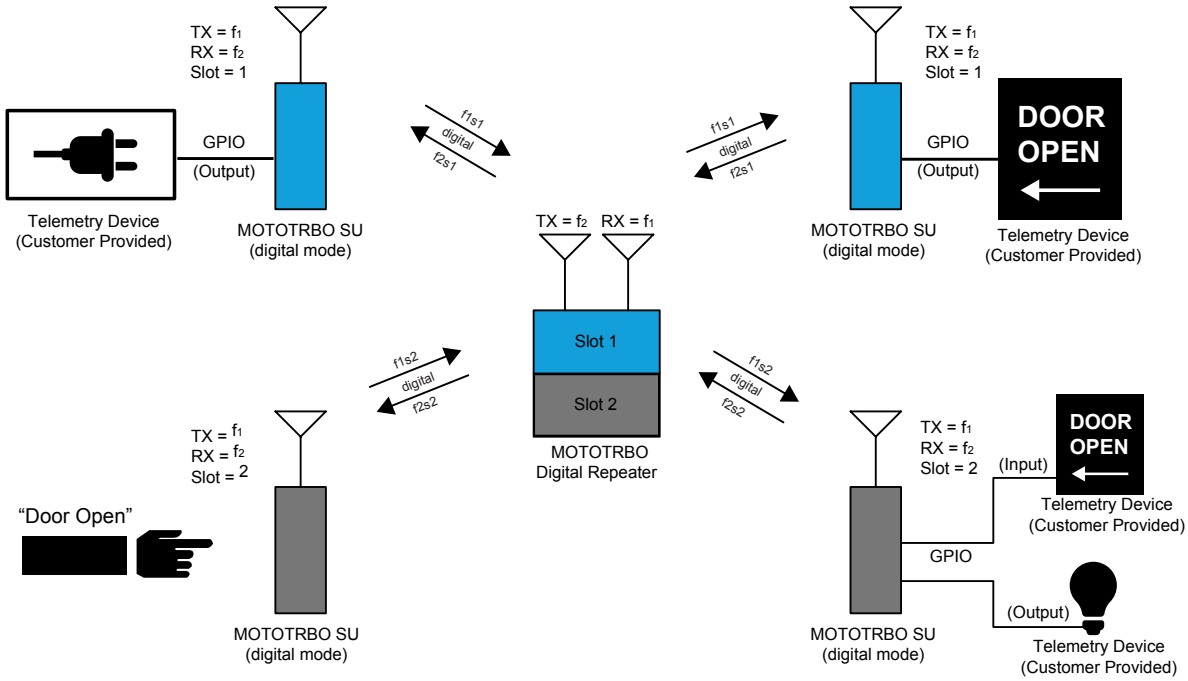


3.2.4.1.2

Telemetry Commands in Repeater Mode

The following figures show some basic telemetry configurations using both time slots of a repeater. A description of each follows.

Figure 112: MOTOTRBO Radios in Digital Two-Slot Digital Repeater Mode with Telemetry Functions



In the first basic configuration a portable radio is programmed with a button (shown by the pointing finger in the figure) that sends a preconfigured telemetry command Over-The-Air on the second time slot to toggle a mobile radio's output GPIO pin. The GPIO pin is connected to external hardware that detects the closure and turns on a light (shown by a light bulb above). This configuration can be extended to such things as remotely opening door locks, turning on pumps, or switching on sprinklers. Another application might be to combine the voice from the radio's external audio lines, a relay closure, and a public announcement system to remotely make announcements over the intercom from the portable radio.

This second basic configuration is a mobile configured on the second time slot, connected to customer supplied external telemetry hardware (shown by the door icon in lower right corner), detects a closure that signifies a door has been opened. Upon detecting the GPIO pin as active, it sends a preconfigured Text Status Message to a particular portable radio. The portable radio displays "Door Opened" to the user as a popup alert. This basic configuration can be used at remote locations to detect a variety of sensors such as water levels, door and window intrusions, or even motion sensors. Combining the first and second configuration, the user can create complex control systems that initiates a large door to close, and then announces when the door physically closes.

The third basic configuration is a mobile configured on the first time slot, connected to customer supplied external telemetry hardware, detecting a closure that signifies a door has been opened (shown by a door in upper right corner). Upon detecting the GPIO pin as active, it sends a telemetry toggle command to another mobile radio on the first time slot. This mobile radio is configured to toggle an output pin which is connected to telemetry hardware that sounds an alarm (shown by alarm on upper left corner). Similar to the other configurations, this method can be extended to a myriad of other solutions such as only opening doors when other doors have been closed or turning on water pumps when water levels reach a particular level. This configuration can be used automate the environment of two remote locations together. The possibilities are only limited by the designer's imagination.

3.2.4.1.3
Server Based Data Applications in Repeater Mode

NOTE: MOTOTRBO also supports server based data applications in repeater mode. This configuration consists of a PC (referred to as the Application Server) running the server software connected to the radio infrastructure through a mobile radio or through the MNIS application. For details on data communication with applications through the repeater network interface instead of a Control Station, see MOTOTRBO Network Interface Service on page 315 and MOTOTRBO Device Discovery and Mobility Service on page 327.

The mobile radio is usually AC powered. The mobile is configured as a Control Station, therefore it routes all data to the Application Server. Since this mobile is the radio gateway to the server, it should be configured to transmit and receive on a single channel (frequency and time slot). The Control Station is programmed with a known radio ID so the field radios know how to contact the server. The server and the Control Station (connected through a USB) must be located in an area that is in good coverage of the repeater it is communicating with. If there are multiple repeaters covering a large geographical area, the Application Server's Control Stations must be located in good coverage of each repeater. This is important since it is common for the overlap between repeaters to be small and often only in low signal strength areas. There can only be one Application Server per system.

One key service offered by the server based configuration is radio presence notification. The Presence Notifier is required to reside on the Application Server. The purpose of the Presence Notifier is to track whether field radios are currently present on the system. Upon power-up or channel change, the MOTOTRBO radio transmits a registration message to the Control Station connected to the Application Server, where the Presence Notifier resides. The Presence Notifier then informs other data applications that the radio is available to receive and transmit data messages.

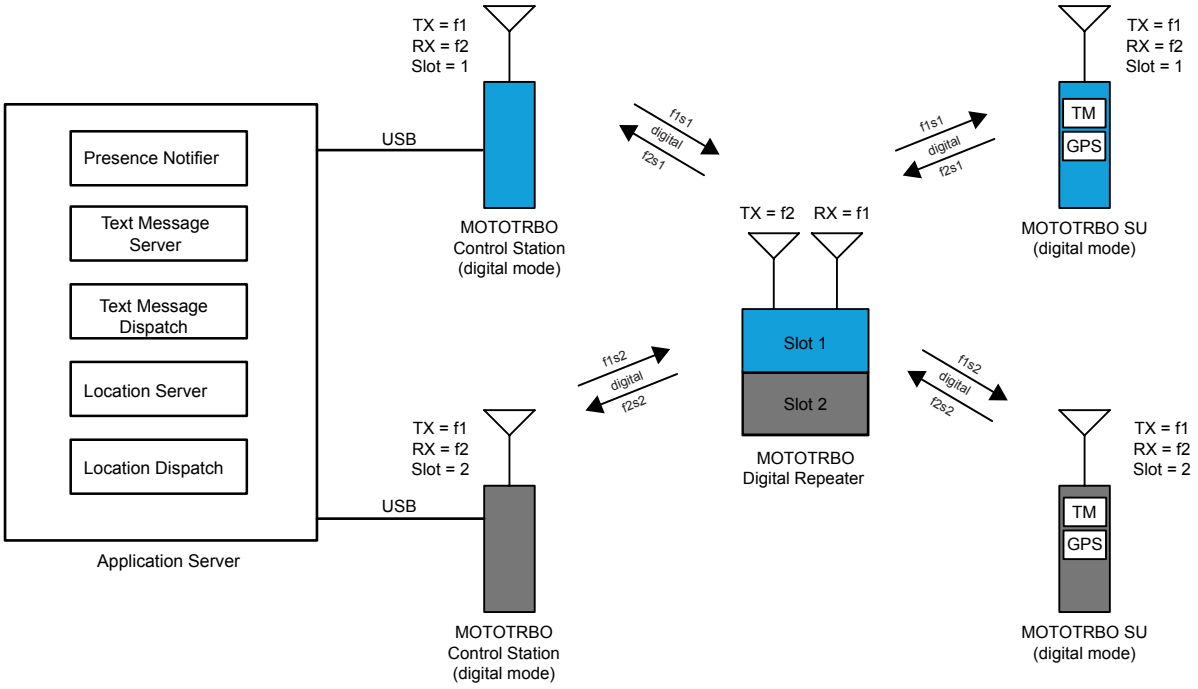
Each frequency and time slot that needs to communicate with the Application Server needs to have its own Control Stations. The Application Server can be connected to up to 16 control stations. Each Control Station is configured to communicate on the specified frequency and time slot and acts as the data gateway for that

channel. Therefore a MOTOTRBO system can support server based data on up to two repeaters, each with two time slots.

When a radio powers up or changes channels, it sends a registration to the Presence Notifier through the Control Station on its frequency and time slot, which in turn informs the applications of the radio's presence. Each Control Station has the same radio ID, therefore the field radios transmit their messages to the same radio ID regardless of which frequency and time slot they are on. Because the field radios are located on different time slots, there needs to be a method to track the location of each radio so that outbound data from the Application Server can be routed to the appropriate time slot. A static IPv4 route may be required to be manually entered in the PC that routes all radio data through the Control Station's network interfaces. This allows data applications to simply transmit a data message to the radio and route to the correct frequency and time slot.

Any channel that supports data and needs to communicate to the Application Server needs a dedicated Control Station. Below is a diagram of this configuration.

Figure 113: MOTOTRBO Radios in Digital Two-Slot Digital Repeater Mode with a Server-Based Configuration Using Control Stations



Typically, location applications require a server-based configuration and the Presence Notifier to operate. The Location Server application can be installed on the Application Server machine with the Presence Notifier. When a radio registers with the Presence Notifier, it informs the Location Server that this radio is now on the system. The Location Server then sends out a service availability message through the Control Station to the radio informing it how often to send in its periodic updates and what to do if an emergency is initiated.

Location Dispatch applications request a radio's location information from the Location Server application, and display the radio's location on a map. A Location Dispatch application can reside on the Application Server as well.

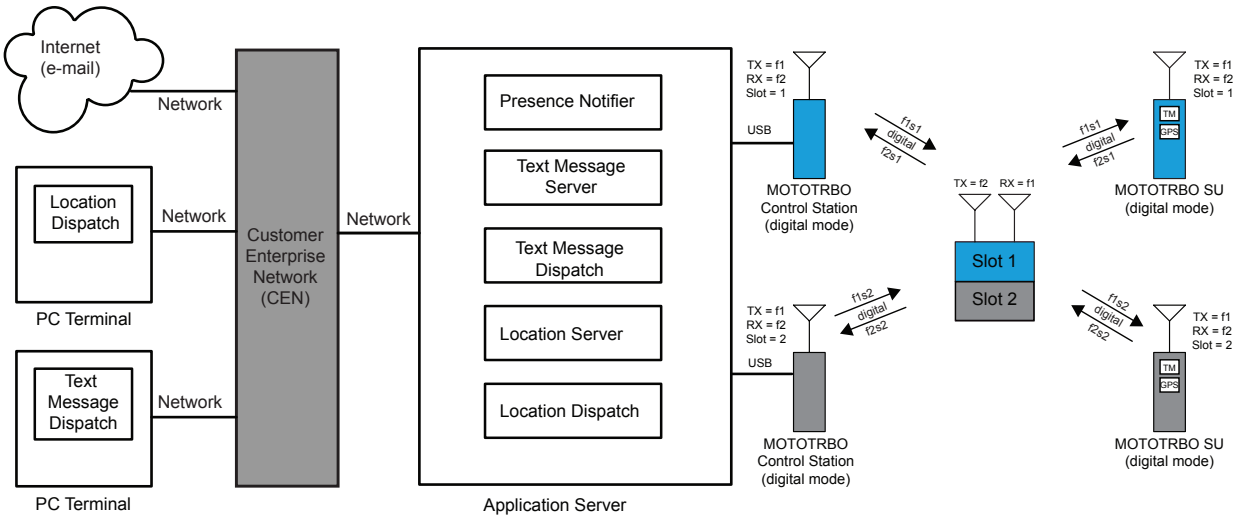
Text messaging also uses a server based configuration. Similar to the Location Server, the Text Message Server application can be installed on the Application Server machine with the Presence Notifier. When a radio registers with the Presence Notifier, it informs the Text Message Server that the radio is now on the system. The Text Message Server then sends out a service availability message through the Control Station to the radio informing it how it can communicate with the Text Message Server. Text Message Dispatch applications communicate with the Text Message Server in order to send and receive messages to and from

the radio network via the connected Control Station. Like the Location Dispatch, the Text Message Dispatch application can reside on the Application Server too.

As previously described, radios can send text messages to each other without communicating through the Text Message Server. But in order to send and receive text messages to Text Message Dispatchers, the Text Message Server configuration is required. This configuration also works with external text message applications connected to the field radios.

This configuration can be expanded by locating up to four Text Message Dispatchers and four Location Dispatchers throughout the customer's Enterprise Network. Up to four installations of each application can be located anywhere on the customer's LAN, as long as they can communicate with the Application Server. The Dispatcher installations on the Application Server counts as one of the instances of the dispatch software. The following diagram shows two instances of each application. One is on the Application Server and one remote. The applications can reside on the same remote machine, if desired.

Figure 114: MOTOTRBO Radios in Digital Two-Slot Digital Repeater Mode with a Server-Based Configuration Using Control Stations and Remote Dispatchers



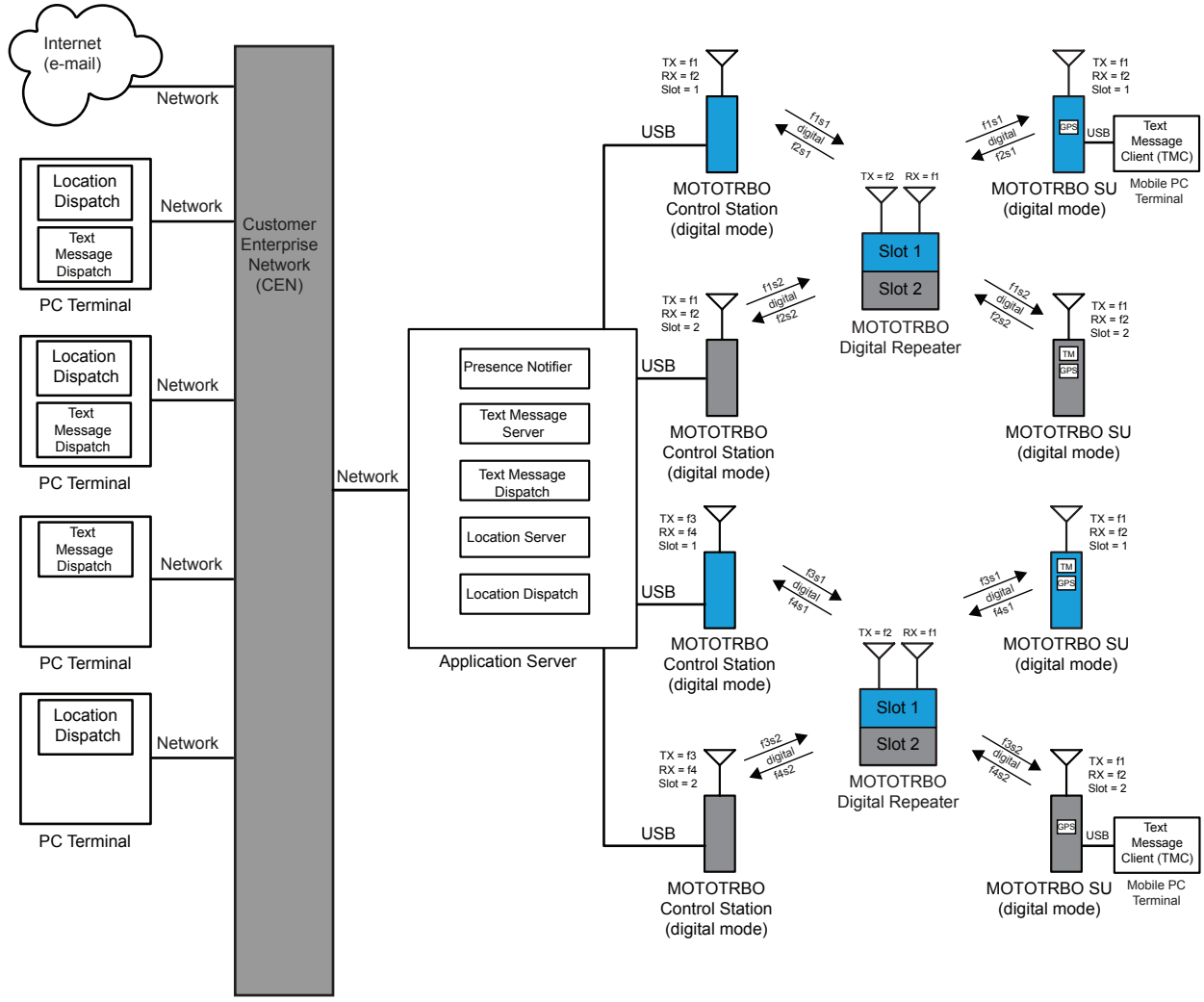
Another Text Message service that is only available in a server based configuration is the ability to receive and send text messages to external e-mail addresses. This allows PCs or pagers and cell phones that are text message capable on the system to send e-mail messages. In order for the Text Message Server to communicate with the outside world, the Application Server must have access to the Internet. When a radio sends a text message to a Text Message Dispatcher, and it is identified as an external e-mail address in the Text Message Server, the Text Message Server forwards the text message to the designated e-mail address. It requires access to the Internet in order to send the message.

The Text Message Server also forwards incoming e-mails in a similar fashion. The source e-mail address must be configured in the Text Message Server for it to forward the text messages to the destination radio. This blocks unknown e-mail traffic from utilizing the bandwidth of the radio system.

The following figure shows is an example of a server based configuration that supports four data capable time slots with local and remote dispatchers.

NOTE: Any mix of external and internal radio Text Message Clients are supported on each channel.

Figure 115: MOTOTRBO Radios in Digital Two-Slot, Digital Repeater Mode with Text Message Server, Location Server Using Control Stations with Local and Remote Dispatchers

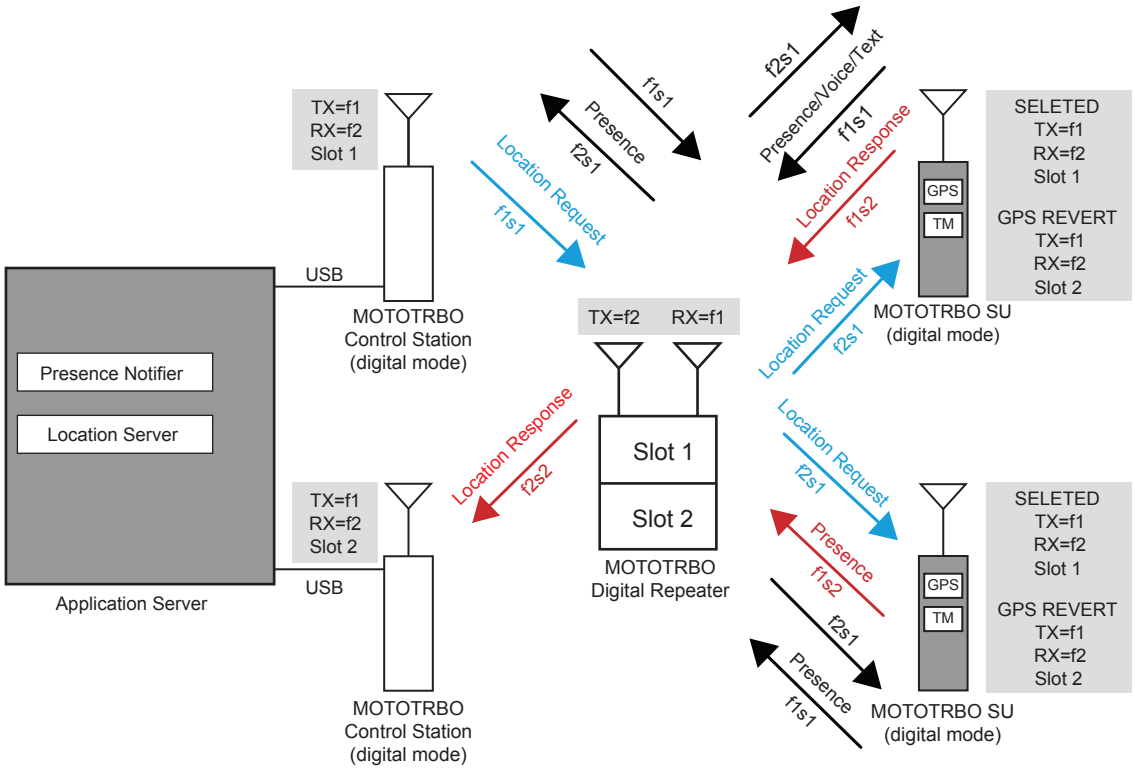


3.2.4.1.4

GPS Revert in Repeater Mode

With the addition of the GPS Revert feature, it is now possible to transmit Location Update messages on channels other than the Selected Channel. See GPS (GNSS) Revert Channel on page 117 for configuration information. Figure 116: MOTOTRBO Radios in Two-Slot Digital Repeater Mode with GPS Revert Configuration on page 354 illustrates this concept in its simplest form while operating in repeater mode. In this example, channels f1s1 and f2s1 compose the Selected Channel frequency pair and channels f1s2 and f2s2 compose the GPS Revert Channel frequency pair. Communications such a presence, location requests (Application Server to radio), text, and voice occur on the Selected Channel, while all location responses (radio to Application Server) including location updates occur on the GPS Revert Channel. Therefore, a minimum of two Control Stations are required to support GPS Revert.

Figure 116: MOTOTRBO Radios in Two-Slot Digital Repeater Mode with GPS Revert Configuration



For details on data communication with applications through the repeater network interface instead of a Control Station, see MOTOTRBO Network Interface Service on page 315 and MOTOTRBO Device Discovery and Mobility Service on page 327.

Under a typical scenario, the radio is powered on, and then registers on the Selected Channel with the Presence Notifier and the Location Server. The radio receives a Periodic Location Request and an Emergency Location Request from the Location Server on the Selected Channel. This Periodic Location Request instructs the radio to send location updates at a specific rate, while the Emergency Location Request instructs the radio to send a single Emergency Location Update when an emergency is initiated.

The radio spends the most time on the Selected Channel. The radio only switches to the GPS Revert Channel when a Location Update requires to be transmitted. Since voice transmissions have priority over data transmissions, when the radio is involved in a call on the Selected Channel, the Location Update is queued until after the call is completed. To minimize the amount of time spent away from the Selected Channel while on the GPS Revert Channel, the radio does not attempt to qualify traffic on the GPS Revert Channel. Therefore, all voice, data, and control messages transmitted to a radio should never be transmitted on the GPS Revert Channel, as they cannot reach their destination.

The example in Figure 116: MOTOTRBO Radios in Two-Slot Digital Repeater Mode with GPS Revert Configuration on page 354 illustrates only one GPS Revert Channel. However, depending on the GPS data load, more than one GPS Revert Channel may be needed. For example, a single large group that generates significant Location Update traffic must be sub-divided across several GPS Revert Channels. Each GPS Revert Channel requires a Control Station, which must be connected to the Application Server PC. The maximum number of Control Stations that can be connected to the PC is four.

3.2.4.1.5
Enhanced GPS Revert in Repeater Mode

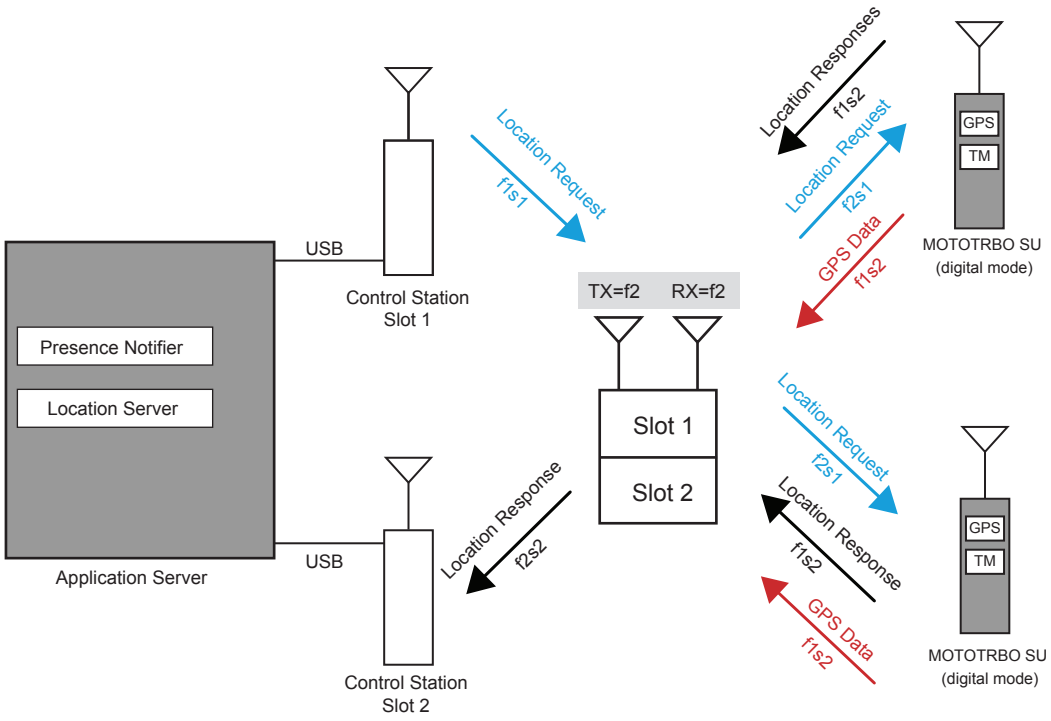
This section provides the recommended system topologies for the Enhanced GPS Revert feature in Single Site, Capacity Plus Single Site, Capacity Plus Multi Site and IP Site Connect modes of operation.

System	Description
 IP Site Connect	Enhanced GPS Revert feature is supported in IP Site Connect mode of operation.
 Capacity Plus Single Site	Enhanced GPS Revert feature is supported in Capacity Plus Single Site mode of operation.
 Capacity Plus Multi Site	Enhanced GPS Revert feature is supported in Capacity Plus Multi Site mode of operation.

3.2.4.1.5.1
Single Site Conventional

Figure 117: Single Site Conventional System with an Enhanced GPS Revert Channel on page 356 is a system configuration that shows how the Enhanced GPS Revert feature can be used in single site mode operation. It is assumed that the repeater has slot one configured for Voice, Text and ARS data and slot two for location responses. When a radio powers on, the radio registers on the Home channel with the Presence Notifier, which notifies the Location Server. All outbound data from the server (including location request) is routed on the Home channel whereas all location responses are on the Enhanced GPS Revert Channel. There should not be any non-GPS traffic on the GPS Revert Channel as it affects GPS reliability. Voice calls on an Enhanced GPS Revert Channel are not repeated.

Figure 117: Single Site Conventional System with an Enhanced GPS Revert Channel



For details on data communication with applications through the repeater network interface instead of a Control Station, see MOTOTRBO Network Interface Service on page 315 and MOTOTRBO Device Discovery and Mobility Service on page 327.

A user may also configure both slots of the repeater for enhanced GPS through the CPS. In this scenario, the user needs another repeater for voice and regular data, because only GPS data is supported on slots configured with Enhanced GPS.

3.2.4.1.5.2
IP Site Connect Mode

IPSC

Figure 118: IP Site Connect System with an Enhanced GPS Revert Channel on page 357 shows a typical IP Site Connect system where slot 2 of all the repeaters have been configured as a wide area Enhanced GPS Revert Channel and slot 1 as the Home channel. Only location responses are routed on slot 2, whereas voice, text and ARS messages are routed using slot 1 (Home channel). The Enhanced GPS revert slot (slot 2) of all the repeaters and all subscribers in the system that send GPS data using the Enhanced GPS revert functionality should have the same window size.

The total number of windows are shared among all the wide area Enhanced GPS revert repeaters in the system. Only one repeater in the system should have a value (90%, 75%, 60% or 45%) selected for Period Window Reservation (this does not have to be the Master repeater, a peer is also possible), whereas all the other repeaters in the system select a value of “None” using CPS. The repeater scheduler then schedule windows for all the other wide area enhanced GPS revert repeaters.

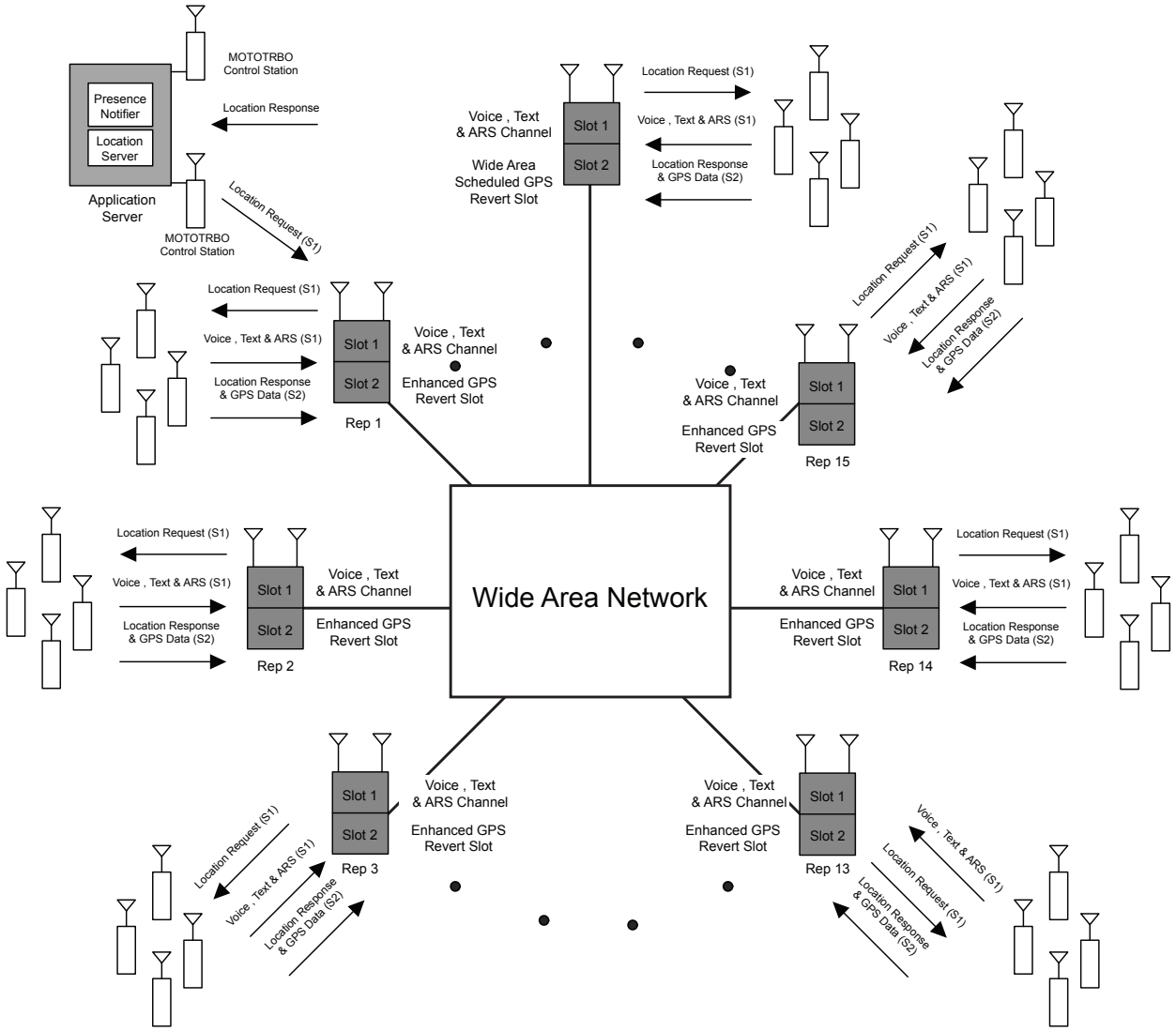
The Application Server and Control Stations can be in the coverage area of any repeater in the IP Site Connect system. In below, they are shown to be in the coverage area of repeater 1. For a window size of

5 or 6, it is recommended to use a network with an inter-repeater communication delay of 60 milliseconds or less. In case delay is observed to be higher than 60 milliseconds, then a window size greater than 7 is recommended for system reliability even if the amount of data requires a smaller window size.

NOTE: Increasing the window size decreases the system throughput.

The user may also configure both slots of the wide area system for enhanced GPS revert. In this scenario, the user will need to configure both voice and other data on a different IP Site Connect system.

Figure 118: IP Site Connect System with an Enhanced GPS Revert Channel



For details on data communication with applications through the repeater network interface instead of a Control Station, see MOTOTRBO Network Interface Service on page 315 and MOTOTRBO Device Discovery and Mobility Service on page 327.

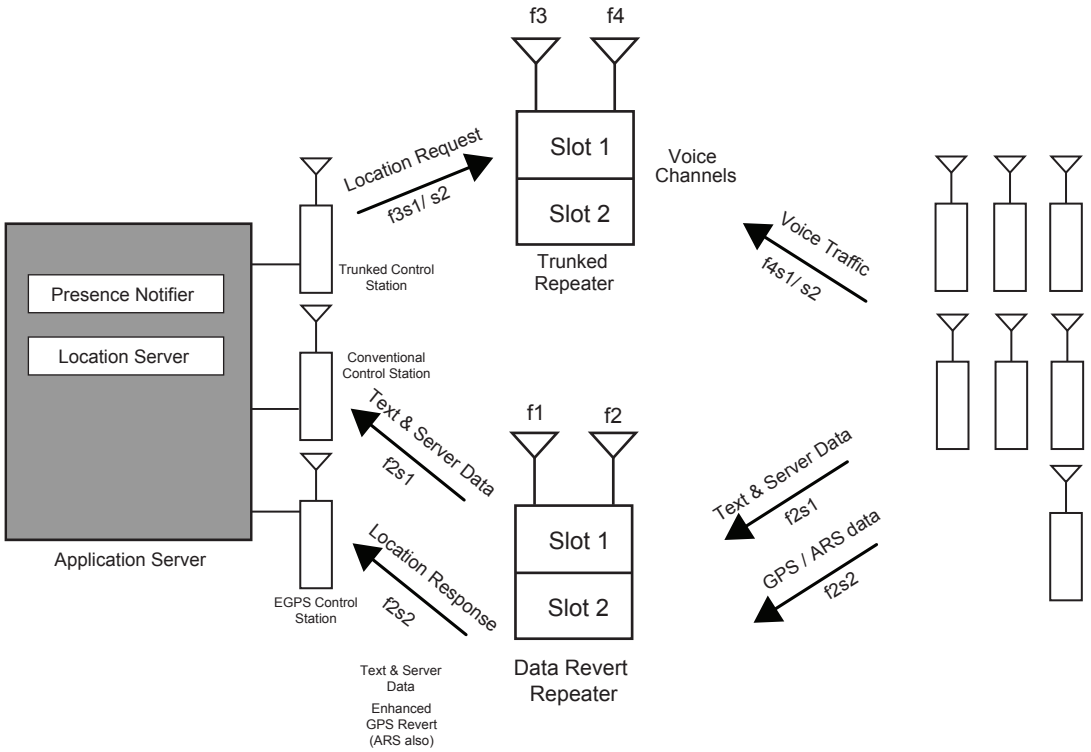
3.2.4.1.5.3
Capacity Plus Single Site Mode

CPSS

In Capacity Plus Single Site mode, one or both slots of a Data Revert repeater can be configured as Enhanced GPS Revert Channels.

Text and server data are routed on the slot configured for Data Revert whereas GPS and ARS registration data is routed on the slot configured for Enhanced GPS Revert. The location requests are sent on the Trunked Channel while the location responses are sent on the Enhanced GPS Revert Channel.

Figure 119: A Capacity Plus Single Site System with an Enhanced GPS Revert Channel



For details on data communication with applications through the repeater network interface instead of a Control Station, see MOTOTRBO Network Interface Service on page 315 and MOTOTRBO Device Discovery and Mobility Service on page 327.

3.2.4.1.6
Summary of Features in Digital Repeater Mode

The following features are supported in digital repeater mode:

Table 75: Digital MOTOTRBO Radios in Repeater Mode

Voice Features	Signaling Features	Emergency Handling	Data Calls	Other Features
Group Call	PTT ID and Aliasing	Emergency Alarm	Text Messaging	Two channels (slot 1 and slot 2) per repeater frequency pair
Private Call	Radio Inhibit	Emergency Alarm with Call	Location Tracking	Scan*

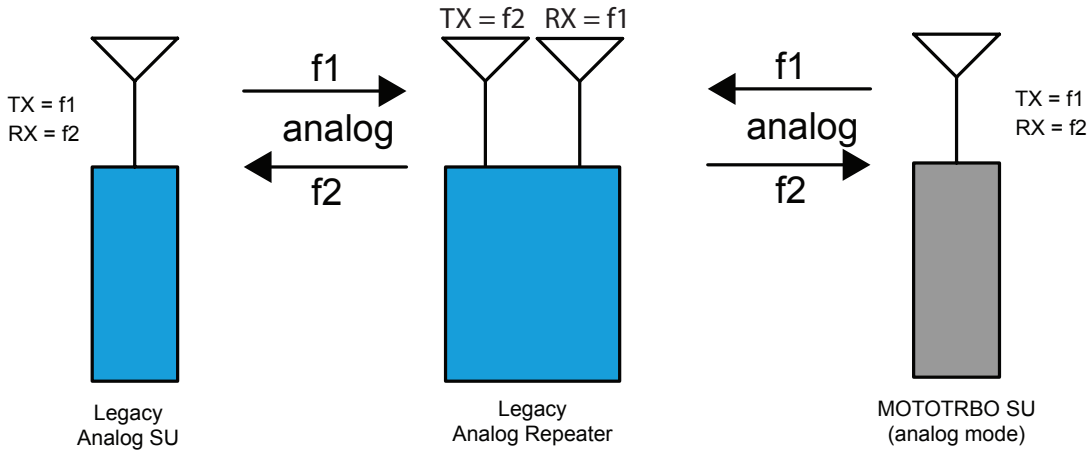
Voice Features	Signaling Features	Emergency Handling	Data Calls	Other Features
All Call	Remote Monitor	Emergency Alarm with Voice to Follow	Telemetry	Time-out Timer
Voice Interrupt	Radio Check	Emergency Revert	Third-Party (ADP) Applications	Polite to All system access
Dual Tone Multi Frequency	Call Alert	Emergency Voice Interrupt	GPS Revert	Polite to Own System channel access
Digital Telephone Patch	Remote Voice Dekey	–	Data Over Voice Interrupt	Impolite channel access

* See Scan Considerations on page 156 for more information on the different scan modes supported by different topologies.

3.2.4.2
Analog MOTOTRBO Radios in Repeater Mode

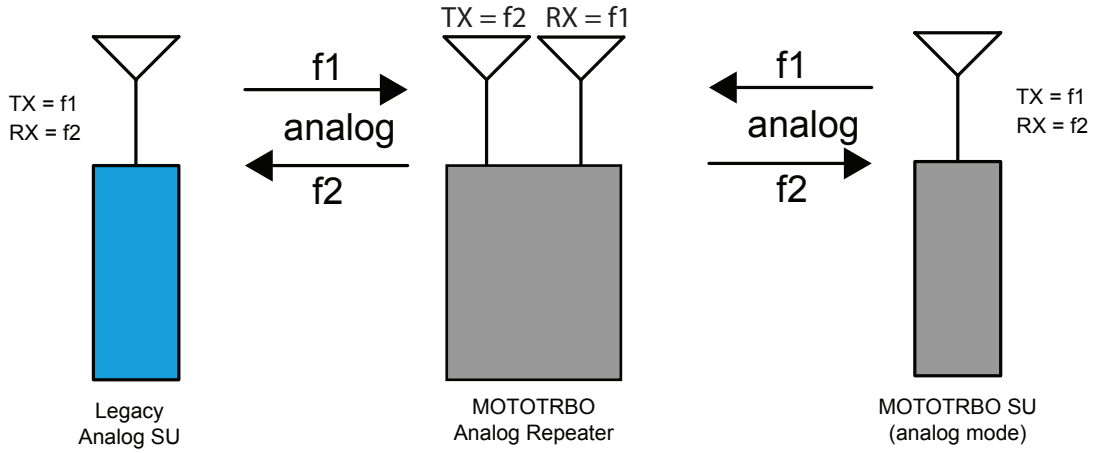
MOTOTRBO radios support analog repeater mode as well.

Figure 120: MOTOTRBO Analog and Legacy Analog Radios on Legacy Analog Repeater



In order for the MOTOTRBO radio to communicate with the existing analog or Dynamic Mixed Mode repeater, it must be programmed for analog mode as well as programmed with the same frequency and other options (PL, DPL, and others), as the existing analog or Dynamic Mixed Mode repeater. While in analog mode, the MOTOTRBO radio supports most standard analog features including a subset of MDC signaling features. While in analog repeater mode, the MOTOTRBO radios do not support any of the digital features. While in Dynamic Mixed repeater mode, MOTOTRBO radios support both analog and digital features.

Figure 121: MOTOTRBO Analog and Legacy Analog Radios on MOTOTRBO Analog Repeater



If required, the MOTOTRBO repeater can be programmed to operate in analog repeater mode. When operating in this mode, it inter-operates with the existing analog radios and the MOTOTRBO radios operating in analog mode. It is important to note that the MOTOTRBO repeater can only be configured to operate in analog mode or digital mode. It does not do both at the same time.

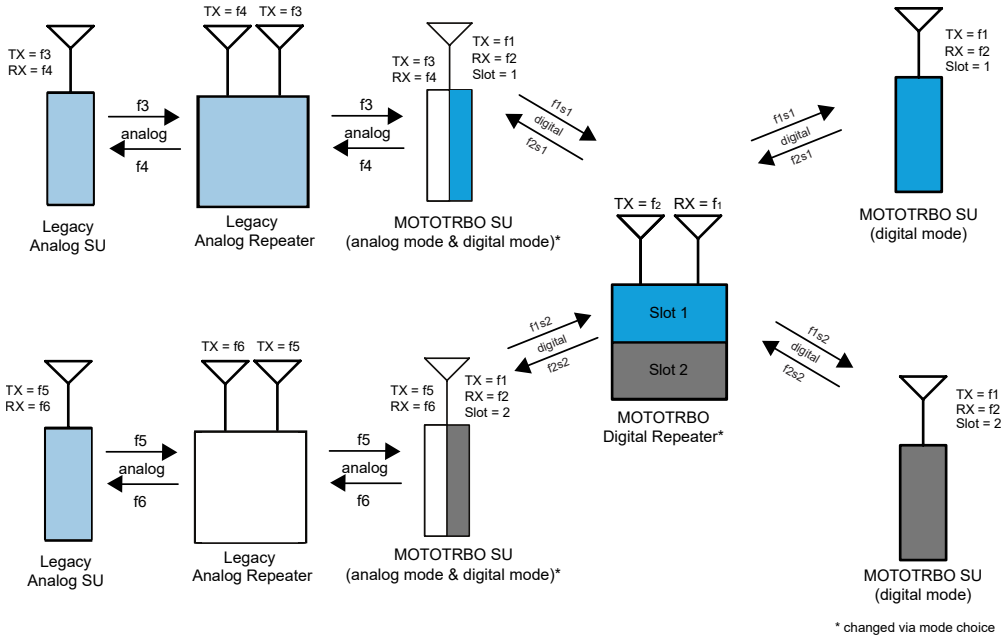
If required, the MOTOTRBO repeater can be programmed to operate in Dynamic Mixed Mode. When operating in this mode, repeater inter-operates with the existing analog radios and the MOTOTRBO radios operating in analog and digital modes. Repeater dynamically switches between analog and digital calls. While the repeater repeats one analog call at a time, it repeats two digital calls at a time (one on each logical channel).

The MOTOTRBO radio can be configured with both analog and digital repeater channels. The user can select between the analog and digital repeaters through the Channel Selector Knob.

Alternatively, the MOTOTRBO radio user can program the radio to scan between the analog and digital channels to ensure that they do not miss a call. The programming can be done from the keypad of the radio or through CPS.

The following is an example configuration of a mixed repeater mode system.

Figure 122: MOTOTRBO Digital Radios on a Two-Slot MOTOTRBO Digital Repeater with Analog Legacy Repeater Support



3.2.4.2.1 Summary of Features in Repeater Mode

All features listed in Wi-Fi Support on page 249 are supported in analog repeater mode.

3.2.5 IP Site Connect Mode

IPSC

In IP Site Connect mode, repeaters across dispersed locations exchange voice, data, and control packets over an IPv4-based backend network.

The potential applications of this mode include:

- Connecting two or more dispersed locations for day-to-day communications. For example, a customer's manufacturing facility and a distribution facility across towns can be connected using MOTOTRBO repeaters in IP Site Connect mode.
- Building a larger or more effective RF coverage area. For example, multiple repeaters installed in an amusement park or a high-rise building can be connected to provide a contiguous area of RF coverage. The need for multiple repeaters may stem from any combination of geography (distance or topographical interference problems) and in-building or cross-building RF penetration issues.
- Broadcasting announcements to all sites. This is useful in case of emergency or special events.
- Connecting repeaters operating in different RF bands. For example, repeaters operating in UHF (UHF-1 and UHF-2) or VHF frequencies can be combined so that voice or data from one system flows into another.

- Connecting to IP-based applications. IP Site Connect mode allows the customers to connect to third-party IP-based dispatch consoles, or call logging and recording applications, or routing calls to/from IP-based phones.

3.2.5.1
Topologies of the IP Site Connect System

IPSC

IP Site Connect Systems can consist of the following topologies:

- A wide area system with a centralized data Application Server.
- Wide and local area systems with distributed data Application Servers.
- Multiple wide area systems with a centralized data Application Server.

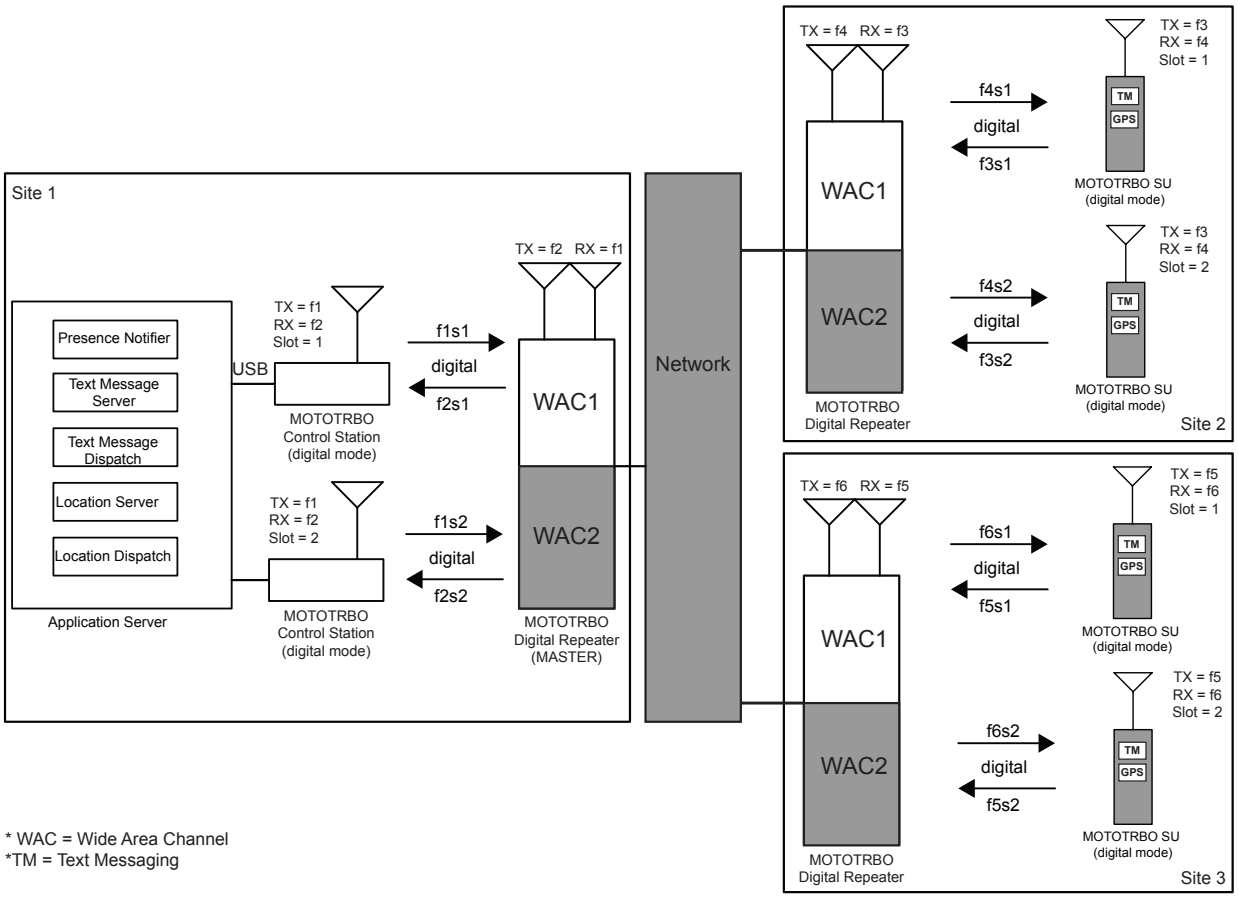
3.2.5.1.1
Wide Area System with a Centralized Data Application Server

IPSC

This basic topology, as shown in Figure 123: Wide Area System with Centralized Data Application Server on page 363, is a single wide area system that consists of multiple single repeater systems operating in digital mode and zero or more Application Servers connected over a back-end network that supports IPv4, where:

- A repeater system consists of a fixed digital repeater, digital radios (with or without an accessory or a data terminal), and two conventional physical channels. Only one of the repeaters, which is called the Master, has an additional role in the IP Site Connect mode. This additional role involves brokering of UDP/IP address and states of repeaters.
- A radio uses one slot of a pair of frequencies (that is, inbound and outbound) to communicate with its repeater. The pair of frequencies and/or the color code used by repeaters are not necessarily the same. Their frequencies may be in different frequency bands. The geographically adjacent repeaters have different frequencies. Two repeaters with the same frequency must be separated by a suitable distance to minimize interference and must use unique color codes.
- An Application Server is a PC-like equipment where one or more application runs. An application can be a data application such as a Location Server, Text Message Server or a voice application such as a Console. An Application Server is connected to one or two Control Stations, and these Control Stations are connected Over-The-Air to a repeater. If the configuration has more than one Control Station, then a static IPv4 route may be required to be manually entered in the Application Server. A third-party application can reside on an Application Server and since the Application Server is connected to Control Stations (one per logical channel), the application is not required to implement any third-party API that partially emulates the behavior of a MOTOTRBO repeater and radio.
- The back-end network can be a dedicated network or an Internet provided by an Internet Service Provider (ISP). For more information, see Considerations for the Back-End Network in IP Site Connect Mode on page 424. A repeater can be behind a firewall and/or a router with or without a NAT. A repeater has USB and Ethernet network interfaces. The USB is used for connecting a local PC and Ethernet is used for connecting to the back-end network of an IP Site Connect system.

Figure 123: Wide Area System with Centralized Data Application Server



For details on data communication with applications through the repeater network interface instead of a Control Station, see MOTOTRBO Network Interface Service on page 315 and MOTOTRBO Device Discovery and Mobility Service on page 327.

There may be an application known as RDAC-IP running on a host PC connected to the backend network of an IP Site Connect system. The application displays the status of repeaters and allows its user to control some of the parameters of a repeater. The host PC maintains its link with the Master and other repeaters using the same protocols as other repeaters in an IP Site Connect system. Note that there may be a local RDAC application running on a host PC connected to a repeater through RNDIS-USB interface. Also, analog, and local area only repeaters can be connected to wide area system so that they may be managed by the RDAC application.

In digital mode, MOTOTRBO offers two logical channels. The configuration above shows both the channels acting as wide area channels. This means that when a call starts at one of the logical channels of a repeater, that repeater sends the call to all the other repeaters and they repeat the call on their corresponding logical channel. Since calls are not repeated on both logical channels, a radio on a logical channel cannot participate in a voice call on the other logical channel or logical channels of other IP Site Connect systems unless scan is utilized. Note that scanning cannot be enabled while roaming. Radio to radio data messages are not repeated on both slots either, although it is possible to support one Application Server to serve multiple wide area channels. The Application Server interfaces with the wide area channels in the same way as it interfaces with the local area channels. This is described in Server Based Data Applications in Repeater Mode on page 350.

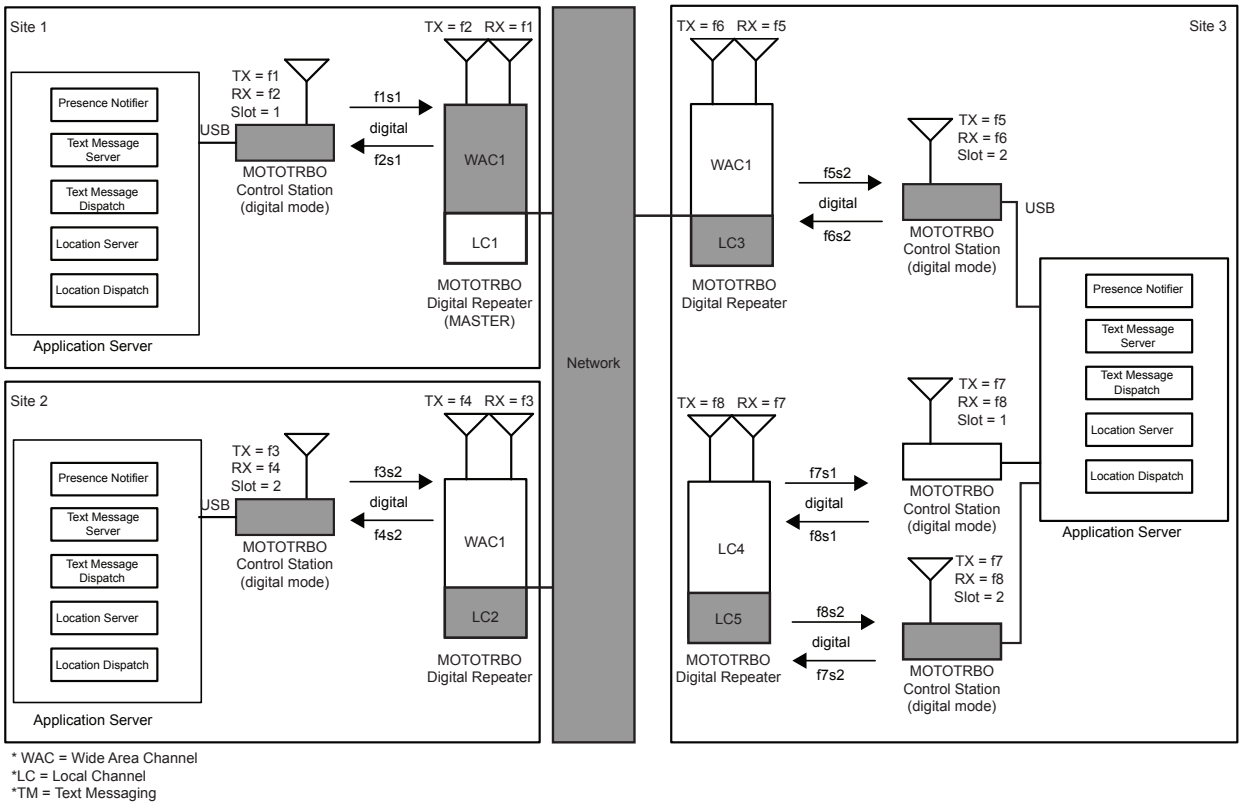
3.2.5.1.2

Wide and Local Area Systems with Distributed Data Application Servers

It is possible that one of the logical wide area channels of the repeaters is configured for local communication only. In this case, each site has its own logical channel for local communication. This is useful in case a customer need a significant load of local communication. This configuration offloads the local communication from the wide area channel.

Figure 124: Wide and Local Area System with Distributed Data Application Servers on page 364 shows an example of such configuration in which one of the logical channels (say, slot 2) is used in IP Site Connect mode (wide area) and the other (slot 1) is used in digital repeater mode (local area). The calls originating on slot 1 are not sent to other repeaters. A customer should use slot 1 for local groups whose members are expected to be present in the coverage area of the repeater; and slot 2 for groups whose members are distributed over the coverage area of multiple repeaters.

Figure 124: Wide and Local Area System with Distributed Data Application Servers



* WAC = Wide Area Channel
*LC = Local Channel
*TM = Text Messaging

For details on data communication with applications through the repeater network interface instead of a Control Station, see MOTOTRBO Network Interface Service on page 315 and MOTOTRBO Device Discovery and Mobility Service on page 327.

The data messages sent over local channel 1 are not delivered to the Application Server 1 and therefore, if required, each geographical location should have their own Application Server with their own Presence Notifier. When a radio manually roams (changes dial positions) between a local area channel and a wide area channel, the radio registers with its respective Presence Notifier. To facilitate this, the radio ID of the Control Stations should be configured to be the same.

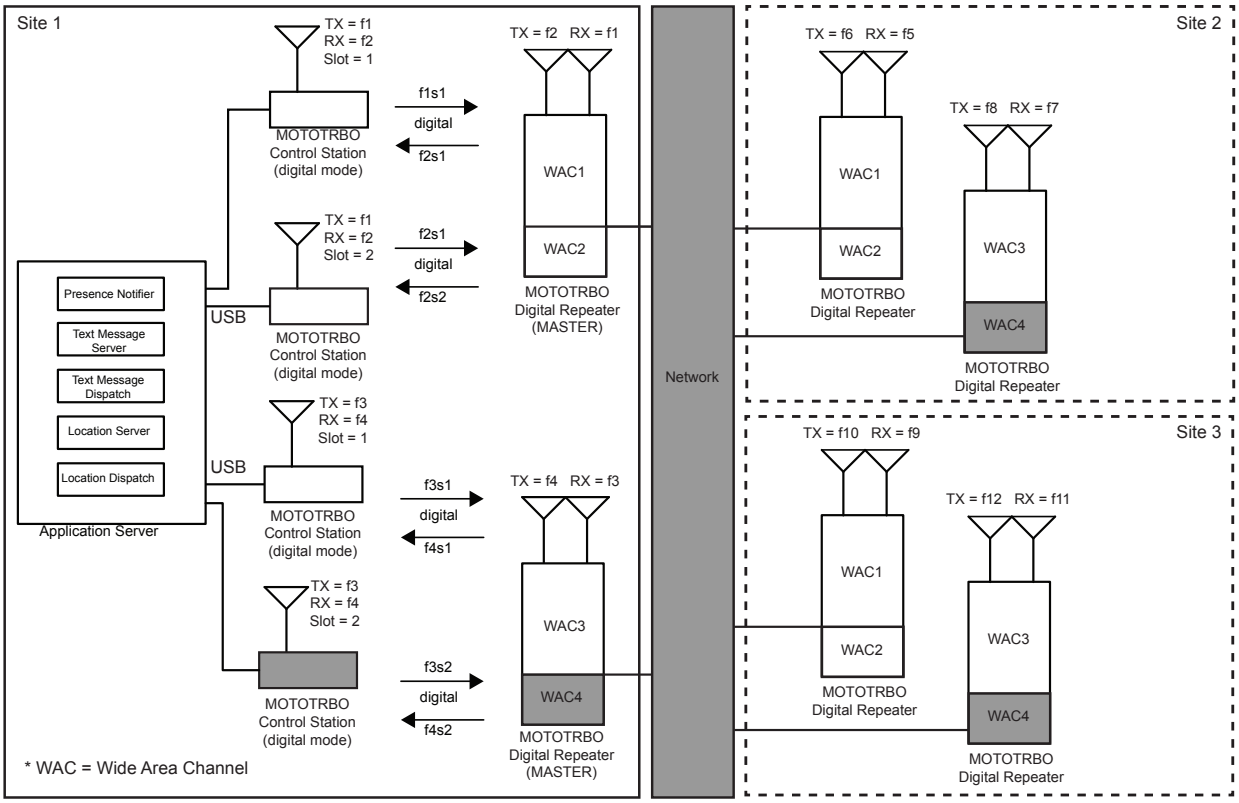
If a customer requires more local capacity at a location then it is possible to add more repeaters working in Single-Site configuration and all the local slots of all the repeaters can share the same Application Server. In that case, the radios on the local channel are not be able to communicate with the wide area channels' Application Server.

3.2.5.1.3

Multiple Wide Area Systems with a Centralized Data Application Server

If a customer requires more wide area capacity, then it is possible to add another set of repeaters working in IP Site Connect mode. It is possible for the repeaters to share the same Application Server, as shown in Figure 125: Multiple Wide Area Systems with Centralized Data Application Server on page 365. In this case, the repeaters at a location may share the same link to the backend network. The bandwidth required for communication through the back-end network should take this into consideration. See Back-End Network Design in IP Site Connect Mode on page 427 for further details.

Figure 125: Multiple Wide Area Systems with Centralized Data Application Server



For details on data communication with applications through the repeater network interface instead of a Control Station, see MOTOTRBO Network Interface Service on page 315 and MOTOTRBO Device Discovery and Mobility Service on page 327.

If a customer requires more wide area capacity for location data, then it is possible to use one or more wide area channels as GPS Revert Channels.

System	Description
IPSC IP Site Connect	The GPS Revert Channel behavior of radios in IP Site Connect mode is the same as the radios behavior in digital repeater mode with the exception that the GPS is sent unconfirmed on a wide area channel. GPS Revert in Repeater Mode on page 353.

3.2.5.2
Network Topologies for IP Site Connect

IPSC

The IP Site Connect topologies described in the previous sections can reside on a range of backend network configurations and technologies.

Logical connections between the wide-area channels can all reside on the same physical network. The chosen network topology is usually driven by the repeater's physical location and the network connectivity available at that location. The network topologies can be broken up into two basic configurations:

- Local Area Network (LAN) Configuration
- Wide Area Network (WAN) Configuration

NOTE: Most network topologies will be a combination of both LAN and WAN network configurations. Each individual configuration will be described and discussed.

NOTE: The same network configurations can be used for Digital or Analog repeaters, Enabled or Disabled repeaters, Wide Area or Local Area repeaters, RDAC, or any other third-party device that utilizes the IP Site Connect link establishment protocol.

3.2.5.2.1
LAN Configuration

IPSC

Customers that have high capacity network connectivity throughout their organization usually have a desire to utilize their existing network for WAN connectivity.

IP Site Connect supports the following technologies:

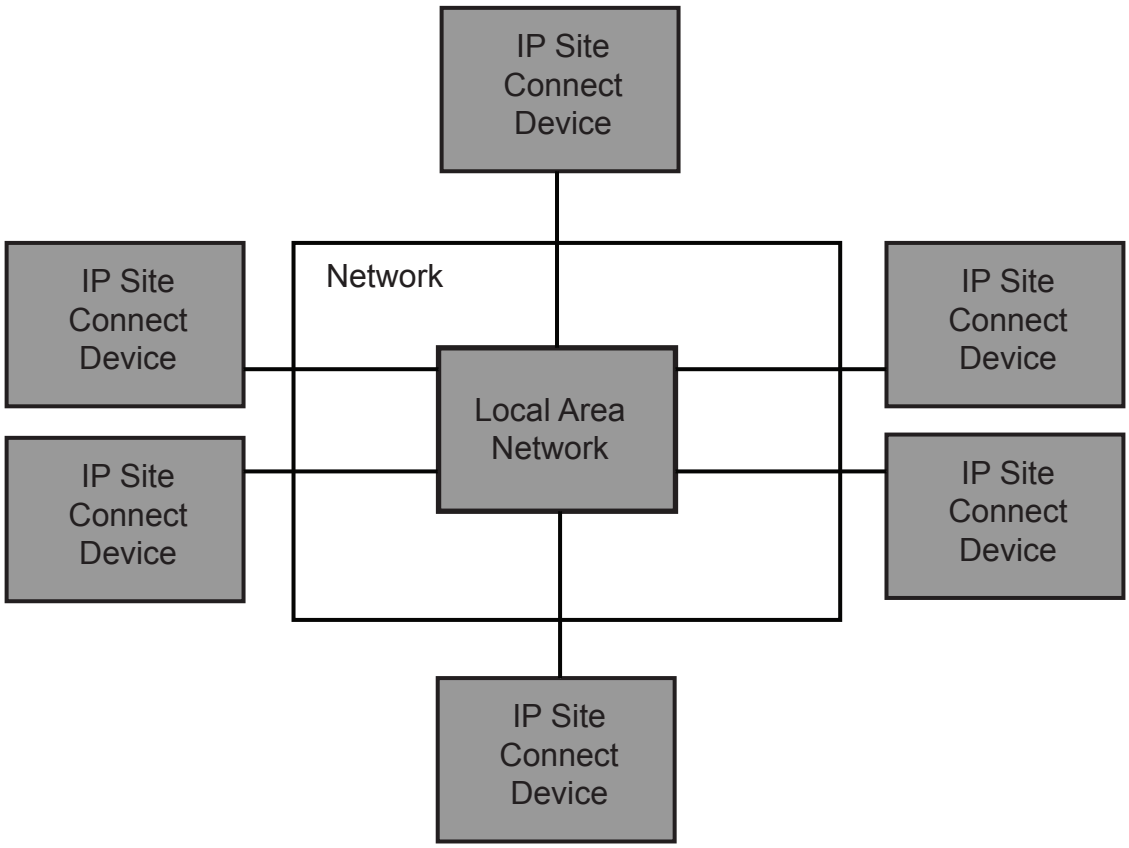
- Private LANs
- Corporate LANs
- Private Wireless Systems

Exact configurations of Local Area Networks (LAN) can vary greatly. As long as the devices are on the same network, or have access to other networks through an internal router or router with NAT configurations, the IP Site Connect system will operate correctly. It is also assumed that in these local configurations that bandwidth is not an issue. Nevertheless, the system installer needs to understand the bandwidth that each IP Site Connect device requires to operate optimally. More information can be found in Back-End Network Bandwidth Considerations on page 428.

Figure 126: IP Site Connect Devices Connected Through LAN on page 367 shows a simple diagram of IP Site Connect devices located at different sites connected through a LAN. Note that in this drawing the IP Site Connect devices could be in one or more Wide Area Systems (more than one Master repeater), could contain local area channels, or even be an analog repeater, a disabled repeater, or RDAC application.

Only the repeaters acting as Masters require a local static IPv4 address, or a static DNS address, that is mapped to a dynamically assigned IPv4 address. The other IP Site Connect devices use this local static IPv4 address or a static DNS address of the Master, to establish their link with the wide area system.

Figure 126: IP Site Connect Devices Connected Through LAN



3.2.5.2.2

WAN Configuration

IPSC

The defining benefit of IP Site Connect is the ability to connect sites over public Internet Service Provider (ISP) links as well as private high-speed connections.

For more information see: Considerations for the Back-End Network in IP Site Connect Mode on page 424.

Keep in mind that because traffic from one repeater is sent to every repeater, the required bandwidth of the ISP link at one site is a function of the number of other repeaters in the system. Adding a repeater will increase the required bandwidth at all sites. For more information see: Back-End Network Bandwidth Considerations on page 428.

A repeater can be (and is suggested to be) behind a router and/or a NAT and/or a firewall. Although not required, it is highly suggested in order to protect against the undesired solicitations common over the public Internet.

NOTE: Basic NAT provides translation for IPv4 addresses only, and places the mapping into a NAT table. In other words, for packets outbound from the private network, the NAT router translates the source IPv4 address and related fields. For inbound packets, the NAT router translates the destination IPv4 address and related checksums for entries found in its translation table.

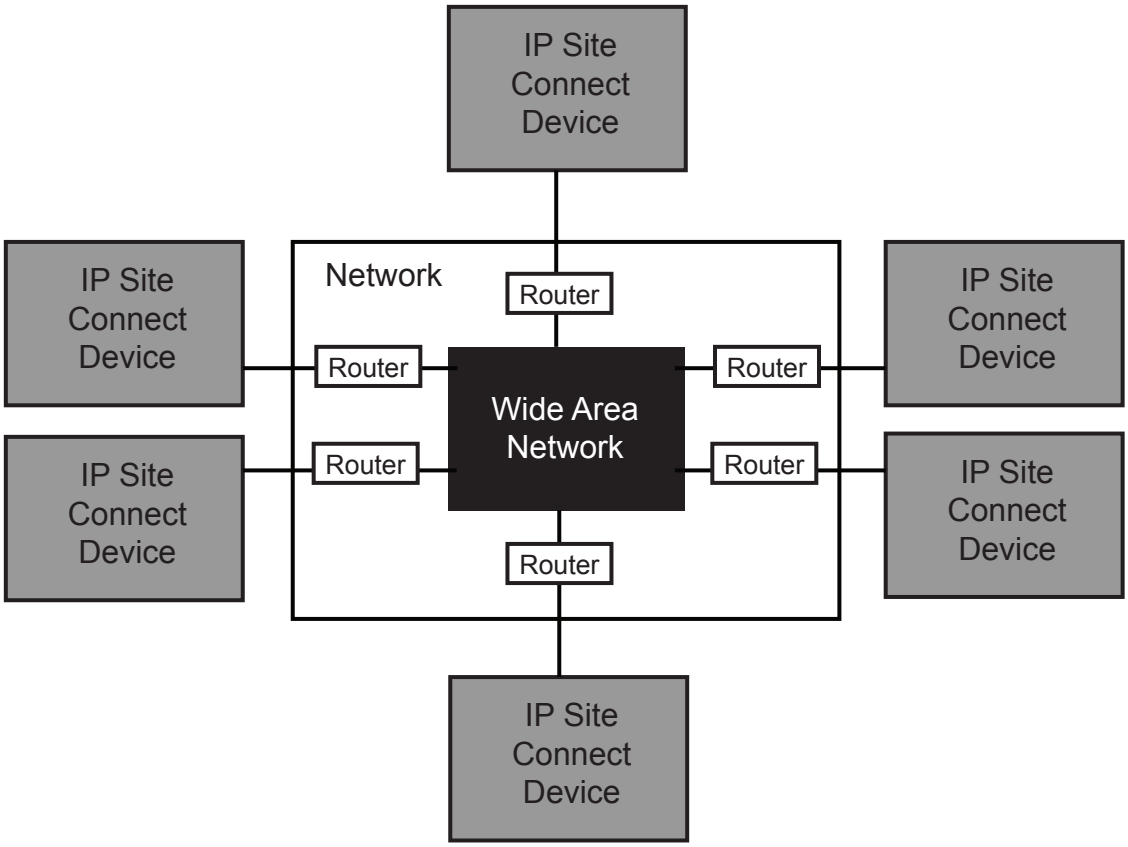
The peer-to-peer communications over the network can be optionally authenticated, and are also encrypted end-to-end if enabled in the radios. If this is not considered sufficient for a particular customer, IP Site Connect supports the ability to work through a Secure VPN (Virtual Private Network). Secure VPN is not a function of the IP Site Connect device but rather of the router. It is important to note that VPN does add the need for additional bandwidth and may introduce additional delays. This should be taken into consideration in bandwidth planning.

.

The following diagram shows a simple diagram of IP Site Connect devices located at different sites connected through a Wide Area Network (WAN).

Note that in this diagram the IP Site Connect devices could be in one or more wide area systems (more than one Master repeater), could contain local area channels, or even be an analog repeater, a disabled repeater, or RDAC application.

Figure 127: IP Site Connect Devices connected through a WAN



3.2.5.2.3

WAN and LAN Configurations

IPSC

Most network topologies are a combination of both Local Area Network (LAN) and Wide Area Network (WAN) configuration. For example, there may be a need to link two or more sites with existing local networks together over a public ISP, or link one or more remote mountain RF sites into a corporate network. When doing this, there are a few extra precautions to consider that are not covered in the previous sections.

The number of IP Site Connect devices connected together behind a single WAN connection (that is, behind one router) can have a large effect on the required bandwidth of the WAN link. The bandwidth requirements of a WAN link are the summation of the bandwidth requirements of all IP Site Connect devices behind the router. In other words, if there are three IP Site Connect devices utilizing a single ISP link, it must have enough bandwidth to support all three. Recall that the traffic from one repeater is sent to every repeater; therefore the required bandwidth of the ISP link at one site is a function of the number of other sites in the system. Adding a repeater at one site increases the required bandwidth at all sites.

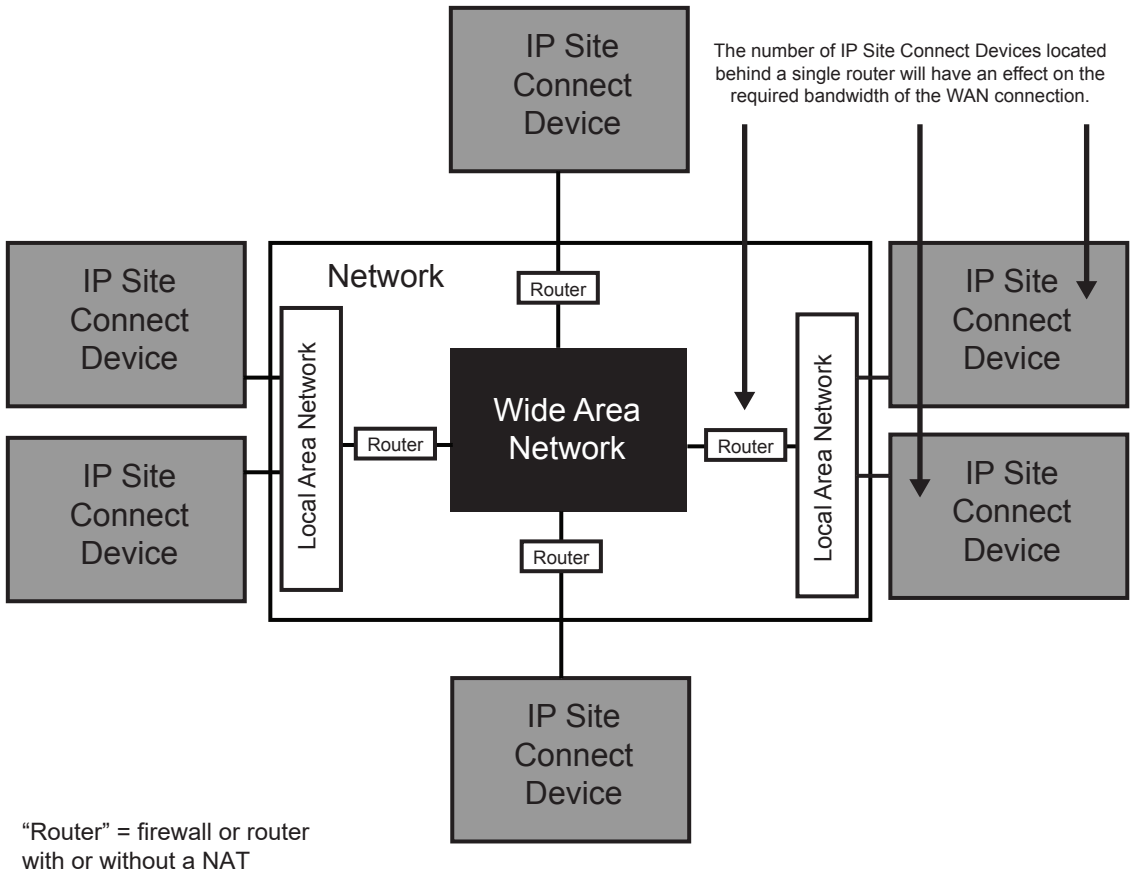
Similar to the WAN configurations, the repeaters acting as the Master will require a publicly accessible static IPv4 address or FQDN name resolved using a public DNS server. The other IP Site Connect devices utilize this publicly accessible IPv4 address, not a local (private) IPv4 address, to establish their link with the wide area system. This is true even for the IP Site Connect devices that are located on the same LAN as the Master.

Again, similar to the WAN configurations, the Master repeater’s site router/firewall with NAT requires some configuration (open port) so that unsolicited messages from other repeaters can reach the Master.

To support the ability of the IP Site Connect devices to communicate to other devices on its LAN using the WAN IPv4 address, the router must support a feature referred to as a hair-pinning. The hair-pinning functionality allows for returning a message in the direction it came from as a way for it to reach its final destination. This is per the router standard RFC 4787.

The following diagram shows a simple diagram of IP Site Connect devices located at different sites connected through a mix of LAN and WAN networks. Note that in this drawing the IP Site Connect devices could be in one or more wide area systems (more than one Master), could contain local area channels, or even be an analog repeater, a disabled repeater, or RDAC application.

Figure 128: IP Site Connect Devices connected through LAN and WAN Network



3.2.5.3

Summary of Features in IP Site Connect Mode

IPSC

The following features are supported in IP Site Connect mode:

Table 76: Digital MOTOTRBO Radios in IP Site Connect Mode

Voice Features	Signaling Features	Emergency Handling	Data Calls	Other Features	
Group Call	PTT ID and Aliasing	Emergency Alarm	Text Messaging	Two Wide Area Channels (slot 1 and slot 2)	Remote Diagnosis and Control
Private Call	Radio Inhibit	Emergency Alarm and Call	Location Tracking	Mix of Wide Area and Local Area Channels	Roaming

Voice Features	Signaling Features	Emergency Handling	Data Calls	Other Features	
All Call	Remote Monitor	Emergency Alarm with Voice to Follow	Telemetry	Scan*	Wide Area Coverage
Dual Tone Multi Frequency	Radio Check	Emergency Revert Per Site	Third-Party (ADP) Applications	Polite to All System Access	Time-out Timer
Voice Interrupt	Call Alert	Emergency Voice Interrupt	GPS Revert Per Site	Polite to Own System Channel Access	Privacy
Digital Telephone Patch	Remote Voice Dekey	–	Data Over Voice Interrupt	Impolite Channel Access	–

* See Scan Considerations on page 156 for more information on the different scan modes supported by different topologies.

The following section discusses some of the considerations to take while designing a MOTOTRBO system. It focuses more on how the user uses the system, and the configuration needed to support it. Although a basic system topology may already have been chosen, the next chapter helps dig deeper into how the end user utilizes the system, and therefore gives additional ideas on how it should be configured.

3.2.6
Capacity Plus Single Site Mode

CPSS

Prior to R02.30.00, Capacity Plus Single Site allows up to 6 Trunked repeaters (12 logical channels) and 12 Data Revert repeaters (24 logical channels). For the system to operate properly, all the repeaters must have the same software version. From software version R02.30.00 onwards, up to 8 Trunked Repeaters (16 logical channels) and 12 Data Revert repeaters (24 logical channels) are allowed.

For more details see: System Capacity in Capacity Plus Single Site on page 437.

The Rest Channel IPv4/UDP address must be configured using a valid subnet IPv4 address where the system resides, and cannot be left as 0.0.0.0.

NOTE: The CPSS system requires at least one Trunked repeater.

In Capacity Plus Single Site mode, all the radios share the channels of all the Trunked repeater(s). The probability of all channels being busy at the same instant is low. Hence, radio finds less blocking of calls compared to when only one channel is available to the radio. Similarly, for the same quality of service, sharing of channels allows more calls and thus increases channel capacity.

In CPSS, a channel is configured either for Trunking or Data Revert. Radio has a list of all Trunked Channels and a list of Data Revert Channels. While configuring channels, observe the following rules:

- Both channels of a repeater should be used for the same purpose. This implies that if one channel of a repeater is a Trunked Channel, then the other channel is also a Trunked Channel. Similarly, if one channel of a repeater is a Data Revert Channel, then the other channel is also a Data Revert Channel.
- The CPS provides a zone for keeping all the Trunked and Data Revert Channels, called **Channel Pool**.

3.2.6.1
Topologies of Capacity Plus Single Site System

CPSS

Capacity Plus Single Site Systems can consist of the following topologies:

- System with No Data Application Server and Local RDAC on page 372
- System with No Data Application Server and Remote RDAC on page 374
- System with Data Application Server on Trunked Channels on page 375
- System with Data Application Server on Revert Channels on page 377
- System with a Dispatch Console on page 378

3.2.6.1.1
System with No Data Application Server and Local RDAC

CPSS

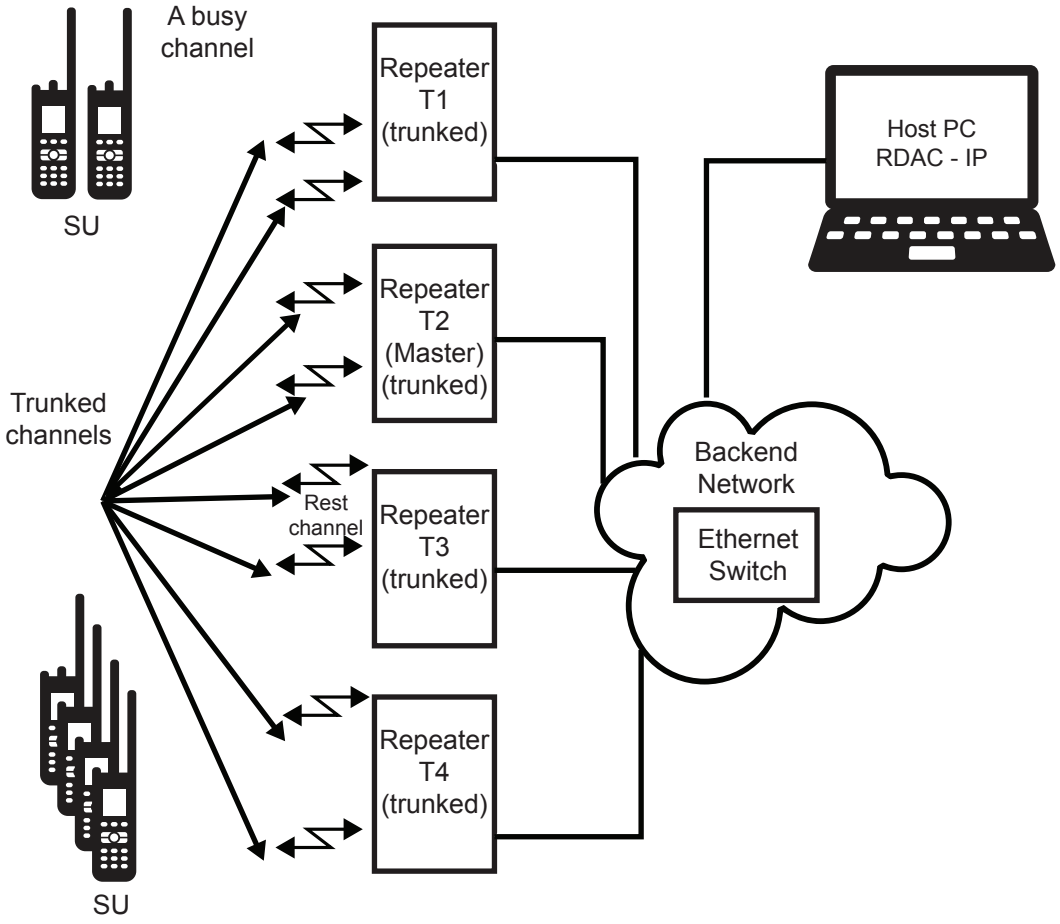
This configuration is the most basic of the Capacity Plus Single Site topologies. It does not support a remote RDAC or data messages to or from a Server.

One of the repeaters has an additional role of Master repeater; a broker for discovering repeaters. The Master has a static address (that is, IPv4 address and UDP port number), which is configured in all the repeaters and RDAC. A static address is an address that does not change over time. If the IPv4 address of the Master repeater changes, then all the repeaters and RDAC must be reconfigured with the new address. To avoid this issue, the user can configure all of the devices with an FQDN (Fully Qualified Domain Name) of the Master to be resolved with a DNS server instead.

Anytime the IPv4 address for a Master changes, then the DNS server must be updated with the Master's new IPv4 address. It is the job of the entity assigning the IPv4 address to the Master to also to update the DNS Server with the updated IPv4 address to minimize any interruptions in connectivity to Master.

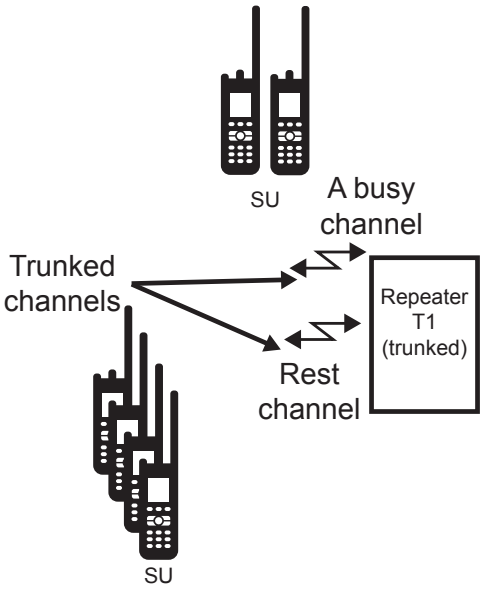
NOTE: The DNS feature is only available on SLR Series Repeaters.

Figure 129: Capacity Plus Single Site Devices with Local RDAC and no Data Application Server



A minimal configuration of the setup displayed in Figure 129: Capacity Plus Single Site Devices with Local RDAC and no Data Application Server on page 373 can have just one repeater without RDAC. In this case, the system behaves as a 2-channel trunked system.

Figure 130: 2-Channel Capacity Plus Single Site System without Data Application Server



3.2.6.1.2

System with No Data Application Server and Remote RDAC

CPSS

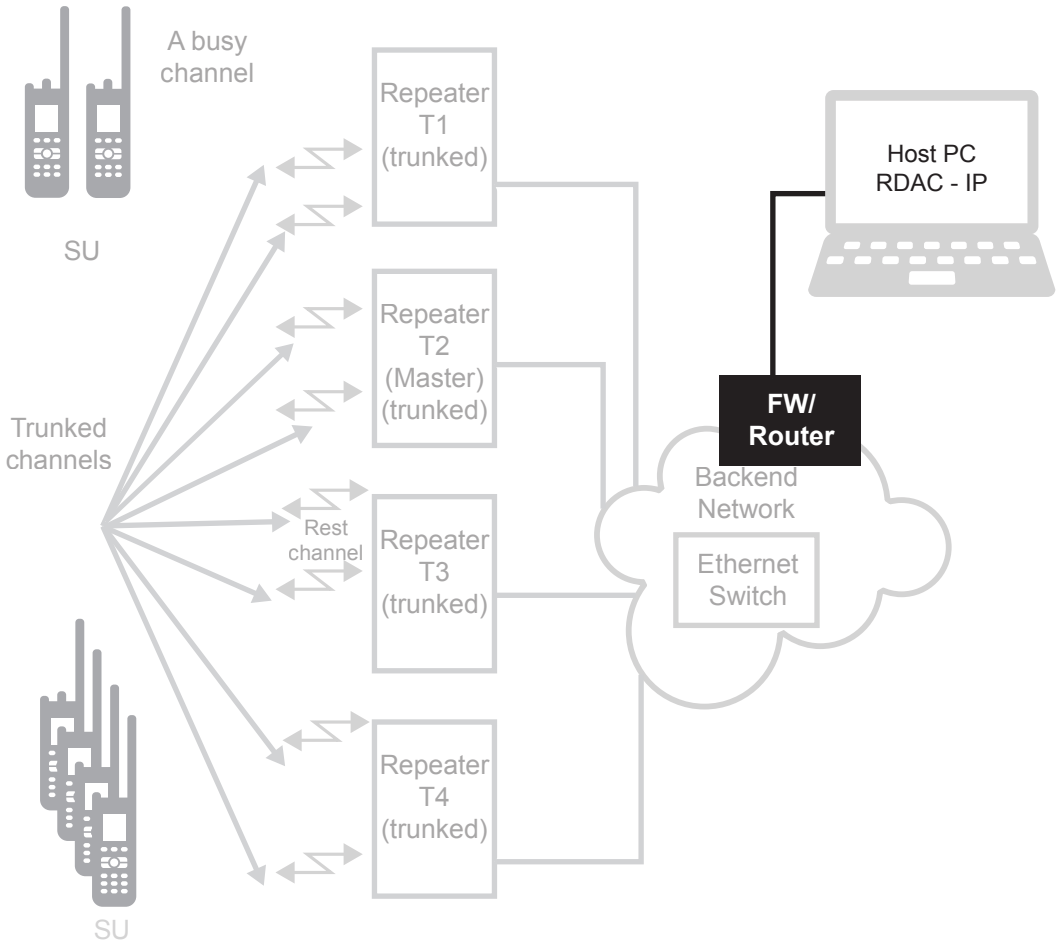
If RDAC is located in a different IPv4 network than the Capacity Plus Single Site repeaters, then the back-end network of CPSS should be connected to the external IP network using a router. In this case, use the static address of the Master repeater, as seen from the WAN side of the router, to configure the repeaters and RDAC.

Note that in the case of using network address translation (NAT) on the router; it may be required to do static IPv4 NAT for each repeater. Before software version R02.20.12, the router should support hair-pinning functionality and be able to handle all the messages between repeaters using hair-pinning. The hair-pinning functionality allows for returning a message in the direction it came from as a way for it to reach its final destination. This is per the router standard RFC 4787.

In software version R02.20.12 or later, CPSS can work with, or without hair-pinning capabilities in the router. When a non-hair-pinning router is utilized, each repeater must be configured with a LAN IPv4/UDP address of the Master repeater while the Master repeater must be configured with WAN IPv4/UDP address as the Master IP. The Rest Channel IPv4/UDP address must be configured as a unique static IPv4/UDP address from the same subnet as the repeaters and is common for all repeaters on the site. For more information about repeater configuration types and hair-pinning requirements see: Repeater Network Configuration Options in Capacity Plus Single Site and Capacity Plus Multi Site on page 386

NOTE: If a router with NAT configuration is utilized, the router must be configured to “no port address translation / port preservation for UDP”.

Figure 131: Capacity Plus Single Site Devices with Remote RDAC and no Data Application Server



3.2.6.1.3
System with Data Application Server on Trunked Channels

CPSS

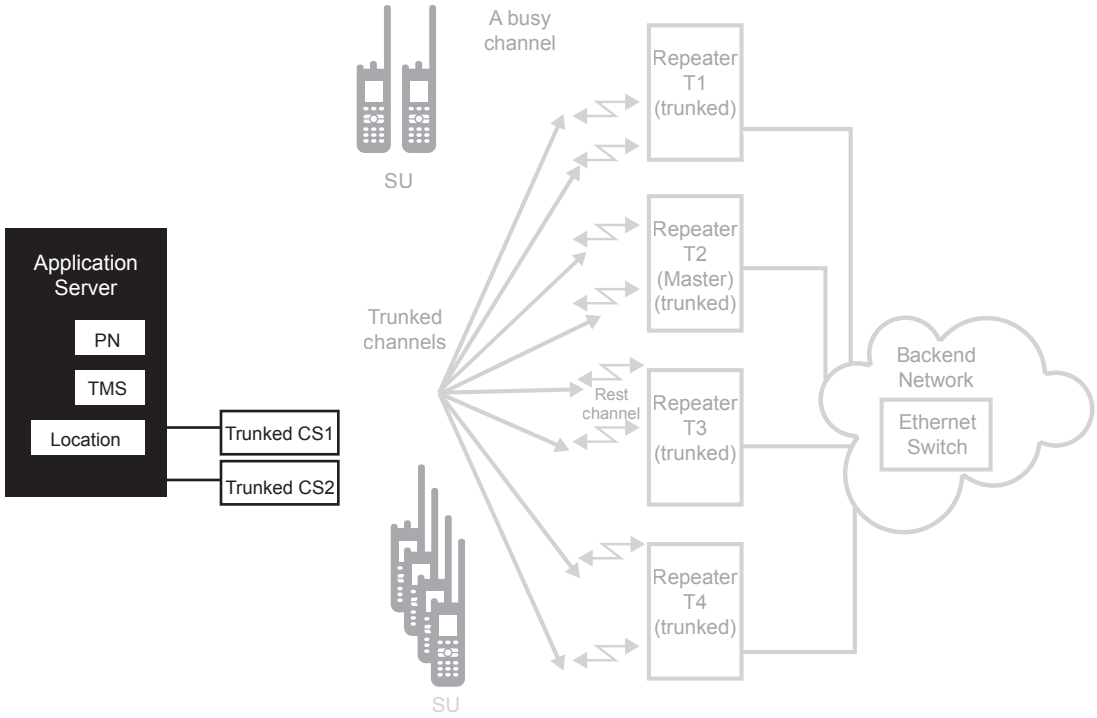
It is possible to send data messages to an Application Server over the Trunked Channels. This is recommended for a system that requires sending a limited number of data messages to the Application Server. This configuration requires one or more Trunked Control Stations.

If there is more than one Trunked Control Station, the configuration should adhere to the following rules:

- The maximum number of Trunked Control Stations should not be more than the number of Trunked Channels.
- To achieve a success rate of 90%, the number of data messages per minute per Trunked Control Station should be less than 10. It is assumed here that the payload of a data message is 50 bytes or characters long.
- The Radio IDs of all Trunked Control Stations should be different.
- The radios should be grouped into ‘n’ sets, where ‘n’ is the number of Trunked Control Stations.

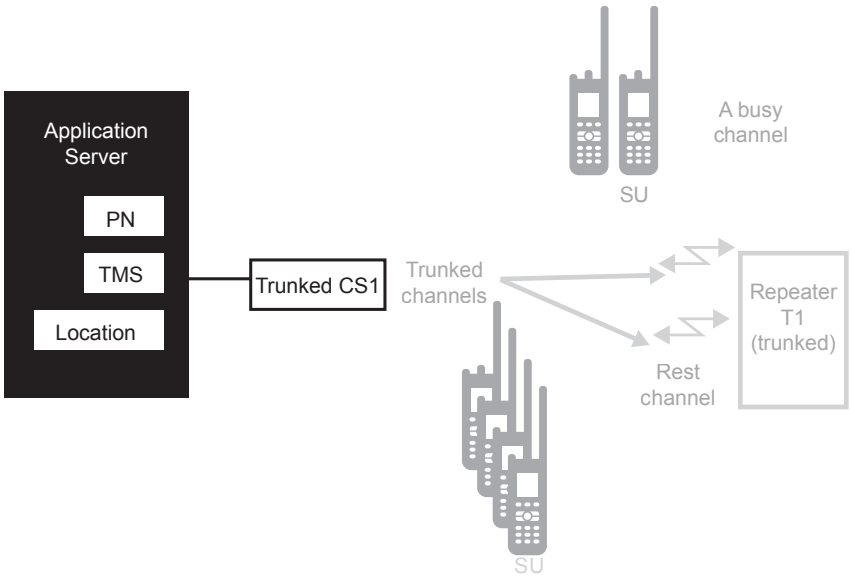
- Each set of radios is associated with the one Trunked Control Station. This implies that the configured IPv4 address of the server in the radio is the IPv4 address of its Trunked Control Station's peripheral.
- For each set of radios, it is required to make one or more entries in the IPv4 routing table of the Application Server such that a data packet transmitted to radio is routed to the port of the Trunked Control Station associated with this set of the radio.

Figure 132: Capacity Plus Single Site Devices with Data over Trunked Channels



A minimal configuration of Figure 132: Capacity Plus Single Site Devices with Data over Trunked Channels on page 376 is shown in Figure 133: Two-Channel Capacity Plus Single Site Devices with Data over Trunked Channels on page 376.

Figure 133: Two-Channel Capacity Plus Single Site Devices with Data over Trunked Channels



3.2.6.1.4

System with Data Application Server on Revert Channels

CPSS

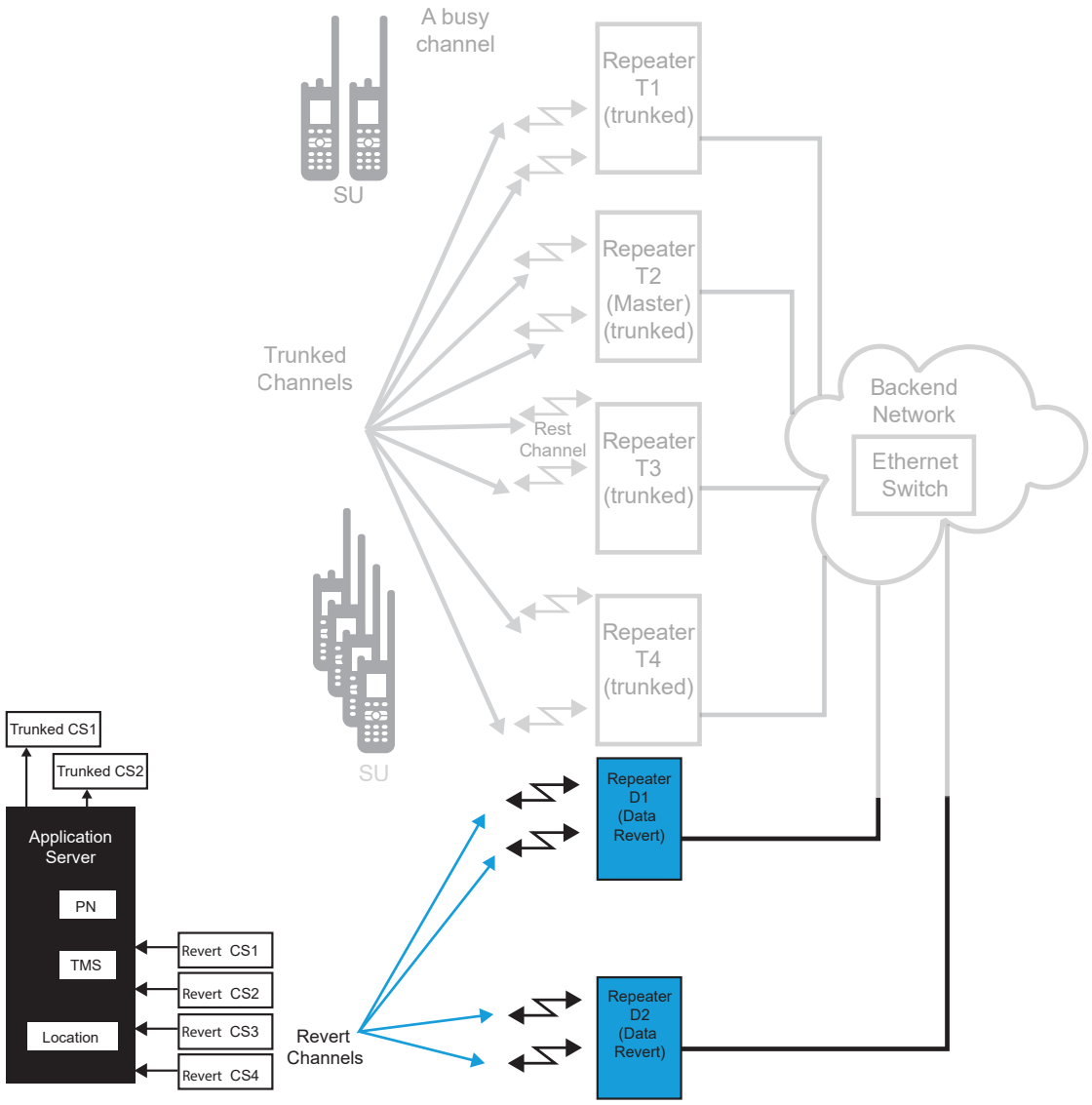
If a system requires sending a large number of data messages (for example Location Data) to an Application Server, Capacity Plus Single Site is able to dedicate up to a maximum of 12 repeaters for this transmission to take place. This configuration requires one Revert Control Station per one Data Revert Channel (that is, slot) and at least one Trunked Control Station.

The Radio IDs (and therefore the IPv4 address) of all Revert and Trunked Control Stations are the same. The IPv4 address of the Application Server (as seen by a radio) is derived from the Radio ID of the Control Stations.

The Application Server sends data packets to the radios through Trunked Control Stations, and not through the Revert Control Stations.

A CPSS system can have more than one Trunked Control Station. Therefore, it is required to distribute the data packets fairly among the Trunked Control Stations and the distribution should be transparent to the applications in the Application Server. A simple way to achieve fair distribution is to group the radios into ‘n’ sets, where ‘n’ is the number of Trunked Control Stations, and associate each set to one Trunked Control Station. For each set of radios, it is required to make one or more entries in the IPv4 routing table of the Application Server so that a data packet transmitted to radio is routed to the port of the Trunked Control Station associated with the radio.

Figure 134: Capacity Plus Single Site Devices with Data over Revert Channels



3.2.6.1.5
System with a Dispatch Console

CPSS

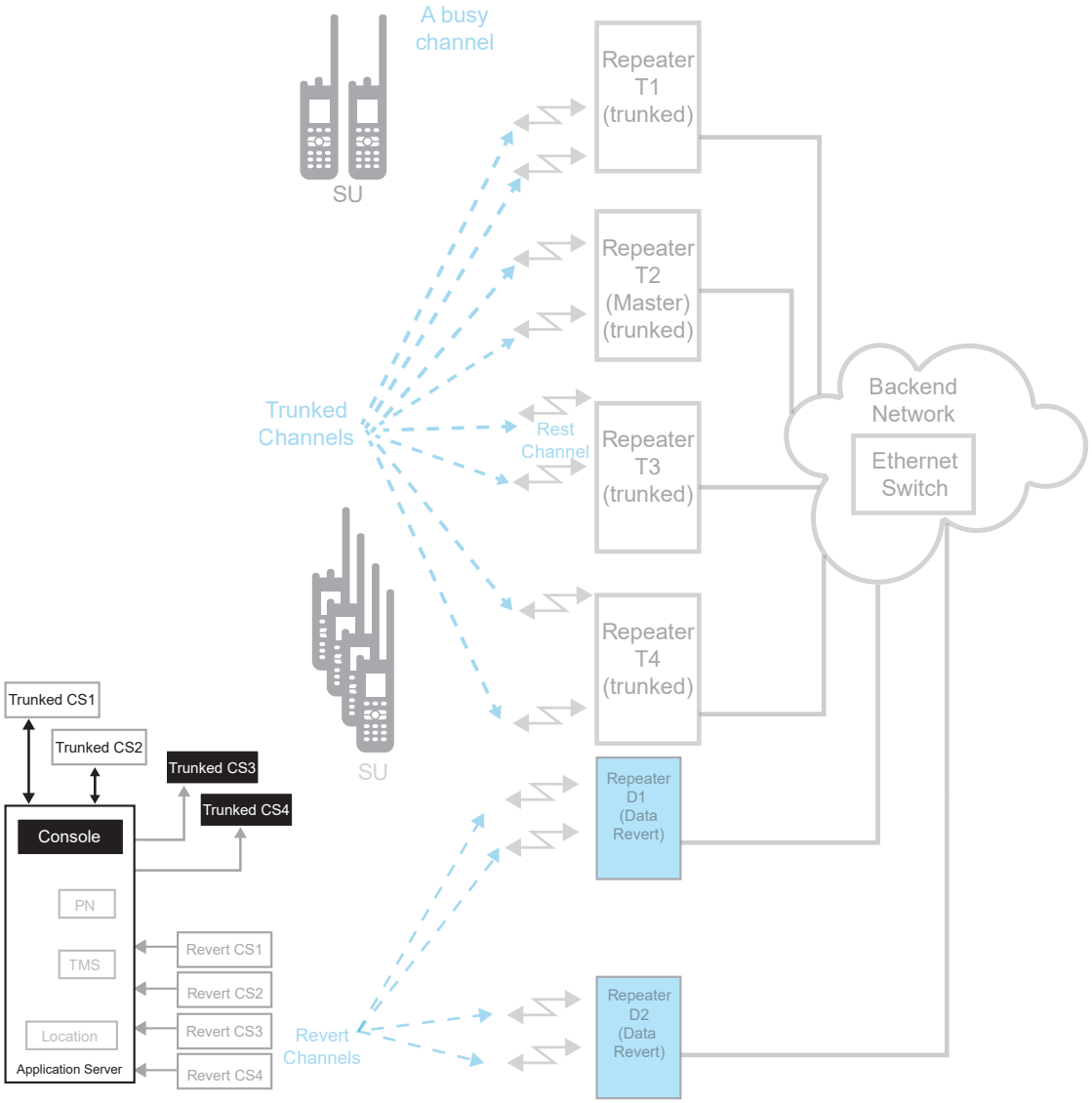
A Dispatch Console can be connected to a Capacity Plus Single Site system using one or more Trunked Control Stations. The interface between the Dispatch Console and the Trunked Control Stations can either be 4-wire or XCMP/USB. The Dispatch Console could either be a single position console, or a multiple position server-based system.

The number of Trunked Control Stations depends on the number of concurrent paths supported by the Dispatch Console. A simple configuration will have one Trunked Control Station dedicated to each group.

The Dispatch Console maintains the association between the group and the Trunked Control Station. To make a call to a group, the Dispatch Console uses the Trunked Control Station associated within the group. The configuration may have a Trunked Control Station dedicated to a Private Call. All the radios have this Trunked Control Station listed in their address book as a dispatcher.

If the configuration has data applications, then the Trunked Control Stations for both data and Dispatch Console should be mutually exclusive. This means that a Trunked Control Station should not be used for both data and voice. The configuration is shown in the following figure

Figure 135: Capacity Plus Single Site Devices with a Dispatch Console



For details on data communication with applications through the repeater network interface instead of a Control Station, see MOTOTRBO Network Interface Service on page 315 and MOTOTRBO Device Discovery and Mobility Service on page 327.

3.2.7
Capacity Plus Multi Site Mode

CPMS

Capacity Plus Multi Site (CPMS) supports up to 15 sites with a maximum of 140 (200) peers across all sites and up to 12 Repeaters (24 logical channels) per site. At any given site, there can be up to 8 Trunking Repeaters (16 logical channels) and up to 11 Data Revert Repeaters (22 logical channels) however, the total number of Trunked repeaters plus Data Revert repeaters must not exceed 12. For example, if there are 8 Trunked Repeaters at a site, then up to 4 Data Revert Repeaters can be supported at that site.

For more details, see: System Capacity in Capacity Plus Single Site on page 437.

NOTE: The CPMS system requires at least one Trunked repeater in each site.

It is not a requirement to have the same number of repeaters at each site but all the repeaters at the site must have the same software version. A CPMS system supports local calls (calls received by radios at only one site) and the number of repeaters at a site is a function of the expected volume of the local calls. Additionally, due to co-channel interference or failure of repeaters, the number of available repeaters may be different at different sites.

All repeaters at a site must be on the same LAN, in other words, they must be behind the same router and plugged into the same LAN switch or set of Layer2 switches. It is strongly recommended that no other device except RDAC be present on the LAN.

In software version R02.10.00 and prior, CPMS Master site router should be capable of hair-pinning feature, to enable returning of the message in the direction it came from as a way for it to reach its final destination. In software versions R02.20.00 and later, CPMS can work with, or without hair-pinning capabilities in the router at the Master repeater's site.

When a non-hair-pinning router is utilized, each repeater in the Master site must be configured with a LAN IPv4/UDP address of the Master repeater while the Master repeater must be configured with WAN IPv4/UDP address as the **Master IP**. The Rest Channel IPv4/UDP address must be configured as a unique static IPv4/UDP address from the same subnet as the repeaters and is common for all repeaters on the site. For more information about repeater configuration types and hair-pinning requirements go to Repeater Network Configuration Options in Capacity Plus Single Site and Capacity Plus Multi Site on page 386.

NOTE: The router must be configured to "no port address translation / port preservation for UDP" if a router with NAT configuration is utilized.

The CPMS system supports many topologies regarding the back-end network. For more information see: Considerations for the Back-End Network in Capacity Plus Multi Site on page 445.

Only repeaters with 32 MB of internal memory can support the CPMS configuration.

Every CPMS system needs one repeater to act as the Master which requires an IPv4 address that does not change over time. The other repeaters can have static IPv4 addresses or can obtain them dynamically from the DHCP server. All repeaters in the CPMS system register with the Master using its static or DNS resolved IPv4 address.

Each site of the CPMS system must be assigned a virtual IP/UDP address for Rest Channel. This IP/UDP address must be configured in each repeater on the site. IPv4 address and UDP port for the Rest Channel are common per site and must be unique across the CPMS system.

The CPMS system may have many repeaters and applications like the RDAC and MNIS that are considered as repeaters by the Master. However, satellite receivers are not treated as repeaters. When the number of repeaters and these applications called "peers" in a system exceeds 140, a dedicated Master repeater must be deployed in the system. This dedicated Master should be added to a site as a Data Revert repeater, but adding it does not reduce the number of Data Revert repeaters that can be normally deployed at that

site. This dedicated Master repeater should have no RF-related activities such as CWID and OTA receiving/transmitting. Using a dedicated Master repeater, the maximum number of peers in the system is increased to 200.

In CPMS, a channel is configured either for Trunking or Data Revert. But both channels of a repeater should be used for the same purpose. This implies that if one channel of a repeater is a Trunked Channel, then the other channel is also a Trunked Channel. Similarly, if one channel of a repeater is a Data Revert Channel, then the other channel is also a Data Revert Channel. In CPMS, a Data Revert Channel can be configured either as a local Data Revert Channel or as a wide area Data Revert Channel.

At least one Trunked Repeater shall be present at each site.

A Data Revert Channel could be either an Enhanced GPS Revert Channel or a normal Data Revert Channel. Each logical channel of a Data Revert Repeater can be independently configured either as an Enhanced GPS Revert Channel or as a normal Data Revert Channel. Radio has a list of all Trunked Channels and a list of Data Revert Channels for each site.

Capacity Plus Multi Site system can be deployed for various system topologies. Topologies of Capacity Plus Multi Site System on page 381 defines some of the key topologies.

3.2.7.1
Topologies of Capacity Plus Multi Site System

CPMS

Capacity Plus Multi Site systems can consist of the following topologies:

- A Capacity Plus Multi Site system with data over Trunked Channels
- A Capacity Plus Multi Site system with data over local Revert Channels
- A Capacity Plus Multi Site system with data over wide area Revert Channels

3.2.7.1.1
Capacity Plus Multi Site System with Data over Trunked Channels

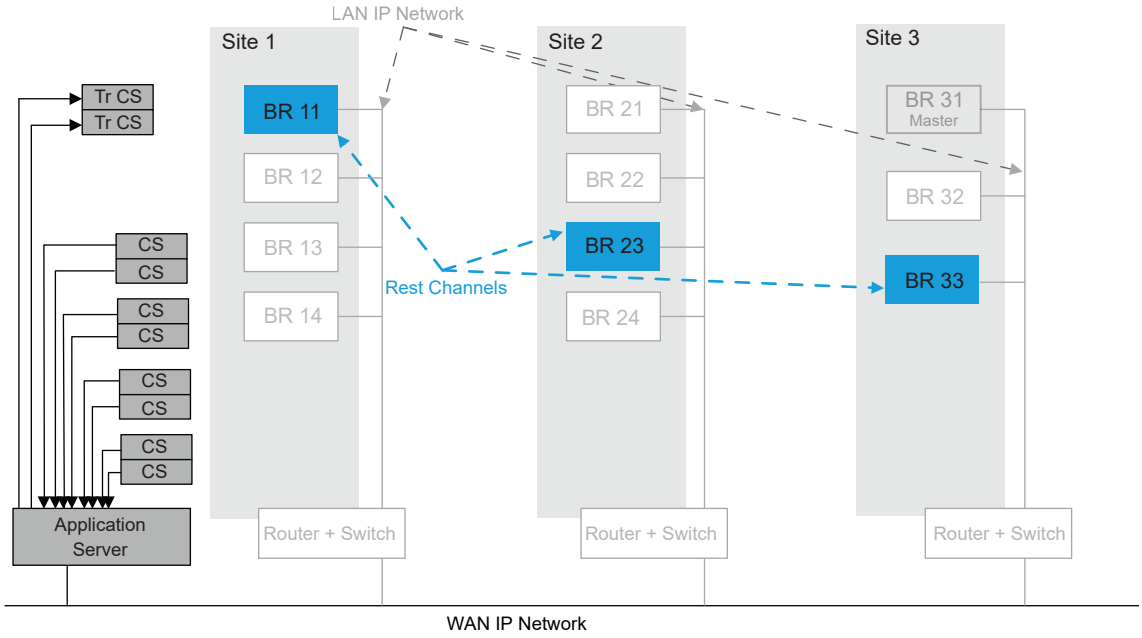
CPMS

Figure 136: Capacity Plus Multi Site System with Data over Trunked Channels on page 382 shows a basic Capacity Plus Multi Site system having three sites. Site 1 and 2 have four Trunked repeaters and site 3 has three Trunked repeaters. The number of repeaters at each site need not be the same. In this configuration, all the repeaters are configured for Trunked mode of operation – there is no Data Revert Repeater. One of the repeaters has an additional role of Master repeater.

The Master has a static IPv4/UDP address, which is configured in all the repeaters. If the address of the Master will change, then all the repeaters must be reconfigured with the new address. To avoid the issue of needing to reconfigure all the devices that link with the Master when it's IPv4/UDP address changes, you can configure all of the devices with an FQDN name of the Master resolved by DNS server instead. For more detail, see: Considerations for the Back-End Network in Capacity Plus Multi Site on page 445.

To avoid the issue of needing to reconfigure all the devices that link with the Master when its IPv4 address changes, you can configure all of the devices with a static DNS address for the Master instead. Anytime the IPv4 address for a Master changes, then the DNS server must be updated with the new IPv4 address. It is the job of the entity assigning the IPv4 address to the Master to also update the DNS Server with the updated IPv4 address to minimize any interruptions in connectivity to Master. It should be noted that the DNS feature is only available on SLR Series Repeaters.

Figure 136: Capacity Plus Multi Site System with Data over Trunked Channels



It is possible to send data messages to an Application Server over the Trunked Channels. This is recommended for a system that requires sending a limited number of data messages to the Server. If the data has to be sent to and from the Server, then one Revert Control Station per Trunked Channel and one or more Trunked Control Stations need to be added at a site in the basic topology. In this configuration, all the repeaters are configured for Trunked mode of operation, and there are no Revert repeaters to receive data messages nevertheless, we need to use Revert Control Stations. For this topology, the radio does not require a data channel list. The Trunked Control Stations are configured with no talkgroups and therefore ignore the calls received Over-the-Air. A Trunked Control Station follows the Rest Channel and when requested by an Application Server, transmits the message sent by the Server.

NOTE: Revert Control Station uses Digital channel type and listens only on one repeater's time slot of the configured frequency, regardless if the repeater is Trunked or Data Revert. In contrast, Trunked Control Station uses Capacity Plus channel type and in the idle state follows with the Rest Channel.

If there is more than one Trunked Control Station, the configuration should adhere to the following rules.

- The maximum number of Trunked Control Stations should not exceed the number of the Trunked Channels.
- To achieve a success rate of 90%, the number of data messages per minute per Trunked Control Station should be less than 10. It is assumed here that the payload of a data message is 50 bytes or characters long.
- The IDs of all Trunked Control Stations should be different.
- The radios should be grouped into 'n' sets, where 'n' is the number of Trunked Control Stations.
- Each set of radios is associated with one Trunked Control Station. This implies that the configured IPv4 address of the server in the radio is the IPv4 address of its Trunked Control Station's peripheral.

For each set of radios, it is required to make one or more entries in the IPv4 routing table of the Application Server such that a data packet transmitted to radio is routed to the port of the Trunked Control Station associated with the set of the radio.

For group data that needs to be sent to multiple sites, the data talkgroup needs to be a wide-area. For data to be sent to the Server, the data can be sent as an individual data call. Individual data calls engage only the source and destination sites of the call.

Like CPSS, CPMS requires Trunked Control Stations for data from an Application Server to the radio. The Trunked Control Stations must be upgraded with CPMS software. The Trunked Control Stations sending the Server's data as an application layer acknowledgment shall delay the acknowledgment by 420-480 ms, for a reliable reception by a radio. If more than one Trunked Control Stations are connected in the system, then the acknowledgment is sent based on the routing table in the Application Server.

NOTE: The Application Server cannot access the repeater interface, only the radio interface.

This topology is recommended when there are fewer RF frequencies for communication and where data calls are less frequent compared to voice calls. This topology is also preferable for small data throughput. The following CPMS topology with a dedicated revert repeater provides higher data throughput.

A minimal variation of this configuration can have only one repeater per site. In this scenario, the CPMS system is similar to an IP Site Connect system with the following differences. The minimal CPMS system provides:

- Faster automatic roaming compared to an IP Site Connect system
- Additional SAT time of approximately 180 ms
- Reduced battery life by 45-60 minutes compared to an IP Site Connect system
- Higher call handling capacity because the system:
  - Works as a 2-slot Trunked system
  - Can have local talkgroups
  - Uses at most two sites for Private Calls
  - Uses statically associating sites for wide-area talkgroups

Another minimal variation of this configuration consists of only one site. In this case, the CPMS system is similar to a CPSS system.

3.2.7.1.2
Capacity Plus Multi Site System with Data over Local Revert Channels

CPMS

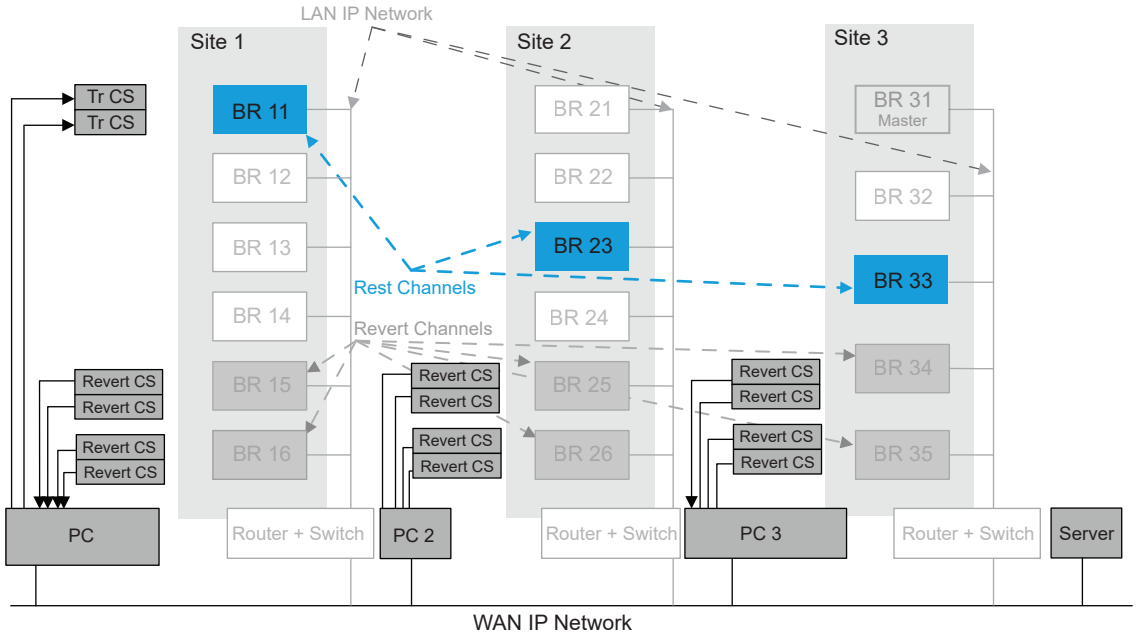
For a higher data throughput, the preferred configuration is to have channels dedicated for data only. Such channels are defined as Data Revert Channels. In a Revert repeater configuration, a Revert repeater is connected in local mode.

Whenever a radio has to send data to the server, it switches to one of the data channels in the data channel list and transmits data on the Revert Channel. The Revert Control Station listening to each Revert Channel of the Revert repeater receives the data and sends it to the connected PC. The PC at each site routes the data to the server PC, hence only one server PC can manage the radios at different sites. A PC at each site routes the data to the server PC based upon its prior routing configuration.

Similar to Capacity Plus Single Site, in Capacity Plus Multi Site, the server uses Trunked Control Stations to send messages to a radio. To simplify the system topology, the Trunked Control Station needs to be present at one site only.

This system configuration can also be used with the Enhanced GPS mode of the Revert repeater. The overall revert topology remains the same.

Figure 137: Capacity Plus Multi Site System with Data over Local Revert Channels



3.2.7.1.3

Capacity Plus Multi Site System with Data over Wide Area Revert Channels

CPMS

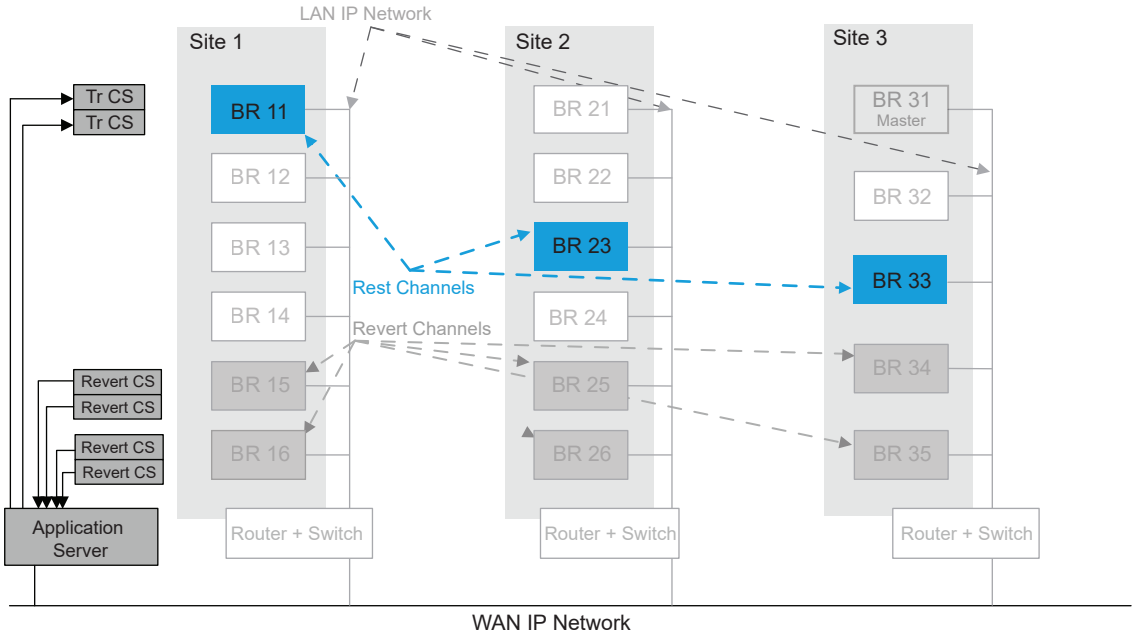
This topology is similar to Capacity Plus Multi Site System with Data over Local Revert Channels on page 383, except that the Revert repeaters are connected in a wide-area mode. This topology requires fewer Control Stations compared to the previous topology since the Revert repeaters are connected in a wide-area mode configuration. This topology also supports a wide-area mode of an Enhanced GPS Revert repeater. This topology requires the same number of Revert repeater channels at each site.

The Revert data call capacity of this configuration is *n* times less than the configuration in the previous topology, where *n* is the number of sites. The other configuration details for this topology are identical to the previous topology.

It is possible to combine topology 2 and 3. In a combined topology, some Revert Channels could be wide-area channels and some local.

For example, radios in the wide-area talkgroup personality can use the wide-area Revert Channels while the radios using local communication can use the local area Revert Channels.

Figure 138: Capacity Plus Multi Site System with Data over Wide Area Revert Channels



For details on data communication with applications through the repeater network interface instead of a Control Station, see MOTOTRBO Network Interface Service on page 315 and MOTOTRBO Device Discovery and Mobility Service on page 327.

3.2.7.2

Summary of Features in Capacity Plus Single Site and Capacity Plus Multi Site Modes

CPSM

The following features are supported in Capacity Plus Single Site and Capacity Plus Multi Site modes:

Table 77: Digital MOTOTRBO Radios in Capacity Plus Single Site and Capacity Plus Multi Site Modes

Voice Features	Signaling Features	Emergency Handling	Data Calls	Other Features	
Group Call	PTT ID and Aliasing	Emergency Alarm	Text Messaging	Trunked Channels	Remote Diagnosis and Control
Private Call	Radio Inhibit	Emergency Alarm and Call	Location Tracking	Two Channels (Slot 1 and Slot 2)	Privacy
All Call	Remote Monitor	Emergency Alarm with Voice to Follow	Telemetry	Shared Channel Support	Time-out Timer

Voice Features	Signaling Features	Emergency Handling	Data Calls	Other Features	
Dual Tone Multi Frequency	Radio Check	Emergency Revert Group	Third-Party (ADP) Applications	Call Initiation by a Listening Radio	Option Board
Voice Interrupt	Call Alert	Emergency Voice Interrupt	Data Revert Channels	–	–
Digital Telephone Patch	Remote Voice Dekey	–	Data Over Voice Interrupt	–	–

The System Design Considerations on page 395 section discusses some of the considerations to take while designing a MOTOTRBO system. It focuses more on how the user uses the system, and the configuration needed to support it. Although a basic system topology may already have been chosen, the System Design Considerations on page 395 section helps dig deeper into how the end user utilizes the system, and therefore gives additional ideas on how it should be configured.

3.2.7.3

Repeater Network Configuration Options in Capacity Plus Single Site and Capacity Plus Multi Site

When topology with NAT is deployed, a site router with hair-pinning can be required. This requirement depends on the repeaters' network configuration and software version. Below is a description of three possible types of those configurations. Although those topologies are mainly for Capacity Plus Multi Site systems, the Capacity Plus Single Site systems are also the case when remote RDAC, MNIS, or other application PCs exist.

Repeater Configuration for Topology without NAT

Topology without NAT is used when the sites are interconnected using tunnels or are inside the corporate network. In this case, all devices use IPv4 addresses from the private address space.

The repeater network configuration consists of:

- **Ethernet IP**, **Gateway IP,** and **Gateway Netmask** in the **Network Settings** section of **General / Network** settings;
- **Link Type**, **Master IP**, **Master UDP Port,** and **UDP Port** in the **Network Settings** section of **General / Link Establishment** settings;
- **Site ID**, **Rest Channel/Site IP**, and **Rest Channel/Site UDP Port** in the **Capacity Plus** section of**General / Link Establishment** settings.

The parameters: **Ethernet IP**, **Gateway IP,** and **Gateway Netmask** are the repeater's Ethernet interface IPv4 settings. The **Master IP** and **Master UDP Port** are IPv4 settings of the Master repeater that all repeaters in the system need to know to establish communication with the Master. The **Link Type** decides whether the repeater will be the Master (**Master**) or the peer (**Peer**) repeater in the system. The **UDP Port** is the IPv4 UDP port, the repeater will be used as a source port in every UDP session and on which it listens to incoming sessions. The same is with **Master UDP Port** regarding the Master repeater.

NOTE: For CPSS and CPMS systems, in Master repeater configuration, the Master UDP Port and UDP Port parameters need to be the same.

All parameters in the **Capacity Plus** section of **General / Link Establishment** settings are common for the site and need to be the same in all repeaters with the same **Site ID**. Repeaters with the **Site ID** equal to the Master repeater **Site ID** are local peers from the Master point of view. Repeaters with different **Site ID** than the Master are remote peers from the Master point of view.

The Master repeater always uses peer's repeaters IPv4 address as they are seen from the Master site router WAN interface. When NAT configuration is not used, the peer repeaters are seen with their real (physical) IPv4 addresses.

Repeater Configuration for Topology with NAT

Topology with NAT is used when the sites are interconnected using public Internet access.

Because the Master repeater always uses the peer's repeaters IPv4 address as they are seen from the Master site router WAN interface, when NAT configuration is used, the peer repeaters are seen with the NAT'ed IPv4 addresses. That usually means the peer site router's WAN IPv4 address and the original peer repeater's UDP port.

NOTE: It is possible that the site router does NAT using a public IPv4 address other than the router WAN interface but this is rarely used.

Repeater Configuration Version 1

In software versions lower than R02.20.00, the site router for the Master repeater site should be capable of the hair-pinning feature. It is required because all peer repeaters in the system (local peer and remote peer repeaters from the Master repeater point of view) use the public IPv4 address of the Master repeater in the **Master IP** parameter. Public IPv4 means the address that is used by the site router for NAT configuration (usually routers WAN interface IPv4 address). In the Master repeater configuration, the **Master IP** parameter should be the same as **Ethernet IP**.

NOTE:
Using this configuration the hair-pinning router is required regardless of the repeaters software version.

Regardless of software version, in non Master site, the site router must support hair-pinning when any application PC (RDAC, MNIS, or other) exists in the repeater or other subnet of the site router.

Repeater Configuration Version 2

Starting from software versions R02.20.00 for CPMS and from R02.20.12 for CPSS, site routers for the Master repeater site can work with or without the hair-pinning feature. When a non-hair-pinning router or configuration is used, all remote peer repeaters in the system use the public IPv4 address of the Master repeater in the **Master IP** parameter. Public IPv4 means the address that is used by the site router for NAT configuration (usually routers WAN interface IPv4 address). Local peers, from the Master repeater point of view (it can be repeaters and/or application PCs), use the private (physical) IPv4 address of the Master repeater in the **Master IP** parameter. In contrast this time, in the Master repeater configuration, the **Master IP** parameter must be set to the public IPv4 address of the Master repeater same as in the remote peer repeaters configuration.

NOTE: Regardless of software version, in non Master site, the site router must support hair-pinning when any application PC (RDAC, MNIS, or other) exists in the repeater or other subnet of the site router.

Site Router Hair-Pinning Requirement Overview

The following table provides guidelines for when a hair-pinning router is needed.

Table 78: Site Router Hair-Pinning Requirement Overview

System	Hair-pinning Router	Method of Deployment
IPSC	Not Required	Sites are communicating using VPN tunnels and routers do not use NAT configuration.

System	Hair-pinning Router	Method of Deployment
IP Site Connect	Required	When a site router with NAT configuration is used and more than one networked applications or repeaters are behind the site router.
CPSS Capacity Plus Single Site	Not Required	All the networked applications and the repeaters are in the same subnet as the Master repeater.
	Required	When the remote networked application (RDAC, MNIS, or other) is in use and a site router with NAT configuration is deployed.
CPMS Capacity Plus Multi Site	Not Required	• Sites are communicating using VPN tunnels or over enterprise networks. • When using NAT topology, in non-Master repeater sites if there are only repeaters without networked applications or only one networked application without repeaters. • When using NAT topology, in the Master repeater site with firmware R02.20.00 and higher, and all the networked applications and the repeaters are in the same subnet as the Master repeater.
	Required	• When using NAT topology, in non-Master repeater sites if there are repeaters with networked applications or more than one networked application without repeaters. • When using NAT topology, in Master repeater site, when the networked applications are deployed on a different subnet than Master repeater. • When using NAT topology, in the Master repeater site with firmware below R02.20.00.

NOTE: If more than one networked application is installed on the same PC, then they are counted as separate applications from the hair-pinning feature point of view.

3.2.8
Digital Voting

Digital voting is available in the following system configurations:

- Digital Conventional Single Site

System	Description
IPSC IP Site Connect	Digital Voting is available in IP Site Connect

System	Description
 Capacity Plus Single Site	Digital Voting is available in Capacity Plus Single Site
 Capacity Plus Multi Site	Digital Voting is available in Capacity Plus Multi Site

When installing a receiver site (that may contain multiple receivers for Capacity Plus Single Site or Capacity Plus Multi Site system) in any of the system configurations, the receiver site must be in the same LAN that the voter site is in.

In order for the voting functionality to be working properly, the one way network delay between the repeater and any of its receivers must be less or equal to 40 milliseconds. Additionally, the network asymmetry between the repeater and any of its receivers must be less or equal to 12 milliseconds. The network asymmetry is the absolute value of the time difference for an IP packet to travel from the repeater to the receiver, and from the receiver to the repeater. This applies to all system configurations. Since the distance between the repeater and receiver is normally less or equal to 90 miles (approximately 145 kilometers), most of the business grade IP networks are able to meet this 40 milliseconds per 12 milliseconds network requirement.

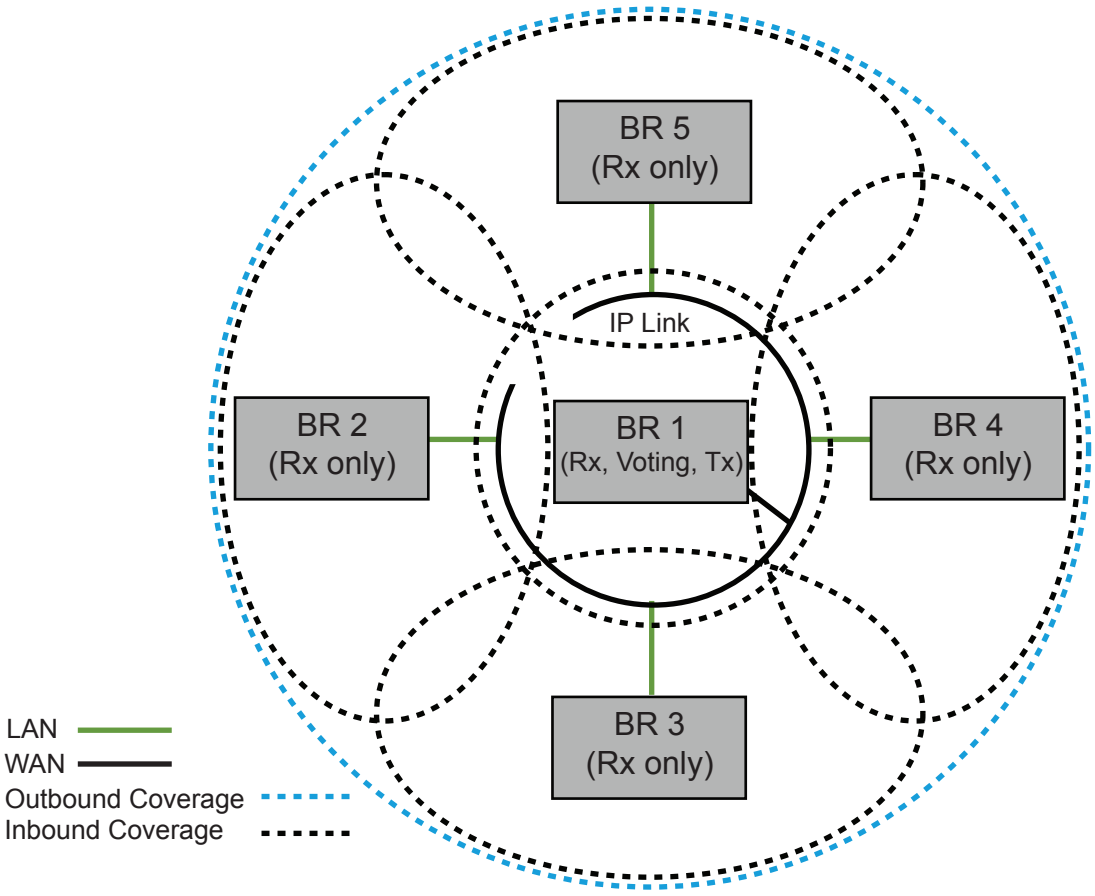
3.2.8.1
Digital Voting in Digital Conventional Single Site/Local Channels

In a voting configuration for Conventional Single Site system or for local channels, one voting repeater may be deployed with none, or up to eight satellite receivers. If RDAC, MNIS and other repeater peer applications are present in the system, a general rule applies – for every four RDACs or data applications, the maximum number of satellite receivers are reduced by one; for every two-voice applications, the maximum number of satellite receivers are reduced by one.

The satellite receivers receive the radio's transmission, verify and forward it to the voting repeater over an IP based network. The voting repeater then selects the best copy of the radio's transmission and repeats it over the air. This not only extends the repeater's inbound range, but also improves the inbound signal quality.

The following diagram shows a Conventional Single Site system with four satellite receivers.

Figure 139: Digital Voting Topology for Conventional Single Site or IP Site Connect Local Channel



3.2.8.2

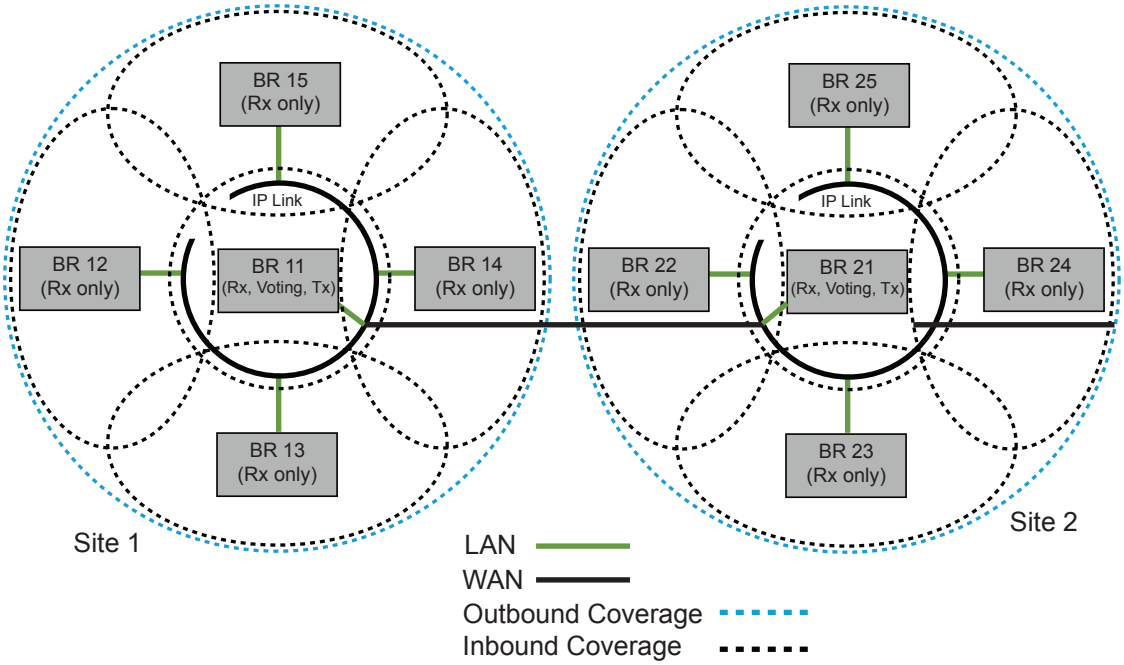
Digital Voting in IP Site Connect (Wide Area Channels)

IPSC

In a voting configuration for IPSC, each site can have none or a few satellite receivers. It is not necessary for the number of satellite receivers to be the same at each site.

The following diagram shows the topology of a two-site IPSC voting system with each site having four satellite receivers.

Figure 140: Digital Voting Topology for a Two-Site IP Site Connect System



The maximum number of satellite receivers for a specific voting repeater at a site depends on the number of repeater sites and RDAC/MNIS. The following table shows the maximum number of satellite receivers supported per voting repeater per site in a multi-site system including IPSC and Capacity Plus Multi Site.

Table 79: Maximum Number of Satellite Receivers Supported per Voting Repeater per Site in a Multi-Site System

Number of Sites	Maximum Number of Satellite Receivers Supported Per Voting Repeater Per Site
1	7
2	6
3	5
4	5
5	5
6	4
7	4
8	4
9	3
10	3
11	3
12	3
13	2
14	1

Number of Sites	Maximum Number of Satellite Receivers Supported Per Voting Repeater Per Site
>=15	0

NOTE: In general, for every four RDACs or data applications included in the system, the maximum number of satellite receivers is reduced by one. For every voice application included in the system, for example voice console, the maximum number is reduced by two.

3.2.8.3
Digital Voting in Capacity Plus Single Site

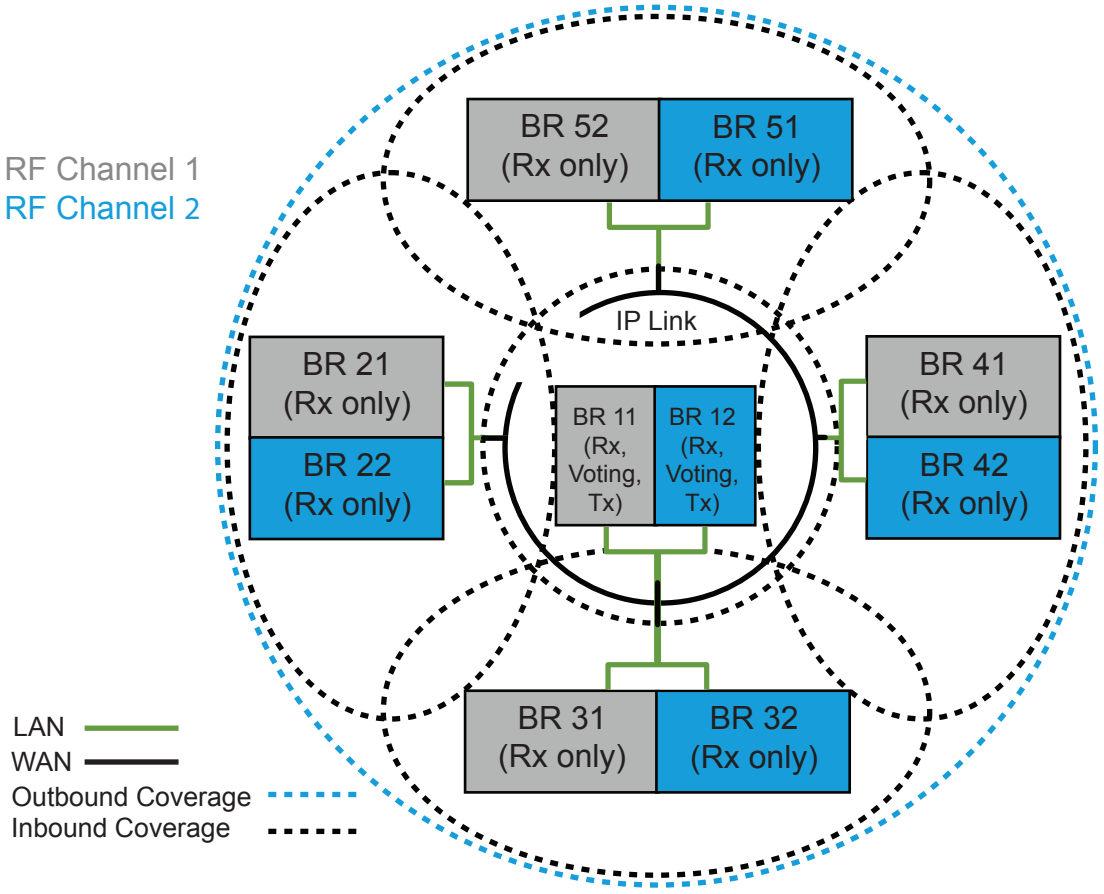
CPSS

In a Capacity Plus Single Site voting configuration, the maximum number of satellite receivers supported for an RF channel is eight. If RDAC, MNIS and other repeater peer applications are in the system, in general, for every four RDACs or data applications, the maximum number of satellite receivers are reduced by one. For every voice application included in the system, for example voice console, the maximum number is reduced by two.

In order to obtain the same Trunked Channel inbound/outbound coverage from channel to channel, each Trunked RF Channel requires a satellite receiver at any selected satellite receiver location. Hence, each Trunked RF Channel requires the same number of satellite receivers altogether. It is recommended to place a satellite receiver for each Data Revert RF Channel to achieve the same inbound/outbound coverage as the voice channels. However, this is not a requirement.

Figure 141: Digital Voting Topology for a Capacity Plus Single Site System on page 393 shows the voting topology for Capacity Plus Single Site with two RF channels, where each channel has four satellite receivers.

Figure 141: Digital Voting Topology for a Capacity Plus Single Site System



3.2.8.4 Digital Voting in Capacity Plus Multi Site

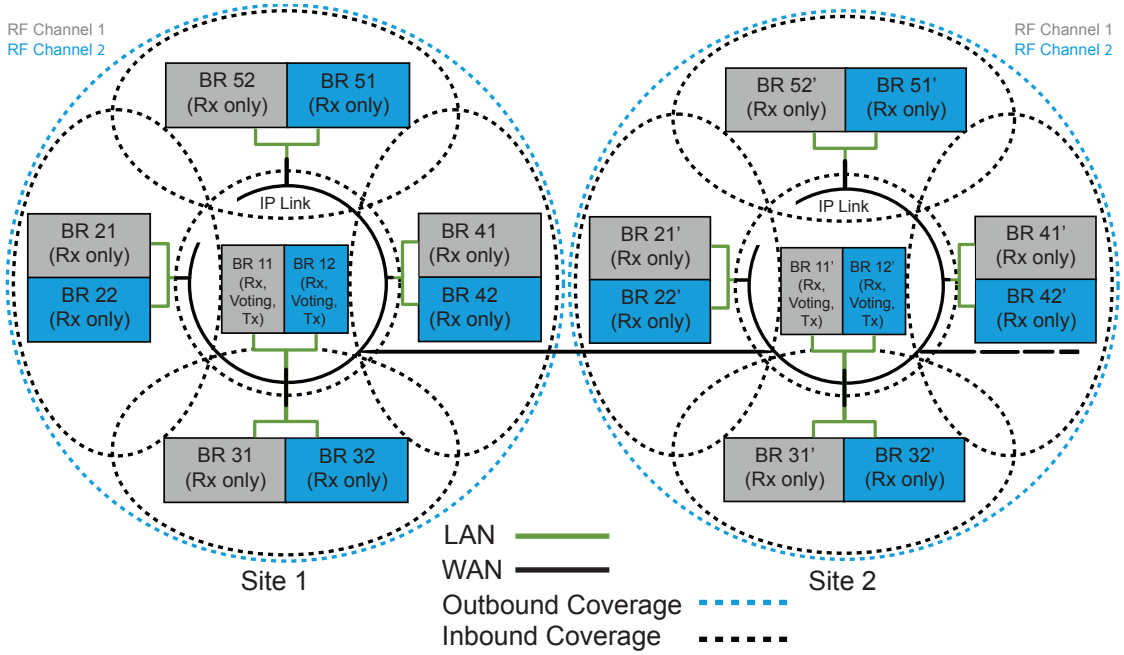
CPMS

The voting configuration in CPMS, is a combination of the IPSC and Capacity Plus Single Site voting configurations. Each site can have none or a few satellite receivers.

For each CPMS site, similar to Capacity Plus Single Site, in order to obtain the same Trunked Channel inbound/outbound coverage from channel to channel, each Trunked RF Channel requires a satellite receiver at any selected satellite receiver location. Hence, each Trunked RF Channel requires the same number of satellite receivers altogether. It is recommended to place a satellite receiver for each Data Revert RF Channel to achieve the same inbound/outbound coverage as the voice channels. However, this is not a requirement. It is not necessary for the number of satellite receivers to be the same at different CPMS sites.

Figure 142: Digital Voting Topology for a 2-Site Capacity Plus Multi Site System on page 394 shows the topology of a 2-site CPMS voting system with an RF channel at a site having four satellite receivers. The maximum number of satellite receivers supported at a site for an RF channel depends on the number of repeater sites and RDAC/MNIS.

Figure 142: Digital Voting Topology for a 2-Site Capacity Plus Multi Site System



Chapter 4

System Design Considerations

Table 80: System Design Considerations

System	Description
IPSC	Indicates IP Site Connect feature related content.
CPSS	Indicates Capacity Plus Single Site feature related content.
CPMS	Indicates Capacity Plus Multi Site feature related content.
CPSM	Indicates Capacity Plus Single Site AND Capacity Plus Multi Site shared feature related content.

4.1 Overview

This section describes various system configurations readers need to know before deciding how to best support the needs and usage of their customers. It explains the usage supported on a single repeater system, as a guideline for design. It then identifies the customer needs that need to be considered when optimizing system performance. It continues to cover various other considerations that may need to be addressed during the design phase.

NOTE: MOTOTRBO also supports server based data applications in repeater mode. This configuration consists of a PC (referred to as the Application Server) running the server software connected to the radio infrastructure via a mobile radio or via the MNIS application. For details on data communication with applications through the repeater network interface instead of a Control Station, refer to the applicable sections.
All data application modules contained in this system planner are depictions of typical third-party data application modules and have been included simply to illustrate certain MOTOTRBO application enabling features.

4.2
Analog-to-Digital Migration Plans

System Migration is the process of moving from one operating platform to another. The following sections elaborate system migration from a two-way radio platform to a digital two-way radio platform.

4.2.1
Pre-Deployment System Integration

Where applicable, the dealer should perform system assembly, configuration, adjustment, and brief testing of the MOTOTRBO system. Each component contains documentation necessary for system installation and optimization.

The benefits of staging a system in a controlled environment include:

- Equipment accountability in preparation for system assembly
- System assembly and programming in a controlled test environment
- Documentation of programming information
- Fabrication of cables and connectors
- Test of complete functionality and initial level-setting for system optimization

4.2.2
Preparation and Migration of Analog to Digital

A Dynamic Mixed Mode repeater does not enable communication between legacy and MOTOTRBO digital radios operating in digital mode. When the repeater receives an analog call, it retransmits in digital mode. When the repeater receives a digital call, it retransmits in digital mode. It is the scanning feature in the subscriber that allows the MOTOTRBO radios, programmed with both analog and digital channels, to listen to analog calls from legacy analog radios. While the MOTOTRBO radio is listening to an analog call through PL scanning, it talks back in digital mode, if keyed up within the call hang time.

NOTE: The MOTOTRBO radio needs to be in analog mode to initiate or return an analog call with legacy analog radios.

- To migrate a system with a single non-MOTOTRBO repeater channel, radio users are encouraged to use MOTOTRBO radios in digital direct mode/dual capacity direct mode.
  This gives them an opportunity to familiarize themselves with the MOTOTRBO digital feature set, while communicating with legacy analog radios through the legacy analog repeater. If the analog system does not use any PL/DPL encoding, then analog radios hear noise caused by digital radio transmissions communicating in direct mode/dual capacity direct mode.

  Over time, as the number of MOTOTRBO radios increases, a cut-over day is pre-determined. On that day, the legacy analog repeater will be replaced by a MOTOTRBO digital repeater. Radio users communicate with each other in Talkaround while the new repeater is being installed. Once the MOTOTRBO repeater is operational, MOTOTRBO radio users switch to digital repeater mode, while legacy analog radio users communicate in Talkaround.
- To migrate a system with two repeater channels, MOTOTRBO radios are programmed with both the current analog channels as well as future digital channels. A recommended approach is to place all the analog channels in one ‘zone’, and all digital channels in another ‘zone’. Analog and digital channels are programmed into the MOTOTRBO radios to allow users to communicate on both repeaters. Scan Lists are configured to allow users to monitor both analog and digital voice transmissions.
  Both the existing analog repeater and the MOTOTRBO repeater (in digital mode) should be set-up to operate side-by-side. This configuration requires two frequency pairs: one pair for the analog repeater and one pair for the MOTOTRBO repeater. Users gradually migrate over to the MOTOTRBO repeater

(for example, legacy analog radios are swapped for MOTOTRBO radios). Once every analog radio has been swapped with a MOTOTRBO radio, the legacy analog repeater can be replaced with another MOTOTRBO digital repeater. The system is now fully digital with two digital repeater channels.

- To migrate a system with a single MOTOTRBO repeater channel, load/upgrade the MOTOTRBO repeater with firmware version R01.06.10 or later. Configure the repeater to Dynamic Mixed Mode using the CPS. This configuration requires one frequency pair. Analog and digital channels are programmed into the MOTOTRBO radios to allow users to communicate through the same repeater. Scan Lists are configured to allow users to monitor both analog and digital voice transmissions on the same frequency.
  In Dynamic Mixed Mode, MOTOTRBO system does not enable some of the digital only features like IP Site Connect, Capacity Plus Single Site, Transmitter Interrupt and RDAC over IP. The system allows digital and analog voice transmission at one site.

  Once every radio has been swapped with a MOTOTRBO radio, the MOTOTRBO repeater can be reconfigured to fully operate in digital mode, therefore allowing the user to experience all available digital features.

4.2.3
New/Full System Replacement

The new/full system replacement strategy involves replacing all existing equipment with MOTOTRBO equipment.

Typically, a new/full system replacement involves minimal downtime as the repeater is replaced immediately with the MOTOTRBO digital repeater. Radio users carry their existing radios as well as MOTOTRBO radios on cut-over day. Initially, users continue to access the radio system in the same manner as before. Once the analog repeater is removed from the system, the radio users switch to digital direct mode/dual capacity direct mode communication using MOTOTRBO radios. After the MOTOTRBO repeater is installed and becomes operational, radio users switch their MOTOTRBO radios to digital repeater mode.

The new/full system replacement relies on the MOTOTRBO equipment being properly programmed and tested before being deployed.

4.3
New Frequency Licensing (Region Specific)

The licensing process varies from region to region. Generally, before the license process begins, detailed information about the proposed radio system must be provided to the frequency coordinator, such as:

Frequency/ Frequency Band
Frequency band or specific frequency it operates on.

Subscriber Radio Count
The number of radios that will operate on the system.

Output Power/ERP
The output power of the system amplifier, as well as the effective radiated power (ERP), which is the system's power at the antenna.

Emission Designators
Includes several pieces of vital information, such as modulation, signal, type of information and size of the channel. This determines the channel width your system will occupy. For MOTOTRBO systems, the Emissions Designators are as follows:

- Data only: 7K60FXD
- Voice and Data: 7K60FXE

The first four values are defined as the ‘Necessary Bandwidth’. This can be derived from the 99% Energy Rule as defined in Title 47CFR2.989. The next two values are the ‘Modulation Type’ and the ‘Signal Type’.

The final value is the ‘Type of Information’ being sent. More information can be found with the region’s frequency coordinating committee.

International Coordination

For stations near another country’s border, refer to a frequency coordinating committee for licensing frequencies adjacent to that country.

Antenna Information

You must also provide the following information about your antenna:

- Structure. The most common codes are:
- B – Building with side mounted antenna
- BANT – Building with antenna on top
- MAST – Self-supported structure
- PIPE – Pipe antenna
- POLE – Any type of pole antenna
- TOWER – Free standing guyed structure used for communications purposes
- Height
- Antenna Height – Antenna height from ground to tip, in meters.
- Support Structure Height – If antenna is mounted on top of a building, it is the distance from ground to the top of the building. Check with the building management company for this information.
- Coordinates – Latitude and longitude should be listed in degrees, minutes and seconds.
- Site Elevation – The antenna site ground elevation above sea level. This information should always be in meters.

4.4 Converting Existing 12.5/25 kHz Licenses

The process for converting 25 kHz to 12.5 kHz varies between regions. It is recommended to contact the local frequency coordinator’s office to inquire how to re-file existing frequency allocations. There are also consultants that specialize in frequency coordination and can advise on the filing process. In the US, the following are general guidelines for frequency licenses:

Procedure:

1. For existing 12.5 kHz license(s), the user must file an update to the emission designators indicating 7K60FXE (for voice) and 7K60FXD (for data) for all applicable frequencies.
2. If the user has existing 25 kHz licenses(s), they must file an update to the emission designators to include 7K60FXE (for voice) and 7K60FXD (for data) for all applicable frequencies.

   Typically, the user is then allowed to transmit a 12.5 kHz signal bandwidth at the same center frequency as the original 25 kHz license. Note that it is not a straightforward process to convert an existing 25 kHz license into a pair of 12.5 kHz channels. Users are generally NOT allowed to split their 25 kHz channel into two 12.5 kHz sub-channels that would operate off center from the original license and adjacent to one another.

4.5
Repeater Continuous Wave Identification (CWID)

The repeater can be configured to transmit the CWID if required by the region. The CWID is also known as the Base Station ID. The CWID is a transmission of the station in Morse code that takes place every 15 minutes. This identification, as well as the transmit interval, can be configured in the repeater using the CPS.

To ensure proper Dynamic Mixed Mode operation, only exclusive CWID transmission is supported in MOTOTRBO repeater operating in Dynamic Mixed Mode. Mixed CWID is not supported in order to be compliant with the digital mode of operation. Furthermore, the exclusive CWID transmission cannot be interrupted by either Over-The-Air transmissions or PTT transmissions by the repeater's accessories.

4.6
Repeater Narrow IF Filter

If Adjacent Channel Selection (ACS) is poor, the following problems may occur:

- Near/far adjacent channel interference scenario at the Repeater’s receiver: With a current protection of 57 dB, if signal on adjacent channel is 57 dB above desired signal, then there is 3 dB Rx degradation.
- Impact to voice: There is 3–5 dB range from no audio to acceptable DAQ 3.0 audio.
- Impact to data: For confirmed data, there is 15 dB range that is impacted and results in more retries and lower throughput.

Interference from adjacent channel can be reduced by reducing the receive bandwidth. DMR modulation sideband power falls at 10 dB/kHz. 1 kHz narrowing of bandwidth would improve adjacent channel protection by 5 dB on each side. Decreasing receiver bandwidth requires mechanism to control reference oscillator drift over time (aging). Subscribers use high stability Repeater frequency to persistently tune the Subscriber reference oscillator. 900 MHz requires 0.1 ppm this option is also available for 800 MHz. To support current deployments with no impact to range, there is a need to allow selection of Narrow or Wide (existing) filter in the repeater through a CPS option. This is applicable only to digital channels and not analog channels. Analog channels always use the default Wide IF Filter. Selection of narrow IF Filter improves ACS by 3–4 dB and degrades the sensitivity by 0.5 dB.

The following configurations are recommended for system deployment:

- For digital channels with adjacent channel separation of 12.5 kHz – select Narrow IF filter
- For digital channels with adjacent channel separation greater than 12.5 kHz – select Wide IF filter

4.7
Digital Repeater Loading

The designer is able to choose the number of channels required to support his customer’s expected traffic after understanding how much traffic a single slot (channel) can support. The amount of traffic on a channel is dependent on numerous variables, which are difficult to estimate exactly at design time.

Since MOTOTRBO comprises of Voice traffic, Text Messaging traffic, Location Tracking traffic, Registration and Signaling traffic, the previous voice traffic methods to gauge repeater capacity may not be sufficient. Because this traffic is mostly initiated by the end user, it is difficult to predict how often it occurs. Standard usage profiles of existing customers have been created for voice and data services. These profiles act as a baseline for estimating how much traffic a user creates on a system. If the standard profiles do not match your customer’s expected usage, further estimations based on the trend lines need to be considered. After the system is used, and real life usage is identified, further adjustments may be required.

4.7.1

Assumptions and Precautions for Digital Repeater Loading

Channel loading analysis involves several assumptions:

- Generalized high-level view of data and voice services interaction represents true interaction.
- An estimated amount of blocking, interference, reliability, and call denials varies with the traffic profile and could change some of the results used.
- An estimated number of radios using the location tracking feature (100%) and the rate of those messages for the high-end traffic profile (once every minute for every mobile) is used.

Given these assumptions, the chart presented can be used to provide customers with a general rule of thumb for levels of user experience expected based on the number of users. In addition, for this analysis, the term “number of users” is used to indicate the number of active/participating users generating traffic, and does not include the number of users who monitor the activity of other radios on the channel.

4.7.2

Voice and Data Traffic Profile

The following table summarizes the standard traffic profiles for voice and data. The three traffic types considered are voice calls (Group Calls and Private Calls), data transmitted for location tracking and text messaging. For each traffic type, two levels are set. One, is for the case of a typical low usage or light traffic user, and the other is for a typical high usage or heavy traffic user. The voice and text messaging profiles are derived using assumed typical behaviors.

These profiles act as a baseline for estimating how much traffic a user creates on a system. If these standard profiles do not match your customer’s expected usage, further estimations based on the trend lines need to be considered. Further, this is the profile of how all users on a channel will act together. It is understandable that not all users will use this profile all the time. These profiles should be used to estimate the number of users per channel that yield an acceptable user experience.

Table 81: Voice and Data Traffic Profiles

Profile Name	Traffic Type	Call Description	Traffic Per User Per Hour	
High Voice	Group Voice Call	10 second call, 2 transmissions per call	3.0 Calls per User per Hour	90%
	Individual Voice Call	20 second call, 4 transmissions per call		10%
Low Voice	Group Voice Call	10 second call, 2 transmissions per call	1.0 Calls per User per Hour	90%
	Individual Voice Call	20 second call, 4 transmissions per call		10%
High GPS	Location Updates	660 milliseconds (for Single Repeater and IP	60 GPS Transmissions per User per Hour For example, 1 Minute Update Period (Cadence)	

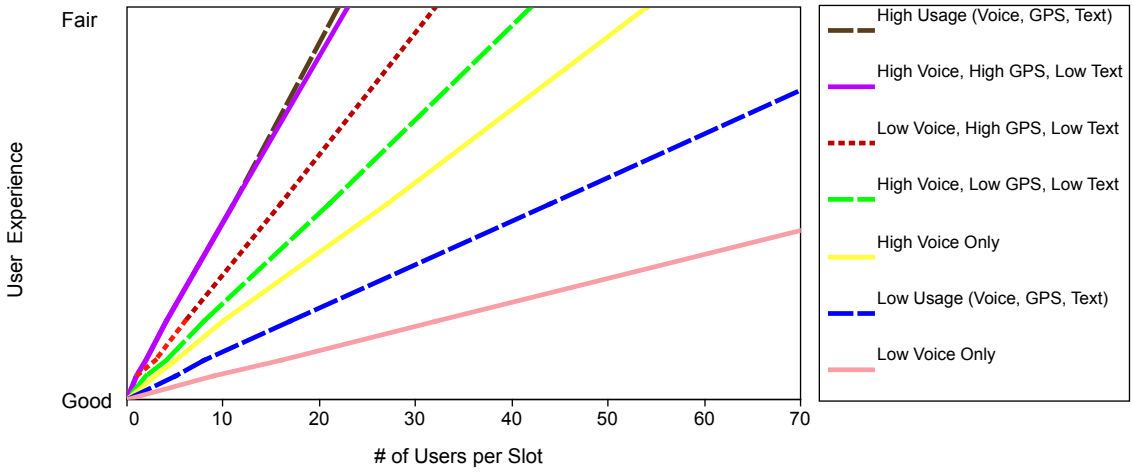
Profile Name	Traffic Type	Call Description	Traffic Per User Per Hour
		Site Connect) per transmission and 540 milliseconds (for Capacity Plus Single Site mode) per transmission	
Low GPS	Location Updates	660 milliseconds per transmission	6 GPS Transmissions per User per Hour For example, 10 Minute Update Period (Cadence)
High Text Messaging	Text Messaging	100 characters per message	2.5 Text Messages per User per Hour
Low Text Messaging	Text Messaging	100 characters per message	0.5 Text Messages per User per Hour

4.7.3
Estimate Loading (for Single Repeater and IP Site Connect)

IPSC

Figure 143: Number of Users per Slot versus User Experience on page 401 indicates the user experience level (the impact on the network) that the number of active users, using combinations of the defined profiles of Voice and Data Traffic Profile on page 400 experiences.

Figure 143: Number of Users per Slot versus User Experience



Each line in the chart has a combination of Voice, GPS, and Text Message at different usage levels. For example, the blue line identified as “Low Usage (Voice, GPS, Text)” represents a channel where each user transmits 1 Group Call an hour, 0.5 text messages an hour, and has a GPS Update Period (Cadence) of 10 minutes. If the defined profiles do not exactly match the estimated usage, the reader will need to extrapolate between two trend lines.

There are two levels shown in the graph to describe user experience – good to fair. The good level means that the system is supporting this level well and if the customer is operating in this level the majority of the time, then the system is adequately provisioned. This means that the fair level may be reached for short periods of time as long as the system returns to supporting a lower level of traffic for the majority of the time.

It is advised to avoid operating in the fair level when possible. If the customer experiences issues with reliability and/or call denial, this could indicate that the system is operating in the fair level for longer periods of time. If this occurs, the customer may require additional repeaters to support their traffic load. A system that operates in the fair level for the majority of the time results in longer wait times and having a significant number of unsuccessful attempts to acquire the channel on the user's first attempt. These conditions would result in an unsatisfactory level of performance for the end users, even though the system itself is capable of operating in this region.

There are trends indicated in the chart that are worth noting. One is the impact in going from a Low Voice usage traffic environment to a High Voice usage traffic environment. The chart shows that a customer using the system for voice services only should be capable of supporting approximately 45 users on the channel if the user traffic falls into the Low Voice usage traffic profile (one call per user per hour). However, if the customer intends to support a higher level of voice traffic, a single channel should be capable of supporting between 15 and 20 users and still remain in the good user experience level.

It is always difficult to accurately predict a customer's usage as being either high or low. It is expected that most customers will operate somewhere in between these two profiles. The designer must use knowledge of the customer's organization and their expected usage to predict where on this chart they will operate. Note that the voice-only lines are a good frame of reference for existing customer with analog voice systems. These trend lines represent those of a voice-only system and a voice-only digital system. Understanding what user experience level a customer is currently operating at can help with predicting the new user experience, when adding data services.

Two other trends from the chart are also worth pointing out. The first is that the level of adding data (low traffic for location tracking and text messaging) does not cause a huge impact to the number of users supported. For example the lines for High Voice usage traffic (one with voice only and the other with the addition of low location tracking and text messaging) both show that supporting 15–20 active users on one channel will keep the system from approaching the stressed level. Similarly, both curves for the Low Voice traffic show that 30–35 users could be supported well on a single channel.

Another important note is that these trend lines are associated with a single slot of a MOTOTRBO repeater. Since MOTOTRBO is a two-slot TDMA system, a customer that is upgrading from a traditional FDMA one channel conventional system will have the ability to split users into two slots. For example, if a high usage voice only customer is currently supporting 30–40 users on a single channel, they are most likely operating in a "fair" or "stressed" environment and will likely need to expand their system. If they switch to a MOTOTRBO system, they can divide their users into the two available channels. This means a single channel now has only 15–20 users, which would bring the customer back to a good user experience level. Subsequently, adding on low usage data services on both channels will cause minimal impact to performance.

When GPS CSBK data is enabled, twice the number of radios can be supported with a similar GPS success rate. However, if the voice and TMS traffic are increased along with the number of radios, the voice and TMS user experience will drop.

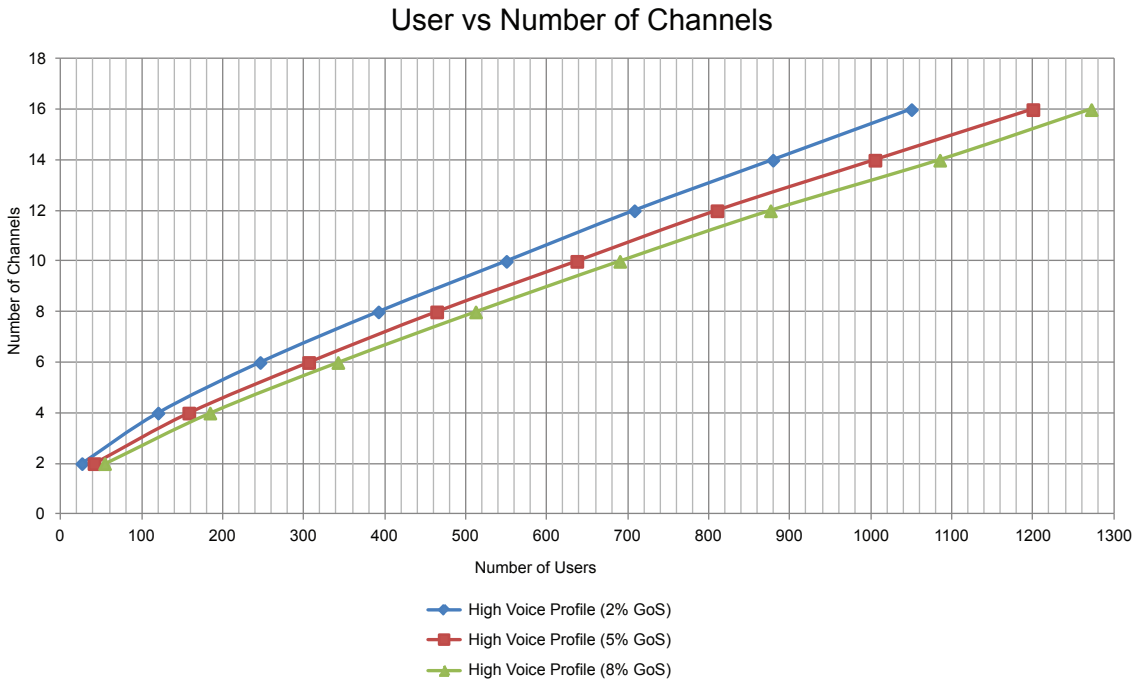
4.7.4
Estimate Loading (for Capacity Plus Single Site)

CPSS

The following charts, Figure 144: Number of Users Versus Number of Channels for Voice-Only Profile on page 403 and Figure 145: Number of Users Versus Number of Channels for Mixed Profiles on page 404 indicate the number of Trunked Channels (slots) a Capacity Plus Single Site system requires for a given user

experience, for a given number of active users, and for different combinations of the Voice and Data Traffic profiles as defined in Voice and Data Traffic Profile on page 400. It is assumed here that the number of groups are more than the number of channels.

Figure 144: Number of Users Versus Number of Channels for Voice-Only Profile



Number of Channels	High Voice Profile (2% GoS)	High Voice Profile (5% GoS)	High Voice Profile (8% GoS)
2	26	41	54
4	120	158	184
6	246	306	342
8	392	464	512
10	550	637	690
12	708	810	876
14	879	1005	1085
16	1050	1200	1272

The charts represent a radio user's experience in making a call in terms of Grade of Service (GoS). GoS is directly related to the probability of a call getting blocked (that is probability of all the Trunked Channels being busy). For example, a GoS of 2% means that 2% of the calls made by the radio users will be either denied or will need to wait for a channel to become available.

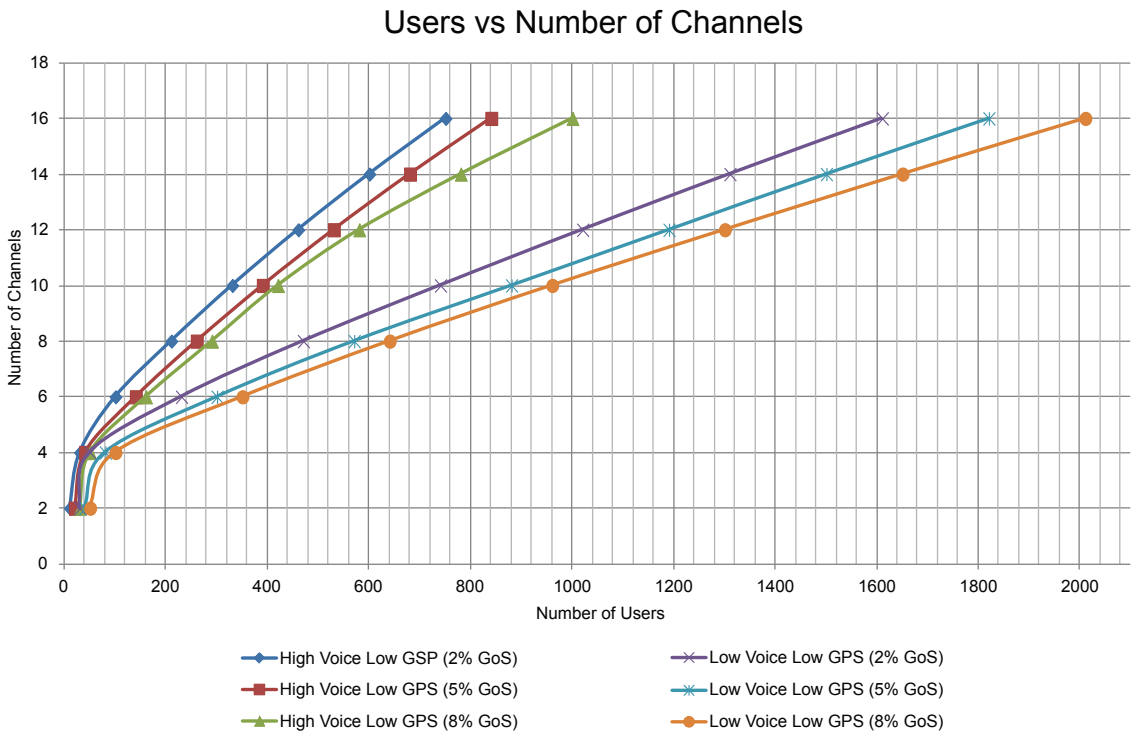
The "channel" in the chart refers to a logical channel (a slot). In Capacity Plus Single Site, both channels of a repeater are in either trunked mode or none. Therefore, the charts provide the number of users only for an even number of channels.

The number of calls handled by a Capacity Plus Single Site system may vary considerably based upon the quantity of users and volume of calls. Most systems are heavily loaded for a few hours in a day. It is recommended that the system be designed with an adequate amount of channel resources to handle peak as well as off-peak traffic.

The first chart is for High Voice profile (Three Calls per User per Hour) with no GPS data. The same chart can also be used for other voice-only profiles by adjusting the “number of users” (the x-axis) of the chart. For example, in the case of Low Voice profile (1 Call per User per Hour), the “number of users” should be multiplied by three.

Figure 145: Number of Users Versus Number of Channels for Mixed Profiles on page 404 is for mixed voice and GPS data profile. It has two sets of graphs – one for High Voice with low GPS data and the other for Low Voice with low GPS data. Both voice and GPS data are using the Trunked Channels. Take note of the trend indicated in the chart. The number of users do not increase proportionally with the number of channels. The rate increases as the number of channels increase. This is due to the fact that the efficiency of trunking increases with the increase in the number of channels.

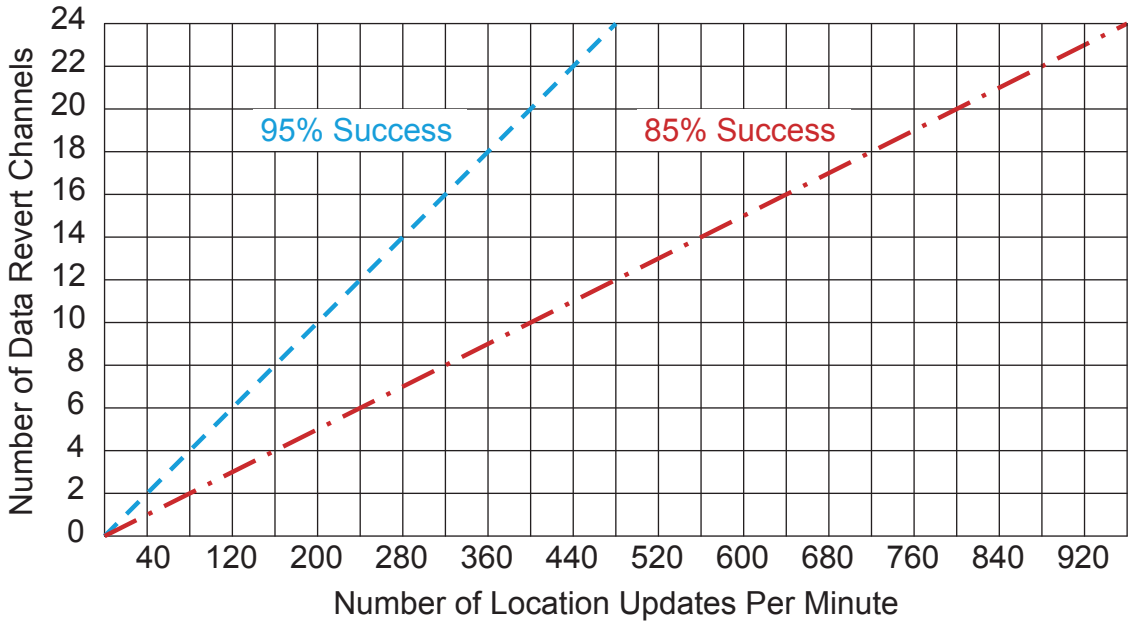
Figure 145: Number of Users Versus Number of Channels for Mixed Profiles



Number of Channels	High Voice Low GPS			Low Voice Low GPS		
	2% GoS	5% GoS	8% GoS	2% GoS	5% GoS	8% GoS
2	10	20	30	30	40	50
4	30	40	50	50	80	100
6	100	140	160	230	300	350
8	210	260	290	470	570	640
10	330	390	420	740	880	960
12	460	530	580	1020	1190	1300
14	600	680	780	1310	1500	1650
16	750	840	1000	1610	1820	2010

In the case of high GPS data, it is recommended that a Capacity Plus Single Site system have exclusive channels for data called Data Revert Channels. Figure 146: Number of Location Updates versus Number of Data Revert Channels on page 405 shows graph for high GPS data over Revert Channels. A Data Revert repeater offers two Data Revert Channels and a Revert Channel can carry up to 20 location updates per minute with a success rate of 95% and 40 location updates per minute with a success rate of 85%. When GPS CSBK data is enabled, twice the number of radios can be supported with a similar GPS success rate. However, the trunked channel may not be able to support more radios.

Figure 146: Number of Location Updates versus Number of Data Revert Channels



4.7.5
Estimate Loading (for Capacity Plus Multi Site)

CPMS

If the number of Trunked Channels are not the same at all sites, the loading for Capacity Plus Multi Site can be estimated by estimating the loading of a Capacity Plus Single Site system having ‘n’ Trunked Channels, where ‘n’ is the number of Trunked Channels at the smallest site.

For 12 trunked channels (that is six trunked repeaters), high voice only profile (Voice and Data Traffic Profile on page 400), and Grade of Service = 2%, a Capacity Plus Single Site system can support approximately 700 radios. See Figure 144: Number of Users Versus Number of Channels for Voice-Only Profile on page 403.

A Capacity Plus Multi Site system handles the local calls as efficiently as Capacity Plus Single Site. Therefore if all calls are local, then for three sites, a Capacity Plus Multi Site system can handle 3*700 = 2100 radios. If all the calls are wide area talkgroup calls, then the number of radios supported by a Capacity Plus Multi Site system is 700, which is the same as the number of radios supported by a Capacity Plus Single Site system.

To estimate supported loading in both local and wide area talkgroup calls, assume the following:

- S = Number of sites (maximum of 3);
- W = Average number of sites associated with wide area talkgroups;

- L = Number of local calls as a fraction to total number of calls (for example, if there are 500 local calls out of total 1500, then L=1/3);

With the above assumptions, the supported loading by a Capacity Plus Multi Site system is: R*S (L + (1-L)/W) radios, where ‘R’ is the number of radios supported by a Capacity Plus Single Site system.

Example: For 3 sites (S=3), 12 trunked channels, 2% Grade of Service, one third local calls (L=1/3), and an average of 2 sites associated with wide area talkgroups (W=2), a Capacity Plus Multi Site will be able to support 700*3 (1/3 +(1-1/3)/2) = 1400 radios.

NOTE: 700 is the number of radios supported by a 12-channel Capacity Plus Single Site system at 2% Grade of Service.

If the number of trunked channels is different at all the sites, the loading for Capacity Plus Multi Site can be estimated by first estimating the loading of a Capacity Plus Multi Site system having ‘n’ trunked channels, where ‘n’ is the number of trunked channels at the smallest site.

Example: A Capacity Plus Multi Site system has four sites – A, B, C, and D. Sites A and B has two trunked repeaters and sites C and D has three trunked repeaters. Then, for 2% Grade of Service, one third local calls (L=1/3), and an average of 2 sites associated with wide area talkgroups (W=2), a Capacity Plus Multi Site will be able to support 120*4 (1/3 +(1-1/3)/2) = 320 radios. Note that ‘120’ is the “number of users”, which comes from number of channels = 4 and 2% grade of service. If the additional capacity at site C and D are designed for local calls, then Site C or Site D can support 240 users (number of channels = 6), that is, an additional 120 users at Site C and an additional 120 users at Site D. Thus, the total number of users supported by the system is 320 + 120 + 120 = 560 radios.

In the case of high GPS data, it is recommended for a Capacity Plus Multi Site system to have exclusive channels for data defined as Data Revert Channels. The figure shows a graph for high GPS data over Revert Channels. A Data Revert repeater offers two Data Revert Channels and a Revert Channel can carry more than 20 location updates per minute with a success rate of 95% and 40 location updates per minute with a success rate of 85%.

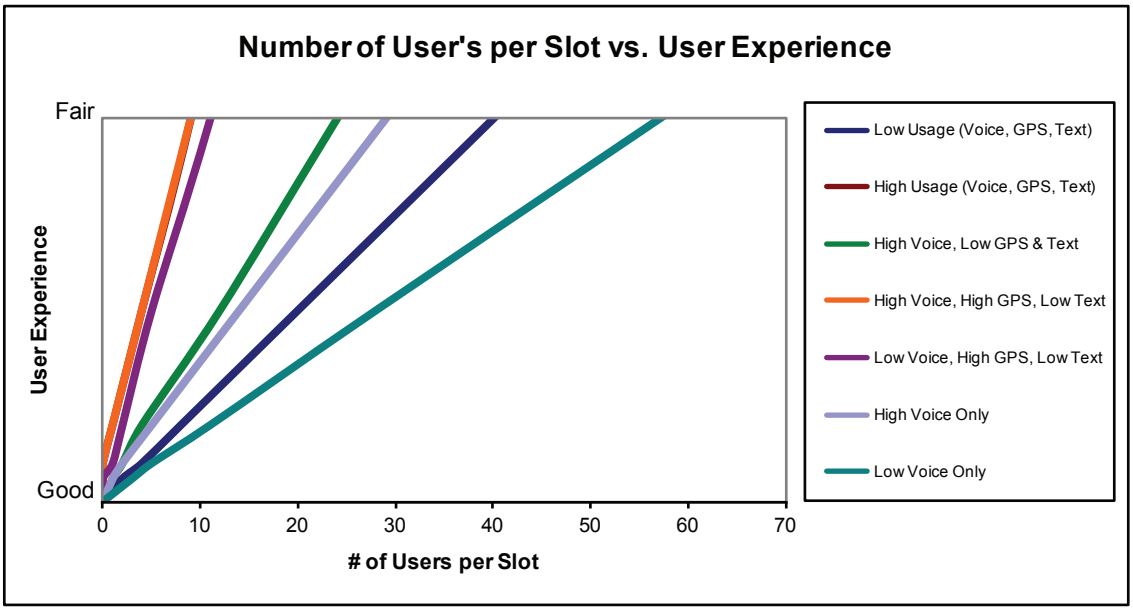
4.7.6
Estimate Loading (for MOTOTRBO Link)

Compared to a Single Repeater and IP Site Connect mode, MOTOTRBO Link mode introduces the concept of Over-The-Air (OTA) hops and the Number of Backhaul Chains. The number of users that can be supported per slot depends on the usage profile, number of backhaul sites and whether the customer has more than one backhaul chain. Due to the transmission delay introduced by OTA hops between the repeater backhaul sites, the throughput of the system is lower than IP Site Connect mode.

Both figures indicate the user experience level that the number of active users, using combinations of the defined profiles of Voice and Data Traffic Profile on page 400 experiences in MOTOTRBO Link mode.

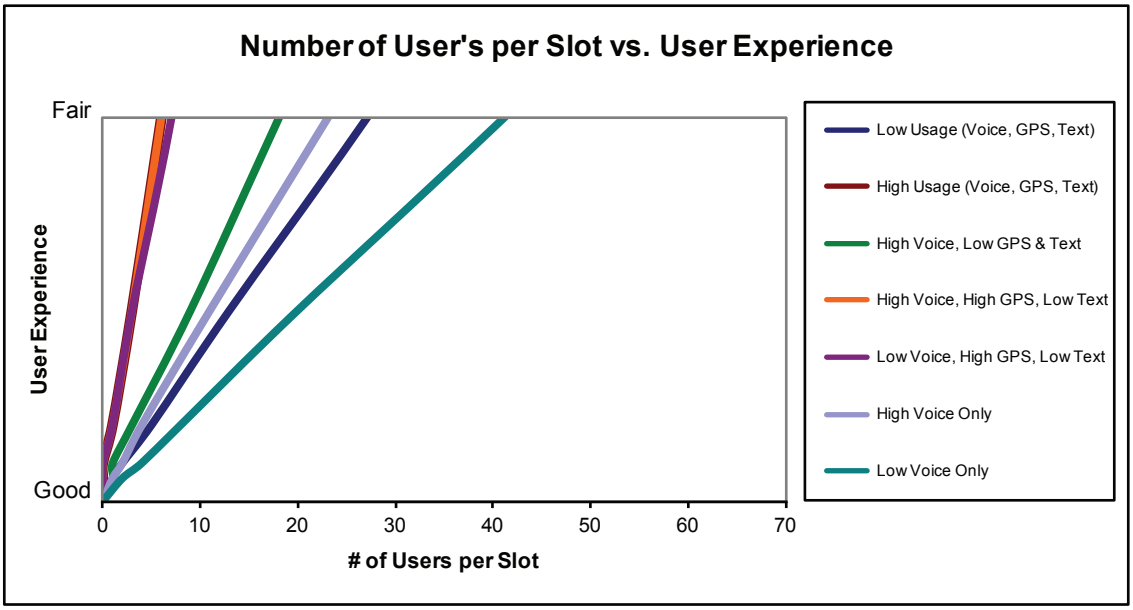
The following figure is for the MOTOTRBO Link system which has one chain with three sites.

Figure 147: Number of Users per Slot Versus User Experience (One Chain, Three Sites)



The following figure is for the system which has two chains. Each chain has five sites. When more sites and another chain are added to the system, the number of radios that can be supported for one slot is decreased.

Figure 148: Number of Users per Slot Versus User Experience (Two Chains, Five Sites Each)



The GPS transmissions have high impact on the number of users supported per slot. Since MOTOTRBO is a 2-slot TDMA system, a customer could off load the GPS transmission to the second slot and using the first slot for voice only if the GPS profile is high. Furthermore, GPS transmission can be configured as unconfirmed in order to reduce the traffic introduced by it.

To get the details or the number of users per slot with another deployment of a MOTOTRBO Link system with a different number of MOTOTRBO Link Sites and Chains, see the MOTOTRBO System Design Tools.

4.7.7
Load Optimization (for Single Repeater and IP Site Connect)

System	Description
IPSC IP Site Connect	The following contents in section Load Optimization (for Single Repeater and IP Site Connect) on page 408 and all its subsections explain about Loading Optimization in IP Site Connect.

There are further considerations to take when configuring your MOTOTRBO system to ease the traffic load on a channel. These considerations should always be taken into account, especially if the designer is forced to operate outside of the “good” user experience range, although operating in such a manner is not recommended.

4.7.7.1
Distribution of High Usage Users

It is good design practice to identify and distribute high usage users and groups between slots of a single repeater, or even other repeaters. This keeps the number of users that follow a high usage traffic profile to a minimum per channel. Groups are generally assigned to operate on a particular slot of a repeater. Through discussions with the customer, the designer should identify high usage groups and distribute them over different slots.

Groups and users that are on different slots cannot communicate with each other. They need to manually change their selector knobs to communicate with the users and other groups on the other slot. In most cases, this is not a problem since organizations can usually be broken into at least two groups of users. But in the case where a customer only has one group of users who all need voice communication between each other at all times, then evenly distributing the voice and data load between two channels becomes more complicated.

If there is only one group in a system, its users can be programmed to operate on a particular slot. Their Group Calls, Private Calls, text messages, location updates are transmitted on the programmed slot. This is an acceptable configuration, although it leaves the other slot completely unused. If the number of users and their usage grows, the slot may be unable to support their traffic. For example, if a customer has 50 users with voice and GPS usage all on one time slot, their user experience may be poor due to the traffic loading. It is highly recommended that the users in this case be broken into two unique groups of 25, and distributed between the slots.

In the event, that all users could be broken into two unique groups, but are required to maintain voice communication with each other, the solution is to split the same group across the two slots, and enable scan. One half of the group should be assigned to slot 1, and the other half assigned to the same group, but on slot 2. They should use the same group number. This can be done by having two channels with the same frequencies but different slots, and with the same group as the TX Call Member. All radios should include both (and only) these two channels in their selected Scan List. Scan hang time duration should be set to the Group Call hang time duration in the repeater, which defaults to two seconds. Talkback scan should always be enabled so that users can talkback during the scan hang time. When assigning all users to the same group, the use of scan primarily serves to aggregate the multiple channels into a single logical channel for voice. Location data is transmitted out the selected channel when no voice is taking place. Therefore location data will be evenly distributed across two slots. Note that when a voice call occurs, all radios are scaned and land on a particular slot. The other slot is empty at this time since all radios are monitoring the voice call.

The drawback of this operation, and why it is not generally recommended, is that this configuration essentially cuts the voice capacity of a repeater in half since only one voice call can take place at any given time, although this does allow for data transmission to occur at the same time on the different slots of a repeater. Furthermore, if two radios transmit at the same time on different slots, some of the radios scan to one slot, and some scan to the other slot. It is not possible to predict the distribution since all radios are scanning. Also note, that while scanning, the probability of missing a voice header and entering a call “late entry” increases, therefore missed audio may occur. Because of these drawbacks, it is highly recommended to break users into at least two unique groups and distribute them across slots, and only use this scanning strategy if completely necessary.

4.7.7.2

Minimize Location Periodic Update Rate

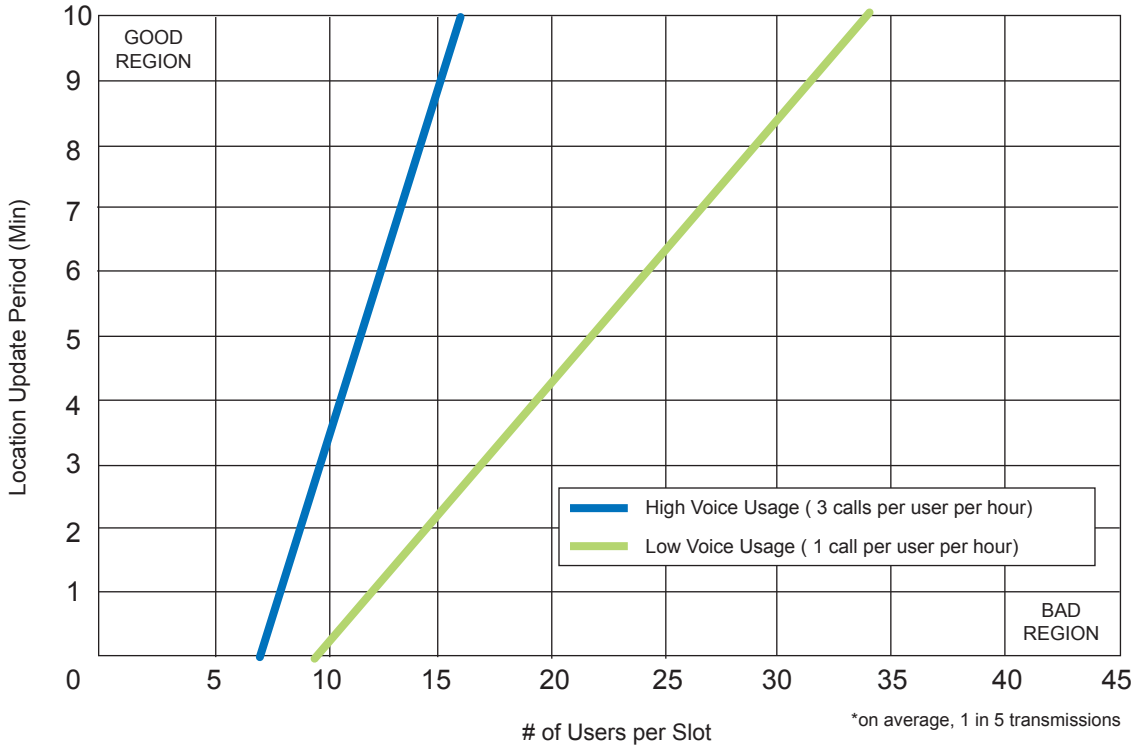
The high usage location profile defined assumes that every user on the channel has location capability and uses a one minute refresh rate. In actual fact, if every user actually has a one minute refresh rate, this increases the traffic loading tremendously. Users should be configured to use a 10 minute update, and to only increase individual radios to a one minute update rate during emergencies or special situations. Although each customer scenario may be different, knowing a user’s location every 10 minutes is usually considered sufficient. If a user reports an emergency, his location update rate can be increased by the location dispatcher for a short period of time. The minimum interval between updates (High Cadence setting) can be set as low as 10 seconds, but with the concerns mentioned above kept in mind.

In order to help visualize the impact of setting the Location Update Period between one minute and 10 minutes, Figure 149: Number of Users Versus Location Update Period on page 410 was created using the data presented in . The following assumes a specific desired user experience (approximately mid-way between good and fair). The graph was plotted using the intersection of the Low GPS (10 minute Cadence) and High GPS (one minute Cadence) lines for High Voice and Low Voice with the desired user experience design goal.

The chart provides a method to easily set the Location Update Period for a particular number of users on a channel, while keeping their voice usage in mind. The intersection between the number of users and the Location Update Period should always be above the line for the applicable voice usage. For example, if a channel has 10 users, and the users have been determined to be High Voice users (three calls per user per hour), then it is recommended that the Location Update Period be set to 3.5 minutes or higher (longer). Because it is very difficult to determine the true voice usage profile, the administrator/dealer needs to make a judgment call on whether the usage leans towards the High Voice Usage trend or the Low Voice Usage trend.

Although the impact is not substantial, it should be noted that using a high cadence location update rate lowers the overall battery life of the radio since transmits often.

Figure 149: Number of Users Versus Location Update Period



The value chosen for the location periodic update rate directly affects scan performance. Most users realize that a radio pauses scanning when transmitting voice, and then resumes scanning once the voice transmission is over. The more voice a user transmits, the less the radio is scanning, which means, its probability of missing traffic increases. This is also true when transmitting data. The more a radio transmits data, the less it is scanning, and therefore the higher the probability of missing traffic. Additionally, if the channel used to transmit the data is busy, it takes longer to deliver the message; therefore the radio's scanning will be further interrupted. This means that the higher the location periodic update rate is for a radio, its scan performance degrades. This should be kept in mind when using scan with a high cadence location period update. It is recommended that radios be configured to use a 10-minute update, and that scanning radios should NEVER use a value lower than two minutes.

4.7.7.3

Data Application Retry Attempts and Intervals

The interval a data application will retry to send a message and the number of retries it will send if the target does not respond is configurable in the external data applications like Location and Text Messaging. The following table shows the default values provided:

Table 82: Data Application Retry Attempts and Intervals

External Data Application	Number of Retries	Interval Time Period between Retries
Text Messaging	2	70 seconds
Location Application	3	30 seconds

It is recommended to not change the default values. If this value is lowered too low, messages may become unreliable when a user is on the system, but will free up some bandwidth if the user is not available.

Increasing too high until it is past the default will increase the load on a channel although it may increase the probability of delivering a message.

4.7.7.4
Optimize Data Application Outbound Message Rate

Text Message and Location Applications both set the outbound message rate. The outbound message rate is defined as the interval in-between subsequent messages sent by the applications to its connected Control Stations. It is important to note that the Application Server is connected to up to four channels, and is not aware of which channel is used to route a message. Therefore, it is reasonable that the outbound message rate setting is increased to a greater value than the default, if there is more than one channel on a system. The default value for the text message server is 14 messages per minute distributed uniformly. The default value for the Location Server is 20 messages per minute, distributed uniformly.

For example, if a system only has one data capable channel, and therefore only one Control Station, the default value of the Outbound Message Rate paces the messages appropriately to not overload the Control Station or add excessive load to the channel. If there is more than one channel (two to four channels), and the users are distributed fairly evenly over these channels, the Outbound Message Rate could be increased, since only a portion of the messages is going to any single channel. It is difficult to predict which channel users are registered on, and even harder to predict how many messages are sent to a particular user on a particular channel.

It is recommended that the outbound pacing rates remain as default, though special considerations for GPS Revert are discussed in GPS Revert and Loading on page 411. If they are increased, and the target radios are not evenly distributed over multiple channels, one channel may experience excess loading. The MOTOTRBO radio can buffer only up to 10 messages. If there is RF congestion on the system, the radio may encounter a situation where its message transmit buffer becomes full. This is due to the radio queuing up messages, because it cannot find an available slot to transmit data. The radio cannot process new messages from the application, once its buffer becomes full.

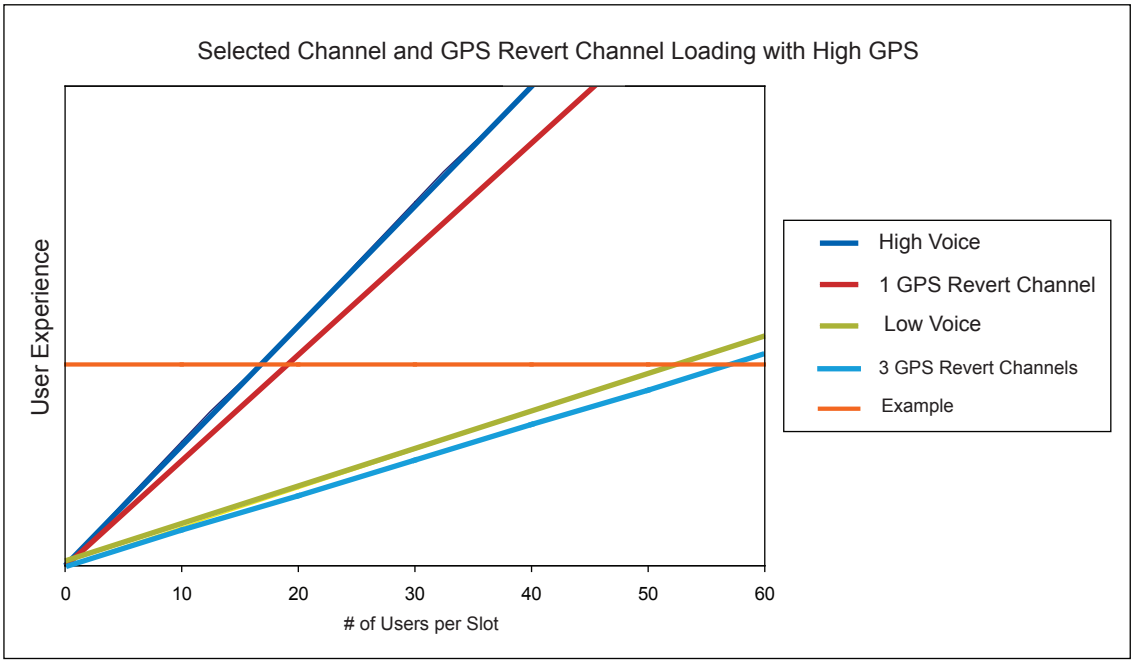
4.7.7.5
GPS Revert and Loading

The GPS Revert feature supports the transmission of voice, control and non-location update data transmissions on the Selected Channel, while off loading Location updates onto one or more GPS Revert Channels. A primary goal of the feature is to support location updates without degrading features on the Selected Channel. The ultimate performance of the system will depend upon at least two loading factors (1 and 2), while a third loading factor (3) needs to be considered if most radios are powered on in a relatively short period of time. These factors are listed below.

- The average number of transmissions on the Selected Channel (Voice, Text Messaging, and others).
- The average number of transmissions on a GPS Revert Channel.
- The peak number of transmissions on the Selected Channel to account for registration and periodic re-registration messaging.

The chart in Figure 150: Channel Loading with GPS Revert Channels on page 412 illustrates the Good to Fair user experience area, for voice traffic loading on the selected channel and GPS traffic loading on one or more GPS Revert Channels. Note that this only accounts for loading the first and second factors and assumes registration messaging is evenly spread throughout the day.

Figure 150: Channel Loading with GPS Revert Channels



It can be seen in Figure 150: Channel Loading with GPS Revert Channels on page 412 that the High Voice Selected Channel User Experience and the single GPS Revert Channel User Experience are fairly similar in terms of user experience versus number of users on a slot. In this example, for the desired User Experience (identified on the above chart as the red horizontal example line), the Selected Channel supports about 16 radios at a High Voice profile and the single GPS Revert Channel supports about 18 radios at a high GPS profile. For the High Voice profile, which is defined in Voice and Data Traffic Profile on page 400, 16 users would equate to a little less than 2 transmissions per minute. For a high GPS profile, which is also defined in Voice and Data Traffic Profile on page 400, 18 users would equate to 18 transmissions per minute.

It can also be seen in Figure 150: Channel Loading with GPS Revert Channels on page 412 that the Low Voice Selected Channel User Experience and the three GPS Revert Channel User Experience are fairly similar in terms of user experience versus number of users on a slot. In this example, for the desired User Experience, the Selected Channel supports about 51 radios at a Low Voice profile and the three GPS Revert Channels support about 57 radios at a high GPS profile. For the Low Voice profile, which is defined in Voice and Data Traffic Profile on page 400, 51 users would equate to a little less than two transmissions per minute. For a high GPS profile, which is also defined in Voice and Data Traffic Profile on page 400, 57 users would equate to 57 transmissions per minute, distributed over three channels.

In the previous examples, it can be seen that the voice rate and the GPS rate cannot always be considered as independent when designing a system. Though three GPS Revert Channels are able to support 57 high GPS profile users, the Selected Channel is unable to support 57 High Voice profile users. Therefore, when designing a system, both the Selected Channel loading and the GPS Revert Channel(s) loading must be thoroughly considered.

The following table provides guidance for determining the maximum number of radios supported on various numbers of GPS Revert Channels with one minute and two minutes update rates. It is important to note that maximum loading essentially keeps a repeater keyed up at all times. Update rates of less than one minute are not recommended in order minimize the impact on the Selected Channel features (voice, control and/or data). Care must also be taken to analyze if the Selected Channel can accommodate the anticipated voice traffic for a large number of subscribers.

Table 83: GPS Revert Channels

Radio Type	1 GPS Revert Channel	2 GPS Revert Channels	3 GPS Revert Channels
Radios supported at 1 minute update rate	20	40	60
Radios supported at 2 minute update rate	40	80	120

When GPS CSBK data is enabled, twice the number of radios can be supported with a similar GPS success rate. However, the home channel may not be able to support more radios.

Though GPS Revert Channels can significantly increase the number of radios providing location updates, it is important to remember that when powered up, an radio needs to register with both Presence and Location Applications before it can send location updates. If a large number of radios happen to be powered up in a relatively short period of time, the Selected Channel may become overwhelmed with registration traffic and the system's voice handling capacity will be impacted. Therefore, if this situation must occur, the following should be kept in mind.

- Keep voice traffic on the Selected Channel to a minimum. This causes the registration messages to be queued in the radio and the control station.
- As a rule of thumb, expect about three successful registrations per minute. Therefore, a fleet of 60 radios could require 20 minutes to successfully register. In order to minimize registration traffic, the radios can be gradually powered on at a rate of three per minute during the estimated time frame.

Generally, a GPS Revert Channel can support more radios when a lower GPS update rate (that is larger update period) is being used. On the contrary, the channel supports fewer radios if a higher update rate (that is smaller update period), is being used. The following chart illustrates the relationship between the location update period and number of radios assigned to a particular GPS Revert Channel. When the CSBK data feature is enabled, twice the number of radios can be supported. The blue line in Figure 151: Minimum Location Update Period versus Number of Subscribers on page 414 illustrates this case.

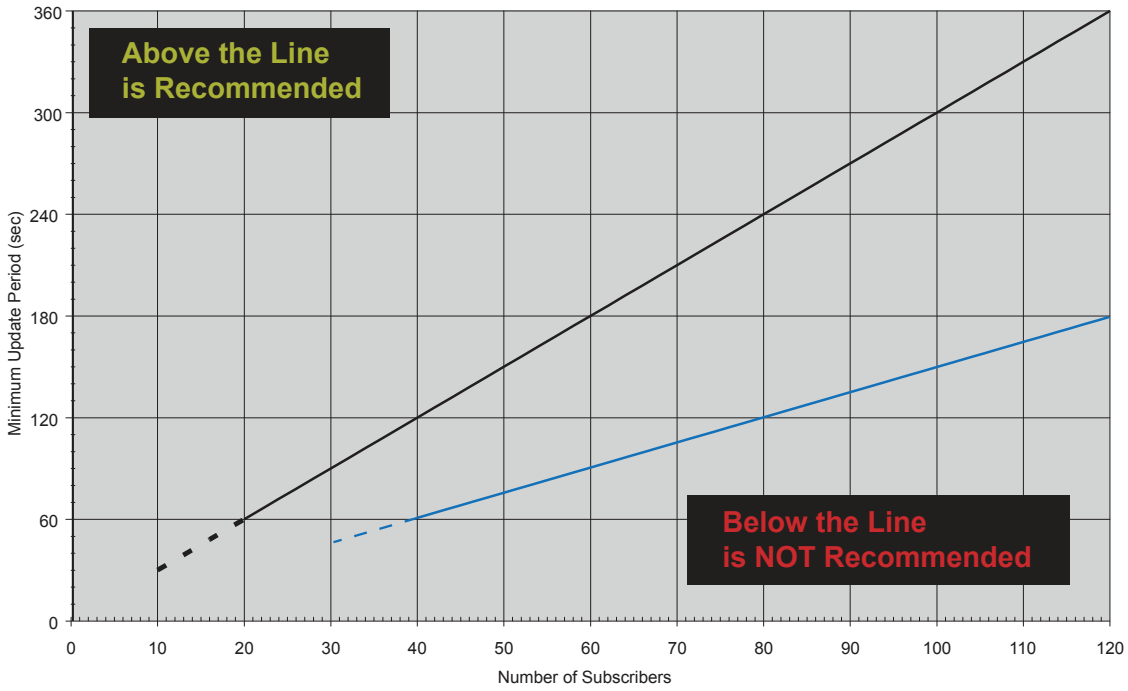
Example: No more than 20 radios should be assigned to a particular GPS Revert Channel, if an update period of 60 seconds (that is 60 updates per hour) is desired.

Example: If 120 radios are assigned to use a GPS Revert Channel, the minimum recommended update period is 360 seconds (that is 10 updates per hour).

Hence, some flexibility is provided as to whether a large number of radios with a slow update rate, or a small number of radios with a fast update rate is used on a GPS Revert Channel. Alternatively, depending on whether having a large number of radios assigned to a GPS Revert Channel or having a fast update rate is more desirable for a particular system, the system can be provisioned to accommodate either scenario.

A higher GPS update rate can impact the service (voice, control and/or data) presented on the channel selected by the radio user because the radio spends a longer time transmitting its GPS location on the GPS Revert Channel. The recommended rate is to not exceed 60 GPS updates per hour per radio (that is 60-second GPS update period).

Figure 151: Minimum Location Update Period versus Number of Subscribers



4.7.7.6

Enhanced GPS Revert – Loading and Reliability

System	Description
IPSC IP Site Connect	This section is applicable to MOTOTRBO IP Site Connect Configurations.
CPSS Capacity Plus	This section is applicable to MOTOTRBO Capacity Plus Configurations.
CPMS Capacity Plus Multi Site	This section is applicable to MOTOTRBO Capacity Plus Multi Site Configurations.

The number of subscribers supported on an Enhanced GPS slot is a function of the window size, (derived from the size of the location data), and the update rate. Additionally, the success rate of the location updates is also a function of the call duration on the selected/primary channel and the repeater loading. The following figures illustrates the relationship between these variables.

The curves in Figure 152: 1-Minute Update Rate with a 10-second Call per Minute at 75% Loading on page 415 illustrate the average location update success rate against the number of subscribers for a 1-minute update rate per subscriber, a 10-second call for the talkgroup per minute and 75% repeater loading ("loading" refers to percentage of periodic window reservation). If there are no talkgroup calls, the subscribers would update 100% of the time as long as the number of subscribers are less than or equal to the maximum number of allocated reserved windows. (The maximum allocated reserved windows is the repeater loading.)

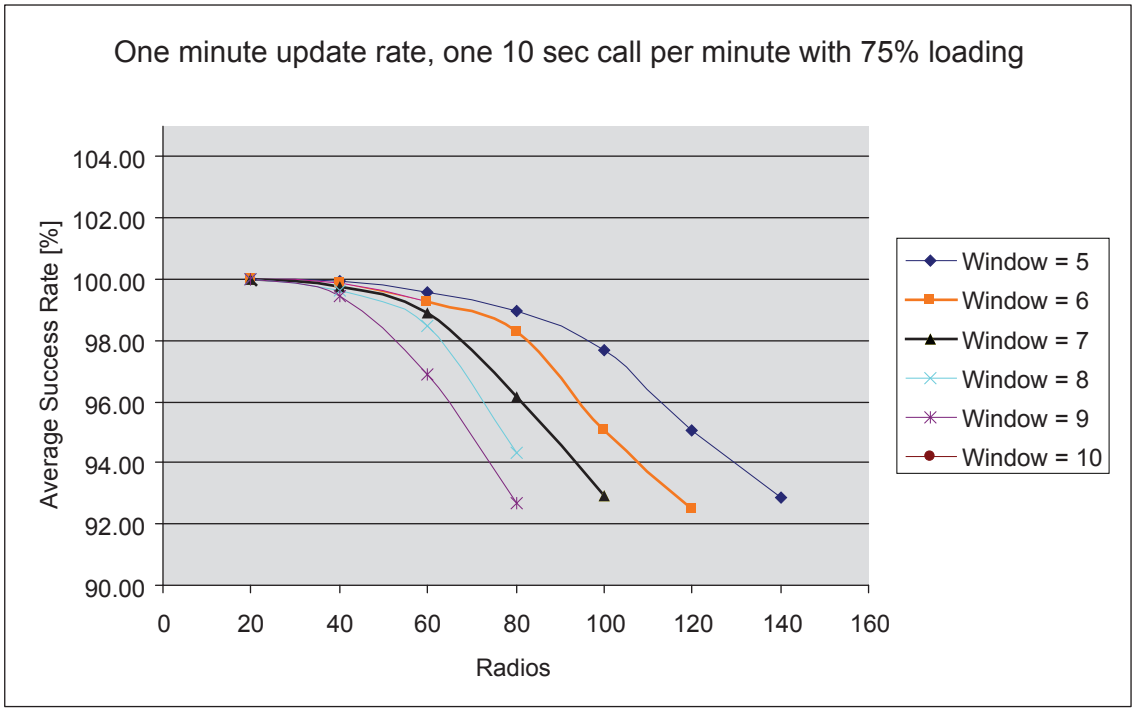
However, voice calls keeps a subscriber from sending location updates on its reserved slot. Hence the subscriber makes a request to send in the data on the unreserved windows after the call. Therefore in Figure 152: 1-Minute Update Rate with a 10-second Call per Minute at 75% Loading on page 415, it is noticeable that larger talkgroups (more subscribers) decreases the average success rate. This is because there are not enough unreserved windows to support all the missed reserved data transmissions.

The CSBK data feature improves system capacity. The following figures describe the average location update Figure 152: 1-Minute Update Rate with a 10-second Call per Minute at 75% Loading on page 415 rate against the number of subscribers.

The curve in Figure 152: 1-Minute Update Rate with a 10-second Call per Minute at 75% Loading on page 415 illustrates the average location update success rate against the number of subscribers for a 1-minute update rate per subscriber, a 10-second call for the talkgroup per minute and 75% repeater loading when the CSBK data feature is enabled for GPS data.

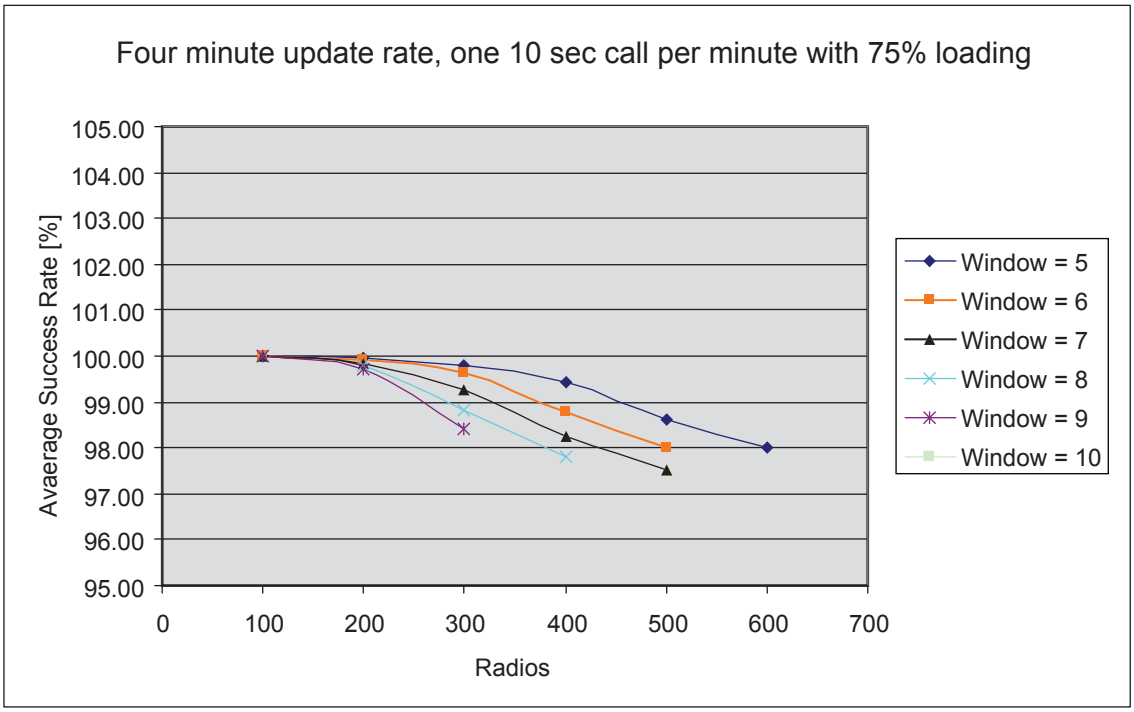
The curve in Figure 152: 1-Minute Update Rate with a 10-second Call per Minute at 75% Loading on page 415 illustrates the average location update success rate against the number of subscribers for a 1-minute update rate per subscriber, a 20-second call for the talkgroup per minute and 75% repeater loading when the CSBK data feature is enabled for GPS data.

Figure 152: 1-Minute Update Rate with a 10-second Call per Minute at 75% Loading



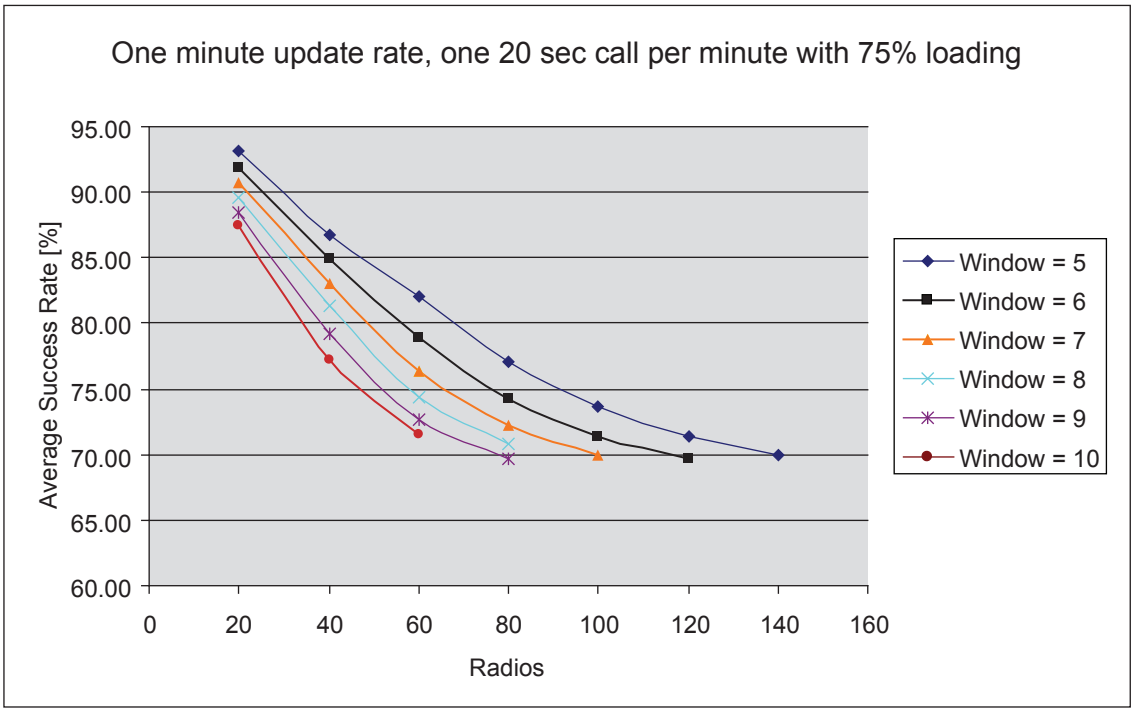
In Figure 153: 4-Minute Update Rate with a 10-second Call per Minute at 75% Loading on page 416, the update rate is increased to 4 minutes. A quick evaluation of the situation might cause the assumption that increasing the update rate by 4 times would lead to the same average success rate with 4 times as many subscribers. However, the success rate is much higher than expected for 4 times the number of subscribers. Such an improvement is triggered because the number of subscribers that miss their reserved window at any one time is decreased. This leads to an overall increase in success rate.

Figure 153: 4-Minute Update Rate with a 10-second Call per Minute at 75% Loading



The curves in Figure 154: 1-Minute Update Rate with a 20-second Call per Minute at 75% Loading on page 416 illustrates the average location update success rate against the number of subscribers for a 1-minute update rate per subscriber, a 20-second call for the talkgroup per minute and 75% repeater loading. In this situation, the call duration is very long (an update rate of 0.3) and many subscribers miss their assigned update window. As the number of subscribers approaches the maximum number of reserved windows, a large number of retries can be unsuccessful and the average success rate drops.

Figure 154: 1-Minute Update Rate with a 20-second Call per Minute at 75% Loading



In Figure 155: 1-Minute Update Rate with a 20-second Call per Minute at 45% Loading on page 417, the repeater loading is decreased to 45%. A comparison to Figure 154: 1-Minute Update Rate with a 20-second Call per Minute at 75% Loading on page 416 shows that the average success rate improves dramatically because now there is a large number of unreserved slots to accommodate subscribers that miss their reserved window. Note that the 75% loading case carry more updates than the 45% loading case, hence the success rate has improved.

Figure 155: 1-Minute Update Rate with a 20-second Call per Minute at 45% Loading

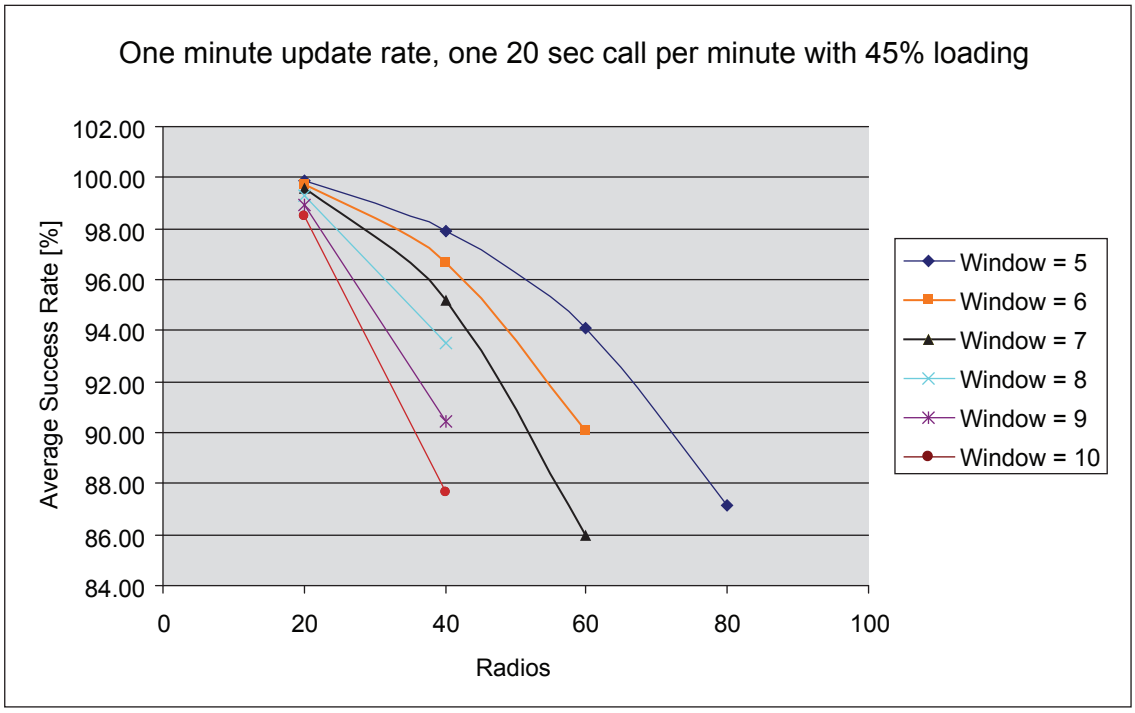
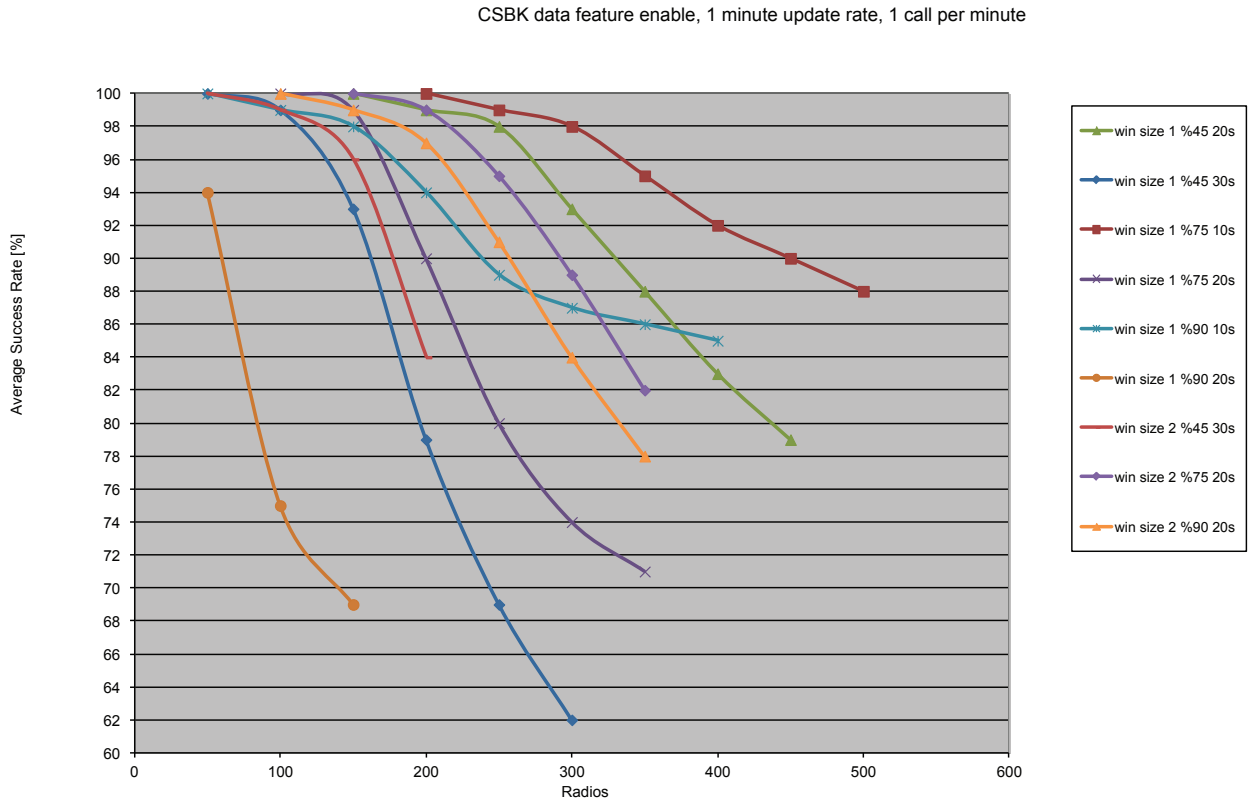


Figure 156: 1-Minute Update Rate with Different Window Sizes, Loading and Call Duration on page 418 describes the location update success rate against the number of subscribers when the CSBK data feature is enabled. The data in the figure is obtained from simulation, that should only be used for initial system planning. Actual testing is still required to adjust the group call size, periodic GPS loading and update rate. Keep in mind the following notes:

- Window size 1 cannot support dedicated requests. The radios will request a one-time window to send the GPS update missed periodic window. A big group size will cause many radios to miss the periodic window after a group voice call, while a 90% periodic loading cannot reserve many free windows. Therefore a big group size cannot be supported by window size 1 with 90% loading.
- With other conditions being the same, window size 2 can support a bigger group size than window size 1. It is more apparent when the periodic GPS loading is higher.
- With other conditions being the same, window size 1 can support a bigger group size than window sizes 5 to 10 when the periodic GPS loading is 45 or 60.

Figure 156: 1-Minute Update Rate with Different Window Sizes, Loading and Call Duration



4.7.8

Load Optimization (for Capacity Plus Single Site and Capacity Plus Multi Site)

System	Description
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	Section Load Optimization (for Capacity Plus Single Site and Capacity Plus Multi Site) on page 418 and its subsections explain Loading Optimization in Capacity Plus Single Site and Capacity Plus Multi Site.

4.7.8.1

Preference for Using a Frequency

The Capacity Plus Single Site and Capacity Plus Multi Site systems are designed to operate efficiently in a shared channel environment. The term “shared channel environment” is typically used when more than one system uses the same frequency for communication within the same coverage area. For system owners having licenses for shared use of frequencies, it is recommended to set a preference level for the use of a frequency. A repeater whose frequencies have lower interference from other system(s) should be given higher preference level over the repeater whose frequencies have higher interference. Repeaters with the same amount of interference should have the same preference level. For trunking operation, a Capacity Plus

Single Site/Capacity Plus Multi Site system always prefers to use a repeater of a higher preference level over a repeater of lower preference level.

For system owners having a mix of shared frequency channel licenses and exclusive frequency licenses, the repeaters with exclusive frequency licenses should have a higher preference level than the repeaters with shared frequency licenses.

4.7.8.2
Improving Channel Capacity by Adjusting Hang Times

MOTOTRBO supports message trunking by keeping a channel reserved for the duration of hang time after a transmitting radio has unkeyed the microphone. During the hang time, only the members of the ongoing call can start a transmission. The advantage of the message trunking is that it provides guaranteed access to the channel for the duration of a call. The disadvantage of the message trunking is that the channel remains unused during the hang times. To improve channel utilization, a customer may choose to reduce the call hang time in the repeater. Experienced radio users respond quickly and therefore require a shorter hang time.

Capacity Plus Single Site/Capacity Plus Multi Site allows a customer to program a near zero call hang time in repeaters. By programming a zero call hang time, MOTOTRBO acts as if the channel is allocated for only one transmission and in this case, MOTOTRBO supports Transmission Trunking.

However, there are some trade-offs in reducing call hang time. The channel will no longer be reserved for a group in the system. Thus, every time a group member of the same call presses PTT to initiate a call, the call will land on a different frequency channel. In some cases, some of the Group Call participants may switch to other high-priority Group Calls. While in other cases, the system may become busy with other calls and no channels are available to initiate the call.

Customers may choose to reduce call hang time from the default value rather than setting it to zero based upon channel usage. If there are more members in a group, and if members of the group are replying instantly to the Group Call, then lowering call hang time from the default value may improve overall call throughput. However, if the group members are not replying instantly to the communication and the channel still needs to be reserved, then call hang time should be increased. Call throughput reduces by increasing call hang time and vice versa.

Since all repeaters in the system needs to exhibit the same behavior, it is recommended that the same call hang time is programmed in all trunked repeaters.

4.7.8.3
Call Priority

A radio joins its most preferred call in the following conditions:

- The call that the radio was participating in, ends,
- A radio powers on, or returns from a fade when all Trunked Channels are not busy.

The preference list for a radio (in decreasing order) is an Emergency Call of interest, All Call, the radio’s transmit group, and the radio’s receive group list. The preference of groups in a radio’s receive group list are displayed in decreasing order.

A radio enforces the call priority only when it enters a call. Upon joining the call, the radio searches for only All Calls and Emergency Calls whereby the emergency group is in either the transmit group, or the receive group list.

4.7.8.4
Call Initiation

System	Description
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	In Capacity Plus/Capacity Plus Multi Site modes, while a radio is listening to a Group Call, a radio user can initiate a non data call (for example, using the menu). The radio moves to the Rest Channel and starts the requested call if there is an idle channel. If all channels are busy, the radio informs the user (by generating a busy signal) that the call cannot be initiated and the radio stays on the traffic channel.

4.8
Multiple Digital Repeaters in Standalone Mode

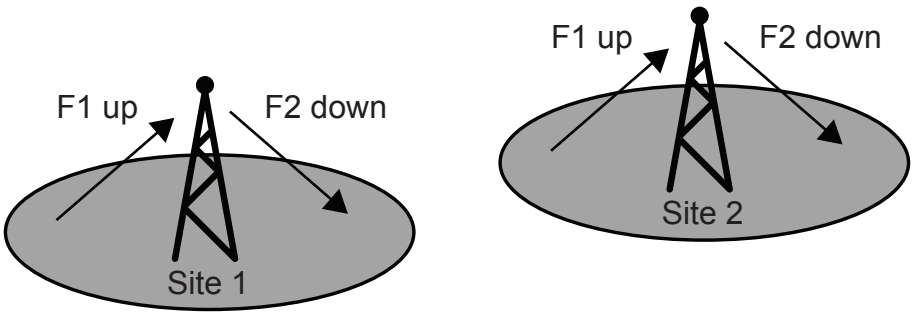
Multiple repeaters may be required to provide sufficient RF coverage. Large geographical regions and areas with large natural boundaries (mountains) are two examples. Also, regions with a large number of subscribers may need additional repeaters to relieve RF congestion.

The digital mode of operation of the MOTOTRBO repeater provides new capabilities to resolve common problems associated with deploying multiple repeaters in a system. The techniques described in the sections below can also be used to resolve problems associated with interfering RF signals from adjacent radio systems.

4.8.1
Overlapping Coverage Area

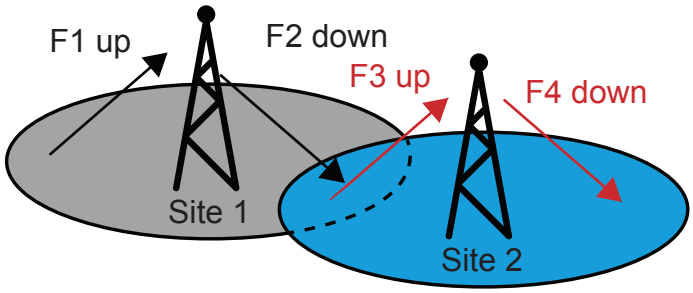
As with radio systems, when digital radio systems are separated by frequency or distance there are no negative interactions between the systems which need to be addressed. Figure 157: Multiple Repeaters on page 420 shows two systems which operate on a common set of frequencies but are physically separated so that there are no interactions between the systems.

Figure 157: Multiple Repeaters



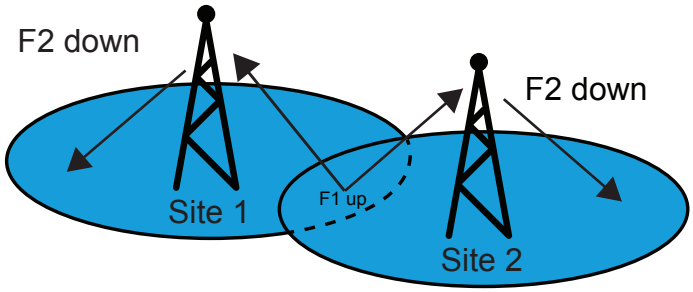
Similarly, Figure 158: Multiple Repeaters with Overlap on page 421 shows two systems which overlap in space but operate on a difference set of frequencies so that there are no negative interactions.

Figure 158: Multiple Repeaters with Overlap



Issues arise, however, when repeaters operate on common frequencies and have overlapping regions. Figure 159: Multiple Repeaters with Overlap and Common Frequencies on page 421 shows that when a radio transmits in a region of overlap, repeaters from both systems retransmit the received signal. Analog radio systems often use PL/DPL to resolve these types of problems. With the MOTOTRBO repeaters operating in digital mode, this issue can be resolved by assigning a unique color code to each repeater and programming the associated radios, using CPS, with the matching color code.

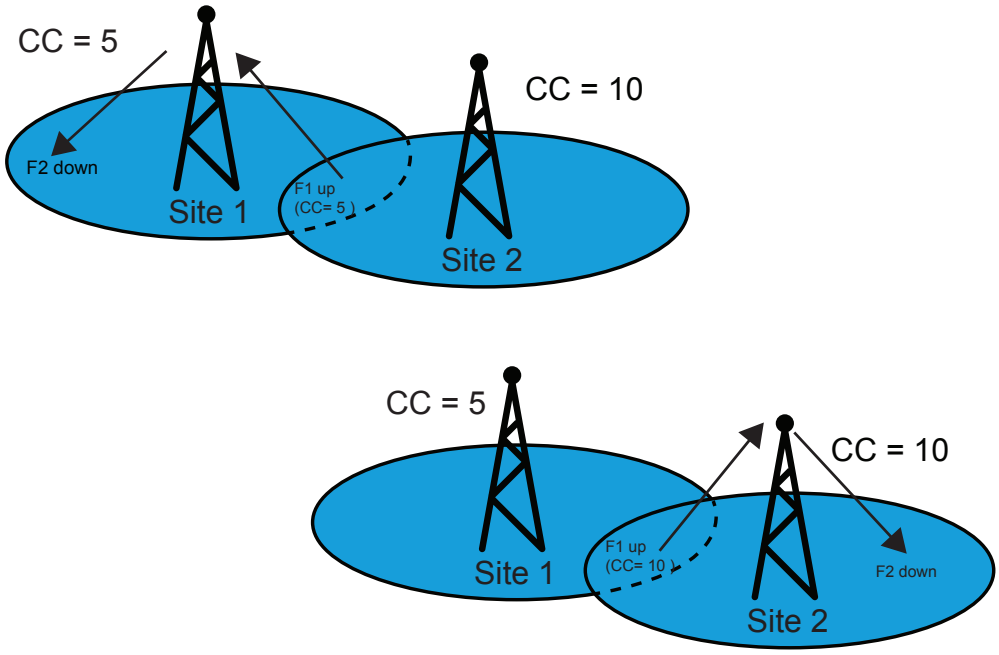
Figure 159: Multiple Repeaters with Overlap and Common Frequencies



4.8.2
Color Codes in a Digital System

Color codes (or “CC” in the images) are defined by the Digital Mobile Radio (DMR) standard and can be used to separate two or more MOTOTRBO digital radio systems which operate on common frequencies. Figure 160: Multiple Digital Repeaters with Unique Color Codes on page 422 shows two MOTOTRBO radio systems which operate on common frequencies but have uniquely defined color codes.

Figure 160: Multiple Digital Repeaters with Unique Color Codes



Color codes are assigned as channel attributes on the radios, allowing a single radio to communicate with multiple sites each having a uniquely defined color code.

4.8.3
Additional Considerations for Color Codes

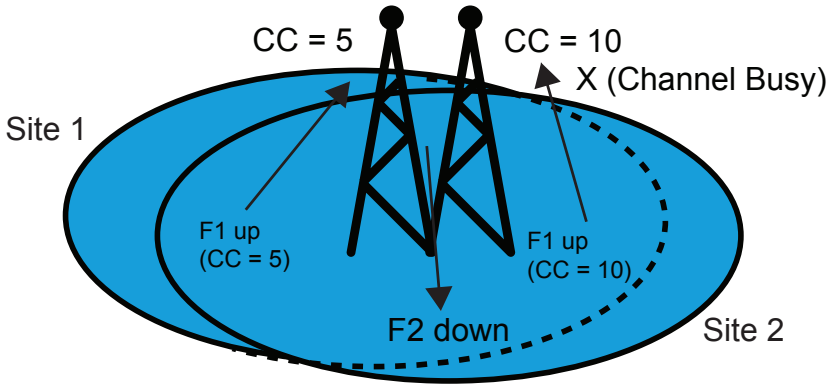
The total number of available color codes per frequency is 16. From a radio user's perspective the color code is similar in nature to a Group ID. However, it should not be used for this purpose. Just as Groups are intended to separate users into groups, the color code is intended to uniquely identify systems or channels which operate on common frequencies.

Multiple repeaters operating on common frequencies with large areas of overlap, as shown in Figure 161: Color Code with Site Congestion on page 423, could be configured with unique color codes. This would allow both repeaters to operate with some degree of independence. However, the radio users should expect to see an increase in "Channel Busy" indications since transmissions from both repeaters will be detected by users of both systems. In other words, the RF congestion for this region would be the sum of transmissions from both repeaters. It should be noted that under all circumstances the users with the correct corresponding color codes receive only the transmission intended for them.

When two sites with the same frequency but different color codes overlap, it is important to set the subscriber's Admit Criteria appropriately. It is recommended that the subscribers are provisioned with Admit Criteria set to Channel Free to ensure subscriber's from a Site is polite when another on the overlapping Site is transmitting, and also polite to any other transmission on the frequency. If configured to Color Code Free, the subscribers are only polite to their own color code, and will wake up their repeater even if the other repeater is currently transmitting. When there is a large overlap between adjacent sites, this usually causes major interference and results in both repeater signals being unusable in the overlapping areas. When configured to Always, the subscribers are never polite, even to their own color code. Again, this results in both repeaters being awake and transmitting at the same time which causes interference in areas of overlap.

If this configuration is necessary, it is recommended to minimize the areas of overlap as much as possible and to use an Admit Criteria of Color Code Free. Remember that these two repeaters will be sharing bandwidth and should be loaded appropriately.

Figure 161: Color Code with Site Congestion



4.9

Multiple Digital Repeaters in IP Site Connect Mode

System	Description
IPSC IP Site Connect	Section Multiple Digital Repeaters in IP Site Connect Mode on page 423 and its subsections explain Multi Digital Repeaters in IP Site Connect.

The main problem with the standalone configuration of multiple digital repeaters is that a radio at a site can participate only in the calls that originate at that site. The IP Site Connect configuration removes this restriction and allows a radio to participate in a call originating at any site. In IP Site Connect configuration, repeaters communicate among themselves using a back-end wire line network. A call originating at a repeater is transmitted by all the repeaters in the IP Site Connect system. Since all repeaters participate in a call, it is necessary that all the repeaters have the same call related parameters (for example, Call Hang Times, System Inactivity Time, Time Out Time).

4.9.1

System Capacity in IP Site Connect Mode

In IP Site Connect configuration, MOTOTRBO supports a maximum of 15 IP Site Connect devices, where IP Site Connect devices include a maximum of five host PCs of RDAC-IP applications, disabled repeaters, enabled repeaters in mode, and enabled repeaters in digital mode (both slots in wide area mode, one slot in wide area mode and one in local mode, and both slots in local mode).

A channel in IP Site Connect configuration supports the same number of radios supported by a single site configuration.

NOTE: An IP Site Connect configuration increases the coverage area and not the call capacity of a single site configuration.

4.9.2

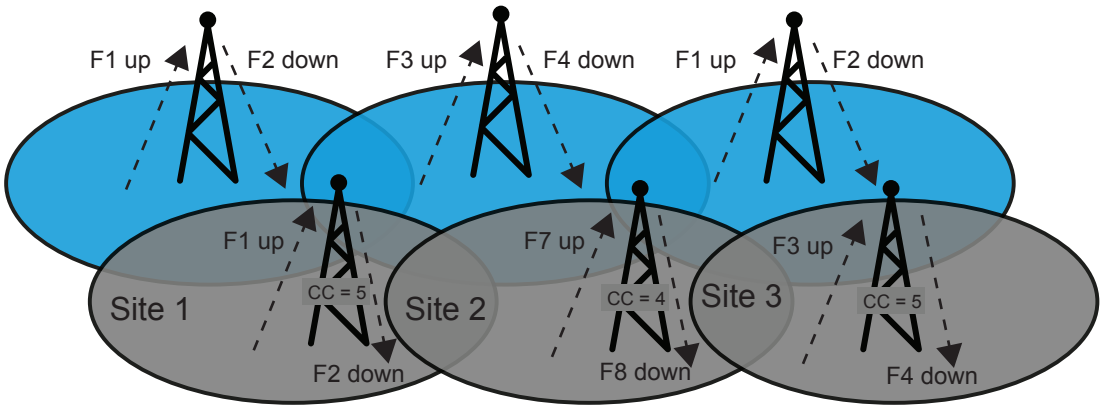
Frequencies and Color Code Considerations

The following figure shows an example of two IP Site Connect systems with overlapping coverage areas.

The frequencies and color code of repeaters should follow the following rules:

- The geographically adjacent repeaters of an IP Site Connect system should use different frequencies. Their color code can be either same or different.
- If the frequencies of the geographically adjacent repeaters of two IP Site Connect systems are the same, then their color codes should be different. It is not advisable to keep the same frequencies because in areas of overlap, there will be destructive interference. Note that an IP Site Connect configuration does not support simulcast.
- If the frequencies of non-adjacent repeaters of an IP Site Connect system are the same, then their color codes should be different. It is not advisable to keep the same frequencies and color code because a roaming radio is not able to distinguish between them, and may use the wrong GPS Revert Channels or emergency system.
- A system may be sharing the channels with other systems over multiple sites. It is possible that two systems (named here as Sys1 and Sys2) may be using the same (frequencies, color code) pair at two different sites (say, Site1 and Site2). During automatic site search (Passive Site Search), a Sys1's radio at Site2 finds Sys2's repeater and stays on that channel. This is not a desirable situation. A way to avoid this situation is to ensure that all the (frequencies, color code) pairs of all the overlapping systems are unique.

Figure 162: Example of Two IP Site Connect Systems with Overlapping Coverage Areas



4.9.3

Considerations for the Back-End Network in IP Site Connect Mode

The back-end network can be a dedicated network or an Internet. ISPs provide a range of technologies such as dial-up, DSL (typically ADSL), cable modem, broadband wireless access, Canopy, Satellite Internet access, and more. In some cases, dedicated links or networks can be effectively used or deployed, removing the monthly fees associated with public networks. The back-end network cannot be based on a dial-up connection (due to small bandwidth) or Satellite Internet access (due to large delay).

A repeater has three network interfaces: Ethernet, USB, and Over-the-Air. A repeater uses its Ethernet port to communicate with other network devices using IPv4/UDP. Since UDP does not support confirmation, the IP Site Connect system provides its own acknowledgment and retries mechanism for critical activities.

The Ethernet port is not the default IP gateway of the repeater. An IP datagram that arrives from USB or Over-the-Air is not automatically routed to the Ethernet port.

It is not necessary to assign a static IPv4 address to the IP Site Connect devices (except for the Master). The IPv4 address of an IP Site Connect device can be dynamic. In this case, the IPv4 address is allocated by a DHCP server. The dynamic nature of the IPv4 address implies that the address may change every time it powers on or even periodically (every few hours) while the IP Site Connect device is on. The DHCP option needs to be selected in the repeater CPS to allow dynamic address assignment for a repeater. It is recommended to set a long lease time in the DHCP server configuration. Note that a change in the IPv4 address of an IP Site Connect device causes a short disruption of service. For static IPv4 address assignment, the DHCP option should be unselected and then the CPS user must provide the static IPv4 address, gateway's IPv4 address, and network mask.

An IP Site Connect system uses a procedure called "Link Management" to keep an IP Site Connect device aware of the presence, current IPv4 addresses, and UDP ports of other IP Site Connect devices. The Link Management requires only the Master repeater to act as a broker of IPv4/UDP addresses. The Master IPv4/UDP address is configured into all the IP Site Connect devices. For this reason, the **Master IP** must be a static IPv4 address or FQDN (Fully Qualified Domain Name) resolved with a DNS server. Anytime the IPv4 address for a Master repeater changes, then the DNS server must be updated with the new IPv4 address. It is the job of the entity assigning the IPv4 address to the Master repeater to also update the DNS server with the updated IPv4 address to minimize any interruptions in connectivity to Master.

The IP Site Connect devices will determine the current IPv4 address of the Master repeater by requesting from the DNS server the IPv4 address using its FQDN. When the Master stops responding to requests from an IP Site Connect device, then the device will request from the DNS server the current Master IPv4 address. If the address has changed, then it will acquire the new address and begin using the new IPv4 address provided by the DNS server.

NOTE: The DNS feature is only available on SLR Series Repeaters.

The Master's IPv4/UDP address refers to its address as seen from the back-end network. Note that a firewall/NAT may translate the address in the customer network into another address in the back-end network.

An IP Site Connect device registers its IPv4/UDP address during power on and upon a change in its IPv4/UDP address with the Master. The Master notifies all the IP Site Connect devices whenever the IPv4/UDP address of an IP Site Connect device changes. An IP Site Connect device maintains a table of the latest IPv4/UDP addresses of other IP Site Connect devices and it uses the table to send a message to another IP Site Connect device.

The IP Site Connect devices may be behind firewalls. For successful communication between two IP Site Connect devices (say R1 and R2), the firewall of R1 must be open for messages from R2 and vice versa. Since the IPv4/UDP address of an IP Site Connect device can be dynamic, it could be not possible to manually configure the firewalls. The Link Management procedure overcomes this problem by periodically, for example, setting the Keep FW Open Time to every 6 seconds, sending a dummy message from R1 to R2, and vice versa. On a receipt of an outbound message (say, from R1 to R2), the R1's firewall keeps itself open for a short duration of approximately 20 seconds for an inbound message from R2. An IP Site Connect device (say, R1) sends the dummy message to another IP Site Connect device (say, R2) only if R1 has not sent any message to R2 in the last Keep FW Open Time. The value of Keep FW Open Time is customer-programmable and should be kept less than the duration for which the firewall remains open for inbound messages. Exchange of dummy messages between two IP Site Connect devices also acts as a "Keep Alive" message. They are required, even if there is no firewall or the firewall is configured to keep itself open for any message transmitted to the IP Site Connect device.

4.9.3.1

Automatic Reconfiguration

An IP Site Connect system automatically discovers the presence of a new IP Site Connect device. The new IP Site Connect device is configured with the IPv4/UDP address of the Master. On power-on, the new IP Site Connect device informs its IPv4/UDP address to the Master and the Master informs all the other IP Site Connect devices about the presence of a new IP Site Connect device. This allows adding an IP Site Connect device to a live IP Site Connect system. This simplifies the installation/addition of an IP Site Connect device as there is no need to take the system down and configure other IP Site Connect devices with the IPv4/UDP address of the new IP Site Connect device.

The periodic link management messages between an IP Site Connect device and the Master also act as “keep alive” messages. In absence of messages from an IP Site Connect device for one minute, the Master concludes that either the IP Site Connect device has failed or the network in-between and the Master informs all the other IP Site Connect devices about the absence of the IP Site Connect device. An IP Site Connect device also maintains periodic link management messages with every other IP Site Connect device. In absence of messages from another IP Site Connect device for one minute, the IP Site Connect device concludes that either the other IP Site Connect device has failed or the failure is within the network in between. Thus, the link management messages allow an IP Site Connect system to reconfigure itself on failure of one or more IP Site Connect devices and the system continues to provide services with the available IP Site Connect devices. In case of network failure, it is possible that an IP Site Connect system becomes multiple IP Site Connect systems, where each system has a subset of original set of IP Site Connect devices. All the new systems continue to provide the services that are possible with their subset of IP Site Connect devices. Note that there will be only one system that has the Master. When the back-end network recovers, the multiple systems automatically become one system. When an IP Site Connect system has only one repeater, then both the slots of the repeater repeat only locally (that is Over-The-Air) as per the MOTOTRBO Single Site specifications.

A repeater operates in multiple modes such as disabled, locked, knocked down, enabled and digital with voice/data or control services, and single or multiple site operation for each slot. The repeater informs the Master whenever its mode of operation changes and the Master informs to all the other IP Site Connect devices. This allows the IP Site Connect system to adapt its operation when the mode changes. Note that only an enabled and digital repeaters (with a channel enabled for multiple site operation) participate in voice/data/control communication across multiple sites.

A disadvantage of link Management is that the Master becomes a single point of failure. But the consequence of failure of the Master is limited. The IP Site Connect system continues to function except that it is not possible to add an IP Site Connect device into the system. If an IP Site Connect device powers on, while the Master is in failed state, then it will not be able to join the IP Site Connect system. On failure of the Master, it is possible to switch a redundant IP Site Connect device to act as an Master. The static IPv4 address and the UDP port number of the redundant IP Site Connect device should be same as that of the failed Master; otherwise all the IP Site Connect devices will require to be reconfigured with the IPv4 address and the UDP port number of the new Master.

To avoid the issue of needing to have the same static IPv4 address configured on both the primary and redundant Master repeaters, all of the IP Site Connect devices can be configured to use instead of IPv4 address an FQDN (Fully Qualified Domain Name) DNS address of the Master resolved with a DNS server. The primary and redundant Master repeaters can still be configured with static IPv4 addresses, but they could be unique when an FQDN DNS address is used. If the primary Master fails, then the DNS Server could be updated such that the FQDN DNS address configured into all of the IP Site Connect devices now maps to the IPv4 address of the redundant Master repeater. To minimize any downtime, the DNS Server should be updated immediately with the IPv4 address of the redundant Master upon detection that the primary Master has failed.

NOTE: The DNS feature is only available on SLR Series Repeaters.

4.9.3.2

Back-End Network Design in IP Site Connect Mode

To create a proper back-end network design, it is important to know its characteristics. This section explains four issues dealt within the back-end network.

4.9.3.2.1

Delay/Latency in IP Site Connect Mode

Back-end network delay or latency is characterized as the amount of time it takes for a voice to leave the source repeater and reach the destination repeater. Three types of delay are inherent in the back-end networks:

- propagation delay
- serialization delay
- handling delay

Propagation delay is caused by the distance a signal must travel via light in fiber or as electrical impulses in copper-based networks. A fiber network stretching halfway around the world (13,000 miles) induces a one-way delay of about 70 milliseconds.

Serialization delay is the amount of time it takes the source repeater to actually place a packet byte by byte onto the back-end network interface. Generally, the effect of serialization delay on total delay is relatively minimal but since the IPSC system sends a voice packet one-by-one to all the repeaters, the serialization delay for the last destination repeater is (# of repeaters - 1) times the serialization delay for the first destination repeater.

Handling delay defines many different types of delay caused by the devices (for example, secure routers) that forward the packet through the back-end network. A significant component of the handling delay is the queuing delay, which occurs when more packets are sent out to a network device than the device can handle at a given interval.

The CPS allows setting the **Total Delay** (that is the sum of propagation delay, serialization delay, and handling delay) to be **High** (90 ms) or **Normal** (60 ms) in both the repeaters and the radios. Note that radios also support higher values (500 ms) of total delay, which should not be used in the case of a IPSC system. The default is **Normal**. This is used to derive values for other parameters such as **Arbitration Interval** and **Call Hang Times** in repeaters and **Ack Wait** times in radios. For the proper functioning of a IPSC system, all the repeaters and radios should have the same delay setting.

It is recommended that propagation and handling delays between repeaters should be measured (for example, by “pinging”) between all pairs of repeaters.

The total delay is equal to the maximum of the measured values + (# of repeaters - 1) * (1/2 + 1000/BW in kbps) ms, where the BW is the available bandwidth of the back-end network.

If the total delay is less than 60 ms then the setting should be **Normal**. If the total delay is more than 60 ms but less than 90 ms then the setting should be **High**. The IPSC system will not work satisfactorily, with occasional failure of arbitration, hang time and data link layer acknowledgments, for a back-end network having a total delay of more than 90ms. The disadvantage of the setting at 90ms is that there is an increase in audio throughput delay.

4.9.3.2.2

Jitter

Jitter is the variation of packet inter-arrival time. The source repeater is expected to transmit voice packets at a regular interval (that is every 60 ms for one channel). These voice packets can be delayed throughout the back-end network and may not arrive at that same regular interval at the destination repeater. The difference between when the packet is expected and when it is actually received is called Jitter.

To overcome the effect of jitter, the CPMS system employs a **Jitter Buffer** of fixed 60 milliseconds. If a packet does not arrive at a destination repeater within the 60 ms after the expected time then the repeater assumes the packet is lost, replays a special erasure packet, and discards the late arriving packet. Because a packet loss affects only 60 ms of speech, the average listener does not notice the difference in voice quality. Thus, a jitter of more than 60 ms degrades the audio quality.

4.9.3.2.3
Packet Loss

Packet loss in IP-based networks is both common and expected. To transport voice bursts in timely manner, IP Site Connect system cannot use reliable transport mechanisms (that is confirmed packets) and therefore while designing and selecting the back-end network it is necessary to keep packet loss to a minimum. The IP Site Connect system responds to periodic packet loss by replaying either a special packet (in the case of voice) or the last received packet (in the case of data). In the case of voice, the ongoing call ends if six consecutive packets do not arrive within 60 ms of their expected arrival time. In the case of data, the repeater waits for the expected number of packets (as per the data header) before ending the call.

4.9.3.2.4
Back-End Network Bandwidth Considerations

Bandwidth is the amount of data transferred to and from a network device, often referred to as the bit rate. Bandwidth is measured in bits per second or kilo-bits per second (kbps). When designing a Capacity Plus Multi Site system, it is important to understand the needs of each CPMS device so that the appropriately rated network connection for each site can be chosen.

If a customer has high-speed network connections between sites, these calculations may not be as important, but if they are working on lower-speed public ISPs, it is good practice to understand these values and plan accordingly. If the minimum amount of bandwidth is not available, the end-user may experience audio holes or even dropped calls. Radio-to-radio data messaging or RDAC commands may not be successful on the first attempt or may be dropped altogether. In general, the QoS may suffer if substantial bandwidth is not available.

Note that for most Internet Service Providers, the uplink bandwidth is the limiting factor. The downlink bandwidth is usually multiple factors above the uplink bandwidth. Therefore, if the uplink requirements are met, the downlink requirements are almost always acceptable. Some ISPs may state they provide a particular bandwidth, but it is important to verify the promised bandwidth is available once the system is installed and throughout operation. A sudden decrease in available bandwidth may cause the previously described symptoms.

If the WAN connection is utilized by other services (file transfer, multimedia, web browsing, and others), then the CPMS devices may not have the appropriate bandwidth when required and the QoS may suffer. It is suggested to remove or limit these types of activities. Additionally, excessive usage of the RDAC application itself may cause increased strain on the network during times of High Voice activity. It is recommended that RDAC commands be kept to a minimum unless appropriate bandwidth has been allocated.

4.9.3.2.4.1
Required Bandwidth Calculations

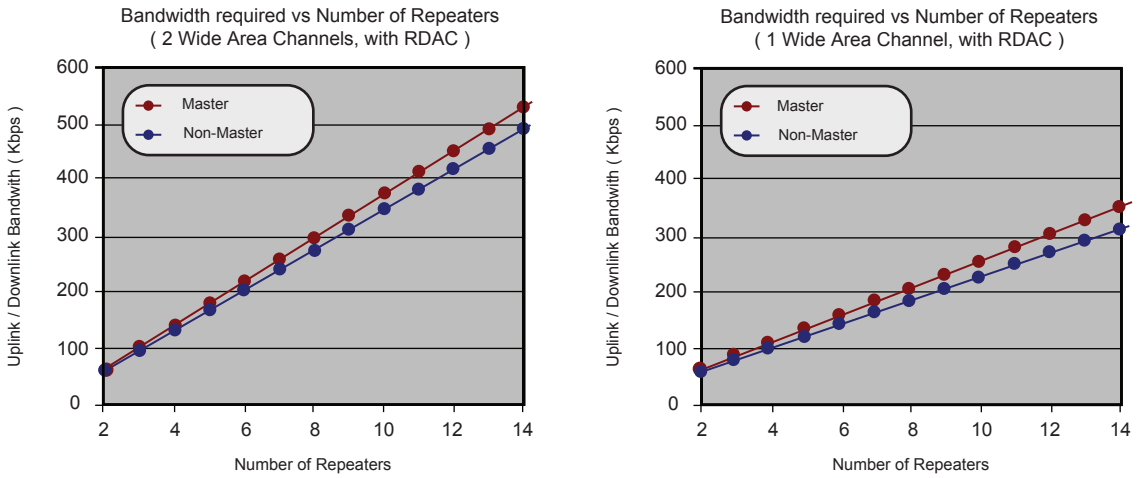
The amount of bandwidth an IP Site Connect device requires is dependent on a variety of factors. It is important to understand that the bandwidth required for one particular device is dependent on the number of other devices or peers it has in the IP Site Connect system. The type of the devices is equally important.

An IP Site Connect system can contain repeaters that have two channels operating in wide area, one channel operating in wide area, or no channels operating in wide area, such as local channels only. Channels, or slots, operating in local area mode do not send their voice traffic over the network. Remember that one repeater within the IP Site Connect system acts as the Master. This repeater requires some additional bandwidth. The IP Site Connect system may also contain repeaters, disabled repeaters, and

RDAC applications. These devices do not send voice over the network, but they do require the bandwidth to support the standard link management and control signaling.

For a quick reference, the graphs Figure 163: Required Bandwidth for Two Simple IP Site Connect System Configurations on page 429 show the required bandwidth for two simple IP Site Connect system configurations. The first one shows the required bandwidth for various size systems where every repeater in the system uses both channels, or slots, as wide area channels. The second one shows the required bandwidth for various size systems where every repeater in the system uses one channel, or slot, as a wide area channel, and the other channel, or slot, as a local area channel. In each system, one RDAC is present, repeater authentication is enabled, and Secure VPN is not used in the routers.

Figure 163: Required Bandwidth for Two Simple IP Site Connect System Configurations



Note that although the examples in Figure 163: Required Bandwidth for Two Simple IP Site Connect System Configurations on page 429 may represent typical IP Site Connect configurations, and may provide a quick snapshot of the bandwidth requirements for a particular size system, more complicated configurations require additional calculations.

The following equation should be used to calculate the bandwidth for each IP Site Connect device in the IP Site Connect system. The results should then be added together at sites where multiple devices reside behind one wide area connection.

BW_{VC} = 15 kbps = Bandwidth required to support Wide Area Voice or Data (1 slot)

BW_{LM} = 6 kbps = Bandwidth required to support Link Management

BW_{IR} = 3 kbps = Bandwidth required to support Master Messaging

BW_{RD} = 55 kbps = Bandwidth required to support RDAC commands

Table 84: IP Site Connect Device Bandwidth Equation

Number of Wide Area Channel Peers* for Slot 1	x	BW_{VC}	kbps =		kbps
Number of Wide Area Channel Peers* for Slot 2	x	BW_{VC}	kbps =		kbps
Total Number of IP Site Connect Peers*	x	BW_{LM}	kbps =		kbps
If Master, Total Number of IP Site Connect Peers*	x	BW_{IR}	kbps =		kbps
RDAC Traffic				BW_{RD}	kbps

	+	
Required Uplink/Downlink Bandwidth		kbps

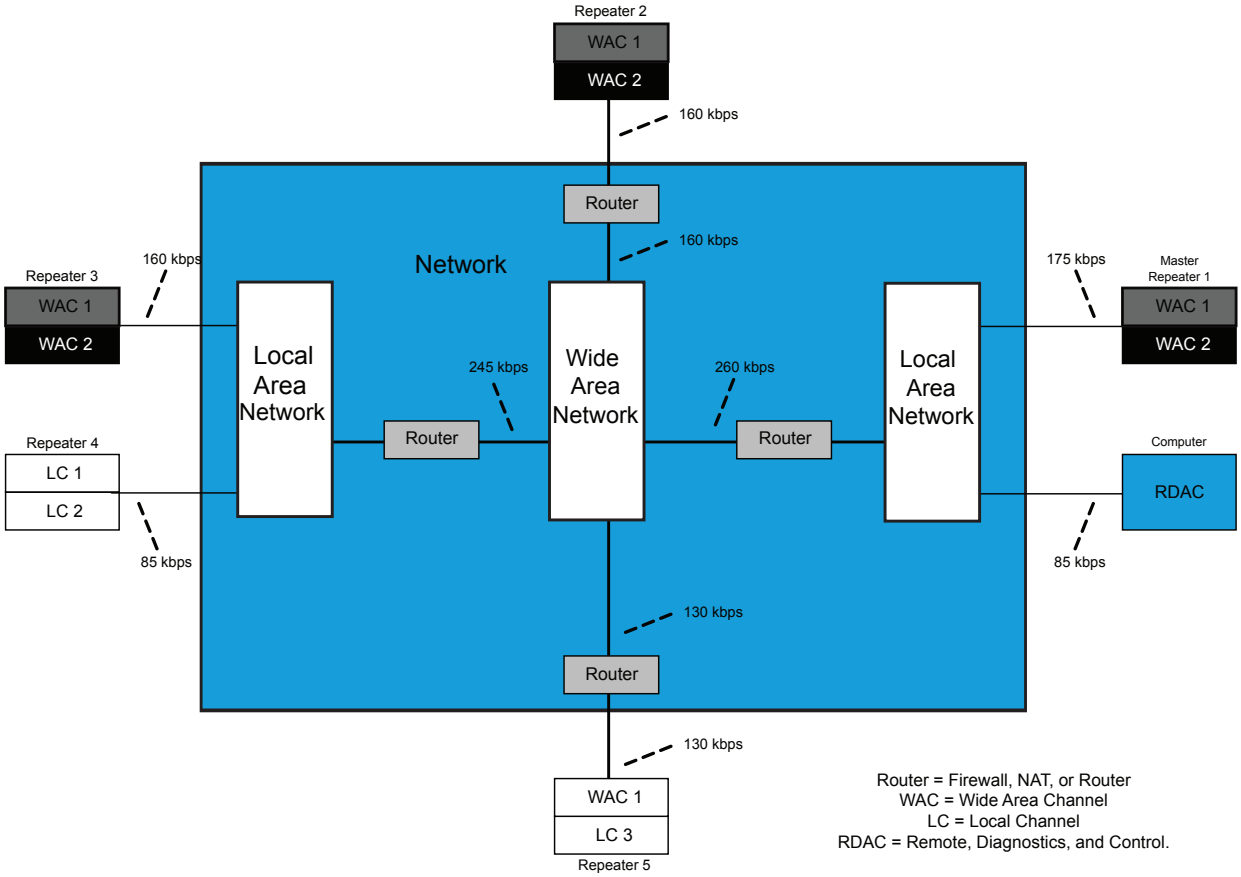
* Peer does not include self.

To demonstrate the use of the equation in Table 84: IP Site Connect Device Bandwidth Equation on page 429 on a more complicated IP Site Connect system, take the following example system shown in Figure 164: Example System for Calculating Bandwidth Requirements without Secure VPN on page 430. This system has a total of six IP Site Connect devices at three sites; five repeaters and one RDAC. Three of the repeaters have both channels configured as wide area, one has a wide area channel and a local channel, and the last repeater has two local channels. The routers do not use Secure VPN.

Repeater 1 is a Master, and it has two wide area channels. The first wide area channel has three peers and the second wide area channel has two peers. Note that since Repeater 4 and Repeater 5 have local area channels, these are not considered wide area channel peers. It is also important to remember that a peer does not include the currently calculated device.

Each calculation provides enough bandwidth to support an RDAC command during the times of high activity. It is assumed that only one RDAC command occurs at a time and that it is not used often. If it is expected for the multiple RDAC applications to perform commands on repeaters often and simultaneously, it is advisable to increase the bandwidth to support these types of activities.

Figure 164: Example System for Calculating Bandwidth Requirements without Secure VPN



The detailed bandwidth calculation for Repeater 1 is as follows:

Table 85: Detailed Bandwidth Calculation for Repeater 1 in IP Site Connect Mode

Number of Wide Area Channel Peers* for Slot 1	3	x	15	kbps =	45	kbps
Number of Wide Area Channel Peers* for Slot 2	2	x	15	kbps =	30	kbps
Total Number of IP Site Connect Peers*	5	x	6	kbps =	30	kbps
If Master, Total Number of IP Site Connect Peers*	5	x	3	kbps =	15	kbps
RDAC Traffic					55	kbps
				+	–	–
Required Uplink/Downlink Bandwidth					175	kbps

* Peer does not include self.

Using the same method for all IP Site Connect devices in the example system yields the following results:

Table 86: Detailed Bandwidth Calculation for Repeaters in IP Site Connect Mode

	Repeater 1	Repeater 2	Repeater 3	Repeater 4	Repeater 5	RDAC
Number of Wide Area Channel Peers* for Slot 1	3	3	3	0	3	0
Number of Wide Area Channel Peers* for Slot 2	2	2	2	0	0	0
Total Number of IP Site Connect Peers*	5	5	5	5	5	5
If Master, Total Number of IP Site Connect Peers*	5	0	0	0	0	0
Required Uplink/Downlink Bandwidth (kbps)	175	160	160	85	130	85

* Peer does not include self.

IP Site Connect devices behind a single router must be added together to acquire the wide area network bandwidth requirements. See the final bandwidth requirements in Figure 164: Example System for Calculating Bandwidth Requirements without Secure VPN on page 430.

NOTE: A repeater or a disabled repeater connected to the IP Site Connect system would require the same amount of traffic as a local only repeater (Repeater 4). Keep in mind that if the disabled repeater is eventually enabled without disabling a different repeater, the bandwidth of the enabled repeater should be accounted for in the bandwidth plan.

4.9.3.2.4.2
Required Bandwidth Calculations While Utilizing a Secure Virtual Private Network

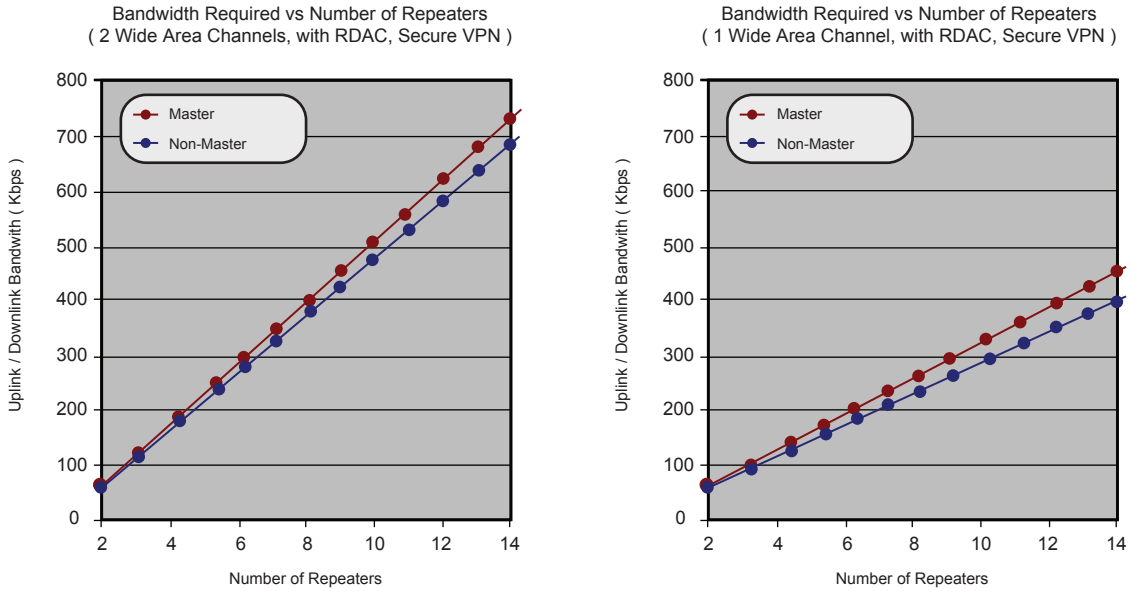
As was discussed in previous chapters, peer-to-peer communications over the network are optionally authenticated and are also encrypted end-to-end if enabled in the radios. Voice and Data Privacy on page 181 If this is not considered sufficient for a particular customer, IP Site Connect supports the ability to work through a Secure Virtual Private Network (VPN). Secure VPN is not a function of the IP Site Connect device

but rather of the router. It is important to note that Secure VPN does add the need for additional bandwidth and may introduce additional delay.

For a quick reference, the graphs below show the required bandwidth for the two previously discussed simple IP Site Connect system configurations, but in this case utilizing routers with Secure VPN enabled and repeater Authentication Disabled. When utilizing Secure VPN routers, repeater authentication is not necessary since the Secure VPN utilizes its own authentication.

As can be seen, the bandwidth requirements per device increase substantially. This should be taken into account when planning for bandwidth.

Figure 165: Required Bandwidth Calculations While Utilizing a Secure Virtual Private Network



The following parameters should be used in the previous equation to calculate the bandwidth requirements of each device in the system when secure VPN in the routers is enabled and repeater authentication is disabled.

BW_{VC} = 23 kbps = Bandwidth required to support Wide Area Voice or Data with Secure VPN

BW_{LM} = 5 kbps = Bandwidth required to support Link Management without authentication

BW_{IR} = 4 kbps = Bandwidth required to support Master Messaging

BW_{RD} = 64 kbps = Bandwidth required to support RDAC commands

NOTE: The preceding data was compiled using the Linksys EtherFast Cable/DSL VPN Router with four-port switch. Model: BEFVP41. Other routers using different algorithms may yield different results.

4.9.4
Flow of Voice/Data/Control Messages

The flow of voice/data/control messages from a radio to its repeater for an IP Site Connect configuration is the same as that of single-site configuration of MOTOTRBO system. The major changes in the flow of messages (between single site operations and multiple site operations) are in the processing of a message in the repeaters and the additional delays introduced due to reasons such as serialization, propagation, arbitration, and the nonalignment of slots between repeaters. This section describes the changes.

On receipt of a start up of a voice/data/control call from a radio over a slot, a repeater sends it over the backend network to all the repeaters that are enabled, operating in digital mode, and the corresponding slot

is configured for multiple site operation. This implies that at any time at most two calls are active in an IP Site Connect system if both slots are configured for multiple site operation.

In an IP Site Connect configuration, calls can start concurrently at more than one repeater and due to different messaging delay between repeaters, it is possible that different repeaters select different calls for repeating Over-The-Air. To overcome this problem, on receipt of a start up of a voice/data/control call either Over-The-Air (from a radio) or over the backend network (from other repeaters), a repeater starts an arbitration window for a duration of twice the Inter-Repeater Messaging Delay. At the end of the arbitration window, the repeater selects one of the calls received during this window using a procedure that ensures that all the repeaters select the same call. After selection, a repeater starts repeating the bursts of the selected call. A disadvantage of the arbitration procedure is that it increases the System Access Time.

The voice/data/control messages are sent burst by burst between repeaters. Like a single-site system, a repeater does no data link layer processing (for example, acknowledgment, decryption). If required, the voice and data messages are encrypted / decrypted by the source and destination radios. A repeater sends the voice or data packet to other repeaters as it receives Over-The-Air. Also in case of data message, the destination radio sends the Ack/Nack and if required the Selective ARQ takes place between the source and destination radios and not between a radio and its repeater.

A call is a session of one or more transmissions from participating radios. To ensure continuity between transmissions, the single site configuration of MOTOTRBO has Hang Time, during which the channel is reserved for participant(s) of the ongoing call. The IP Site Connect configuration extends the concept of session to include Remote Monitor call, Individual and group data call, and CSBK Call (for example, Call Alert, Radio Check, Inhibit/Uninhibit). The Hang Time ensures that a call continues with minimum interruptions.

The flow of data messages from a radio to an application (for example, Location or Text Messages) in an IP Site Connect system is similar to a single-site configuration of MOTOTRBO. A data packet flows burst-by-burst to a Control Station connected to the Application Server. The Control Station assembles the bursts into a PDU. If the PDU is confirmed then the Control Station handles the data link layer acknowledgment. If the PDU is encrypted then the Control Station decrypts the PDU. The Control Station strips the data link layer headers and forwards the resulting datagram to the Application Server.

All the data applications of the single site configuration of MOTOTRBO are compatible with IP Site Connect configuration. An IP Site Connect configuration supports the Revert Channels, where a Revert Channel can be a channel of another IP Site Connect system. The GPS data on a GPS Revert Channel are sent unconfirmed in IP Site Connect mode. This increases the throughput of the GPS data as the data link layer acknowledgment over the back-end network is slower due to delays associated with the back-end network.

4.9.5
Security Considerations

The single site configuration of MOTOTRBO offers three types of privacy mechanisms Over-The-Air:

- Basic
- Enhanced
- AES

For more information, see: Voice and Data Privacy on page 181.

The IP Site Connect configuration not only supports those mechanisms but also extends them over the back-end network. A repeater does not decrypt the encrypted packets, it simply passes the packets as received Over-the-Air to other repeaters. Since the privacy mechanisms are not compatible, all the radios and repeaters in a system should support the same privacy mechanism. Repeaters are required to be configured with used by the radios privacy option but do not require the privacy keys.

NOTE: The privacy mechanisms protect only the voice or data payloads. They do not protect the voice or data headers, nor control messages (CSBK), nor system messages (between repeaters).

An IP Site Connect system optionally offers authentication of all the packets sent over the back-end network between IP Site Connect devices. Each packet has a 10 bytes long cryptographic signature. The signature is created using the Keyed-Hash Message Authentication Code (HMAC), which is a National Institute of Standards and Technology (NIST) standard. The hashing is done using the SHA-1 algorithm. The HMAC uses 20 bytes long symmetric keys and generates a 20 bytes long signature. To reduce the bandwidth requirement over the back-end network, the 20 bytes long signature is truncated to 10 bytes before attaching to the packet. Packet authentication prevents an attacker from using an impersonator as an IP Site Connect device in order to get access to the IP Site Connect system. This feature, if selected by a customer, requires the customer to manually configure the same key to all the IP Site Connect devices. Note that the IP Site Connect system does not support rekeying remotely.

The HMAC authentication mechanism does not protect against replay attacks. For more secure communication, an IP Site Connect system should use Secure VPN routers to connect over the back-end network. Secure VPN routers can optionally provide confidentiality of all the messages including system messages (between IP Site Connect devices), control messages (CSBK), and voice or data headers. A disadvantage of using Secure VPN routers is that the IP Site Connect requires more inbound and outbound bandwidth from the back-end network. The use of Secure VPN routers makes the HMAC authentication mechanism of IP Site Connect redundant and it is recommended that it should be disabled. This saves some bandwidth over the back-end network.

Another security option is Restricted Access to System (RAS). For more information, see: Restricted Access to System (RAS) Design Considerations on page 469

4.9.6

General Considerations When Setting Up the Network Connection for an IP Site Connect System

Network setup and configuration varies significantly depending on the complexity of the equipment and IP network the system resides on. It is always wise to communicate with the Network Administrator during installation and during the design phase as they are likely be the individuals configuring the network equipment and own a great deal of knowledge in this area. Below is a short list of items to keep in mind when setting up or when troubleshooting the networks of IP Site Connect systems.

- When assigning Static IP addresses within a **Network**, it must not conflict with another static IP address. As with any IP conflict, this can cause a disruption to the IP Site Connect traffic. Also, ensure that the static IP address does not fall into the DHCP assignable range. This can cause an IP conflict if the address is dynamically assigned to another device on the network.
- If other network devices are present on the same IP network as the IP Site Connect devices, it is good practice to setup Quality of Service (QoS) rules in the Router. This ensures that the IP Site Connect packets have priority over other traffic on the system. Not doing this could cause audio performance degradation or lost transmissions when other devices on the system are excessively utilizing the network. There are various methods routers use to provide QoS. It is commonly performed by configuring a range of UDP ports or IP Addresses a specific amount of upstream and downstream bandwidth. The default UDP port for IP Site Connect is 50000. For details on calculating the required bandwidth, see Required Bandwidth Calculations on page 428.
- Verify that the customer network equipment is not blocking the IP Addresses or UDP Ports (default 50000) utilized by the IP Site Connect system. This is commonly done by a firewall or other security device. Consult the customer’s Network Administrator or Internet Service Provider.
- Inquire with the Internet Service Provider if there are any caps on bandwidth usage per month. Some ISPs do not allow the customer to exceed a particular upload or download limit per month. Since IP Site Connect systems stream voice over the Internet, it may be possible to surpass this limit on extremely high usage systems. As a reference point, a five site system under nominal load could use around 20GB per month, where as a 15 site system under nominal load could use around 65GB per month. For most ISPs, this will not be an issue.

- When configuring routers with VPN links, it is wise to increase the IPSec Key Life Time (KLT) Timers to around 13 to 24 hours. It is recommended to set Phase 1 KLT to 24 hours, and Phase 2 KLT to 13 hours. Some low-end routers cause a disruption to ongoing voice and data when renegotiating keys after the Key Life Time Timer expires. This is especially noticeable when multiple VPNs are configured with identical Key Life Time Timers since the router will need to re-calculate numerous keys at the same time. It is best practice to offset the Key Life Time Timers of each VPN by 10 minutes.

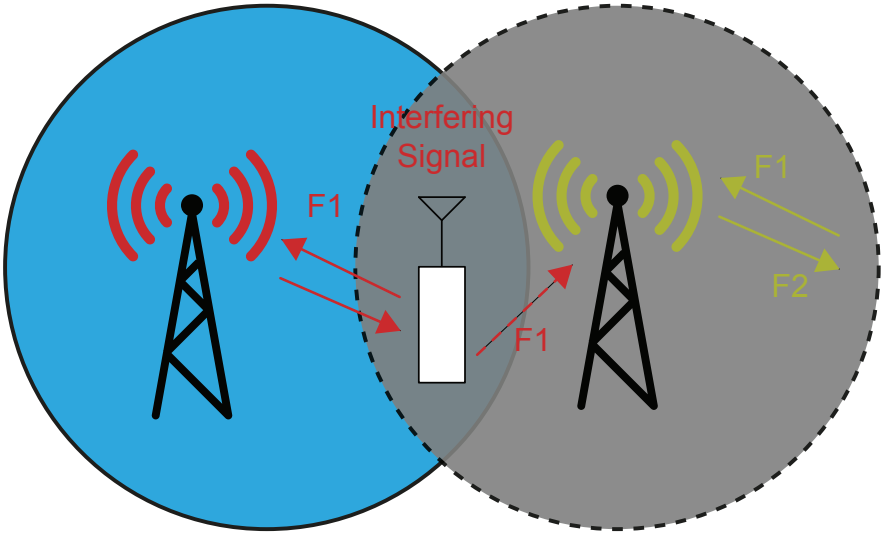
4.9.7

Considerations for Shared Use of a Channel

To take care of shared use of a physical channel, a repeater (for example, green repeater) of an IP Site Connect system always monitors its Rx frequency and does not transmit if the Received Signal Strength Indicator (RSSI) from radio(s) of some other radio system is greater than a configurable threshold. This ensures that an IP Site Connect system does not use a channel if another repeater, in vicinity, is currently using the channel. The RSSI threshold is CPS programmable in the range of 40 dB to 130 dB. The threshold should be chosen wisely, otherwise interference from background noise may inhibit a repeater from transmitting. The RDAC application can be used to measure the inbound RSSI of an interfering signal if required.

The following figure shows the transmission of red radio interfering with the green repeater.

Figure 166: An Example of Interference at Receive Frequency



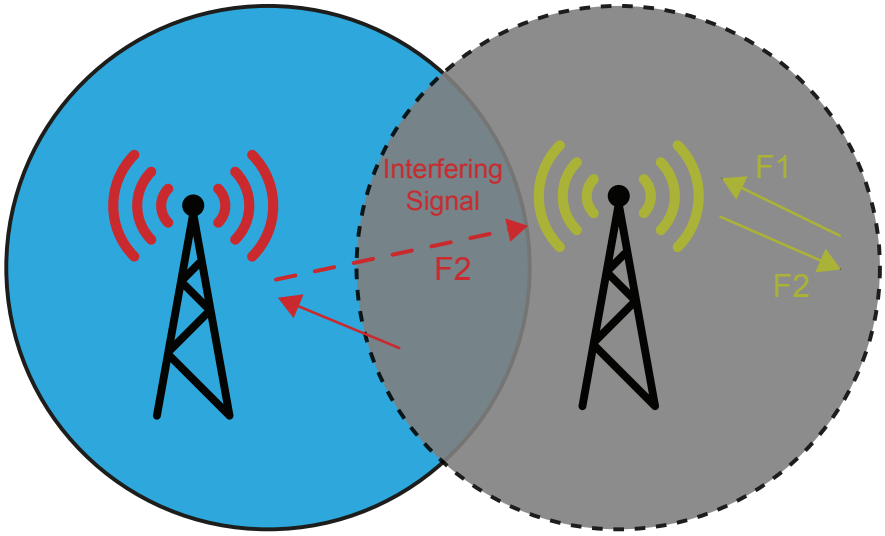
This monitoring scheme of Rx frequency is not sufficient in the following conditions:

- In VHF range, in some countries (including USA), the transmit frequency is not tightly bound to a receive frequency.
- There is no radio in the other radio system that is currently using the system.

- The other radio system is being used by a console.
- The radio that is using the other radio system is too far from the IP Site Connect system.

To address these conditions, it is recommended that a repeater of an IP Site Connect system should use an external RF receiver. The external RF receiver is tuned to the transmit frequency of the repeater and activates a GPIO compatible output when it receives RF signal. The output of the receiver is connected to the “Transmit Inhibit” (an input GPIO line) of the repeater. The repeater does not wake up if its “Transmit Inhibit” line is active. An attenuator can be inserted between the antenna and the receiver, if it is required to change the threshold of the received signal. The net effect of this configuration is that the repeater does not wake up if there is another repeater transmitting at its Tx frequency. The repeater CPS allows its user to associate an input line of the GPIO lines with “Transmit Inhibit”. This arrangement is also applicable to single-site repeaters. The following figure shows the transmission of red repeater interfering with the green repeater.

Figure 167: An Example of Interference at Transmit Frequency



4.9.8
Migration from Single Site Systems

The hardware of radios (both portables and mobiles) and repeaters of a MOTOTRBO single site system are fully compatible with the IP Site Connect configuration. To migrate to IP Site Connect system the customer is required to update the software of repeaters and reconfigure them.

Some of the features of the single site radios may work in the IP Site Connect system but it is highly recommended that the software of the radios should also be updated. Data applications of single site configuration are fully compatible with the IP Site Connect configuration.

4.9.9
Migration from an Older IP Site Connect System

IP Site Connect repeaters provide a robust migration for upcoming software versions for repeaters. IP Site Connect repeaters exchange their respective link protocol version information and validate interoperability support when they detect repeaters having different firmware/software versions loads.

NOTE: Assume an IP Site Connect system running on software version R01.05.00 is being upgraded to R01.06.00. The upgraded R01.06.00 repeater initiates the discovery, exchanges link protocol version information with the R01.05.00 repeaters, and synchronizes the protocol versions for optimal repeater operations.

While the repeater's versioned IP link protocol provides a clean migration methodology between repeater software versions, there are limitations associated with this feature. Repeaters support the current and previous two releases. Hence, repeater operations and interoperability beyond the previous two releases would result in incompatibility between repeaters. In such abnormal scenarios, customers are required to upgrade the system such that all repeaters operating on the system remain compatible; meets the requirement of the current and previous two releases.

A service degradation is expected in scenarios that include multiple repeater firmware versions running in the system. Therefore, usage of the same repeater firmware version throughout the system, and only allow usage of different firmware versions during the upgrade period is preferred.

The IP Site Connect repeaters discover each other through the Master repeater (configurable via the CPS); which is a centralized entity of the system. The recommendation is to have the Master repeater upgraded first to minimize system downtime, optimize IP link connectivity and improve system access time across the back-end IP network.

4.10
Multiple Digital Repeaters in Capacity Plus Single Site

System	Description
CPSS Capacity Plus Single Site	Section Multiple Digital Repeaters in Capacity Plus Single Site on page 437 and its subsections explain Multi Digital Repeaters in Capacity Plus Single Site.

The main problem with the standalone configuration of multiple digital repeaters is that a radio can only use one channel of a repeater at any instance of time. Capacity Plus Single Site resolves this restriction and allows a radio to use all the repeaters at a site. The sharing of repeaters improves the utilization of channels.

4.10.1
System Capacity in Capacity Plus Single Site

In Capacity Plus Single Site (CPSS), starting from software version R02.30.00 onwards, MOTOTRBO supports a maximum of 20 back-end network devices called "peers" (for example, repeaters and RDAC PC), where network devices include a maximum of 8 Trunked repeaters (16 Trunked Channels), 12 Data Revert repeaters (24 Revert Channels), and 5 RDACs or similar applications.

NOTE: The CPSS system requires at least one Trunked repeater.

A CPSS channel mode supports more radios compared to a single repeater configuration. The ID of radios in Capacity Plus Single Site ranges from 1 to 65535 (16 bit) and the ID of talkgroups ranges from 1 to 254 (8 bit). The Talkgroup ID of 255 is reserved for “All Call”.

When adding a new Trunked repeater to a CPSS system, all the radios should be configured with the channels of the new repeater, before the new repeater is connected to the Capacity Plus Single Site system.

4.10.2
Frequencies and Color Code Considerations

As Capacity Plus Single Site, is a single site trunking system, all the repeaters should use different frequencies. Their color code can be the same or different. A Capacity Plus Single Site system has the ability to share RF channel(s) with other systems, but it is necessary to ensure that all channels in all overlapping systems have a unique frequency pair and color code combination.

A Capacity Plus Single Site radio requires lists of all trunked and Revert Channels. This makes it necessary to reprogram all the radios when a frequency is added to the system. If a Capacity Plus Single Site system is to be expanded in the future, and if these frequencies are known, then it is recommended to keep all future frequencies in the trunked list. Keeping additional trunked frequencies in the radio marginally slows down the radio operations when the radio is powered on, or when the radio comes out of fade. But this prevents the need to reconfigure all the radios when new repeaters are added.

If a Capacity Plus Single Site repeater needs to be removed from service for an upgrade or for repair, there is no need to reconfigure the radios. The MOTOTRBO Capacity Plus Single Site system can still operate as long as there is one Capacity Plus Single Site repeater functioning in the system. Additionally, there is no need to power down the whole MOTOTRBO system while removing or adding a repeater in the Capacity Plus Single Site system.

This recommendation is also true for Revert Channels but with a condition. A radio may experience delay in transmitting data over Revert Channels. During this delay, a radio may miss a call taking place on the Trunked Channel.

4.10.3
Considerations for the Back-End Network in Capacity Plus Single Site

A Capacity Plus Single Site system requires a back-end network if it has more than one repeater. The back-end network for CPSS is an Ethernet switch used to connect all repeaters. To add a remote RDAC, application PC, or the MNIS, connect the switch to a router). This router is connected to either a dedicated network or to the Internet (provided by an Internet Service Provider). In the case of using NAT on the router, hair-pinning support can be required.

Although Capacity Plus Single Site works with most off-the-shelf network devices, the following Ethernet switches and routers are suggested for use:

- Aruba 2530-24 Ethernet Switch (J9782A)
- Aruba 2530-24G Ethernet Switch (J9776A)
- Juniper EX 2300 Ethernet Switch
- Juniper SRX 300 Service Gateway Router
- Juniper SRX 345 Service Gateway Router

A repeater has three network interfaces: Ethernet, USB, and Over-the-Air. A repeater uses its Ethernet port to communicate with other network devices using IPv4/UDP. Since UDP does not support confirmation, CPSS provides its own acknowledgment and retry mechanism for critical activities. The Ethernet port is not the

default IP gateway of the repeater. An IP datagram that arrives from USB or Over-the-Air is not automatically routed to the Ethernet port.

A Capacity Plus Single Site repeaters use IPv4 Limited Broadcast Address (255.255.255.255) to distribute a message to all the repeaters at a site. The broadcast messages may have some adverse effects on the other devices present on the LAN.

NOTE: It is highly recommended that only the CPSS repeaters and RDAC PC are present on the LAN.

A Capacity Plus Single Site configuration uses “Link Management” to keep a device aware of the status, current IPv4 address, and UDP port of other devices. The Link Management requires only the Master repeater to act as a broker of IPv4/UDP addresses of system devices.

In a Capacity Plus Single Site system repeaters may have either static or dynamic IPv4 addresses. The dynamic IPv4 addresses may change every time the network device powers on or periodically every few hours. The lease time of the IPv4 address should be kept as large as possible. A change in the IPv4 address of the network device causes a short disruption of service. To enable the use of static IPv4 addresses, do not select the DHCP option; ensure the static IPv4 address, the gateway IPv4 address, and network mask is provided.

Repeaters can have static or dynamic IPv4 addresses however all devices must be manually configured with the IPv4/UDP address of the Master repeater. For this reason, it must be a static IPv4 address or an FQDN (Fully Qualified Domain Name) to be resolved with a DNS server. Anytime the IPv4 address for a Master repeater changes, then the DNS server must be updated with the new IPv4 address. It is the job of the entity assigning the IPv4 address to the Master repeater to also update the DNS server with the updated IPv4 address to minimize any interruptions in connectivity to Master.

NOTE: The DNS feature is only available on SLR Series Repeaters.

The Master’s IPv4/UDP address refers to its address as seen from:

- the back-end network (router’s WAN side); when there is any remote application PC connected to CPSS system;
- the LAN; when all CPSS devices are in the Master repeater subnet and there is no remote application PC connected to the CPSS system.

4.10.4
Behaviors in Presence of Failures

A Capacity Plus Single Site system has no centralized controller and this makes it tolerant to failures. It automatically detects most types of failures, reconfigures itself, and continues to provide the services although with decreased capacity.

A repeater detects the failure of other repeaters or the back-end network. “Keep Alive” messages are periodically exchanged between repeaters. The absence of such messages from a repeater indicates a failure of either that repeater or of the network in between. A failed repeater is not selected as a Rest Channel repeater. If a Rest Channel repeater fails, a new Rest Channel is selected by the system.

To help a radio detect the failure of the Rest Channel repeater, the Rest Channel repeater periodically broadcasts system status over the Rest Channel. If a radio misses the broadcast, then it knows that either the repeater has failed or it is not within the coverage area of the repeater and the radio starts searching for the Rest Channel.

When the back-end network switch fails, each repeater cannot connect to all other repeaters. Each repeater then starts working as a two-channel trunking system. At the time of the switch failure, all radios may be on the Rest Channel or busy on other channels. In the first instance, the call capacity is severely impacted while in the second, radios on different channels are unable to communicate.

To resolve a failure of a Revert Channel repeater, a radio makes multiple attempts to transmit a data message on different channels.

If a Trunked Control Station fails, a set of radios do not receive data messages from the Application Server.

4.10.5
Adaptive Rest Channel Rotation (ARCR)

Starting with software version R02.40.00 onwards, Capacity Plus Multi Site and Capacity Plus Single Site System supports ARCR functionality. The ARCR functionality provides resilience to rarely occurring fault mechanisms that can occur in trunked systems and therefore applies to Capacity Plus Multi Site and Capacity Plus Single Site systems only. The functionality ensures that a rest channel is available even in the presence of very specific adverse channel conditions and protects the system in the event of certain types of rarely occurring hardware failures.

The functionality adds additional resilience in the following scenarios:

- Co-channel interference on the uplink that is below the System RSSI detect threshold configured in a repeater but high enough to prevent the repeater from receiving all radios call request. A subset of the above includes the deployment where:
  - The ‘System RSSI’ detect threshold is intentionally set high to lower the likelihood of “losing” channel (for example, have it temporarily taken out of the trunk pool) due to a co-channel licensee’s activity. For example, it is set intentionally high to “tolerate” the negative effects of simultaneous co-channel use, albeit with some negative side effects on range performance.
  - The System RSSI threshold isn’t set or isn’t set properly.
  - Previously unknown/unanticipated co-channel interference occurring after commissioning due to a co-channel license being granted.
- Failures in the receiver line-up of a repeater, including:
  - Receiver antenna issues (for example, broken and damaged),
  - Receiver transmission line issues,
  - Receiver antenna distribution network issues,
  - Receiver hardware failure.
- Inter-modulation (IM) Products:
  - Previously unknown/unanticipated interference due to a frequency being granted which results in an undesirable inter-modulation product.
  - Sites which use multiple antennas, potentially as many as two antennas (Tx and Rx) per repeater at a site (for example, a large rooftop installation to provide sufficient separation between antennas, while saving the cost and complexity of a combining network).
  - Operation in densely populated and changeable RF environments.

With ARCR functionality, a site of a system continues to operate and allow communication with other working channels (Repeater and the Hardware links) as long as there are working external RF links, Hardware links, and Repeaters on the site.

In nutshell, the ARCR functionality forces a rest channel to automatically move to another channel if there is no incoming call on the rest channel for a specific duration. The duration is adaptively changed, based on the volume of incoming calls. To ensure a guaranteed rest channel rotation in all call volume conditions, the duration is limited between a minimum time that is equal to a ‘SIT + a beacon duration’ time and the maximum time which can be set via the CPS ‘Rest Channel TOT’ field. For proper operation, the Rest Channel TOT value must be same on all the repeaters of a site.

Guidelines for choosing Rest Channel TOT:

- The Rest Channel TOT is most effective during idle or low call volume condition. For the site where the repeaters have different channel preference level, it is suggested to use larger Rest Channel TOT value, so that high-preference channels are more frequently utilized even during low call volume conditions. Note that the force rest channel mechanism steers the rest channel through all preference level repeaters in round-robin manner, whereas the incoming calls mechanism selects higher preference channels more often than lower preference channels.
- Shorter Rest Channel TOT leads to faster Rest Channel rotation and better resilience to the failure, however may have minor impact to battery life, because radios receive new rest channel assignment information more often.
- The Rest channel rotation may cause minor delay in call access time during force rest channel switching period. The Faster the rotation, the more frequent is such access time delays. Note the impact of such delays should be unnoticeable to radio users.
- If necessary, the ARCR functionality can also be disabled completely by disabling Rest Channel TOT value.

If a rest channel assignment is repeatedly force rotated from a specific repeater, while all other channels rotate as rest channels due to normal radio calls, the software algorithm suspects that the particular channel has failed and reduces its rest channel preference to the lowest level. Consequently, that suspected repeater is used less, to minimize the likelihood of a rest channel becoming unavailable on that repeater and blocking system access. In due course, if a suspected repeater is found to be working then the preference level is reverted back to the configured level.

4.10.6
Limiting Interference to Other Systems

Capacity Plus Single Site is designed to be compatible with both exclusive and shared channels. To help a radio detect the unavailability of a Rest Channel, the repeater periodically transmits a very short system status message beacon. If the radio misses this transmission on a Rest Channel, then the radio is either not within the coverage area of the repeater or the repeater cannot transmit (due to interference by other systems or a failure). The radio then starts searching for a new Rest Channel. The interval of periodic transmissions of the system status messages can be selected within certain limits by an authorized technician.

There are two points to consider:

- A more frequent beacon transmission helps a radio detect the unavailability of the Rest Channel faster, and thus reduces the downtime caused by interference from other systems and improves capacity. Hence, it is recommended to keep the beacon interval at the default value.
- If the system incorporates a shared channel causing interference to other systems, the default value of the beacon interval can be increased.

4.10.7
Plan for Talkaround Mode

In Capacity Plus Single Site, a MOTOTRBO radio does not support Talkaround. To ensure a communication channel is available when the Capacity Plus Single Site system is completely shut down or when a radio has moved out of the coverage area, it is recommended to program at least one common channel in Talkaround mode, that is at least one of the channel knob position should be programmed for Talkaround mode.

The Talkaround mode configuration is useful when the Capacity Plus Single Site system fails or the radio is out of coverage area. All that a user needs to do is to switch to Talkaround personality.

The radio user may define their own protocol for when to switch to Talkaround mode. For example, all radio users may switch to Talkaround mode when their radio is not on the Capacity Plus Single Site system for more than 10 minutes.

A customer may decide to plan the Talkaround mode configuration according to the number of groups that need such an operation. The available Talkaround mode frequencies should be distributed to the different groups based on their call profiles. Radios users can use scan mode in Talkaround.

To detect if the Capacity Plus Single Site system is once again up and running, radio users may periodically switch to a Capacity Plus Single Site channel and observe the activity on the channel.

4.10.8
Ways to Improve Battery Life

To improve battery life of a portable radio, a user can switch the radio power to low power mode by using the radio menu or power button. Low power mode improves battery life of a portable radio significantly over the high power mode.

When a user notices that the radio is not providing talk-permit tone for multiple PTT attempts in low power mode and that the signal strength bar is still visible, the radio should be switched to high power mode when initiating a call. When switching to different power modes, the radio user will not miss any incoming calls. The call listening capability of radio does not change with the radio transmit power.

Additionally, a radio user may turn off the radio when calls are not expected or when the radio is out of coverage.

4.10.9
MOTOTRBO Telemetry Connection Details

For more details about the telemetry GPIO pin assignments, see the MOTOTRBO Telemetry ADK Guide available.

4.10.10
Considerations for Configuring Combined Firmware Versions

In cases where legacy repeaters and other higher versions of repeaters needs to be connected together, it is highly recommended to make one of the higher version repeaters as the Master repeater, to avoid service degradation issues.

In scenarios where the MTR3000 repeaters are combined with the MOTOTRBO repeaters, it is possible that the MOTOTRBO repeater firmware is of a higher version than the MTR3000 repeater firmware. Configure the MOTOTRBO repeater as the Master repeater to avoid service degradation in this scenario.

4.10.11
Upgrading from Capacity Plus Single Site

NOTE: Repeaters running on software version RR02.30.00 or later are not interoperable with repeaters running on software version before R02.30.00. Hence, if there is a repeater with software version R02.30.00 or later present in a Capacity Plus Single Site system, all the other repeaters must be upgraded to R02.30.00 or later altogether.

When upgrading a Capacity Plus Single Site system, upgrade the Master first, followed by all other repeaters at the site. During the upgrade, the Capacity Plus Single Site system acts as two mutually exclusive systems, but calls are still supported. The radios remain tracking the legacy system until the last legacy repeater is switched off and upgraded. Afterward, the radios locate the new system and operate as normal.

4.11

Multiple Digital Repeaters in Capacity Plus Multi Site

System	Description
CPMS Capacity Plus Multi Site	Section Multiple Digital Repeaters in Capacity Plus Multi Site on page 443 and its subsections explain Multi Digital Repeaters in Capacity Plus Multi Site.

4.11.1

System Capacity in Capacity Plus Multi Site

The Capacity Plus Multi Site (CPMS) system, starting from software version R02.03.00 onwards, supports up to 15 sites, including application PCs, and a maximum of 8 Trunked repeaters (16 Trunked Channels) per site. For the Data Revert, up to 11 Revert repeaters (22 Revert Channels) are supported per site. However, the number of Trunked repeaters plus the number of Data Revert repeaters must not exceed a total of 12. For example, if there are 8 Trunked repeaters at a site, only up to 4 Data Revert repeaters can be supported at that site.

NOTE: The CPMS system requires at least one Trunked repeater in each site.

The CPMS system supports up to 140 peers which include the Trunked repeaters, Data Revert repeaters, MNIS, RDAC, and other applications. A Master role may exist on a repeater that also has RF responsibilities.

When the system requires more than 140 peers, a dedicated Master repeater with no RF responsibilities is required and it is recommended to reside on a Data Revert repeater. The site with a dedicated Master repeater is allowed to have up to 13 repeaters if the Master resides on the Data Revert repeater. In this case, the CPMS system can support up to 200 peers.

A Capacity Plus Multi Site system supports more radios per channel compared to a single repeater configuration or IPSC configuration. This is based on the following reasons:

- A customer can configure a talkgroup as a local talkgroup. The local talkgroup call is transmitted Over-the-Air at only one site.
- A customer can associate a set of sites with a talkgroup. The talkgroup call is transmitted Over-the-Air at only the associated sites.
- After initial handshakes, a Private Call is transmitted at either one or two sites only.

The Radio IDs and Talkgroup IDs in Capacity Plus Multi Site are the same as in the Capacity Plus Single Site. The ID of radios in CPMS ranges from 1 to 65535 (16-bit) and the ID of talkgroups ranges from 1 to 254 (8-bit). The Talkgroup ID of 255 is reserved for “All Call”.

When adding a new Trunked repeater to a Capacity Plus Multi Site system, all radios should be configured with the channels of the new repeater before the new repeater is connected to the system. Up to 160 personalities can be configured for the CPMS configuration, for a radio.

4.11.2

Considerations for Frequencies, Color Code, and Interference

In a Capacity Plus Multi Site system, the frequencies and color code of repeaters should satisfy the following rules:

- All the repeaters at a site should use different frequencies. Their color code can be the same or different.
- If the system incorporates a shared channel, then the beacons cause interference to other systems. In such scenarios, the value of the beacon interval can be increased.
- The repeaters of the non-adjacent sites of a Capacity Plus Multi Site system should use different frequencies and color code combinations. It is not advisable to keep the same frequencies and color code because a roaming radio is not able to distinguish between them, and may use incorrect Data Revert Channels or an incorrect list of neighboring sites.
- A Capacity Plus Multi Site system can share one or more of its channels with other systems. However, it is necessary to ensure that all the overlapping channels of different systems have a unique frequency and color code combination. If the frequencies of the geographically adjacent repeaters of two systems are the same, then their color codes should be different. It is not advisable to keep the same frequencies because in areas of overlap, destructive interference can occur.
- A system may be sharing the channels with other systems over multiple sites. It is possible that two systems (named here as Sys1 and Sys2) may be using the same (frequencies, color code) pair at two different sites (for example, Site1 and Site2). During automatic site search, a Sys1 radio at Site2 finds a Sys2 repeater and stays on that channel. This is not a desirable situation. One way to avoid this situation is to ensure that all the (frequencies, color code) pairs of all the overlapping systems are unique.

To take care of shared use of a physical channel, a Capacity Plus Multi Site repeater always monitors its Rx frequency and does not transmit if the RSSI from radio(s) of some other systems is greater than a configurable threshold. This ensures that a Capacity Plus Multi Site system does not use a channel if another repeater in the vicinity, is currently using the channel. The RSSI threshold is CPS programmable in the range of -40 dBm to -130 dBm. The threshold value should be chosen wisely. A value lower than the background noise, inhibits a repeater from transmitting due to interference from background noise. A value higher than the RSSI of the radio of some other system makes the system unfriendly to systems sharing the frequency. The RDAC application can be used to measure the inbound RSSI of an interfering signal, if required.

The above Rx frequency monitoring scheme is deficient if the Capacity Plus Multi Site repeater is unable to deduce that an interfering signal is present on its outbound channel based on the presence of an interfering radio transmission from another radio system on its inbound channel. This situation may arise for any of the following reasons:

- There is no radio in the other radio system that is currently using the system.
- The other radio system is being used by a console.
- The radio that uses the other radio system is too far from the Capacity Plus Multi Site system.

To take care of the above conditions, it is recommended that a repeater of a Capacity Plus Multi Site system should use an external RF receiver. The external RF receiver is tuned to the Tx frequency of the repeater and activates a GPIO compatible output when receiving an RF signal. The output of the receiver is connected to the “Transmit Inhibit” (an input GPIO line) of the repeater. The repeater does not wake up if its “Transmit Inhibit” line is active. An attenuator can be inserted between the antenna and the receiver, if it is required to change the threshold of the received signal. The net effect of this configuration is that the repeater does not wake up if there is another repeater transmitting at its Tx frequency. The repeater CPS allows the user to associate an input line of the GPIO lines with “Transmit Inhibit”. This arrangement is also applicable to single site repeaters.

Capacity Plus Multi Site is designed to be compatible with both exclusive and shared channels. To help a radio detect that it is out of range of its repeater and to facilitate automatic roaming by the radio, the repeater

periodically transmits a very short beacon. If the radio misses this transmission on a Rest Channel, then the radio is either not within the coverage area of the repeater, or the repeater cannot transmit (for example, due to interference by other systems or a failure). The radio then starts searching for a new Rest Channel. The interval of periodic transmissions of the beacon can be selected within certain limits by an authorized technician.

There are two points to consider:

- A more frequent beacon transmission helps a radio detect the “out of range” state faster, and thus reduces the downtime caused by interference from other systems and improves capacity. Hence, it is recommended to keep the beacon interval at the default value. This also makes the roaming faster.
- If the system incorporates a shared channel causing interference to other systems, the default value of the beacon interval can be increased.

4.11.3

Considerations for the Back-End Network in Capacity Plus Multi Site

In a Capacity Plus Multi Site system, the repeaters at a site are connected over a LAN switch that must be behind a router because the CPMS uses locally administered IPv4 addresses. In the simplest and most common configuration, an Ethernet switch with a router is used to connect all the repeaters at a site. Although CPMS works with most off-the-shelf network devices, the following Ethernet switches and routers are suggested for use:

- Aruba 2530-24 Ethernet Switch (J9782A)
- Aruba 2530-24G Ethernet Switch (J9776A)
- Juniper EX 2300 Ethernet Switch
- Juniper SRX 300 Service Gateway Router
- Juniper SRX 345 Service Gateway Router

A Capacity Plus Multi Site repeaters use IPv4 Limited Broadcast Address (255.255.255.255) to distribute a message to all the repeaters at a site. The broadcast messages may have some adverse effects on the other devices present on the LAN. Therefore it is highly recommended that only the CPMS repeaters and RDAC PC are present on the LAN. The site router is connected to either a dedicated network or to the Internet provided by an ISP.

A Capacity Plus Multi Site configuration uses “Link Management” to keep a device aware of the status, current IPv4 address, and UDP port of other devices. The Link Management requires only the Master repeater to act as a broker of IPv4/UDP addresses of system devices.

In a Capacity Plus Multi Site system repeaters may have either static or dynamic IPv4 addresses. The dynamic IPv4 addresses may change every time the network device powers on or periodically every few hours. The lease time of the IPv4 address should be kept as large as possible. A change in the IPv4 address of the network device causes a short disruption of service. To enable the use of static IPv4 addresses, do not select the DHCP option; ensure the static IPv4 address, the gateway IPv4 address, and network mask is provided.

Repeaters can have static or dynamic IPv4 addresses however all devices must be manually configured with the IPv4 address of the Master repeater. For this reason, it must be a static IPv4 address or an FQDN (Fully Qualified Domain Name) to be resolved with a DNS server. Anytime the IPv4 address for a Master repeater changes, then the DNS server must be updated with the new IPv4 address. It is the job of the entity assigning the IPv4 address to the Master repeater to also update the DNS server with the updated IPv4 address to minimize any interruptions in connectivity to Master.

NOTE: The DNS feature is only available on SLR Series Repeaters.

The Master's IPv4/UDP address refers to its address as seen from the back-end network. The back-end network can be a dedicated network or an Internet. ISPs provide a range of technologies such as DSL (typically ADSL), cable modem, broadband wireless access, and more. In some cases, dedicated links or networks can be effectively used or deployed, removing the monthly fees associated with public networks. The back-end network cannot be based on a dial-up connection (due to small bandwidth) or Satellite Internet access (due to large delay).

A Capacity Plus Multi Site device registers its IPv4/UDP address during power-on and periodically with the Master repeater. The Master repeater then notifies all the devices whenever the IPv4/UDP address of a device changes. The devices may be behind firewalls. For successful devices communication between the sites (for example, R1 and R2), the firewall of R1 must be open for messages from R2 and vice versa. Since the IPv4/UDP address of a CPMS device can be dynamic, it can be not possible to manually configure the firewalls. The Link Management procedure overcomes this problem by periodically sending a message from R1 to R2 and vice versa. On a receipt of an outbound message (for example, from R1 to R2), the R1's firewall keeps itself open for some duration (depending on the firewall type it can be from approximately 20 to 60 seconds) for an inbound message from R2. A device sends the keep-alive messages to keep the firewall open.

Network setup and configuration vary significantly depending on the complexity of the equipment and IP network the system resides on. For more information about the possible network topologies, see Back-End Network Topologies in Capacity Plus Multi Site on page 447.

It is advised to stay in touch with the Network Administrator during installation and during the design phase. The following is a short list of items to keep in mind when setting up or when troubleshooting the networks of a Capacity Plus Multi Site system:

- When assigning static IPv4 addresses within a network, it must not conflict with another static IPv4 address. Conflicting IPv4 addresses can cause a disruption to the traffic. Additionally, ensure that the static IPv4 address does not fall into the DHCP assignable range. This can cause an IPv4 conflict if the address is dynamically assigned to another device on the network.
- If other network devices are present on the same back-end IP network, it is good practice to setup Quality of Service (QoS) rules in the routers. This ensures that the Capacity Plus Multi Site packets have priority over other traffic on the back-end IP network. Failure in doing this could cause audio performance degradation or lost transmissions when other devices on the back-end IP network are excessively utilizing the network. There are various methods routers use to provide QoS. It is commonly performed by configuring a range of UDP ports or IPv4 addresses with a specific amount of upstream and downstream bandwidth. The default UDP port for Capacity Plus Multi Site is 50000.
- Verify that the customer network equipment is not blocking the IPv4 addresses or UDP ports utilized by the CPMS system. This is commonly done by a firewall or other security devices. Consult the customer's Network Administrator or ISP.
- Inquire with the ISP if there are any caps on bandwidth usage per month. Some ISPs do not allow the customer to exceed a particular upload or download limit per month. Since CPMS systems stream voice over the Internet, it may be possible to surpass this limit on extremely high usage systems.
- When configuring routers with VPN links, it is wise to increase the IPSec Key Life Time (KLT) timers to approximately 13 to 24 hours. It is recommended to set Phase 1 KLT to 24 hours, and Phase 2 KLT to 13 hours. Some low-end routers cause disruption to ongoing voice and data when renegotiating keys after the KLT timer expires. This is especially noticeable when multiple VPNs are configured with identical KLT timers since the router needs to re-calculate numerous keys at the same time. It is best practice to offset the KLT timers of each VPN by 10 minutes.

4.11.3.1
Back-End Network Topologies in Capacity Plus Multi Site

The following section outlines the main topologies that can be used in CPMS

- **No Tunnels** is a solution where the Capacity Plus Multi Site system is a part of the customer's corporate network. It can be a private enterprise network, fiber optic or microwave links, leased, or private MPLS network. The main benefit of using such networks is that there is no need to tunnel the CPMS system traffic. Creating the IP plan for CPMS, it is important to remember that in this case the IPv4 subnets designed for it must be from the customer's available private IPv4 range and can't overlap with other devices.
- **VPN Tunnels** is a solution where traffic between sites of the Capacity Plus Multi Site system is tunneled inside the IPsec or GRE tunnels. This allows the use of any private IPv4 subnets to create an IP plan until CPMS is used as the closed system without access to existing customer networks. When communication between the CPMS system and other customer devices has required the subnets used in both networks should not overlap. Using IPsec tunnels, the site routers can be interconnected using the public Internet as IPsec securely separates the system traffic from the Internet. The tunnels can be statically configured or the dynamic VPN protocol can be used.
- **NAT** is a solution where traffic between sites of the Capacity Plus Multi Site system is not tunneled but transmitted as is, only the IPv4 addresses of the CPMS devices are translated to IPv4 from the back-end network range. Usually, they are translated to the WAN IPv4 address of the site router. For this reason, all repeaters and application servers (RDAC, Dispatch Consoles) must use static IPv4 addresses.

NOTE: When using NAT depending on the deployment options, site routers with hair-pinning support can be required for some or all sites.

4.11.3.2
Back-End Network Characteristics in Capacity Plus Multi Site

To create a proper back-end network design, it is important to know its characteristics. This section explains three issues dealt with within the back-end network.

4.11.3.2.1
Delay/Latency in Capacity Plus Multi Site

Back-end network delay or latency is characterized as the amount of time it takes for a voice to leave the source repeater and reach the destination repeater. Three types of delay are inherent in the back-end networks:

- propagation delay
- serialization delay
- handling delay

Propagation delay is caused by the distance a signal must travel via light in fiber or as electrical impulses in copper-based networks. A fiber network stretching halfway around the world (13,000 miles) induces a one-way delay of about 70 milliseconds.

Serialization delay is the amount of time it takes the source repeater to actually place a packet byte by byte onto the back-end network interface. Generally, the effect of serialization delay on total delay is relatively minimal but since the CPMS system sends a voice packet one-by-one to all the repeaters, the serialization delay for the last destination repeater is (# of repeaters - 1) times the serialization delay for the first destination repeater.

Handling delay defines many different types of delay caused by the devices (for example, secure routers) that forward the packet through the back-end network. A significant component of the handling delay is the

queuing delay, which occurs when more packets are sent out to a network device than the device can handle at a given interval.

The CPS allows setting the **Total Delay** (that is the sum of propagation delay, serialization delay, and handling delay) to be **High** (90 ms) or **Normal** (60 ms) in both the repeaters and the radios. Note that radios also support higher values (500 ms) of total delay, which should not be used in the case of a CPMS system. The default is **Normal**. This is used to derive values for other parameters such as **Arbitration Interval** and **Call Hang Times** in repeaters and **Ack Wait** times in radios. For the proper functioning of a CPMS system, all the repeaters and radios should have the same delay setting.

It is recommended that propagation and handling delays between repeaters should be measured (for example, by “pinging”) between all pairs of repeaters.

The total delay is equal to the maximum of the measured values + (# of repeaters - 1) * (1/2 + 1000/BW in kbps) ms, where the BW is the available bandwidth of the back-end network.

If the total delay is less than 60 ms then the setting should be **Normal**. If the total delay is more than 60 ms but less than 90 ms then the setting should be **High**. The CPMS system will not work satisfactorily, with occasional failure of arbitration, hang time and data link layer acknowledgments, for a back-end network having a total delay of more than 90ms. The disadvantage of the setting at 90ms is that there is an increase in audio throughput delay.

4.11.3.2.2
Jitter

Jitter is the variation of packet inter-arrival time. The source repeater is expected to transmit voice packets at a regular interval (that is every 60 ms for one channel). These voice packets can be delayed throughout the back-end network and may not arrive at that same regular interval at the destination repeater. The difference between when the packet is expected and when it is actually received is called Jitter.

Jitter is the variation of packet inter-arrival time. The source repeater is expected to transmit voice packets at a regular interval (that is every 60 ms for one channel). These voice packets can be delayed throughout the back-end network and may not arrive at that same regular interval at the destination repeater. The difference between when the packet is expected and when it is actually received is called Jitter.

To overcome the effect of jitter, the CPMS system employs a **Jitter Buffer** of fixed 60 milliseconds. If a packet does not arrive at a destination repeater within the 60 ms after the expected time then the repeater assumes the packet is lost, replays a special erasure packet, and discards the late arriving packet. Because a packet loss affects only 60 ms of speech, the average listener does not notice the difference in voice quality. Thus, a jitter of more than 60 ms degrades the audio quality.

4.11.3.2.3
Packet Loss

Packet loss in IP-based networks is both common and expected. To transport voice bursts in a timely manner, CPMS systems cannot use reliable transport mechanisms (that is confirmed packets), and therefore while designing and selecting the back-end network it is necessary to keep packet loss to a minimum. The CPMS system responds to periodic packet loss by replaying either a special packet (in the case of voice) or the last received packet (in the case of data). In the case of voice, the ongoing call ends if six consecutive packets do not arrive within 60 ms of their expected arrival time. In the case of data, the repeater waits for the expected number of packets (as per the data header) before ending the call.

4.11.3.3
Back-End Network Bandwidth Considerations

Bandwidth is the amount of data transferred to and from a network device, often referred to as the bit rate. Bandwidth is measured in bits per second or kilobits per second (kbps). When designing a Capacity Plus

Multi Site system, it is important to understand the needs of each CPMS device so that the appropriately rated network connection for each site can be chosen.

If a customer has high-speed network connections between sites, these calculations may not be as important, but if they are working on lower-speed public ISPs, it is good practice to understand these values and plan accordingly. If the minimum amount of bandwidth is not available, the end-user may experience audio holes or even dropped calls. Radio-to-radio data messaging or RDAC commands may not be successful on the first attempt or may be dropped altogether. In general, the QoS may suffer if substantial bandwidth is not available.

For most ISPs, the uplink bandwidth is the limiting factor. The downlink bandwidth is usually multiple factors above the uplink bandwidth. Therefore, if the uplink requirements are met, the downlink requirements are almost always acceptable. Some ISPs may state they provide a particular bandwidth, but it is important to verify the promised bandwidth is available throughout the operation and once the system is installed. A sudden decrease in available bandwidth may cause the previously described symptoms.

If the WAN connection is utilized by other services (file transfer, multimedia, web browsing, and others), then the CPMS Connect devices may not have the appropriate bandwidth when required and the QoS may suffer. It is suggested to remove or limit these types of activities. Additionally, excessive usage of the RDAC application itself may cause increased strain on the network during times of High Voice activity. It is recommended that RDAC commands be kept to a minimum unless appropriate bandwidth has been allocated.

4.11.3.3.1
Required Bandwidth Calculations

NOTE: System Design Tool is a Microsoft Windows application used as a bandwidth calculation tool for Capacity Plus Multi Site and other MOTOTRBO systems. It is available on the Motorola Solutions Online website https://emeaonline.motorolasolutions.com

The tool allows System Administrators to put information about the CPMS system to compute the IP bandwidth required for each site. Search for Capacity Plus Multi Site Bandwidth Calculator.

4.11.4
Behaviors in Presence of Failures

A Capacity Plus Multi Site system has no centralized controller and this makes it inherently tolerant to failures. The system automatically detects most types of failures, reconfigures itself, and continues to provide the services although with decreased capacity. This section provides the consequences of the failure of one or more entities of a CPMS system.

4.11.4.1
Failure of the Master

If the Master repeater is the only static IPv4 address in the Capacity Plus Multi Site system and it fails, and then DHCP resets the dynamic IPv4 addresses of the repeaters at one of the other sites before the static master is replaced, that site loses connectivity with the rest of the CPMS system sites. When the Master repeater is replaced, the site which had IPv4 addresses reset can update the Master’s routing table and regain connectivity with the other sites.

The consequences of a failure of the Master repeater are limited. The system continues to function with the exception that it is not possible to add a new site or repeater into the system. If a repeater powers on while the Master is in a failed state, then the repeater is not able to join the system. Upon failure of the Master, it is possible to switch to a redundant repeater to act as the Master. The static IPv4 address and the UDP port number of the redundant repeater should be identical to that of the failed Master. Otherwise, all repeaters are required to be reconfigured with the new IPv4 address and the UDP port number of the new Master.

To avoid the issue of needing to have the same static IPv4/UDP address configured on both the primary and redundant Master repeaters, all of the CPMS devices can be configured to use instead of IPv4 address an FQDN (Fully Qualified Domain Name) DNS address of the Master resolved with a DNS server. The primary and redundant Master repeaters can still be configured with static IPv4 addresses, but they could be unique when an FQDN DNS address is used. If the primary Master fails, then the DNS Server could be updated such that the FQDN DNS address configured into all of the CPMS devices now maps to the IPv4 address of the redundant Master repeater. To minimize any downtime, the DNS Server should be updated immediately with the IPv4 address of the redundant Master upon detection that the primary Master has failed. The CPMS devices will determine the current IPv4 address of the Master repeater by requesting from the DNS server the IPv4 address using its FQDN. When the Master stops responding to requests from a CPMS device, the device requests from the DNS server the current Master IPv4 address.

If the address has changed, the device acquires the new address and begins using the new IPv4 address provided by the DNS server.

NOTE: The DNS feature is only available on SLR Series Repeaters.

4.11.4.2
Failure of a Site

In absence of the periodic “Keep Alive” messages between some site and the Master repeater, the Master concludes that either the Capacity Plus Multi Site device or the network in-between has failed. The Master informs all the other sites about the absence of the failed site. The system continues to provide services with the available sites. During a network failure, a CPMS system may become multiple systems, whereby each system has a subset of the original set of sites. All new systems continue to provide the services that are possible with their subset of sites. Note that there is only one system that has the Master. When the backend network recovers, the multiple systems automatically become one system again. When a system has only one site, then the system behaves like a Capacity Plus Single Site system.

4.11.4.3
Failure of a Repeater

A repeater broadcasts “Keep Alive” messages periodically over the LAN. This allows a repeater to detect the failure of another repeater at its site. A failed repeater is not selected as a Rest Channel repeater. If a Rest Channel repeater fails, a new Rest Channel is then selected by the system.

To help a radio detect the failure of a Rest Channel repeater, an inactive Rest Channel repeater periodically broadcasts a beacon over the Rest Channel. If a radio misses the beacon(s), then it knows that either the repeater has failed, or it is not within the coverage area of the repeater. Hence, the radio starts searching for a new Rest Channel.

4.11.4.4
Failure of the LAN Switch

When the switch fails, a repeater cannot connect to other repeaters at its site. Each repeater then starts working as a two-channel trunking system. At the time of the switch failure, all radios may be on the Rest Channel or busy on other channels. In the first instance, the call capacity is severely impacted while in the second, radios on different channels are unable to communicate.

4.11.4.5
Failure of the Back-End Network or Router

The failure of a router disconnects the site from the rest of the system. The failure of the back-end network may disconnect one or more sites. When a site gets disconnected, it reconfigures itself and starts operating as a single site trunked system, that is like a Capacity Plus Single Site system.

Intermittent failures of the back-end network causes packet loss or excessive delay. Such failures adversely affect wide area talkgroup calls. A wide area call may fail to start at all the associated sites. Capacity Plus Multi Site has built-in mechanisms to recover from such failures in a few seconds.

4.11.4.6
Failure of a Revert Repeater

To overcome the failure of a Revert Channel repeater, a radio makes multiple attempts to transmit a data message on different channels. If a Trunked Control Station fails, a set of radios do not receive data messages from the Application Server.

4.11.5
Automatic Reconfiguration

A Capacity Plus Multi Site system automatically discovers the presence of a new entity such as a repeater, a site, or an application PC. This new entity is configured with the IPv4/UDP address of the Master repeater. Upon power-on, the new entity informs its IPv4/UDP address to the Master and the Master informs all the other entities about the presence of the new one. Hence, this allows adding a repeater, site, or application PC to a live CPMS system. This simplifies the installation/addition of a CPMS entity as there is no need to take the system down and configure other entities with the IPv4/UDP address of the new entity.

A radio requires lists of all Trunked and Revert Channels. This makes it necessary to reprogram all the radios when a physical channel (repeater) is added to the system. If a system is to be expanded in the future, and if these frequencies are known, then it is recommended to keep all future frequencies in the trunked list. Keeping additional trunked frequencies in the radio marginally slows down the radio operations when the radio is powered on, or when the radio comes out of fade. But this prevents the need to reconfigure all the radios when new repeaters are added.

If a repeater needs to be removed from service for an upgrade or repair, there is no need to reconfigure the radios. The Capacity Plus Multi Site system can still operate. Additionally, there is no need to power down the entire system while removing or adding a repeater in the system.

4.11.6
Security Considerations

MOTOTRBO offers three types of privacy mechanisms Over-the-Air:

- Basic privacy,
- Enhanced privacy,
- AES

For more information go to Voice and Data Privacy on page 181.

In Capacity Plus Multi Site systems, a repeater does not decrypt the encrypted packets. It simply passes the packets as received Over-the-Air to other repeaters over the back-end network. Since the privacy mechanisms are not compatible, all the radios and repeaters in a system should support the same privacy mechanism. Repeaters are required to be configured with used by the radios privacy option but do not

require the privacy keys. It is important to note that the repeaters require an Enhanced privacy type to use AES privacy.

NOTE: The privacy mechanisms protect only the voice or data payloads. They do not protect the voice or data headers, nor control messages (CSBK), nor system messages (between repeaters).

A Capacity Plus Multi Site system optionally offers authentication of all the packets sent over the back-end network between repeaters and host PCs. Each packet has a 10 bytes long cryptographic signature. The signature is created using the Keyed-Hash Message Authentication Code (HMAC), which is a National Institute of Standards and Technology (NIST) standard. The hashing is done using the SHA-1 algorithm. The HMAC uses 20 bytes long symmetric keys and generates a 20 bytes long signature. To reduce the bandwidth requirement over the back-end network, the 20 bytes long signature is truncated to 10 bytes before attaching to the packet. Packet authentication prevents an attacker from using an impersonator as a CPMS device in order to get access to the CPMS system. This feature, if selected by a customer, requires manual configuration of the same key to all the entities. Note that the CPMS system does not support rekeying remotely.

The HMAC authentication mechanism does not protect against replay attacks. For a more secure authentication over the back-end network, CPMS systems should use secure VPN routers. Secure VPN routers can optionally provide confidentiality of all the messages. However, a disadvantage of using these routers is that the system requires more bandwidth on the back-end network. The use of these routers makes the HMAC authentication mechanism of CPMS redundant and should be disabled to save some bandwidth.

Another security option is Restricted Access to System (RAS). For more information go to Restricted Access to System (RAS) Design Considerations on page 469.

4.11.7
Migration

The hardware of radios is fully compatible with the Capacity Plus Multi Site configuration. Only repeaters with 32 MB of internal memory can support the CPMS configuration.

While migrating multiple IP Site Connect or Capacity Plus Single Site systems into a Capacity Plus Multi Site system, it is important to ensure that the Radio IDs, Peer IDs, and also the wide-area Talkgroup IDs are unique.

In Capacity Plus Multi Site, both the Trunked repeaters and the Data Revert repeaters have channel IDs. The range of the channel ID of a Data Revert repeater is 33 to 253.

In Capacity Plus Single Site and IP Site Connect systems, each personality of a radio has an **Rx Talkgroup List**. In Capacity Plus Multi Site, each site of radio has an **Rx Talkgroup List**.

4.11.7.1
Migrating from IP Site Connect

To migrate from one or more IP Site Connect system(s), the following tasks are required:

Procedure:

1. Update the software of repeaters.
2. Update the software of radios.
3. Reconfigure both repeaters and radios. The reconfiguration should consider the following:
   - The range of the Radio ID in Capacity Plus Multi Site is 1 - 65535 compared to 1 - 16776415 in IP Site Connect.

- The range of the configurable Talkgroup ID in Capacity Plus Multi Site is 1 - 254 (the Talkgroup ID of 255 is reserved for “All Call”) compared to 1 - 16776415 in IP Site Connect.

Result: In IP Site Connect, a call over a wide area channel is transmitted Over-The-Air at all the sites. A call over a local channel is transmitted Over-The-Air at the source site only. Capacity Plus Multi Site does not have a local channel; allowing a customer to define a talkgroup as either local or wide-area in the Master repeater. For a wide-area talkgroup, enumerating the sites where the wide-area talkgroup call will be transmitted is allowed. Restricting the scope of a talkgroup to either local or to some sites improves the channel capacity of the system. Additionally, the ID of a local talkgroup can be reused at other sites and thus effectively increases the total number of talkgroup IDs. Unlike local channels, the local talkgroups do not require a radio user to change personality before PTT.

4.11.7.2
Migrating from Capacity Plus Single Site

To migrate from one or more Capacity Plus Single Site system(s), the following tasks are required:

Procedure:

1. Update the software of repeaters.
2. If the existing radios are going to operate at one site only, then it is not essential to update the software of radios. A Capacity Plus Single Site radio continues to operate in a Capacity Plus Multi Site system, within one site, with the following restrictions:
   - A call from a Capacity Plus Single Site radio at a site is not received by Capacity Plus Single Site or Capacity Plus Multi Site radios at other sites. This implies that all the calls from Capacity Plus Single Site radios are local.
   - A Capacity Plus Single Site radio can receive a wide-area call only, but can not transmit.
   - A call from a Capacity Plus Multi Site radio is received by the Capacity Plus Single Site radios at the same site.
   - All the talkgroups used by Capacity Plus Single Site radios should be defined as local talkgroups in a Capacity Plus Multi Site system.
   - In Capacity Plus Single Site, the **Lost Detection Beacon Interval** in the radio is higher than the repeater’s. In Capacity Plus Multi Site, the **Lost Detection Beacon Interval** must be the same in both radios and repeaters.

4.11.8
Upgrade from Capacity Plus Multi Site

Repeaters running on software version R02.20.12 or later are not interoperable with repeaters running on software version prior to R02.20.12. Hence, if there is a repeater with software version R02.20.12 or later present in a Capacity Plus Multi Site system, all the other repeaters will have to be upgraded to R02.20.12 or later altogether.

When upgrading a Capacity Plus Multi Site system, upgrade the Master first, followed by all other repeaters at the Master's site. Continue to upgrade all the repeaters at a non Master site, ensuring completion of all repeaters at the site, before moving on to another peer site. During the upgrade, the Capacity Plus Multi Site system acts as two mutually exclusive systems, but calls are still supported within, just not across the two systems. Therefore wide area calls may not reach all intended sites during the migration. All radios should remain tracking the legacy system until the last legacy repeater is switched off and upgraded at its site, radios will then find the new system and operate as normal.

4.12
Digital Voting

NOTE: The MOTOTRBO digital voting is a proprietary feature introduced in R02.30.00 to resolve the imbalance inbound-outbound issue.

This section specifically documents the major control and monitor through CPS/RDAC for digital voting. Other control/monitor details can be found in corresponding CPS/RDAC manuals.

The devices affected by this feature are the repeaters, satellite receivers and radios. For repeaters and satellite receivers, there are specific voting related software upgrades and configuration changes in firmware R02.30.02. However, for radios, there is none. Any radios running on software version R01.12.02 for MOTOTRBO, R02.30.01 and above for MOTOTRBO 2.0 or later are voting enabled out of factory. For older radios, they need to be upgraded to R02.30.01 or later.

NOTE: Unless specified otherwise, the control/monitor described in this section applies to all system configurations – Conventional Single Site, IPSC, Capacity Plus Single Site and Capacity Plus Multi Site.

4.12.1
Repeater to Receiver Configuration

The satellite receiver is not a new hardware device. It reuses the MTR3000 repeater, 32 MB DR series repeater, and the MTR3000 Receiver only box. In order for these devices to be used as a satellite receiver, they must be configured in the CPS.

System	Description
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	In a Capacity Plus Single Site or Capacity Plus Multi Site system, the Rest Channel/Site IP address of a receiver is not used by the system, therefore it is not necessary to be the same Rest Channel/Site IP address in its voting repeater. Keep it simple by setting the address as 0.0.0.0, or a proper LAN address that the receiver is in.

If Enhanced GPS is enabled in the system, the receiver must not be configured as a scheduler. This means the periodic window reservation field in the “Enhanced GPS” section of the CPS must be set to “None” for both slots.

4.12.2
Enable/Disable Digital Voting

Repeaters: Voting can be enabled/disabled via CPS. When voting is disabled on a repeater, the repeater still performs as a regular repeater. However, the transmission of any call from its satellite receivers will not be accepted.

Satellite Receivers: When the device is configured as a satellite receiver, the voting capability is programmed by default. If a particular satellite receiver needs to be taken down, the user can disconnect the satellite receiver from the system, power it down or use RDAC to disable it by using the “repeater disable” option.

4.12.3
Digital Voting Status

Digital voting status is monitored through RDAC.

Repeater Voting Enabled/Disabled
This status displays whether the voting feature on a repeater is enabled or disabled.

Force Vote
This status indicates when the receiver is force voted.

Voting Status for Satellite Receivers
When voting is disabled on the repeater, RDAC does not display any voting status for its satellite receivers even if there are satellite receivers physically connected to the repeater. When voting is enabled on the repeater, RDAC then displays each satellite receiver's voting status. The repeater pushes this information to the RDAC, and the update frequency is defined by the "Voting Status Update Rate" that is configured via the RDAC. The following voting statuses are possible:

N/A
This is the default value. Before RDAC obtains any information, this value is displayed.

Disabled
The receiver is voting disabled.

Not Synced
The receiver is voting enabled but has not synchronized with the repeater. The satellite does not operate in this state. This could happen during power up, or in a congested IP connection between the receiver and the repeater.

Synced
The receiver is voting enabled. It has synchronized with the repeater, but not receiving valid OTA transmission.

Receiving
The receiver is voting enabled, and is currently receiving valid transmission, but is not the voted winner. While in this condition, RDAC also displays the signal quality estimation (SQE). The SQE result is based on the voting parameters, and is categorized as "Excellent", "Good", "Fair", "Poor", and "Bad/Rejected".

Voted
The receiver is voting enabled, currently receiving valid transmission, and is the voted winner. While in this condition, RDAC also displays the SQE based on the available voting parameters.

Voting Status for Internal Receivers (of the Repeater)
The voting repeater has a built-in receiver, and is defined as the "internal receiver". When voting is disabled, RDAC does not display its internal receiver's voting status. When voting is enabled, RDAC displays its internal receiver's voting status. The repeater pushes this information to the RDAC, and the update frequency is defined by the "Voting Status Update Rate" that is configured through RDAC. The following voting statuses are possible:

N/A
This is the default value. Before RDAC obtains any information, this value is displayed.

Not receiving
The receiver is not receiving any valid OTA transmission.

Receiving
It is currently receiving valid transmission, but is not the voted winner. While in this condition, RDAC also displays the SQE based on the available voting parameters.

Voted
It is currently receiving valid transmission, and is the voted winner. While in this condition, RDAC also displays the SQE based on the available voting parameters.

Receiver Alarm/Failures

The satellite receiver reuses repeater hardware like the alarms and failure reports. All existing repeater alarms/failure reports, except for transmit only ones, are still available for the satellite receivers.

NOTE: The satellite receiver does not transmit over the air.

4.12.4
Digital Voting Controls/Configurations

For repeaters, there is no additional voting related configuration, except enabling/disabling the voting feature.

For satellite receivers, the following controls/configurations are available:

Connected Voting Repeater/Radio ID

A satellite receiver must be connected to a voting repeater through an IP LAN or WAN. In order for the satellite receiver to operate correctly, it needs to know which voting repeater it is associated to. This can be configured by the CPS.

Force Vote/Cancel

There are situations when a particular satellite receiver or the repeater needs to be always selected as the voted winner for a period of time. For example, a critical activity near a particular receiver occurs, thus calls from that receiver need to have higher priority. This can be achieved through force vote from the RDAC. When the RDAC user force votes a particular satellite receiver/repeater, the transmission received from that particular receiver/repeater is always selected as the voted winner, and repeated until force vote is canceled, or until the force voted receiver is disconnected from the system.

Voting Status Update Rate

This controls how often the voting status of the repeater and its satellite receivers should be updated in RDAC. There are three control options:

None

The status is not pushed to the RDAC. This option reduces the traffic between the repeaters and the RDAC, thus alleviates network traffic in the system.

Normal

The status is continuously pushed to the RDAC at an interval of every three (3) seconds. This is the default value.

Diagnosis

The status is continuously pushed to the RDAC at an interval of every one (1) second. This should be used only for diagnosis purpose, because frequent status updates increase the IP traffic, and add heavy workload into the system dramatically.

Voting Log Turn On/Off

Voting log may be turned on/off for a specific voting repeater via RDAC. The update rate of the logged information is decided by the “Voting Status Update Rate”. Once turned on, RDAC logs the following voting related information for the repeater, and each of its satellite receivers:

- Repeater voting enable/disable status with PC time stamp
- Voting status of its receivers with PC time stamp
- Estimated network asymmetry and number of bursts arrived late with PC time stamp

DV Stability Factor

This is configured through CPS. This feature utilizes the crystal oscillator in the device, and the accuracy of the crystal oscillator is decided by lots of factors such as receiver device age and environmental temperature. To achieve optimum system performance, 0.5 is the best default value to handle all common situations and should not be changed. However, if constant timeslot swap due to extreme non-network environmental conditions is observed between the receiver and its voting repeater, the value can be increased to solve this timeslot problem.

Existing RDAC Controls

The satellite receiver reuses repeater hardware, like for example, repeater disable. All existing repeater controls, except for transmit only ones, are still available for the satellite receivers.

4.13 Digital Telephone Patch (DTP)

NOTE: The MOTOTRBO Digital Telephone Patch is a Motorola Solutions proprietary feature introduced in software version R01.08.00.

This section specifically documents the major configuration planning and error-prone configuration details for phone patch calls. Other configuration details can be found in corresponding CPS manuals.

NOTE: Unless specified otherwise, the configuration described in this section applies to all system configurations – Conventional Single Site, IPSC, Capacity Plus Single Site and Capacity Plus Multi Site.

4.13.1 Enable/Disable Phone Gateway Repeater for Phone Calls

When a repeater is connected to an APP box and used for phone calls, it is called a phone gateway repeater. Only phone gateway repeaters are capable of hosting phone calls. The repeater's radio ID is used as the Target ID representing the landline phone user in an individual phone call. Hence, the ID must be different from any subscriber's radio ID or other repeaters' radio ID in the system.

The phone call duration is typically longer than a regular 2-way radio voice call. If the phone gateway repeater's TOT is set to be too short, it is possible that the timer expires and causes a brief interruption during a phone call. In order to eliminate such interruption and to provide a better end-user experience, it is recommended to set the timer to 300 seconds or longer.

System	Description
IPSC IP Site Connect	The APP box can be configured to support none, one or both of the channels of the phone gateway repeater for phone calls. If the APP box needs to support phone calls on only one of the channels, this channel has to be enabled as the phone gateway, while the other channel disabled on this repeater. In IPSC, the APP box may be configured to support one of the WACs, while another APP box at a different site may be configured to support the other WAC. If the APP box needs to be used to support phone calls on both channels, both channels need to be phone gateway enabled. If the APP box cannot be used to support phone calls on either channels (although physically connected to the repeater), both channels need to be phone gateway disabled. If there is a legacy repeater (prior to R01.08.00) on a WAC, any phone capable repeater needs to be phone gateway disabled for that particular WAC, because phone calls are not supported in legacy repeaters. In IPSC LACs configurations, once a repeater channel is phone gateway disabled, no phone calls can take place on this channel. However, in IPSC WACs, there may still be phone calls on the channel hosted by an APP box from another site.

System	Description
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	Because the channels are trunked, the CPS configuration to support phone calls is at the repeater level instead of the channel level. The APP box can only be configured to support either both or none of the channels of the phone gateway repeater for phone calls. The radio ID value of the phone gateway repeater must not exceed 65535 (0xFFFF). In Capacity Plus Single Site configurations, once a repeater channel is phone gateway disabled, no phone calls can take place on this channel. In Capacity Plus Multi Site, phone calls can be received from a remote site. However, a radio can initiate the phone call only from its current site.

4.13.1.1
Conventional Single Site

The APP box can be configured to support none, one or both of the channels of the phone gateway repeater for phone calls. If the APP box needs to support phone calls on only one of the channels, this channel has to be enabled as the phone gateway, while the other channel disabled on this repeater.

If the APP box needs to be used to support phone calls on both channels, both channels need to be phone gateway enabled. If the APP box cannot be used to support phone calls on either channels (although physically connected to the repeater), both channels need to be phone gateway disabled.

In Conventional Single Site configuration, once a repeater channel is phone gateway disabled, no phone calls can take place on this channel.

4.13.2
Enable/Disable a Radio from Initiating/Receiving Phone Calls

A radio's capability of initiating/receiving phone calls can be enabled/disabled on a per digital personality basis. This is especially useful if there is a need to prevent a radio from participating in phone calls on some particular channels.

This configuration capability is done by connecting or disconnecting a phone system to the channel on the selected personality.

Conventional Single Site

If a phone system is connected to the selected Home channel, the radio can initiate/receive phone calls, Otherwise, phone capability is disabled.

System	Description
IPSC IP Site Connect	**IPSC LACs** If a phone system is connected to the selected Home channel, the radio can initiate/receive phone calls, Otherwise, phone capability is disabled. **IPSC WAC** If a phone system is connected to the selected Home channel (not the channel from the roaming list), the radio can initiate/receive phone calls from any site on the WAC. Otherwise, phone capability is disabled.

System	Description
CPSS Capacity Plus Single Site	If a phone system is connected to any channel from the channel list on the selected digital personality, the radio can initiate/receive phone calls on that channel. Otherwise, phone capability is disabled.
CPMS Capacity Plus Multi Site	If a phone system is connected to any channel of the current site, the radio can initiate phone calls. Otherwise, phone capability is disabled. However, a radio can receive a phone call if a site in the system has a phone system.

4.13.3
Enable/Disable Pre-Configured Target ID

A preconfigured Target ID may be used for each phone gateway repeater, and this capability can be enabled or disabled through CPS. Once enabled, one default Target ID can be preconfigured in the phone gateway repeater. Different phone gateway repeaters may use different preconfigured Target IDs.

4.13.4
Phone Channel Configuration

This section provides information on Phone Channel Configuration.

4.13.4.1
One APP Box per Repeater Through 4-wire Interface

In all system configurations, the physical connection for DTP is the 4-wire interface between the repeater and the APP box, which is identical to the APP configuration. The physical connection is through the repeater's GPIO connector, with the following pins:

- TX Audio – Input impedance (AC) of 560 ohms, Single-ended
- RX Audio – Single-ended
- PTT – 5 v level GPIO
- COR – 5 v level GPIO
- Ground

4.13.4.2
Single Site

When a repeater is connected to an APP box in a Single Site configuration, both channels of the repeater can be used as phone channels. The phone calls on either of these two phone channels use the same APP box that is connected to the repeater.

Since both channels are phone channels, the radio or phone user is required to specify which channel to use when initiating the call. The radio user can manually switch to the phone channel where the call starts on. The phone user can specify which channel to use when prompted for Target ID by the repeater.

4.13.4.3
IP Site Connect

IPSC

Each logical channel (either WAC or LAC) can only use at most, one APP box, and the APP box can be connected to any repeater that is part of the logical channel. One APP box may support up to two logical channels if these two channels are on the same repeater that the APP box is connected to. However, only one logical channel can be supported at a time.

Similar to the call initiation in a Single Site configuration, the radio or phone user needs to specify which channel to use when initiating the call. The radio user can manually switch to the phone channel where the call shall start on. The phone user can specify which channel to use when prompted for Target ID by the repeater.

4.13.4.4
Capacity Plus Single Site

CPSS

When a repeater is connected to an APP box in a Capacity Plus Single Site configuration, both channels of the repeater can be used as phone channels. The phone calls on either of these two phone channels use the same APP box that is connected to the repeater. In order to support phone calls, all voice repeaters in the system need to be upgraded to R01.08.00 or later.

The radio user does not select which phone channel to use when initiating a phone call because Capacity Plus Single Site is a trunked system. The system instead selects an available phone channel automatically for the call. When the phone user initiates the call, he/she calls the phone number of the APP box or PBX, but does not specify which channel of the repeater to use.

4.13.4.5
Capacity Plus Multi Site

CPMS

When a repeater is connected to an APP box in a Capacity Plus Multi Site configuration, both channels of the repeater can be used as phone channels. The phone calls on either of these two phone channels use the same APP box that is connected to the repeater. In order to support phone calls, all voice repeaters in the system need to be upgraded to R02.01.00 or later.

The radio user does not select which phone channel to use when initiating a phone call because Capacity Plus Multi Site is a trunked system. The system automatically selects an available phone channel of the local site for the call. When initiating a phone call, the phone user calls the phone number of the APP box or PBX, but does not specify which channel of the repeater to use.

The radio user can initiate an individual phone call or a local talkgroup phone call or a wide-area talkgroup phone call based upon the selected personality. When roaming from one site to another, the radio user can only initiate the phone call on the roamed site. Initiating the phone call from the local site to the phone capable repeater on the remote site is not supported in a Capacity Plus Multi Site system.

4.13.5
APP Box Configuration

The DTP feature is designed to work with most of the COTS APP boxes. The APP box installed is required to have the type approval for the region that the system is deployed. One end of the APP box is connected to the PSTN or an extension of a PBX box, while the other end is connected to a MOTOTRBO repeater through the 4-wire interface. To work with the MOTOTRBO system, the APP box is required to be configured to use half-duplex mode.

Depending on customer requirements and the type of APP boxes, the following services can be optionally configured in the APP box:

Access and De-access Codes (10 characters maximum)

- The access code is made up of an access command and a multi-digit access prefix. Nomenclature may vary based on the types of APP boxes. The access command is typically the asterisk (*) sign, but is programmable in most phone patches. The command is used to wake up the phone patch from the radio system, and is always required for most of the APP boxes. The multi-digit access prefix is used to limit radio user access and is optional. The prefix is usually up to four digits long. Some phone patches allow each prefix to be configurable to allow or block calls starting with 0, 1, 9, and so on. This essentially allows a group of radio users to have access to local dialing.
- The de-access code is made up of a normal release command and a multi-digit release code. Nomenclature may vary based on the types of APP boxes. The normal release command is typically the hash (#) sign, but is programmable in most phone patches. The command is used to hang-up the phone patch from the radio system, and is always required for most of the APP boxes. The multi-digit release code is optional, and only used to limit who can hang up a phone call when required.
- Multi-digit access prefixes and multi-digit release codes can be linked within most phone patches. This allows phone calls that are started with a particular access code to only be hung up on, with the linked de-access code. This is especially useful for Group Phone Calls since any user can attempt to hang up a phone call. Utilization of a particular access code for group calls that is linked to a de-access code most Radio Users do not have limits who can hang up on a Group Phone Call.

Phone Usage TOT

This defines the maximum duration of a phone call. If the phone call lasts longer than this timer, the APP box ends the call automatically. It is recommended to configure this timer appropriately according to the customer's phone usage.

Mobile Inactive Timer

If there is no radio activity for a period longer than the mobile inactive timer, the APP box ends the phone call automatically. It is recommended to configure this timer appropriately according to the customer's phone usage.

Go Ahead Tone

The phone user hears this tone when the radio user de-keys. If this tone is provided by the APP box, it is recommended to enable this option to improve the phone user's experience during a phone patch call.

Busy Tone Disconnect

When this APP option is enabled, the APP box ends the phone call once a PSTN busy tone is detected. It is recommended to turn on this option if it is provided in the APP box.

For further information on how to connect the APP box to the repeater, and APP box tuning details, please refer to the respective repeater service manuals.

4.13.6
Phone System Configuration

There are many phone related configurations that defines how a radio/repeater communicates with the PSTN and support phone calls in the radio system. To make the configurations easier, a data structure called

“phone system” is introduced to group and encapsulate these configurations. Because radios and repeaters act in different roles in a phone call, the configurations encapsulated in the phone system are different for radios and repeaters.

The phone system in a repeater includes configurations such as de-access code, busy TOT, and others. The phone system in a radio includes configurations such as gateway ID, access code, and others.

4.13.6.1

Radio Configuration in a Phone System

For a radio, multiple phone systems can be created and configured via CPS. The phone system defines how the radio interacts with the PSTN through a particular APP box, hence a valid phone system must have a corresponding APP box in the system. However, a radio may interact with the PSTN through an APP box in different ways. Therefore it may have more than one phone system for a particular APP box.

NOTE: If there is only one APP box in the system, but if a radio uses different access/de-access codes on different digital personalities, different phone systems can be created so each phone system has different access/de-access codes.

If a radio requires to initiate or receive phone calls on a selected digital personality, a phone system (or systems, in Capacity Plus Single Site and Capacity Plus Multi Site) must be linked to the channel (or channels, in Capacity Plus Single Site and Capacity Plus Multi Site) on per digital personality basis through CPS. The phone system linking varies according to different system configurations.

Conventional Single Site

The phone system is linked to the channel whereby the corresponding repeater is physically connected to the corresponding APP box.

System	Description
IPSC IP Site Connect	**IPSC LACs** The phone system is linked to the channel whereby the corresponding repeater is physically connected to the corresponding APP box. **IPSC WAC** If there is an APP box on this WAC, the corresponding phone system must be linked to the selected Home channel even if the phone system is physically connected to a repeater at the remote site.
CPSS Capacity Plus Single Site	Multiple phone systems may be available for a selected digital personality. A phone system is linked to the channel whereby the corresponding repeater is physically connected to the corresponding APP box.
CPMS Capacity Plus Multi Site	Multiple phone systems per site may be available for a selected digital personality. A phone system is linked to a repeater at the site whereby the corresponding repeater is physically connected to the corresponding APP box. The destination talkgroup ID of a phone-to-radio call determines whether a phone call is a wide area or a local area phone call. Note that if the destination is an individual radio, then the phone call is initiated at all sites. A radio can initiate the phone call only on its current site. A wide-area talkgroup phone call is successful when all associated sites within the talkgroup have an idle channel to host the call.

4.13.6.2
Repeater Configuration in a Phone System

For a repeater, there is one and only one repeater-wide phone system. The user is allowed to configure the phone system but not allowed to create additional ones. Additionally, only the phone system in a phone gateway repeater needs to be configured.

4.13.7
Access/De-access Code Configuration

Access and de-access codes are encapsulated in the phone system. Depending on the customer requirements and the type of APP box installed in the system, access/de-access codes may be optionally required to initiate/end phone calls. Different sets of access/de-access codes can be used for initiating/ending different types of calls (for example, long distance call, international call, etc). The codes are normally configured and supported in pairs in the APP box; if a particular access code is used to start the call, the corresponding paired de-access code must be used to end the call.

Additionally, administrator access/de-access codes may be used. The administrator codes have the highest priority, and can be used whenever access/de-access code is required. For example, the administrator de-access code can be used to end a phone call, regardless which access code was used to initiate the call.

A system may have more than one APP box installed, and these boxes may be used to simply expand the number of phone channels, or for different purposes. For example, one APP box may be used for international calls, while the other boxes to expand the number of channels. The access/de-access codes in these APP boxes may be configured similarly, or different depending on how phone privileges are assigned among the radios users. The configuration also depends on whether the codes are to be entered by the radio users, or configured in the radios.

4.13.7.1
Repeater Configuration

If a repeater is not used as a phone gateway repeater, there is no access/de-access code configuration for the repeater.

However, if the repeater is used as a phone gateway repeater, a de-access code must be configured in the repeater. This is mandatory even if the multi-digit release code part of the de-access code is not required; the normal release command part of the de-access code must be provisioned. The repeater needs the de-access code to end the phone call when the phone call needs to be ended by the radio system automatically, especially during an Emergency Alarm interrupt. Since the repeater can only hold one de-access code, this code configured in the repeater must be able to end any phone call supported by the APP box that is connected to the repeater. If the APP box supports administrator access/de-access codes, multiple sets of codes can be used in the system, and the administrator de-access code needs to be programmed in the repeater. However, if the APP box does not support administrator access/de-access codes, only one de-access code can be used for this connected APP box and the same de-access code must be programmed in the repeater.

NOTE: The APP box can still use different sets of access/de-access codes, but the de-access codes must be the same.

Otherwise, the repeater may not be able to send the appropriate de-access code to end the call when an Emergency is detected during a phone call.

Since a repeater only interacts with a connected APP box, the repeater configuration does not impact how the access/de-access codes are configured in other APP boxes in the system.

4.13.7.2
Radio Configuration

If access/de-access codes are not required for phone calls, there is no related access/de-access code configuration in the radio.

However, if required, the system can be programmed to have the codes stored in the radio and sent out automatically, or through some simple user interaction like pushing a button. Alternatively, the system can be programmed for the radio user to enter and send out the access/de-access codes manually when needed.

When the codes are configured in the radio through CPS, the radio uses the code programmed for the foreseen channel automatically, before initiating or ending a phone call on that particular channel. This process is transparent to the user. Hence, there is no restriction on the usage of multiple sets of access/de-access codes for a particular APP box, or whether different APP boxes in the system can use different sets of access/de-access codes.

When the access/de-access codes are not programmed in the radio, the code configuration in the APP box is different depending on the system configurations.

4.13.7.2.1
Single Site or IPSC Systems

IPSC

When a phone call is started, the radio user needs to select which channel to make the phone call. Therefore, the radio user knows which channel and which APP box the phone call is occurring on, hence which access/de-access code to use. In these system configurations, multiple sets of access/de-access codes can be used and the codes may differ in different APP boxes in the system.

4.13.7.2.2
Capacity Plus Single Site and Capacity Plus Multi Site Systems

CPMS

Because the phone channel is selected by the system automatically, the radio user does not know the channel information when entering the access/de-access code. Therefore, multiple sets of codes can be used in a Capacity Plus Single Site system, but they must be the same in all the APP boxes if the codes need to be entered manually by the radio user.

4.13.8
Dual Tone Multi Frequency (DTMF) Configuration

During a phone call, the phone numbers are generated and go through the system in the form of DTMF tones. These DTMF tones interact with components that are not part of the MOTOTRBO system. For example, APP, PBX, PSTN, and others. Hence, the generated DTMF tones must be compliant with the local DTMF generating/receiving standards in order for these components to receive and understand the DTMF tones generated from the MOTOTRBO system.

The following DTMF parameters are configurable both in the radio and repeater via CPS:

- DTMF Tone Duration

- DTMF Inter-Tone Delay

NOTE: DTMF Tone Level is a codeplug value, but not CPS configurable because it normally does not require change. DTMF Twist is not configurable and is always set to zero.

4.13.9
Ringing Modes

When a radio user calls a phone user, the phone keeps ringing until the phone user answers. Or, the radio user ends the call, or the call gets timed out by the PSTN.

When a phone user calls a radio user, there is only one ringing mode. The radio continues to ring until the radio user answers the call, or the call gets timed out by the repeater.

When a phone user calls a radio group (talkgroup), there are two ringing modes. These modes are configurable in the repeater through CPS. The first method is where the radio keeps ringing until one of the targeted radio users answers the call by pushing PTT and talking back. Or, the call gets timed out by the repeater. The second ringing mode is to allow the phone user to talk immediately after the first ring. The second method allows phone users to talk first during a phone call.

4.13.10
Enable/Disable Manual Dial

Manual dial allows a radio user to enter the phone number manually using the radio keypad. To prevent misuse of the phone services in the system, this manual dialing option can be enabled/disabled through CPS on a radio wide basis.

4.13.11
Connection of APP Boxes to the Repeater in Capacity Plus Single Site and Capacity Plus Multi Site

CPSM

In Capacity Plus Single Site, only the voice channel repeaters can be connected to the APP boxes to support phone calls. When connecting the APP boxes to the repeaters, it is highly recommended to connect the APP boxes to the repeaters with lowest possible rest channel priorities first. This balances the traffic on the channels. In such a configuration, the non-phone calls are likely to occur on the repeaters with higher rest channel priorities, while phone calls occur on the repeaters with the lowest rest channel priorities.

4.13.12
PBX Routing Configuration in Capacity Plus Single Site

CPSS

PBX can be used with the DTP systems. However, if a repeater is disabled, the repeater does not inform the PBX that it is disabled. In this scenario, the administrator needs to take action to ensure that the PBX does not route the incoming call from the PSTN to the disabled repeater. Otherwise, the phone user is not able to connect to the radio users.

PBX may have different priorities when PBX assigns the extension lines for incoming calls from the PSTN. In Capacity Plus Single Site, the traffic on a channel with higher rest channel priority is normally heavier

than the channel with lower rest channel priority. Therefore, if the system has two or more APP boxes, it is recommended to have the PBX route the incoming phone call first to the APP boxes that are connected to repeaters with lower rest channel priorities. As a result, this balances the voice traffic on all channels.

4.14 Transmit Interrupt System Design Considerations

Transmit Interrupt is a very powerful feature; it is capable of remotely dekeying a radio that is transmitting interruptible voice. Hence, limiting access to these features only to responsible and well-trained radio users is important.

If a radio operates on a channel that supports Direct Mode Transmit Interrupt features, then the “TX Interrupt Direct Mode Compatibility” CPS field should be enabled. This is necessary to minimize potential collisions on the channel during a Direct Mode interruptible voice transmission. This field must be enabled in the CPS; both for Direct Mode channels where interruptible voice transmissions may be present, and Repeater Mode channels where interruptible voice transmissions may be made by some radios in Talkaround Mode. However, it is not necessary to enable this field for Repeater Mode channels where Talkaround mode is not supported by any radio.

4.14.1 Interruptible Radios

The first consideration associated to the Transmit Interrupt features is determining which radios’ voice transmissions should be interruptible. For consistent behavior, the recommendation is that all radios operating on a channel should use interruptible voice transmission. However, it is desirable in some applications, to provide a small number of radios (for example, normally supervisor radios) that are not interruptible.

This sets up a system where supervisors have the ability to interrupt non-supervisor’s interruptible voice transmissions, but non-supervisors cannot interrupt supervisor’s voice transmissions, because the supervisor radios do not transmit interruptible voice. When the system is configured as such, both the supervisor and non-supervisor radios may succeed at interrupting when a non-supervisor is transmitting interruptible voice, and fails at interrupting when a supervisor is transmitting uninterruptible voice. This situation may be perceived by some users as an inconsistent experience. If the system is set up in this manner, the users should be given training on the usage of Transmit Interrupt to better understand the difference in experience.

4.14.2 Voice Interrupt

During an interruptible voice transmission, a transmitting radio periodically checks its receive frequency and determines whether another radio is requesting an interrupt. Therefore, interrupting radios must transmit their interrupt signaling when the transmitting radio is checking its receive frequency. When only one radio within a group is capable of Voice Interrupt (for example, a supervisor radio), then that radio uses one of the periodic signaling intervals to signal an interrupt request, if an interrupt is requested by the radio user.

When two radios are capable of Voice Interrupt (for example, two supervisor radios), it is possible that both radio users request a Voice Interrupt at nearly the same time (for example, during the time between two periodic signaling intervals). If this happens, it is likely that the interrupt procedure fails for both radios, due to a signaling collision that occurs during the periodic signaling interval and neither of the radios succeed at obtaining a clear channel on which to transmit.

Extending this discussion to beyond two radios (for example, additional group members configured with Voice Interrupt capability), it becomes even more likely that more than one radio user requests a Voice Interrupt at nearly the same time, resulting in a signaling collision and a failed interrupt procedure. The likelihood of more than one radio user requesting a Voice Interrupt at nearly the same time is difficult to predict or estimate,

because this depends heavily on the usage characteristic profile of a particular system, operating procedures implemented by the system administrators, and the training provided to the radio users.

Example: Some systems may provide every radio user with Voice Interrupt capability and experience no signaling collisions resulting in Voice Interrupt failures. On the other hand, other systems similarly provisioned would experience many Voice Interrupt failures. Yet other systems may provide only a few radios users with Voice Interrupt capability, but experience high rates of collisions and Voice Interrupt failures.

NOTE: Performance varies by system.

To maintain radio user experience at an acceptable level, the following suggestions can be provided when training radio users on the desired usage of Voice Interrupt on a particular system:

- Provide the Voice Interrupt capability to only radio users that need to have such capability. Minimize the number of users within a group that have Voice Interrupt capability.
- Use good radio protocol. Keep transmissions as short as possible and wait until the transmitting radio user has stopped talking and dekeyed (for example, wait to receive a Channel Free Tone) before beginning a new transmission.
- Be aware of situations near the end of a transmission when the radio user has stopped speaking, but has yet to dekey the radio.
- Create guidelines for acceptable use of the Voice Interrupt feature; define when it is acceptable to interrupt another radio user's transmission. For example, Voice Interrupt is only used when late-breaking information has become available that is critical to disseminate immediately.
- Be aware of situations where the transmitting radio user says something that may elicit an immediate reaction from the listening audience, and either curb the desire to respond immediately or allow a designated radio user (for example, a supervisor or dispatcher) to use Voice Interrupt to respond, to maintain order on the channel. Alternatively, train users to wait a short period of time before responding to the transmitting radio users.

4.14.3
Emergency Voice Interrupt

The Emergency Voice Interrupt feature is used only during emergency conditions, which are presumed to occur relatively infrequently and affect radio users individually. Based on these assumptions, it is appropriate to enable Emergency Voice Interrupt in every radio if so desired. If emergency conditions are expected to occur frequently or affect large groups of users (many radio users initiate emergency or are in an emergency condition simultaneously), then Emergency Voice Interrupt users may experience the collisions described in Voice Interrupt on page 466 and Emergency Voice Interrupt may not perform to the end users' expectations.

System	Description
CPSS Capacity Plus Single Site	In a Capacity Plus Single Site configuration, this feature is used to stop a voice transmission during an emergency based on the following two conditions: • If all channels are busy, a radio starts an Emergency Call after interrupting an ongoing interruptible call on the busy Rest Channel. • If an Emergency Call is active for the same talkgroup on channel 'c', a radio starts the Emergency Call on channel 'c' after interrupting the ongoing interruptible call.

4.14.4

Data Over Voice Interrupt

Data Over Voice Interrupt is not used by any data applications native to the radio (for example, Text Message, Location, Telemetry). It is suggested that third-party data applications only invoke the Data Over Voice Interrupt feature for the most critical of data; data that is more important than the interruptible voice transmission on the radio channel.

NOTE: This feature is only available to third-party data applications on the option board or attached PC.

It is also suggested that the third-party data application be designed to ensure that system events common to multiple radios do not result in Data Over Voice Interrupt transmissions being initiated simultaneously. These guidelines are necessary to minimize the probability of Data Over Voice Interrupt signaling requests from colliding with one another. As discussed in the Voice Interrupt section above, it is likely that the interrupt procedure fails, and none of the radios succeed at obtaining a clear channel on which to transmit, when the signaling collides.

System	Description
CPSS Capacity Plus Single Site	In a Capacity Plus Single Site configuration, a data message invokes this feature, dependent on the following conditions: ● If the radio is transmitting a voice call (either on a traffic channel or on a busy Rest Channel), the radio continues with the voice transmission. ● If the radio is on a busy Rest Channel (either listening or idling) and the data message must be transmitted on a Trunked Channel, this feature is used to stop the ongoing voice transmission. ● If the radio is listening to a voice call on a traffic channel (not on a busy Rest Channel) and the data message must be transmitted on a Revert Channel, the radio moves to a revert channel to invoke this feature. ● If the radio is listening to a voice call on a traffic channel (not on a busy Rest Channel) and the data message must be transmitted on a Trunked Channel, the radio moves to the Rest Channel to invoke this feature. However, if the Rest Channel is busy, this feature is then used to stop the ongoing voice transmission. Note that the receiving radio may be busy on another channel and there is no guarantee that the data message will be received.

In summary, a radio does not attempt to interrupt if:

- The radio is transmitting.
- The data message is for a Revert Channel.
- The Rest Channel is idle.

4.14.5

Remote Voice Dekey

The Remote Voice Dekey feature is capable of dekeying interruptible voice transmissions that the radio is either partied to, or not partied to. Alternatively, the radio user has the ability to remotely shut down a transmission that the user is not able to first monitor. Because of this, it is suggested that the Remote Voice Dekey feature be provided only to well-trained supervisors or radio technicians.

Operational procedures regarding appropriate use of this feature should be established to ensure that the user is not remotely dekeying critical voice transmissions. It is presumed that Remote Voice Dekey is not used frequently, therefore the collisions described in the Voice Interrupt section is not a major concern.

System	Description
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	In Capacity Plus Single Site / Capacity Plus Multi Site mode, a radio can always dekey interruptible voice transmissions that it is partied to; Also, it can dekey the interruptible voice transmission on a busy rest channel that it is not partied to if the radio is not participating in a call on other channel.

4.15 Restricted Access to System (RAS) Design Considerations

NOTE: This feature does not apply to Dual Capacity Direct Mode, Direct Mode or Talkaround Mode transmissions.
The RAS feature applies only to Digital, Single Site, IP Site Connect, Capacity Plus Single Site and Capacity Plus Multi Site system configurations. The usage and user experience in these systems are similar. In order to enable this system wide feature, all the repeaters in the system need to have RAS capability. This feature is software upgradeable for all MOTOTRBO 8 MB and 32 MB repeaters.

Historically, repeaters in the system were not well protected against unauthorized radio access. If an unauthorized radio user (outside of the system) wanted to utilize the repeaters for voice/data/CSBK communications, the user could have illegally programmed their radios with the system's channel information and gained access. It was not difficult to get the system's channel information – the unauthorized user could simply analyze OTA bursts, or just read the CPS configurations from any valid radio in the system.

The RAS feature is designed to prohibit unauthorized radio users from accessing the repeaters in the system. When this feature is enabled, the unauthorized radio user is restricted from using the repeaters in the system to transmit to the targeted user or user group.

This feature has no impact to the existing ADP interfaces except that the repeater notifies the relevant application when blocking of an unauthorized transmission has occurred. Further details are available in the ADP document.

This feature includes two independent methods: RAS Key Authentication and Radio ID Range Check. These two methods apply to all voice, data and CSBK calls of repeater mode. When used together, the combination provides a robust and flexible way to protect the system from unauthorized access.

4.15.1 RAS Key Authentication

In this method, both the repeater and subscriber are configured with a secret RAS authentication key. The length of the key can be 6 to 24 characters long, and may include numbers 0–9, alphabet letters A–Z, a–z, special characters like hyphen, underscore, dollar and pound signs. Similar to the enhanced privacy keys, the RAS authentication key cannot be read out through CPS or cloned from one device to another device once configured and written into the radio or repeater.

Therefore, an unauthorized user cannot see the key, nor clone more radios by simply obtaining a radio programmed with the valid key. Additionally, similar to the enhanced privacy keys, when configuring a RAS enabled radio, the user needs to remember and retype the key when writing back to the radio through CPS.

A subscriber uses its configured authentication key to encode the OTA bursts and generate a RAS enabled transmission. Upon receiving the bursts, the repeater also uses its configured authentication key to decode the bursts. If the authentication keys in the subscriber and repeater are the same, the repeater is able to decode the bursts correctly and repeat the bursts. However, if the radio does not have a RAS authentication key or its key does not match the one that is configured in the repeater, the decoding process in the repeater fails and the transmission is blocked at the repeater. Therefore, the call bursts from the unauthorized subscriber are not repeated and cannot reach the targeted user or user group.

Each system only needs one RAS authentication key, all the repeaters in a system are provisioned with only one key. To simplify the key configuration in a multi-repeater systems, the key only needs to be configured in the master repeater. Subsequently, the key is propagated to all the other peer repeaters automatically. The repeater, and eventually the system may be configured in only one of the three RAS modes:

- RAS Disabled: When the repeaters are configured in RAS disabled mode, the RAS key authentication method is not used. Hence the system supports calls from RAS disabled subscribers and legacy subscribers, including third-party compatible subscribers, but not RAS enabled subscribers.
- RAS Enabled: When the repeaters are configured in RAS enabled mode, only RAS enabled subscribers with valid keys are supported and can successfully make calls through the repeater.

  NOTE: The system must not be configured in RAS enabled mode until all the repeaters and subscribers have been upgraded to have RAS capability. Otherwise, the repeaters or subscribers that are not RAS capable will not be able to operate normally in the system.
- RAS Migration: When the repeaters are configured in the RAS migration mode, the repeater accepts both DMR transmission and RAS enabled transmission in the repeater inbound. If the inbound is DMR transmission, the repeater repeats it out as is. If the inbound is RAS enabled transmission, the repeater converts it to DMR transmission and repeats it out. Therefore, in the RAS migration mode, the system supports all subscribers including RAS disabled, RAS enabled with the valid RAS key and legacy subscribers. The RAS migration mode is recommended when installing a new system, migrating a legacy system to RAS enabled mode, or in any cases where the system needs to support both legacy and RAS enabled subscribers.
  Example: When migrating a legacy system, the administrator may first provision the key to all the repeaters and let the system to operate in the RAS migration mode. Next, the administrator could use the CPS or OTAP to provision the key to all the subscribers in the system. Since the system operates in RAS migration mode, both the legacy subscribers and the RAS enabled subscribers with the valid key can operate in the system normally and make successful calls through the repeater. After all the subscribers are provisioned with the key, the administrator can change the system to operate in RAS enabled mode to prevent any unauthorized subscribers from accessing the system. Therefore, the RAS migration mode provides smooth system installation and migration without interrupting the services.

However, a subscriber can be configured only in two RAS modes:

- RAS Enabled, or
- RAS Disabled.

When the subscriber is RAS disabled, it is not able to transmit or receive RAS enabled transmission, hence operates only in a RAS disabled or RAS migration system. When the radio is RAS enabled, it always transmits the RAS enabled bursts, but receives both DMR bursts and RAS enabled bursts. Therefore, RAS enabled subscribers can operate in RAS migration or RAS enabled systems.

A radio may operate in different systems and these systems may have different RAS keys; up to 16 keys may be provisioned and associated to different digital personalities. When a digital personality is not associated with a key, the radio is considered as RAS disabled when this personality is selected. When the digital personality is associated with a key, the radio is considered as RAS enabled, and uses the particular key that is associated. In this way, if the radio needs to operate in a different system, the radio user can select the appropriate personality with the corresponding key.

When a RAS enabled subscriber transmits in Dual Capacity Direct Mode, Direct Mode, or Talkaround Mode, it always transmits DMR bursts. However, when receiving, it can receive both DMR bursts (from other subscribers) and RAS enabled bursts (from the repeater outbound).

4.15.2
Radio ID Range Check

In this method, only the repeater needs to be configured through CPS. Up to 64 radio ID ranges may be provisioned in the repeaters. For a multi-repeater system, all the repeaters need to be software capable of the RAS feature. However, the configuration can and only needs to be done in the master repeater, and is propagated to other peer repeaters automatically.

Each of the radio ID ranges may be configured as allowed or left as un-configured. When the repeater receives a transmission from a subscriber, it checks whether the subscriber's radio ID is within any of the allowed ranges. If it is, the repeater repeats this transmission. Otherwise, the repeater blocks the transmission. In this way, the transmission from unauthorized subscriber users can be blocked.

In comparison to the RAS key authentication method, this method is much easier to use to configure and maintain the system, because only the repeater needs to be configured. However, this method has drawbacks if used alone, since the unauthorized user may figure out some allowed radio ID ranges by reading a valid subscriber, or analyzing the bursts Over-The-Air, or simply just guessing. The user can then easily program radios with radio IDs in the allowed ranges.

Additionally, the radio ID check method can only prevent the unauthorized radio from transmitting to its target, but can not prevent it from receiving while the RAS key authentication method can perform both. For this reason, it is always recommended to use both methods together. The RAS key authentication provides a very robust way to prevent unauthorized repeater access and is extremely difficult to hack. It can be used as the primary method.

Moreover, radio ID range check provides a flexible way to manage the system and make minor changes.

Example: If the system is hosting customers A, B, and C, the system administrator could provision the whole system with a RAS key and operate in the RAS enabled mode. Secondly, the system administrator could create different radio ID ranges for these three customers. If for some reason, a customer, for instance, customer B needs to be excluded from the system temporarily, the administrator could uncheck the radio ID ranges that customer B's radios fall into, and the system access of the radios in the entire range will be blocked. When customer B needs to be allowed back into the system, the administrator can simply mark these radio ID ranges as allowed.

4.16
Data Sub-System Design Considerations

The following sections describes various data sub-system configurations readers need to know before deciding how to best support the needs and usage of their customers. It continues to cover various other considerations that may need to be addressed during the design phase. It explains the IP network configurations, licensing considerations, server power management considerations, telemetry connection details, and MOTOTRBO Network Interface Service (MNIS) and Device Discovery and Mobility Service (DDMS), as a guideline for design.

4.16.1
Computer and IP Network Configurations

The data applications in a MOTOTRBO system utilize IP/UDP communications, therefore it is necessary to design the IP configuration of the data capable devices. Although complex, it is important to understand how data traffic is routed from one radio to another in a MOTOTRBO system. This section details the different connects, and where they are used within a MOTOTRBO system.

4.16.1.1

Radio to Mobile Client Network Connectivity

As described in earlier chapters, the MOTOTRBO radio connects to a computer through USB. Once connected, the PC detects the connection, loads a driver, and establishes a new network interface. This network interface looks similar to a LAN or WLAN network interface to the PC. The radio acts like a DHCP server providing the PC with an IP, and setting its own IP as the default gateway.

The Radio IP address used for this connection is programmed into the MOTOTRBO radio in the network settings of the CPS. The Accessory IP value is not editable in the CPS. It is derived based on the Radio IP. The first 3 octets are the same as the radio IP, the last octet will be the Radio IP value +1 (for example, if the Radio IP is 192.168.10.1, the Accessory IP is automatically updated to 192.168.10.2).

- Accessory IP – provided via DHCP to the Network Interface on the PC
- Radio IP – used by the Radio to communicate with the PC
  – provided to the PC as the default gateway

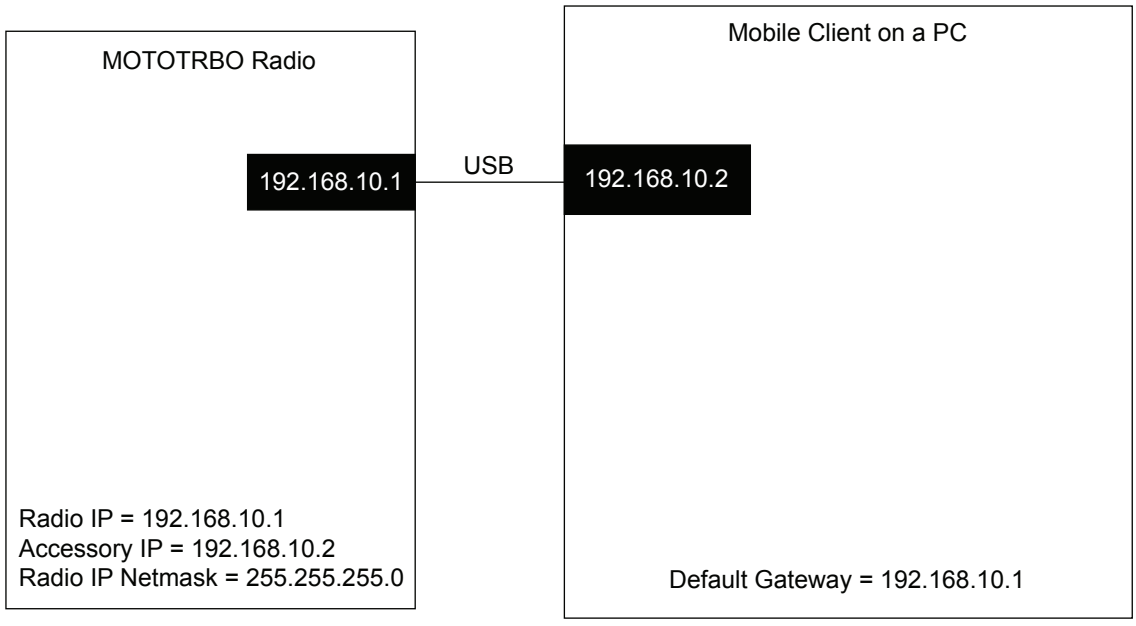
These IP addresses are only used for communication between the MOTOTRBO radio and the connected PC. It is recommended that the default values (Radio IP: 192.168.10.1, Accessory IP: 192.168.10.2) be used in all mobile client configurations. In other configurations where multiple MOTOTRBO radios are connected to one PC, these values need to be different to prevent IP conflicts.

If the default IP address programmed in the radio, or the one provided to the PC conflicts with other network interfaces on the PC, then the Radio IP should be changed using the CPS. The radio also allows for the default UDP ports for the ARS, Text Message and Telemetry applications to be changed if there exists conflict within the PC. These UDP ports are required to be updated in the application configuration as well. Again, it is recommended that the default values be used whenever possible.

For best results, it is recommended that mobile clients do not have additional network interfaces. Additional static routes may need to be manually entered in the mobile client PC if multiple interfaces are present. It is also recommended that any applications that attempt to broadcast network traffic be disabled in the PC. Unnecessary traffic sent to the MOTOTRBO radio may cause undesired congestion Over-The-Air.

The following figure displays the IP connectivity between the Mobile Client and the MOTOTRBO radio. Note that because these IP addresses are private and only used between the radio and the Mobile Client, it is recommended that they be duplicated on all Radio/Mobile Client configurations in the system.

Figure 168: Connectivity between the Mobile Client and the MOTOTRBO Radio



4.16.1.2

Radio to Air Interface Network Connectivity

The MOTOTRBO radio must have an IPv4 address to communicate with the MOTOTRBO network and other radios. The radio and the system use the Radio ID and CAI Network address to construct its Radio Network IP to ensure uniqueness. The **Radio ID** is found in the **General** section of the **General/General Settings** in the MOTOTRBO radio CPS. The **CAI Network** is found in the **Radio Network** section of the **General/Network** settings.

A Radio ID in MOTOTRBO is a 24-bit number that can range from 1 to 16776415 and is written in decimal format in the CPS.

System	Description
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	In Capacity Plus Single Site and Capacity Plus Multi Site, the Radio ID is a 16-bit number (from 1 to 65535), which can be treated as a 24-bit number where the most significant 8 bits are zero. For example, the Radio ID 64250 is represented by a hexadecimal 24-bit number as 00FAFA. When broken into three 8-bit sections, this becomes 00, FA, and FA. This in decimal is 0, 250, and 250. Therefore, a radio that is configured with a Radio ID of 64250 and a CAI Network address of 12 (the default), will have a Radio Network IPv4 address of 12.0.250.250. Below are a few more examples (all assuming the default CAI Network address of 12):

Unit ID = 00012045
Convert to Hexadecimal = 002F0D

Separate into 8-bit sections = 00, 2F, 0D

Each 8 bit section represents 1 octet of the IP address

Convert each section into decimal = 00, 47, 13

Assemble IP address from conversion above = 12.A.B.C where

A = The first 8 bit section in decimal format. In this example, A = 0

B = The second 8 bit section in decimal format. In this example B = 47

C = The third 8 bit section in decimal format. In this example C = 13

The IP address for Unit ID 12045 is: 12.0.47.13

Unit ID = 00000100
Convert to Hexadecimal = 000064

Separate into 8 bit sections = 00, 00, 64

Each 8-bit section represents 1 octet of the IP address

Convert each section into decimal = 00, 00, 100

Assemble IP address from conversion above = 12.A.B.C where

A = The first 8-bit section in decimal format. In this example, A = 0

B = The second 8-bit section in decimal format. In this example B = 0

C = The third 8-bit section in decimal format. In this example C = 100

The IP address for Unit ID 100 is: 12.0.0.100

Unit ID = 05000032

Convert to Hexadecimal = 4C4B60

Separate into 8-bit sections = 4C, 4B, 60

Each 8 bit section represents 1 octet of the IP address

Convert each section into decimal = 76, 75, 96

Assemble IP address from conversion above = 12.A.B.C where

A = The first 8-bit section in decimal format. In this example, A = 76

B = The second 8-bit section in decimal format. In this example B = 75

C = The third 8-bit section in decimal format. In this example C = 96

The IP address for Unit ID 05000032 is: 12.76.75.96

The MOTOTRBO data applications, both in the radio and externally on the PC, perform this conversion to an IPv4 address when sending and transmitting. Understanding this conversion is important because it is possible to send traffic directly to the IPv4 address of the radio, though in most cases this happens transparently to the user. For example, if a user creates a text message, and selects a user from the address book with an Individual Radio ID of 12045 (which can be aliased), the text message is sent Over-the-Air to radio with ID 12045 and is addressed to IPv4 address 12.0.47.13. When a radio with ID 12045 receives the Over-the-Air data message, it opens the data message and looks at the target IPv4 address. Because the target IPv4 address matches its own IPv4, the message is sent to the internal radio application. The target application is dependent on the UDP port number and the destination address used at the source.

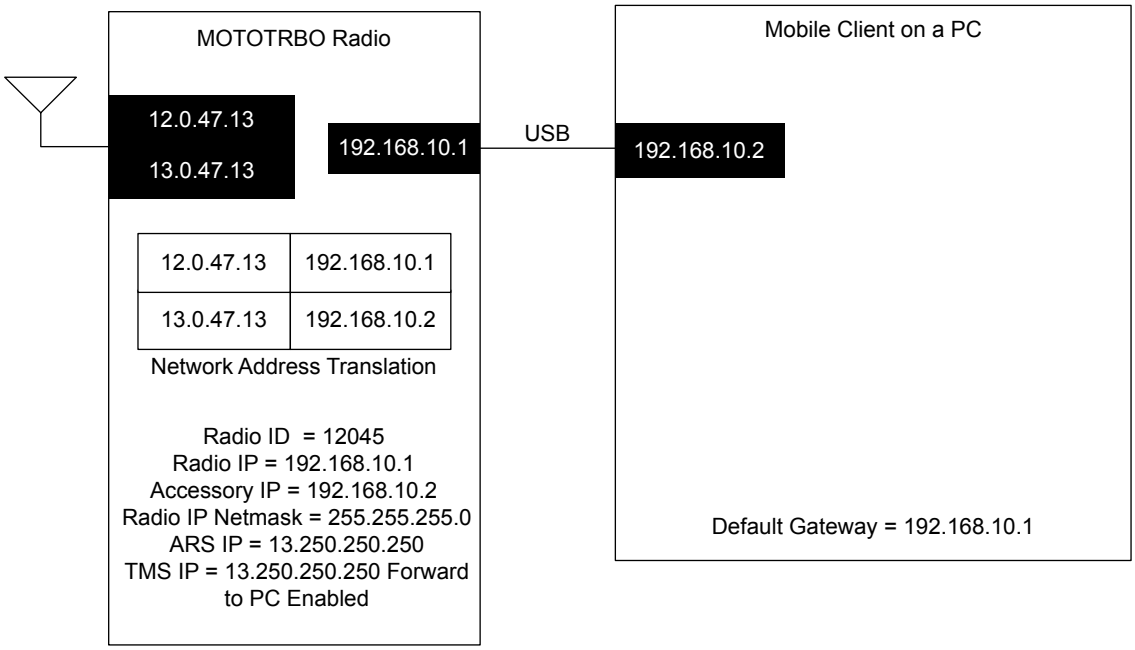
If the target of a data message is an external PC connected to the MOTOTRBO radio, the sending device uses as destination an IPv4 address with the CAI Network plus 1. For example, if a MOTOTRBO radio receives a data message for its Radio ID 12045 (IPv4 address 12.0.47.13), and the data message inside is targeted towards the address 13.0.47.13, it forwards that message to the connected PC.

For ease of use, the MOTOTRBO radio has the option to be configured with a **Forward to PC** parameter, which is available in the **Radio Network** section of the **General/Network** settings in the MOTOTRBO radio CPS. With this option enabled, all messages targeted to both the 12.x.x.x and 13.x.x.x addresses are routed to the PC. It is recommended that this option be chosen whenever a MOTOTRBO radio is connected to the Application Server. The **Forward to PC** parameter also applies to a MOTOTRBO radio (portable or mobile) installed in a mobile environment, such as a vehicle, or a fixed location (a mobile in a tray located on someone's desk). If a radio is not connected to an external PC, the **Forward to PC** parameter should be disabled.

It is recommended that the default value of the **CAI Network** be used. If this value is changed, all MOTOTRBO radios in the system must be updated with the same **CAI Network** parameter. Also available for configuration is the **Group CAI Network** parameter. This is used for broadcast data messages. Again, it is recommended that this value remains at its default value.

Figure 169: Air Interface Network Connectivity on page 475 displays the IP connectivity with the radio network. Also included is a simplified network address translation (NAT) table that shows how the Over-the-Air traffic is routed to either the Radio or the Mobile Client. The NAT is a translation table within the MOTOTRBO radio that allows packets to be routed from the PC through the radio and Over-the-Air to the destination address. As previously mentioned, when the **Forward to PC** parameter is set, traffic for both the 12.x.x.x and 13.x.x.x addresses is forwarded to the PC. If disabled, that NAT table would show the 12.0.47.13 traffic being routed to **Radio IP** of 192.168.10.1. This is the common configuration for MOTOTRBO radios that are not connected to an external Mobile Client.

Figure 169: Air Interface Network Connectivity



4.16.1.3

Application Server to Control Station Network Connectivity

In some system topologies described in previous sections, the Application Server is required to service up to 16 different channels. This requires the Application Server to have a network connection of up to 16 Control Stations at the same time. Similar to the Mobile Client configuration, when each Control Station is connected to the Application Server through a USB, a network interface is created for each. Each interface is provided with the IPv4 address configured as the **Accessory IP** in each Control Station. It is important that the **Radio IP** and the **Accessory IP** of the 4 Control Stations be different from each other to prevent IPv4 conflict and therefore routing problems in the Application Server. The following IPv4 configuration (for 4 Control Stations) is recommended:

Table 87: IPv4 Configuration

	Radio IP	Accessory IP/PC Network Interface IP
Control Station 1	192.168.11.1	192.168.11.2
Control Station 2	192.168.12.1	192.168.12.2
Control Station 3	192.168.13.1	192.168.13.2
Control Station 4	192.168.14.1	192.168.14.2

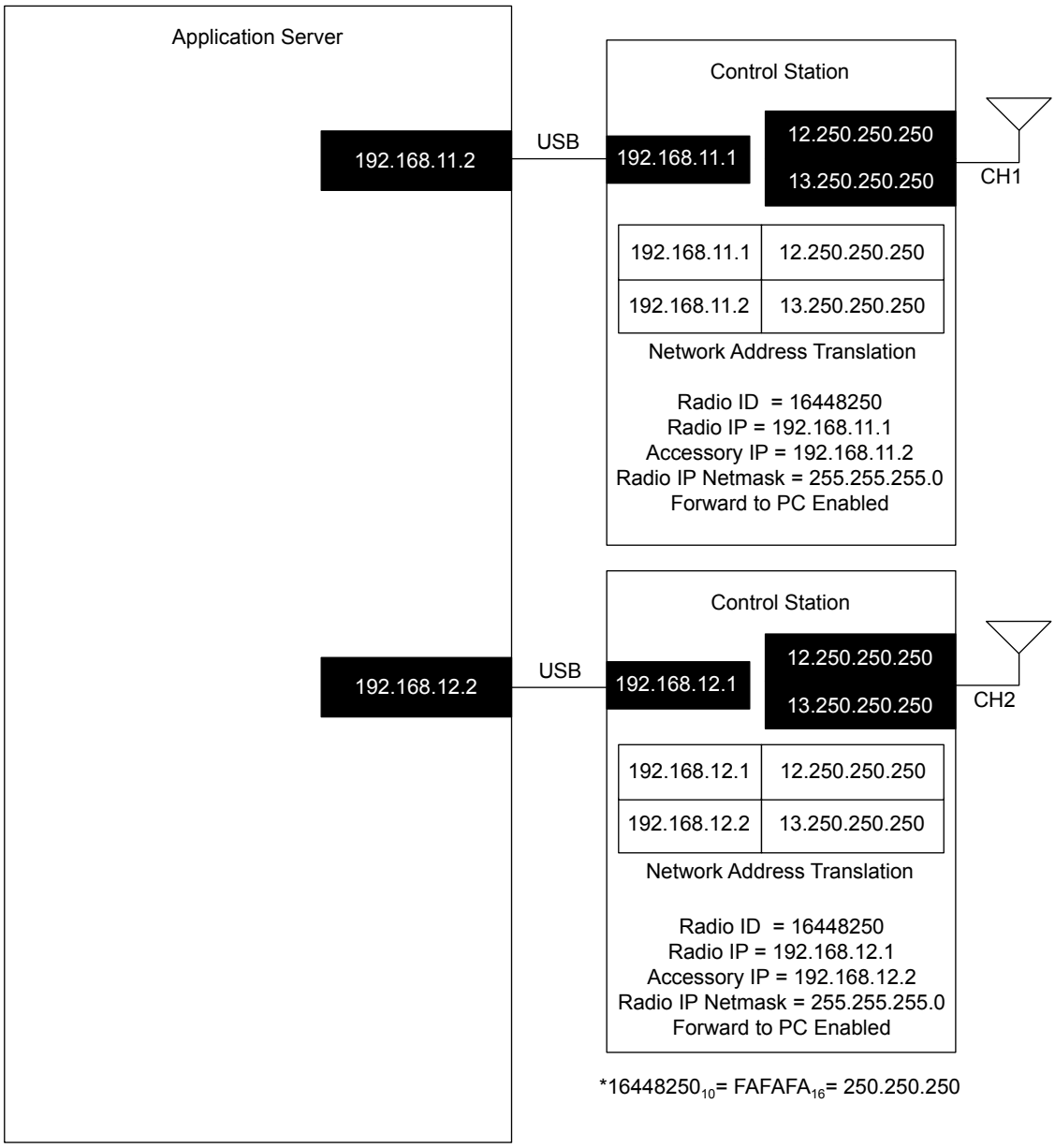
The Radio ID, and therefore the Radio Network IPv4 address, is very important when configuring the Application Server Control Stations. Unlike the **Radio IP** and **Accessory IP**, the Control Station's Radio Network IP should be identical. Each Control Station should be programmed with the same Radio ID, to enable field radios to communicate with the Application Server regardless of what channel they are on. Although it was mentioned that MOTOTRBO radios should not have duplicate Radio IDs, the Control Stations are the exception. Because Control Stations are intended to remain on a single channel, they will always be monitoring the same channel. Although this Radio ID of the Control Stations can be any valid Radio ID, they must be unique, and not duplicate any non-Control Station Radio ID. The suggested Radio ID for the

Control Stations is 16448250 which converts to an easy-to-remember IPv4 address of 12.250.250.250 and 13.250.250.250. Since this Radio ID is so large, it is unlikely to be duplicated on other radios.

NOTE: For Capacity Plus Single Site and Capacity Plus Multi Site systems the suggested Radio ID for the Control Stations is 64250 which converts to an easy-to-remember IPv4 address of 12.0.250.250 and 13.0.250.250.

It is important to note that every MOTOTRBO radio in the system that is intended to communicate with the Application Server must be programmed with the Application Server Control Station IPv4 address. This value must be entered for both the Automatic Registration Service **ARS IP** and the Text Message Server **TMS IP**. Those values are not editable because they are automatically calculated from configured **ARS Radio ID** and **TMS Radio ID** parameters, which can be found in the **Services** section of the **General/Network** settings in the MOTOTRBO radio CPS. Because the Application Server is the target for these messages, the 13.250.250.250 IPv4 address should be programmed into every field radio. For radios that will use the Mobile Text Messaging Client application installed on a PC connected to the radio, the 13.250.250.250 IPv4 address should also be programmed into the application.

Figure 170: Application Server to Control Station Network Connectivity



As previously discussed, the Control Stations should be configured with the correct option of the **Forward to PC** parameter, which can be found in the **Radio Network** section of the **General/Network** settings in the MOTOTRBO radio CPS. This forces all data traffic the Control Station receives to be forwarded to the Application Server.

4.16.1.4

Control Station Considerations

Because the Control Stations connected to the Application Server act as the data gateway for the system, the Control Stations themselves do not require an Automatic Registration Service **ARS IP** and the Text Message Server **TMS IP** to be specified in their CPS **General/Network** settings. These fields should be left blank. In addition, the Control Stations should also have the **ARS Monitoring ID** and **GNSS** options disabled. These

settings are not required for these Control Stations since they will not be transmitting their own GPS or ARS anywhere. There is no need for these Control Stations to be ordered with GPS capability.

Although it is possible to use the Control Stations connected to the Application Server for voice, it is highly recommended that they only act as data gateways. Since Control Stations (except for Trunked Control Stations) must remain on a single channel in order to receive the inbound data, it is recommended that they only contain one channel in their channel list. The Trunked Control Stations must have a list of all Trunked Channels. Control Stations should not have scan enabled. This guarantees that the Application Server is always monitoring the correct channel. Since the Control Stations are only used for data, there is no need to program any **Rx** or **Tx Groups** on the channel. In other words, the **Contact Name** and the **Group List** can both be set to a value of **None**. Similarly, it is not necessary to provision any emergency settings either.

It is important to set the **TX Preamble Duration** of the Control Station to be the same as the other radios in the system. Since most data is targeted towards these Control Stations, the proper preamble must be utilized. Use the same guidelines for setting this duration in the Control Stations as was used in the fielded radios.

The admit criteria of the Control Station should match the settings for which the other radios on the channel are provisioned. The suggested setting is **Color Code Free** unless there are signals on the channel that the data needs to avoid. If there are signals on the channel that the data needs to avoid, then choose **Channel Free** instead.

When considering other CPS options of the Control Station, it is a good rule of thumb to minimize the feature options available. This guarantees that a user cannot accidentally place the Control Station in a state where it is not monitoring inbound data traffic.

In almost all scenarios, it is highly recommended that a mobile radio with an AC power adapter be utilized as the data gateway. Although a portable radio can temporarily be used for this purpose, it is not recommended for long-term installations. The primary reason why a mobile radio is recommended for this purpose is its ability to install the external RF antenna. This is important since computers and their components are sometimes sensitive to RF power. External antennas should be located away from the server itself and isolated from each other. For example, if a server has 4 Control Stations connected to it, it is recommended that the antennas be installed on the roof of the building and separated enough from each other so that they do not interfere. This is also important since inside the building coverage is sometimes difficult to achieve. All inbound data messages pass through these Control Stations so it is important that they are within good RF coverage of the repeater. Additionally, a Control Station is left powered on all the time. A portable radio continuously powered on in a charger is more likely to encounter power-related failures.

In conventional systems, if a Control Station’s power off or a power cycle occurs; host-specific routes are removed from the Application Server's routing tables. In these situations, the Application Server to radio data increases the system load as it has to be transmitted by all connected Control Stations. The actual load increase is based on the amount of Application Server to radio data. This load increase gradually dissipates as the radios re-register with the Presence Notifier and the host-specific routes are added back into the routing table. However, it is recommended to connect Control Stations to an Uninterrupted Power Supply (UPS) and never power them off and on while radios are registered with the Presence Notifier.

In trunked systems, if a Revert Control Station powers down, then the radio to the Application Server data increases the load on the rest of Revert Control Stations. When the failed Revert Control Stations power on, the load is automatically distributed on all the Revert Control Stations. If a Trunked Control Station powers down, then the Application Server is unable to send data to the radios allocated to the failed Trunked Control Station. Therefore, it is recommended to connect Trunked Control Stations to an Uninterrupted Power Supply (UPS) or to have redundant Trunked Control Stations.

During the registration process with the Presence Notifier, the radio is instructed to refresh its registration at a specific time interval. The default time interval is 4 hours, though this is a configurable parameter in the Presence Notifier. If the time interval is decreased, more registration messages are sent to keep the Presence availability information fresh but the system load is increased. If this time interval is increased, the system load is decreased but the Presence availability information may become stale.

If for some reason the host-specific route does not exist, then the global route is used and the data message is transmitted through all Control Stations connected to the Application Server. This scenario increases system loading during situations where there is an Application Server to radio data. An example of this would be network (Text Message Server) sourced text messages targeted towards subscribers in the field.

4.16.1.5
Required Static Routes

CPSS

In conventional systems, the Application Server can have up to 16 different network interfaces that access the radio network.

In order for data messages targeted towards Radio Network IP addresses, such as 12.0.0.1 and 12.0.47.13, to transmit out through a network interface with IP addresses 192.168.11.2 or 192.168.12.2, a static IPv4 route is required to be manually entered in the PC for each radio that registers with the Presence Notifier. For example, when radio 12045 transmits a registration message to its programmed ARS IP address (for example, 12.0.47.13) on one of the channels monitored by a Control Station, the Control Station forwards that address to the Application Server through its network interface (for example, 192.168.11.2). Then manually adds a route for that radio IP (12.0.47.13 and 13.0.47.13) to the 192.168.11.2 network interface. Once that is done, if a message from the Application Server needs to reach 12.0.47.13 or 13.0.47.13, the message is routed to the 192.168.11.2 network interface, and therefore out the correct control station and correct channel that has registered radio 12045. This is how data messages are sent out on the correct channel for a radio.

Additional steps are required to route multicast traffic. Multicast traffic is traffic destined for radio groups. The routing table in the PC must be modified to allow for multicast traffic.

NOTE: Multi-Channel Device Driver (MCDD) has not been maintained and supported.

4.16.1.6
Application Server and Dispatcher Network Connectivity

As described in previous sections, the Application Server can also be configured with a LAN connection to the Customer Enterprise Network (CEN). A few restrictions apply to the network configuration between the Application Server and the Dispatch clients. In most customer cases, the LAN interface on the Application Server is connected to their pre-existing network. The only requirement is that the assigned IP of the LAN network interface must not conflict with those assigned to the Network Interfaces of the Control Stations. Additionally, the Application Dispatchers (such as Location Dispatch or Text Message Dispatch) must be connected through the customer CEN to the Application Server. In order for the Text Message Server to forward e-mail text messages, the Application Server must be connected to the Internet. If the network is configured to operate with a firewall, the programmed ports for the applications should be opened and allowed. Details of this configuration can be found in the Text Message and Location Application install guides.

4.16.1.7
MOTOTRBO Subject Line Usage

A MOTOTRBO Text Message is comprised of three parts: A subject line, subject line delimiter and body. The subject line delimiter is a carriage return (Unicode code point U+000D) and line feed (Unicode code point U+000A) character pair (CRLF). Therefore, anything up to the first CRLF within the Message is interpreted as the subject line and anything after the first CRLF is interpreted as the body. The subject line is left blank if there are no characters before the first CRLF, or if no CRLF pairs are contained in the Message.

When e-mail text messages are received by the Application Server the e-mail subject line and body are converted into the MOTOTRBO Text Message subject line and body respectively.

The maximum length of a MOTOTRBO Text Message is technically 280 (140 for Matrix radio) characters according to the protocol. However, applications that support the use of Subject Lines may reduce the number of the effective payload. The Customer Programming Software (CPS) and the applications in the radios that create text messages limit the effective payload to 278 (138 for Matrix radio) characters. External applications that run on Personal Computers (PC) may further reduce the effective payload to provide indications that messages have been truncated (for example replacing the last character with a horizontal ellipse character '…'). E-mails that are longer than 278 (138 for Matrix characterizers) are truncated to fit. For example, if an e-mail is received with a 200 character subject line and a 300 character body only the first 277 (137 for Matrix radio) characters of the subject line plus a horizontal ellipse '…' at the end is converted into the MOTOTRBO Text Message and the rest of the e-mail is discarded. In another example, if an e-mail is received with a 100 character subject line and a 300 character body, then the 100 characters of the subject line and the first 177 (37 for Matrix radio) characters of the body with an ellipse added at the end is converted into the MOTOTRBO Text Message format.

Radios replying to messages preserve the original message's subject line. In this manner, external services and solutions that use e-mail for communication can use the content of the subject line to correlate between e-mails that are sent and e-mails that are received. For example, an automated service could send out an e-mail with a unique ID string in the subject line. If a radio replies to the message, it preserves the subject line with the unique ID string and the automated system can use the address and subject line of the message to know that a specific unit had replied to a specific message.

The number of characters allowed in a reply by a radio are equal to 278 (138 for Matrix radio) characters minus the number of characters in the subject line. For example, if an e-mail is sent with a 30 character subject line and a 100 character body, the entire message is received by the radio. When the radio replies to the message the subject line is automatically preserved leaving 248 (108 for Matrix radio) characters for the radio to reply with.

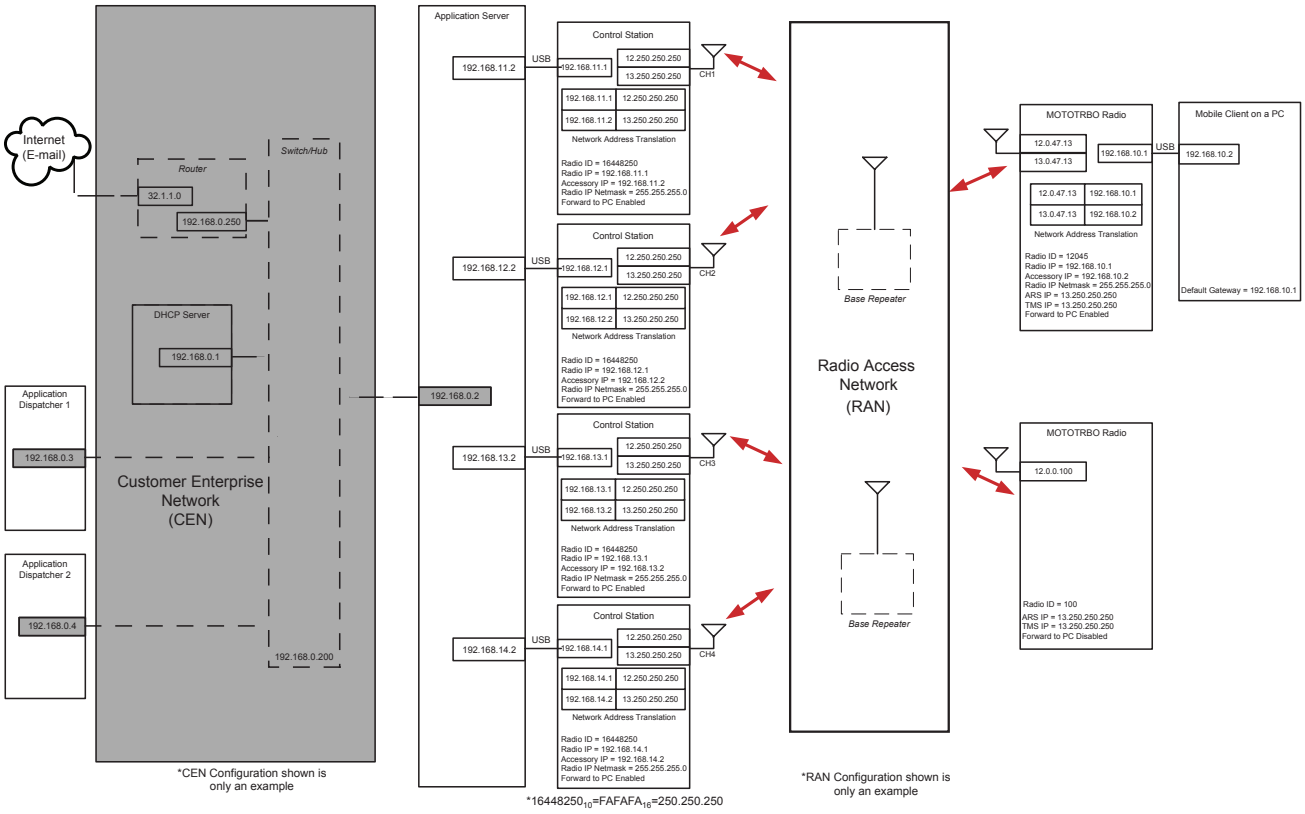
MOTOTRBO Text Messages that originate from the front panel of radios or the Text Messaging Client through the Application Server and destined for e-mails addresses contains blank subject lines. Radios do not have the capability to create or modify a subject line from the front panel. The CPS does not have the capability to create a subject line.

4.16.1.8

MOTOTRBO Example System IP Plan

The following diagram is an example of the information contained in the previous sections. This diagram shows a configuration of multiple digital repeaters at a single site functioning in conventional repeater mode. It should be used as a guideline for configuring a MOTOTRBO System.

Figure 171: Example MOTOTRBO System IP Plan



4.16.1.9

Application Server Network Connection Considerations

Besides being connected to the radio network via the Control Station(s), the Application Server may also be connected to another network such as the Internet. When operating under these conditions, it is important to consider the following:

- Disable all protocol support except for TCP/IP.
- Ensure networking application messages are routed to the Ethernet connector or the wireless network interface and not to the network connection to the Control Station(s).

Sometimes, the Application Server is connected to the radio network via the Control Station(s). When operating under these conditions, it is important to remember that all network traffic generated by the Application Server is routed to the control station(s). In order to optimize the radio network, these messages should be kept to a minimum. The following items should minimize the amount of network traffic being routed to the Control Station(s).

- Disable all protocol support except for TCP/IP.
- Turn off the PC wireless network interface.
- Do not launch any networking application (internet browser, e-mail, and others).

- Disable all automatic updates for network applications that are running in the background; such as virus updates, IM updates, Windows updates, and others.

4.16.1.10

Reduction in Data Messages (When Radios Power On)

When a radio powers on, up to eight data messages are exchanged between the radio and the Server. This may cause congestion in the channels if many radios are powered on within a short duration. The situation worsens if one or more data messages are lost due to the overflow of queues or poor RF transmission conditions. A loss of message causes multiple retries both at the Data Link and Application layers. These additional messages cause further congestion of the data channels.

An example of a use case where a set of mobile radios are powered on within a short period is a Bus Depot. Buses have mobiles to facilitate the tracking of buses from a central location. The MOTOTRBO mobiles have built-in GPS receivers that send the location of a bus periodically. Generally, the buses leave the depot within a short period of each other. All the mobiles in the buses may power up within this period, jamming the channels and hence delaying the registration of mobiles. In this case, the locations of buses are not available at the central location until the registration process completes successfully.

MOTOTRBO provides two mechanisms to reduce the number of data messages triggered by powering a radio. The total reduction is up to one fourth of the original number of messages exchanged between a radio and the Server, i.e. the number of data messages reduces to two. The two mechanisms are described below.

The presence of a radio triggers a Text Messaging application to send a message to the radio. This message is called the Service Availability message and it contains the IP address of the Text Messaging application and the services offered. To reduce the number of Service Availability messages, a customer should do the following:

- Pre-configure the radio with the IP address (as seen by the radio) of the Text Messaging Server using CPS.
- Configure the Text Messaging application not to send the Service Availability message when the radio powers-on.

In the absence of the Service Availability message, a radio uses its preconfigured values for the IP address of the Text Messaging Server. If the Text Messaging Server sends the Service Availability message, then the radio overwrites its values with the values from the received message and stores it persistently. The persistent storage of IP address avoids the need to send the Service Availability message if the IP address of the Text Messaging application remains the same. Upon change of the IP address, a customer should enable the Text Messaging application to send the Service Availability message. Once all the radios have received the Service Availability message, the customer can disable the sending of Service Availability messages.

The presence of a radio also triggers the Location Application to send two requests to the radio: one for location update on emergency and the other for periodic location updates. To reduce the number of messages, the radio saves the requests persistently and the Location Application allows the customer to enable/disable the transmission of the requests, when a radio registers its presence. It is not possible to configure requests in a radio using CPS. A radio without requests should undergo an initialization process. During initialization, the Location Application sends the required location requests to the radio. A radio needs to be initialized only once. If a customer needs to change the IP address or the UDP port number of the Location Application, then the Location Application should delete the requests from all the radios before it changes its address. As it is not always possible to satisfy the above condition, MOTOTRBO provides an alternative to delete all the requests in a radio using the CPS.

NOTE: This feature was introduced in software version R01.05.00. Text Messaging and Location Applications compatible with older software versions may not support this feature. All customers are encouraged to verify their applications for feature compatibility.

4.16.1.11

Optimizing for Data Reliability

It is important to exercise care when optimizing voice quality in two way radio systems such as MOTOTRBO. This commonly consists of verifying if the RF signal, both inbound and outbound, is adequate enough in the desired areas to provide an acceptable level of voice quality. The radius from the transmitting tower that yields the acceptable level of voice quality is often referred to as the coverage of the system. On the fringe of this coverage, voice quality may experience degradation due to errors.

The human mind (with help from the vocoder) can mitigate the loss of a few random syllables of speech and still understand the intended meaning of a spoken sentence. However, when attempting to deliver data to the radios on the fringe, a data application cannot usually just ignore a few errors and still understand the full message.

It is important to understand that there is a probability that data incurs an uncorrectable error when received at particular signal strength, known as Block Error Rate. As the amount of data to be transmitted increases, there is an increasing probability the data message has an error. Because of this, it is more difficult to deliver a long data message without errors to the fringe than a short data message. Another way of looking at this is a short data message can be delivered farther away without errors than a long data message.

To optimize data for reliability, the user should:

- Use confirmed individual data
- Minimize application data payload size
- Disable UDP header compression
- Enable enhanced channel access

4.16.1.11.1

Use Confirmed Individual Data

MOTOTRBO radios can be configured to send individual data messages confirmed or unconfirmed at the link layer. Group data messages (those targeted towards talkgroups) are always sent unconfirmed. If sending long data messages, it is always recommended to use individual confirmed messaging to achieve the best reliability.

When data is sent unconfirmed, the radios send their data messages to the target without any link layer confirmation that it arrived successfully. When sending very short data messages, such as GPS, this method may be acceptable since short messages have a lower probability of arriving with uncorrectable errors. However, as previously described, long data messages have an increased probability of failure at the fringe. It is important to note that sending long unconfirmed data messages multiple times at the application layer only slightly increases the overall probability of success, since each retry is as long as the first attempt, and therefore has the same probability of failure.

When data is sent confirmed, the radios send their data messages to the target with confirmation that each segment within the data message arrived successfully. If one or more of the segments within the data message was received with an uncorrectable error, the target responds to the source requesting only the segments that had uncorrectable errors be resent. This is referred to as selective retries. Because retries are shorter, they have fewer segments than the original attempt and the probability of success increases. This increases the overall success rate of delivering long data messages to radios in the fringe.

NOTE: In software versions R02.20.00, an additional enhancement was made to the selective retry mechanism that increases the probability of success of individual confirmed data messages even more. Therefore, it is recommended to upgrade for best reliability.

4.16.1.11.2
Minimize Application Data Payload Size

Some data applications may allow the size of their data messages sent Over-The-Air to be configured. This is sometimes referred to as their message fragmentation size. For best reliability, it is recommended to utilize a message size less than, or equal to 256 bytes Over-The-Air. Data messages longer than 256 bytes may have decreased coverage even when utilizing confirmed messaging.

4.16.1.11.3
Disable UDP Header Compression

MOTOTRBO radios can be configured to perform UDP header compression. This feature reduces the 28-byte UDP/IPv4 headers to four or eight bytes, but it requires an extra link layer header. The net effect is the saving of 60 milliseconds for confirmed messages, or 120 milliseconds for unconfirmed messages. For short data messages, such as GPS, this approximately reduces the transmission time by 10% to 20%. However, for longer data message (256 bytes), the savings in transmission time is very small and the extra header can decrease reliability in some instances.

Therefore, for best reliability, it is recommended to not utilize UDP header compression when transmitting long data messages since the decrease in reliability is not worth the 60 to 120 milliseconds savings in delivery time of a long data message that may take seconds to complete.

4.16.1.11.4
Enable Enhanced Channel Access

MOTOTRBO radios can be configured to utilize Enhanced Channel Access. Enhanced Channel Access can minimize the number of collisions between radios transmitting data by performing a high speed handshake with the repeater. The high speed handshake takes approximately 120 milliseconds to complete. Collisions can result in both data messages becoming corrupt and therefore requiring each to retransmit. When ECA is enabled on all radios, collisions are detected and mitigated by allowing one radio to gain access to the channel, while the other is held off. Therefore, it is recommended to enable ECA for best reliability.

4.16.1.12
Optimizing for Data Throughput

If utilizing data applications that only send short data messages to radios in great RF coverage, the user might wish to optimize for data throughput since reliability is not a primary concern. An example of this might be the GPS. Rather than utilizing extra bandwidth sending short messages reliably, it may be more useful to minimize the size of the message even more so that messages can be sent more often. The loss of one GPS message is of little concern if another updated message shortly follows.

To optimize data for throughput when sending short messages in great RF coverage, the user should:

- Use unconfirmed individual data
- Enable UDP header compression
- Disable enhanced channel access
- Disable scanning and lower scan preamble
- Minimize battery saver preambles

4.16.1.12.1
Unconfirmed Individual Data

MOTOTRBO radios can be configured to send individual data messages confirmed or unconfirmed at the link layer. Group data messages (those targeted towards talkgroups) are always sent unconfirmed. If

sending short data messages, and if optimizing for throughput, the user should consider using unconfirmed messaging.

When data is sent unconfirmed, the radios send their data messages to the target without any link layer confirmation that it arrived successfully. If the message size is less than 144 bytes (in repeater mode) or 48 bytes (in Talkaround mode), then unconfirmed data messages have lower transmission time Over-The-Air than confirmed data messages.

Short messages have a low probability of arriving with unrecoverable errors. However, as previously described, long data messages have a higher probability of arriving with unrecoverable errors. Therefore sending long messages unconfirmed is only successful to radios within great RF coverage. It is also important to note that sending long unconfirmed data messages multiple times at the application layer only slightly increases the overall probability of success since each retry is as long as the first attempt, and therefore has the same probability of failure.

NOTE: If there are radios with software versions prior to R01.05.00 in the system, and receiving individual data messages from newer radios, the newer radios should be configured to use confirmed individual data messages only, to avoid interoperability issues.

4.16.1.12.2
Enable UDP Header Compression

MOTOTRBO radios can be configured to perform UDP header compression, which reduces the 28-byte UDP/IPv4 headers to four or eight bytes, but requires an extra link layer header. The net effect is the saving of 60 milliseconds for confirmed messages or 120 milliseconds for unconfirmed messages. For short data messages, such as the GPS, this approximately reduces the transmission time by 10% to 20%. If sending short data messages in great RF conditions, and if optimizing for throughput, one should consider utilizing UDP header compression.

A Control Station or a radio sends compressed data messages only if the feature is enabled, but processes compressed data messages even if the feature is disabled. A non-MOTOTRBO radio or a legacy MOTOTRBO radio with software versions prior to R01.05.00 cannot receive compressed data messages and therefore this feature should be enabled in a Control Station only if all the radios in the system are MOTOTRBO radios with software versions R01.05.00 or later. This feature can be enabled in a Control Station or a radio selectively for data messages transmitted to one or more applications, that is based on the destination UDP port.

4.16.1.12.3
Disable Enhanced Channel Access

MOTOTRBO radios can be configured to utilize ECA. The high speed handshake takes approximately 120 milliseconds to complete. If optimizing for throughput, one should consider disabling ECA.

Enhanced Channel Access can minimize the number of collisions between radios transmitting data by performing a high speed handshake with the repeater. Collisions can result in both data messages becoming corrupt and therefore requiring each to retransmit. When ECA is disabled, high volume asynchronous messages from radios collide often, and if utilizing confirmed messaging results in both devices retransmitting, which ultimately results in lower throughput. If utilizing a synchronized data delivery method, for example a request and reply method from a centralized server, collisions may not occur as often.

4.16.1.12.4
Disable Scanning and Lower Scan Preamble

MOTOTRBO radios can be configured to utilize a data preamble, primarily utilized to reach scanning radios. The default value is 960 milliseconds, but can be configured substantially higher. When utilizing unconfirmed messaging, the data preamble adds to the overall length of each message. If utilizing confirmed messaging, the data preamble is added to retransmissions only.

If optimizing for throughput, one should consider disabling scan and lowering the scan preamble to zero. If there are scanning radios remaining, and a data preamble of the transmitting radio is set to zero, the scanning radios will most likely not receive the message.

If only sending data from fielded radios to a centralized data application, it is presumed the Control Stations that are receiving the messages are not scanning. Therefore data preambles are not required on fielded radios.

4.16.1.12.5
Minimize Battery Saver Preambles

MOTOTRBO radios can be configured to send battery saver preambles. These preambles are used to reach radios that have battery saver enabled. If optimizing for throughput, one should consider disabling battery saver and disabling sending battery saver preambles. For a typical location message, this approximately reduces the transmission time by 10%.

If utilizing all mobiles, battery saver, and battery saver preambles are not required.

NOTE: To avoid interoperability issues, it should be configured in the system that either all or none of the radios send battery saver preambles. If there are radios with software versions prior to R01.05.00 in the system, they will always be expecting battery saver preambles, therefore either all the radios in the system should be configured to send battery saver preambles, or all upgraded to a newer release.

4.16.1.13
Data Revert Channels for Capacity Plus Single Site and Capacity Plus Multi Site

CPSM

MOTOTRBO in Single Repeater and IP Site Connect modes support the GPS Revert feature. In Capacity Plus Single Site and Capacity Plus Multi Site, MOTOTRBO extends the GPS Revert feature to include all types of data messages transmitted to the Application Server. The Data Revert Channel feature allows system operators a configurable option to offload all the data messages from radios to a Server onto programmed digital channels (called Data Revert Channels).

Data Revert Channels are different from Trunked Channels. Examples of data messages sent from radios to a Server are registration messages, location responses, text messages to the Server, and their Over-The-Air acknowledgments.

Data Revert Channels are exclusively used for transporting data packets. They are also especially useful for transporting location responses. They are not used for voice communication. However, Trunked Channels are not exclusively used for transporting voice. Data messages from one radio to another, and from an Application Server to radio(s) are always sent through Trunked Channels. As Data Revert Channels offload most of the data communication from Trunked Channels, they facilitate more voice communication over these channels.

There must be a Revert Control Station for each Data Revert Channel. If one channel of a repeater is used as a Data Revert Channel, then the other channel of the repeater is also used as a Data Revert Channel. Thus, the Revert Control Stations are always in a pair. The Revert Channel's Control Station receives a data message from a radio, returns acknowledgment to the radio (if required), and forwards the message to the Application Server connected to the Control Station. The Revert Control Station then operates in single repeater mode but does not understand the trunking messages (for example, System Status CSBK) and does not tune to the Rest Channel. The Revert Channel's Control Stations stay tuned to its assigned Revert Channel.

In the GPS Revert feature (single repeater or an IP Site connect), a radio is programmed with only one Revert Channel. However, for Data Revert in Capacity Plus Single Site and Capacity Plus Multi Site, a radio is programmed with a list of the revert channels. This allows a radio to look for more than one channel (up to four channels) for transmission. This increases the probability of a successful transmission. Additionally, this increases the reliability of the transmission when a revert repeater is down as the radio automatically looks for the next repeater. A radio uses the Revert Channels in a round-robin fashion, distributing the load of data transmission fairly between the channels.

There is at least one Trunked Control Station, which is used by the Application Server to send a data message to a radio. A Trunked Control Station has the Capacity Plus Single Site or Capacity Plus Multi Site software installed and follows the Rest Channel as the Rest Channel changes. There may be more than one Trunked Control Stations in the system. The required number depends on the number of messages from the Application Server to radios. It is recommended to use a Trunked Control Station for every 20 messages, of 50-byte or character size payload, per minute.

To avoid misconfiguration, the CPS does not allow programming a trunked and Revert Channels in the same list. The CPS only performs channel check but not actual frequency check. Thus, while configuring the frequencies for the system, caution must be exercised to not use the same frequency for a Revert Channel and a Trunked Channel.

A Capacity Plus Single Site or a Capacity Plus Multi Site system can have more than one Trunked Control Station, therefore a fair distribution of data packets among the Trunked Control Stations is required. For a simple way to achieve the fair distribution, follow these rules:

- The radios should be grouped into ‘n’ sets, where ‘n’ is the number of Trunked Control Stations.
- Each set of radios is associated to a Trunked Control Station.
- For each set of radios, it is required to make one or more entries in the IP Routing Table of the Application Server such that a data packet transmitted to a radio is routed to the port of the Trunked Control Station associated with the set of the radio.

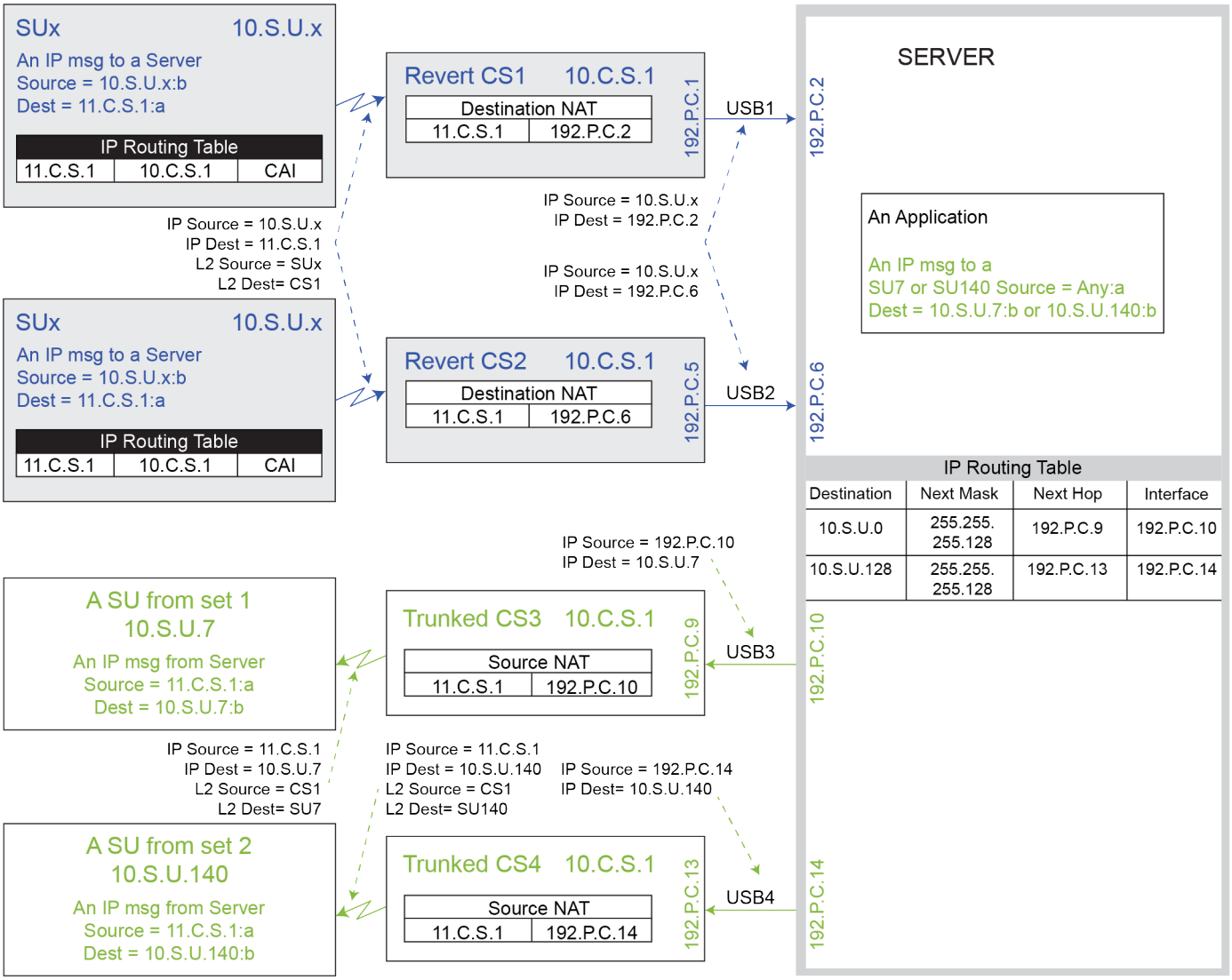
The IPv4 address of the Server (as seen by a radio) is derived from the radio ID of the Control Stations. The example has two Revert Control Stations (shown in blue) and two Trunked Control Stations (shown in green). The example assumes that the IDs of all radios are within {1 to 255}. They have been divided into two sets of {1 to 126} and {127 to 255}.

NOTE:
Say a group of radios is defined as {n..m} where ‘n’ and ‘m’ are the lowest and highest IDs of the radios respectively, and there are two Trunked Control Stations. The radios should be divided into two sets of radios, say {n..p} and {p+1..m}. Here, ‘p+1’ is a power of 2 (for example, 4, 8, 16, 32, 64,...).

The sets of radios are non-overlapping. This means a radio is a member of one and only one set.

Multiple groups can be allocated to a Trunked Control Station by having one entry per group in the IPv4 routing table of the Server.

Figure 172: The example shows IPv4 addresses in a Capacity Plus Single Site Configuration with Data Revert



4.16.2

Data Application Licensing Considerations

The Presence Notifier is included with each Text Messaging Server as well as each Location Server. The Presence Notifier, Text Messaging Server and Location Services Server can all be installed on one physical server.

The Location Services base package consists of a Fixed Client and Server plus one map. The base package includes support for up to 10 radios. Additional fixed clients can be purchased on a single user basis. A mobile client is not available. Additional radio licenses can be purchased in groups of five radios.

The Text Messaging base package consists of a Fixed Client and Server. The base package includes radio licenses for up to 10 radios. Additional fixed clients can be purchased on a single user basis. Additional mobile clients can also be purchased on a single user basis. The mobile client comprises of software installed on a PC. Additional radio licenses can be purchased in groups of five radios.

Typically, one text message dispatcher is required per functional group. Multiple text message dispatchers can be used if the functional group is large or if there are unique communication requirements. The text message dispatchers should have the users of their functional group in their address book. If the dispatcher needs to dispatch text messages outside of the function group, they can use the manual address entry feature of the Text Message Client.

4.16.3
Mobile Terminal and Application Server Power Management Considerations

There are some considerations that have to be taken with regards to the Power Management settings on a PC being used for either a Mobile Terminal or Application Server.

It is recommended that the power management settings of the Application Server and Mobile Client be disabled. Specifically the System Standby and System Hibernation settings should be set to Never.

It is crucial that the Application Server and Mobile Terminal always be active so that they can transmit and receive data messages. If the Application Server or Mobile Client is allowed to enter System Standby or System Hibernation, it will not respond to received data messages. The radio(s) connected to the Application Server or Mobile Client queue the data until messages fail to be delivered. It is the responsibility of the sending device to retry the failed message. A user requires to “awaken” the Application Server or Mobile Client before it accepts messages again.

4.16.4
MOTOTRBO Telemetry Connection Details

For more details about the telemetry GPIO pin assignments, see the MOTOTRBO Telemetry ADK Guide available.

4.16.5
MOTOTRBO Network Interface Service (MNIS) and Device Discovery and Mobility Service (DDMS)

This section documents system design considerations related to MNIS and DDMS deployment in a MOTOTRBO system. It also covers MNIS and DDMS features and capabilities, data application deployment considerations and considerations for migrating from Control Stations to MNIS based deployment. The DDMS is formerly known as the MOTOTRBO Presence Notifier.

The following basic considerations are important and must be noted:

- The MNIS application currently does not support voice and CSBK calls.
- If data support with MNIS and DDMS is desired, ensure that the data application supports MNIS and DDMS.
- MNIS and DDMS configuration details can be found in their respective online and context help. Additional information can also be found at the MOTOTRBO ADP portal.
- Discuss with third-party data application vendor for any questions related to their application support of MNIS and DDMS.

4.16.5.1

MNIS and DDMS Operation Overview

The MNIS is an application, which runs as Windows or Edge Node service, and which supports data applications without requiring Control Stations. MNIS acts as a gateway to the radio system for data applications. It connects with the radio system over an IP network and utilizes the repeaters to transmit and receive data messages between data application servers and MOTOTRBO radios.

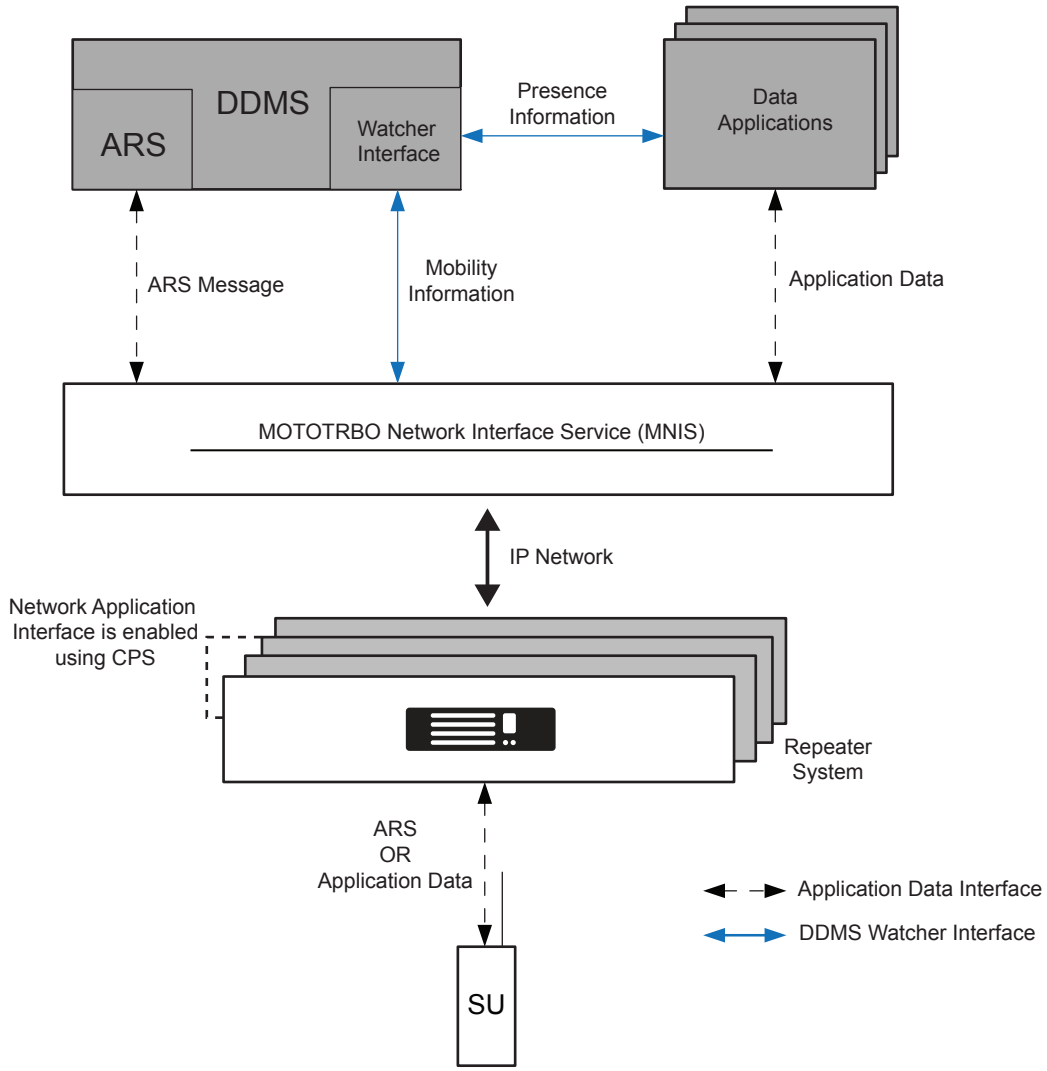
The MNIS has two identifiers: MNIS LE ID and MNIS Application ID. Both parameters are configured in the MNIS using the configuration GUI. The MNIS Application ID is used by the MNIS to receive and transmit on the radio network and is identical to the Radio ID of the Control Stations. The MNIS Application ID is used whenever the radio needs to communicate with the data application or vice versa. For example, the ARS and TMS Radio ID fields in the radios are configured to the MNIS Application ID. The data message from the radios to the ARS or TMS applications has the MNIS Application ID as the destination of the message. Likewise, the data message from ARS or TMS applications to the radios has the MNIS Application ID as the source of the message. The MNIS Application ID plays the role of the Radio ID so fielded radios should not be configured with the Radio ID that is the same as the MNIS Application ID. MNIS LE ID can be equal to the MNIS Application ID or can have other numbers. It plays the role of Peer ID and must be unique in the MOTOTRBO systems.

The MNIS is configured with the Master repeater's IPv4/UDP address, which it uses to discover and connect with the repeater system. Upon connection with the repeaters, the MNIS informs the repeaters of its MNIS Application ID. When a fielded radio transmits a data message with the destination address of the MNIS Application ID, the repeater assembles the blocks of the data PDU received Over-the-Air and forwards it to the MNIS. The MNIS in turn forwards the data message to the data application. When a data application sends a data message to a fielded radio, the MNIS forwards them to a repeater for transmission Over-the-Air.

The radio's presence and mobility management are handled separately by the MOTOTRBO Device Discovery and Mobility Service (DDMS) application. The DDMS can be deployed with either the MNIS (on Windows or Edge Node) or Control Station.

The MNIS and DDMS have multiple interfaces, as shown in Figure 173: MNIS and DDMS Interface Overview on page 491. The interfaces are described in the following sections.

Figure 173: MNIS and DDMS Interface Overview



4.16.5.1.1

Network Application Interface

The MNIS connects with the repeater system using the link establishment procedure of the repeater system. This requires the MNIS to be configured with the Master repeater's IP address and UDP port number. Upon connection with the Master repeater, it discovers the IP addresses and port numbers of all the repeaters in the system. Then, the MNIS establishes the link with the repeaters in the system.

Upon connection with the repeaters, the MNIS uses the repeater's Network Application Interface and underlying services to support data transmit and receive through the repeaters. The MNIS encapsulates the applications UDP/IP data packet in the Network Application Interface packet and sends it to the repeater. The repeater transmits the data message Over-The-Air. Likewise when the repeater receives a message meant for the MNIS, it encapsulates the message in the Network Application Interface's data packet and sends it to the MNIS. The link establishment and Network Application Interface procedures are transparent to the data application.

NOTE: If using MNIS, all the repeaters in a system (IPSC, Capacity Plus Single Site, or Capacity Plus Multi Site) are required to have the Network Application Interface – Data option enabled. If using MNIS with a single site repeater, the same option in the repeater must be enabled. Enabling this option in the repeaters can be done using the CPS.

4.16.5.1.2
Data Application Interface

The MNIS supports the standard UDP/IP based interface for data communication with the radio. This interface is similar to the data communication via Control Stations.

In a Control Station deployment, data messages from the application are routed by the IP stack of the PC to the network adapter of the Control Station. The Control Station then receives the data message and transmits Over-The-Air to the radio. The data message received by the Control Station from the Over-The-Air is sent to the IP stack of the PC from its network adapter. The IP stack of the PC routes the data message to the application.

When utilizing the MNIS the data messages from a data application are routed by the IP stack of the PC to the network adapter (also called the tunnel adapter) of the MNIS. The MNIS forwards the data message to the repeater for transmission Over-The-Air. The data message received by the repeater is sent to the MNIS. The MNIS sends the data message to the IP stack of the PC from its tunnel adapter. The IP stack of the PC then routes the data message to the data application.

NOTE: Configuration with the tunnel described above is not supported in Edge Node-based MNIS deployments. It is supported in Windows-based MNIS deployments only. The Edge Node-based MNIS supports the Control Interface (TCP) protocol only.

4.16.5.1.3
DDMS Watcher Interface

The DDMS watcher interface is an interface for applications, including the MNIS, to obtain the presence and mobility information of the radios from the DDMS. The DDMS maintains both the radio presence and mobility information. It provides an interface to the MNIS, and the data application to get notifications on change in the presence or mobility information of specified radios.

Presence Information

The MNIS forwards the radio ARS message to the DDMS, which updates the radios presence. The DDMS notifies data applications that have subscribed for presence through the watcher interface.

Mobility Information

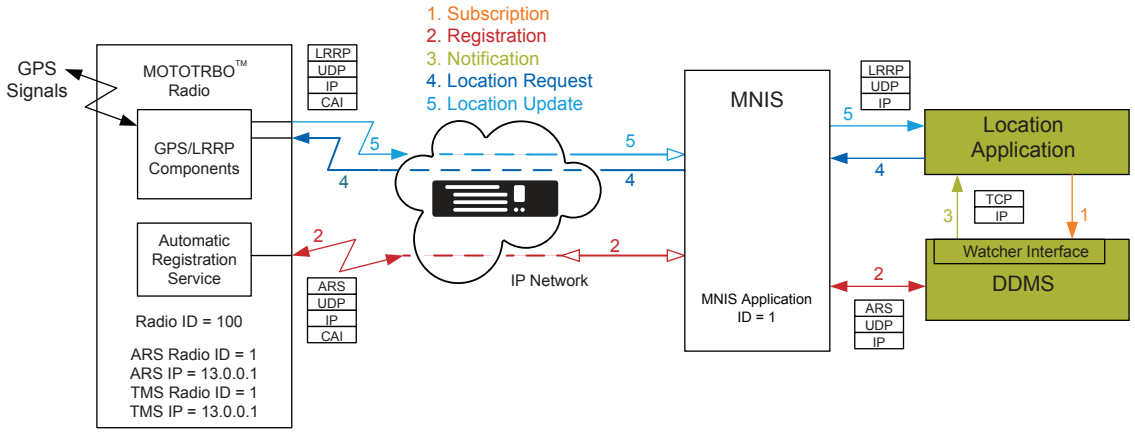
The radio’s mobility is the channel or site where the radio is present. The MNIS uses the mobility information to route outbound data messages for transmission.

The MNIS determines the radio mobility information based on the channel and the site from where the ARS is received. The watcher interface is then used to input the mobility information in DDMS. The DDMS notifies mobility updates to an application, including the MNIS, that has subscribed for radio’s mobility information.

4.16.5.1.4
Flow of Messages DDMS and MNIS Operation

Figure 174: Location Application with MNIS and DDMS in a Single Site Digital System on page 493 shows the flow of messages to facilitate the Location Service with the MNIS and DDMS deployment.

Figure 174: Location Application with MNIS and DDMS in a Single Site Digital System



1. The location application subscribes for the radio's presence information with DDMS.
2. Upon power-up, the radio transmits an ARS message to register with the DDMS. The ARS message is then received by the repeater and sent to the MNIS. The MNIS routes the message to the DDMS. The DDMS updates the radio's mobility information based on the channel from where the ARS is received.
3. The DDMS notifies the location application of the presence of the radio.
4. The location application sends a location request which gets routed to the MNIS. The MNIS refers to the radio's mobility information to determine where to transmit the location request and routes to the appropriate repeater. The repeater transmits the location request to the radio.
5. The radio transmits its location updates, which are received by the repeater and sends to the MNIS. The MNIS routes the location updates to the location application.

4.16.5.2

System Topology with the MNIS

The MNIS supports MOTOTRBO digital Single Site. It can connect with up to 50 conventional or Capacity Plus Multi Site repeater systems with wide or local area channels. It can connect with one Capacity Plus Single Site repeater system.

System	Description
IPSC IP Site Connect	The MNIS supports MOTOTRBO IP Site Connect. It can connect with: ● Up to 50 IP Site Connect with wide or local area channels. ● An IPSC repeater system has: ○ Two wide-area logical channels, or ○ A combination of wide and local area logical channels
CPSS Capacity Plus Single Site	The MNIS supports MOTOTRBO Capacity Plus Single Site. MNIS can connect with one Capacity Plus Single Site system.

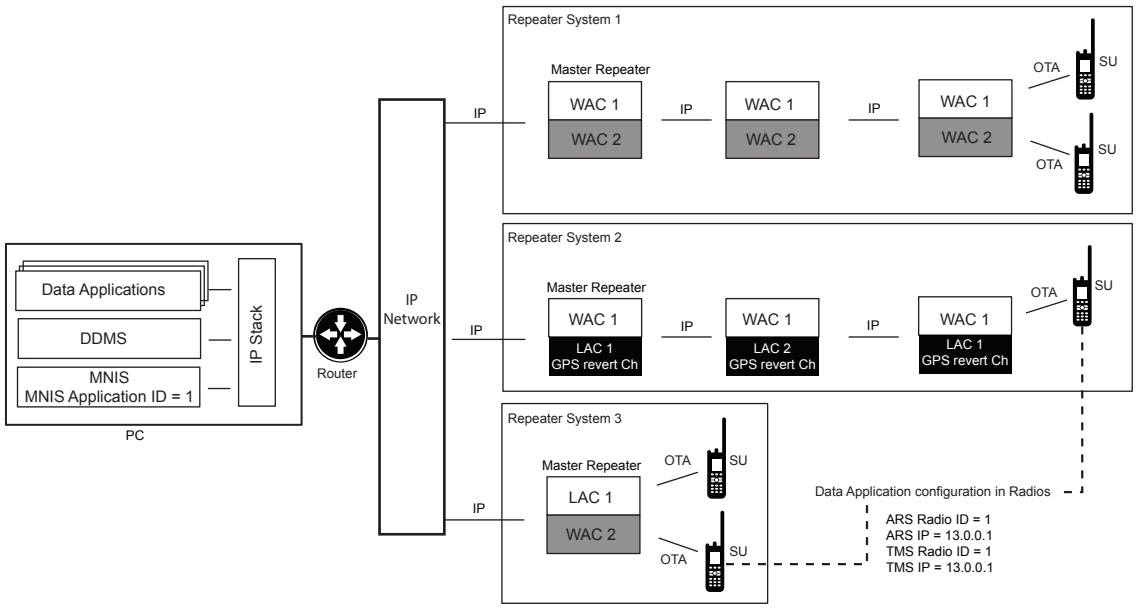
System	Description
CPMS Capacity Plus Multi Site	The MNIS supports MOTOTRBO Capacity Plus Multi Site. MNIS can connect with up to 50 Capacity Plus Multi Site systems.

NOTE: When the MNIS is connected to multiple systems, the data console application is responsible for determining to which system the message should be sent.

4.16.5.2.1
Multiple Conventional Systems Topology

Figure 175: Multiple Conventional Systems with MNIS on page 494 shows an example of a topology with multiple IPSC and Single Site systems. The radios share the same data applications. Multiple data applications such as Location, Text, Telemetry, and others, can be deployed. In this system configuration, the radios must have unique radio IDs across all repeater systems. The ARS and TMS Server addresses must be set to the MNIS Application ID.

Figure 175: Multiple Conventional Systems with MNIS



- In this deployment, with multi-channels, the radios must have ARS enabled. The radios' mobility is updated based on the channel from where the ARS is received. The MNIS uses the mobility information to send outbound messages from the data application to the radio. Without mobility information, the MNIS transmits the data message to all connected channels.
- The location application's address is not configured in the radios. The radio determines the address from the source address field of the location request message. Since the location request is sent from the MNIS, it carries the MNIS' Application ID in the source address field.
- The GPS Revert Channels (or Enhanced GPS Revert Channels) can be configured as local or wide area. However, it is highly recommended to configure the GPS Revert Channel to local. There is no reason to have wide area GPS Revert Channels, if utilizing the MNIS. Wide area for GPS Revert was required so that the data could be routed to one set of Control Stations Over-The-Air. With the existence of the MNIS, the data received on local channels is routed to the data application over the network. In general,

local GPS Revert Channel increases the GPS capacity, since one wide area channel can be replaced by numerous local channels.

4.16.5.2.2

Capacity Plus Single Site System Topology

CPSS

The following figures show examples of topologies for a Capacity Plus Single Site system. The MNIS can be deployed on the same VLAN as the repeaters or in a separate VLAN, where remote connectivity is not required. Alternatively, it can be deployed remotely from the repeaters when remote connectivity is required.

Figure 176: Capacity Plus Single Site System with MNIS Deployed in the Same VLAN as the Repeaters

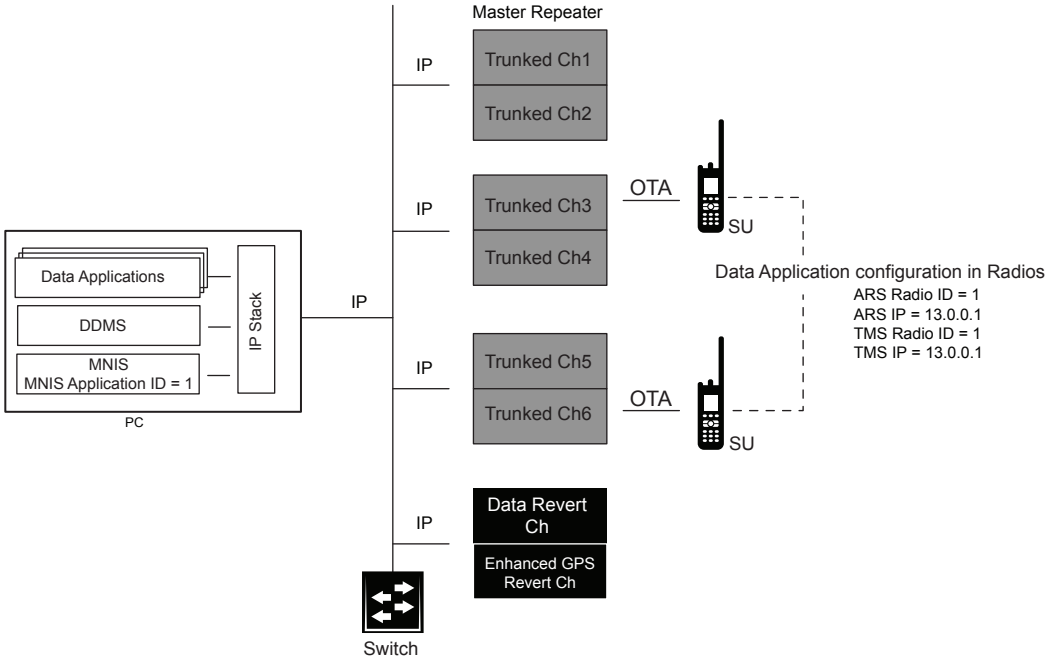


Figure 177: Capacity Plus Single Site System with MNIS Deployed in the separate VLAN

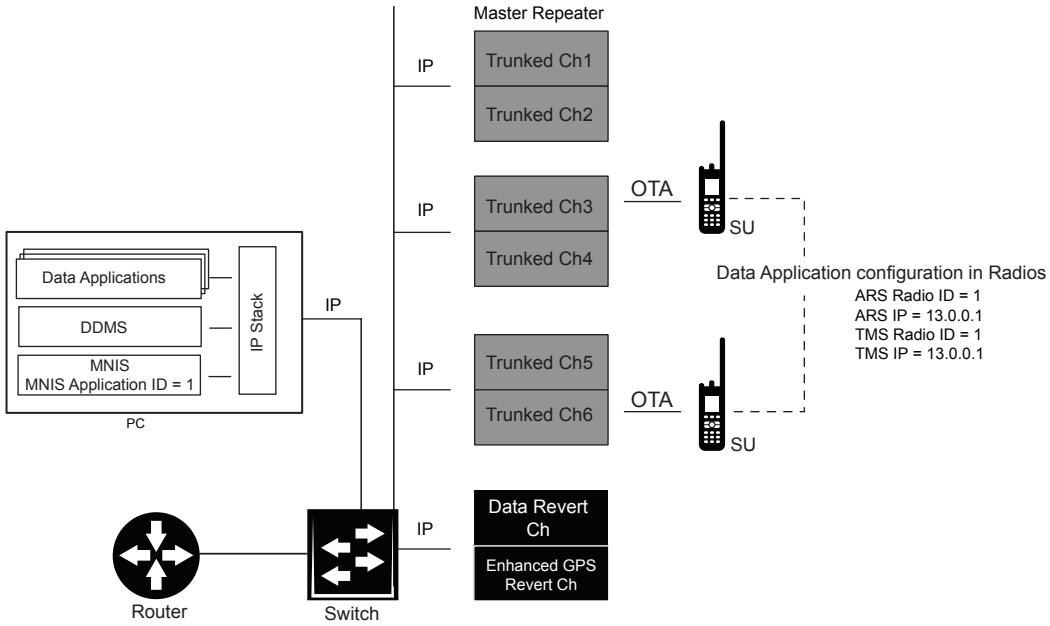
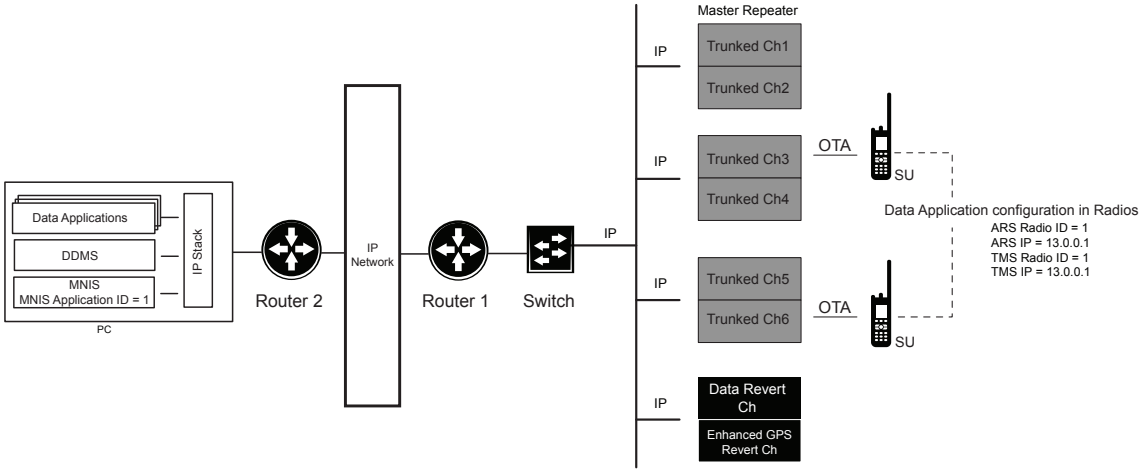


Figure 178: Capacity Plus Single Site System with MNIS Deployed Remotely



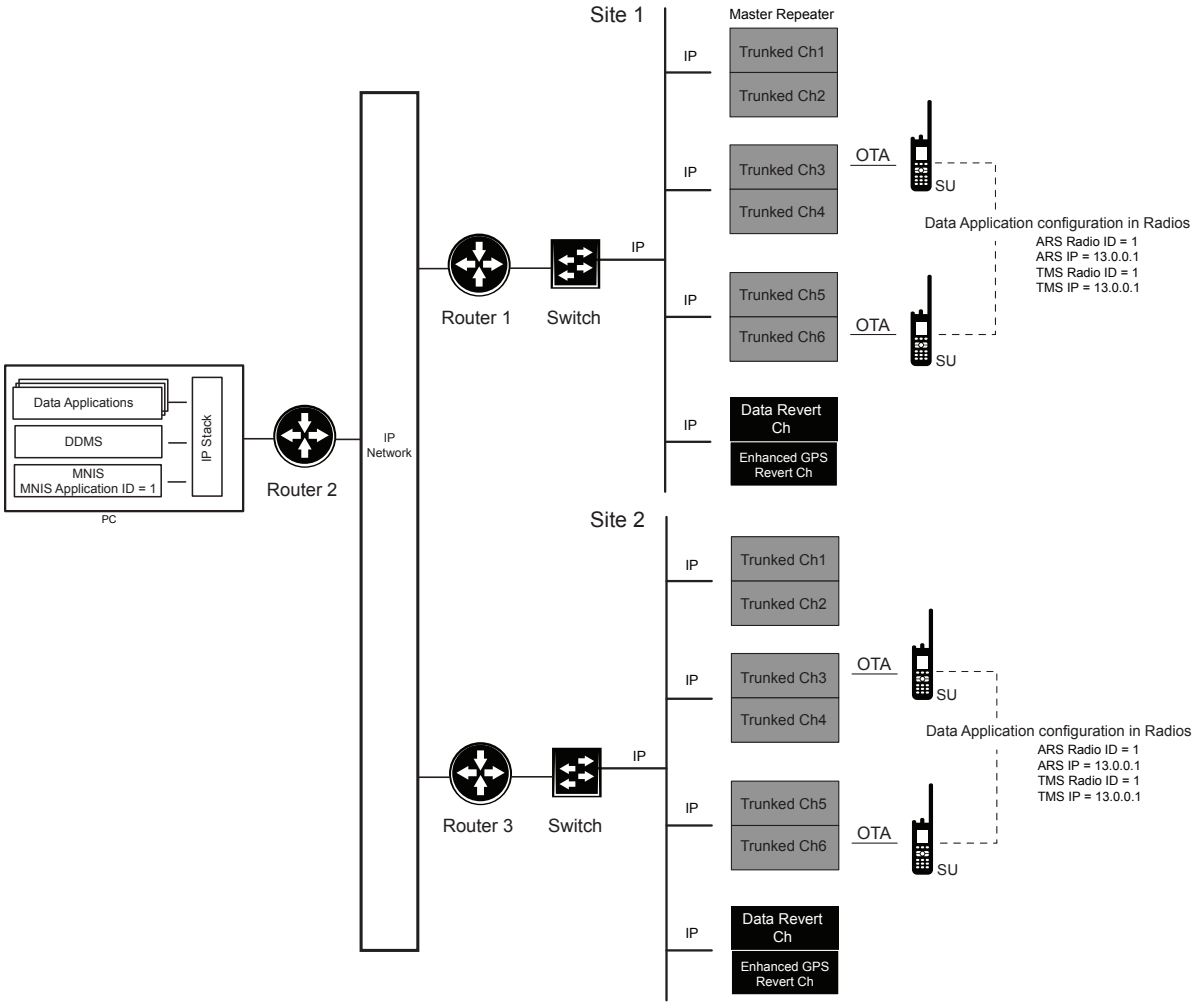
4.16.5.2.3

Capacity Plus Multi Site System Topology

CPMS

The following figure shows examples of topologies for a Capacity Plus Multi Site system with MNIS deployed on a separate subnet than the repeaters.

Figure 179: Capacity Plus Multi Site System with MNIS



NOTE: The Data Revert Channels (or Enhanced GPS Revert Channels) can be configured as “local” or “wide”. However, it is recommended to configure them to “local”. There is no reason to have wide area Data Revert Channels if utilizing MNIS. Wide area Data Revert Channels were required so that the data could be routed to one set of Control Stations Over-the-Air. With MNIS, the data received on local channels are routed to the data application over the network. In general, the local Data Revert Channel increases the bandwidth since one wide area channel can be replaced by numerous local channels.

4.16.5.2.4

System Topology with Multiple MNIS

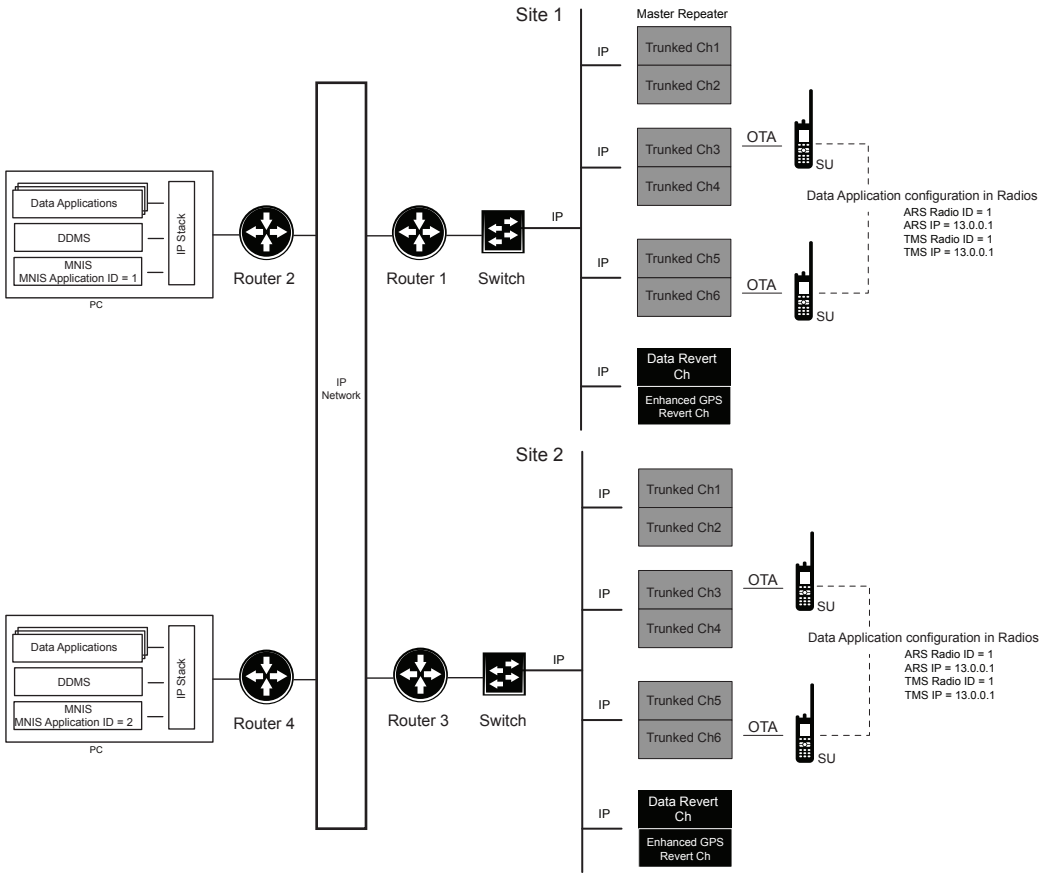
CPMS

In a system where two or more agencies are sharing the radio system, then the agencies can have their independent MNIS deployments.

NOTE: Up to 4 MNIS can be deployed with the repeater system whether it is a conventional system or systems, Capacity Plus Single Site or Capacity Plus Multi Site systems.

Figure 180: Capacity Plus Multi Site System with Two MNIS on page 498 shows an example of topology with two MNIS deployed in a Capacity Plus Multi Site system. The radios can be configured to communicate with either MNIS-1 or MNIS-2.

Figure 180: Capacity Plus Multi Site System with Two MNIS



NOTE: Once the Network Application Interface for data is enabled at the repeater, then multiple MNISs can be connected to it.

4.16.5.2.4.1
Number of Repeater Sites with Multiple MNIS Deployment

System	Description
IPSC IP Site Connect	One MNIS can be deployed on an IP Site Connect with up to 15 repeater sites.

System	Description
CPMS Capacity Plus Multi Site	One MNIS can be deployed on CPMS with up to 15 repeater sites. Starting from software version R02.04.00 one MNIS can be deployed on CPMS with up to 20 repeater sites.

If two or three MNISs are deployed, the number of repeater sites should be decreased by one. If four MNISs are deployed, the number of repeater sites should be decreased by two. The restriction is meant to prevent excess loading on the repeaters due to the maximum number of system sites and additional MNIS instances.

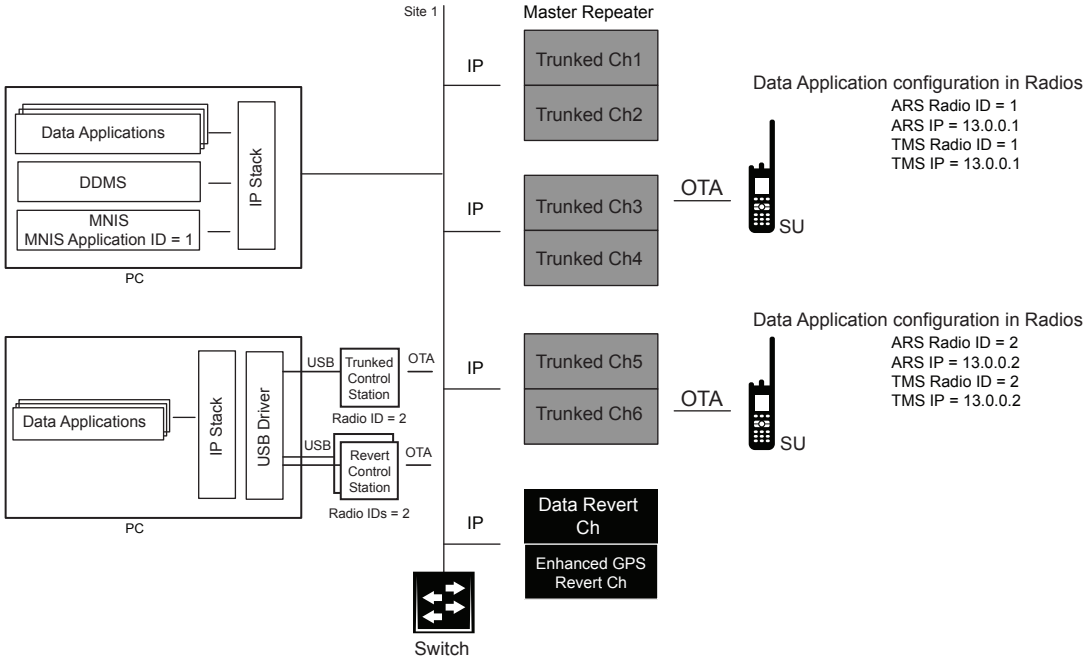
4.16.5.2.5
Topology with MNIS and Control Stations

CPSS

The MNIS and Control Stations can be deployed on the same repeater system.

The following figure shows an example of topology with the MNIS and Control Stations deployed in a Capacity Plus Single Site system. The radios can be configured to communicate with either the MNIS, or the Control Station.

Figure 181: Capacity Plus Single Site System with MNIS and Control Stations



4.16.5.3
Data Applications and MNIS Deployments

There are a couple of options for data applications and MNIS deployments.

The deployment can consist of one of the following options:

- MNIS and data applications deployed on the same PC

- MNIS and data applications deployed on separate PCs
- A combination of both options
- MNIS deployed on the Edge Node

The MNIS deployed on the Edge Node is the simplest (automated) and recommended deployment. The data applications and the MNIS deployed on the same computer are also supported, but require maintenance of the application and operating systems patches. Moreover, the computer must meet the total performance requirement for the MNIS, DDMS, and other data applications. For details about requirements go to MNIS Data Gateway and DDMS Computer Specifications on page 508.

Configuration of port forwarding is not required when the data application is deployed on the same computer as the MNIS. Therefore, no configuration of port forwarding is specified for the ARS data since the DDMS and MNIS are on the same PC.

It is recommended that the DDMS be deployed on the same computer as the MNIS. This reduces the IP traffic on the network. The data applications are configured with the IPv4 address of the computer with the DDMS application and the DDMS watcher interface port.

When the MNIS receives a data message from the repeater system, regardless of what it contains, (a text message, GPS location, and others) it sends the message to all Dispatch Consoles connected over the MNIS TCP Control Interface, and to the UDP Tunnel interface. A new message and opcode are defined in the MNIS TCP Control Interface Protocol Document for sending the received message to the console, which enables the following:

- Multiple consoles of the same type (TMS, GPS, ARS, and others) connect to the same MNIS and receive messages of the same type.
- Multiple console applications connect to the same MNIS to listen to the messages it receives, without needing a separate MNIS for each one.

However, there is no way for a subscriber radio to send a message to a specific Dispatch Console; all connected consoles see incoming messages.

NOTE: Configuration with the UDP tunnel interface described above is not supported in Edge Node-based MNIS deployments. It is supported in Windows-based MNIS deployments only.

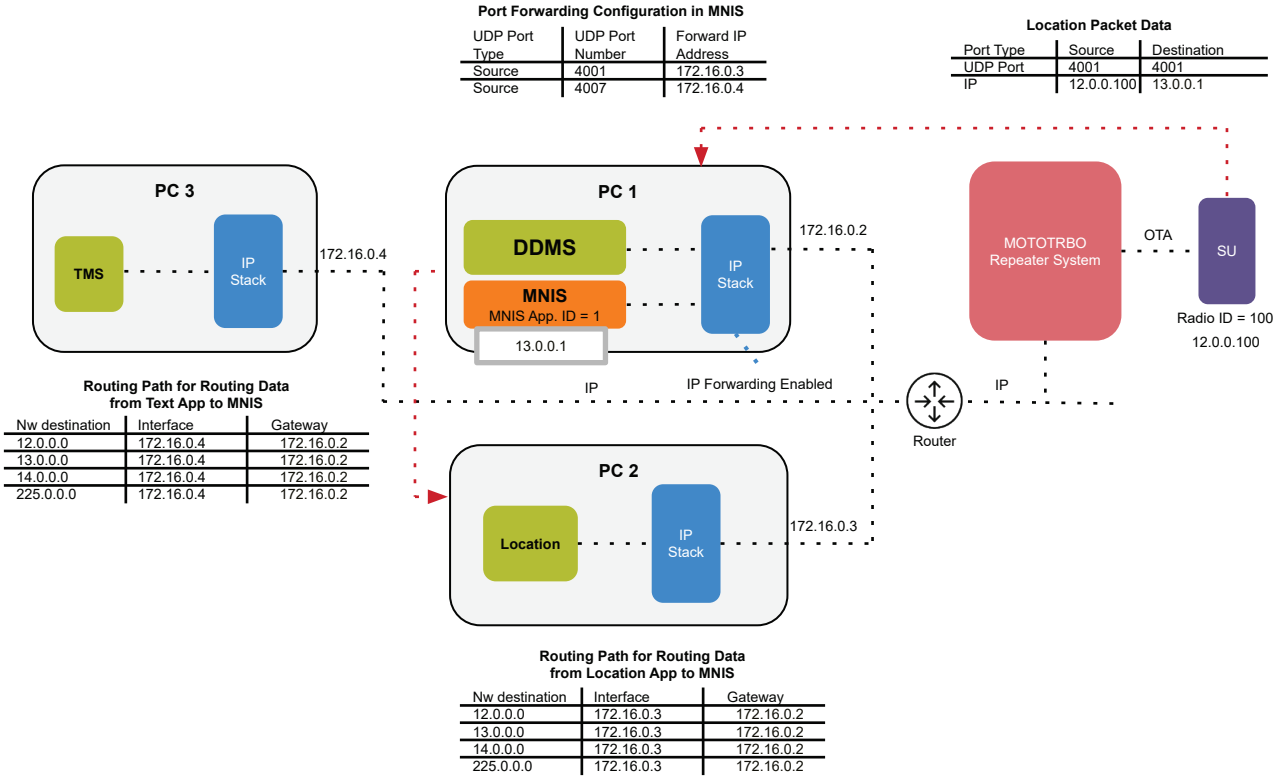
4.16.5.3.1
Data Applications and MNIS Deployment on Separate PCs

The data applications and MNIS can be deployed on different computers for several reasons:

- The computer does not meet the total performance requirement for the MNIS, DDMS, and data applications.
- The data application vendor requires it to be not deployed with other applications.
- The data application is not a Windows application.
- Unstable data applications can be prevented from interfering with the MNIS operation. An example would be an OS crash.

The MNIS has data message port forwarding support to facilitate the deployment of data applications and MNIS on separate PCs. Figure 182: Application and MNIS Deployed on Separate PCs on page 501 shows this.

Figure 182: Application and MNIS Deployed on Separate PCs



The MNIS needs to be configured to forward location and text data messages from the radios to the PCs with Location and Text applications. The UDP port type configured is the source port because the radios' standard data services ports are fixed (with Location = 4001 and Text = 4007). The MNIS also allows the selection of the destination port type. This option can be used for non-standard data services, such as third-party raw data. The PCs with the Location and Text applications require IPv4 routes to be configured to route messages from the data application to the computer with the MNIS. Figure 182: Application and MNIS Deployed on Separate PCs on page 501 shows a route for data messages belonging to system CAI Network IDs = 12, 13, 14 and 224. When the data applications and MNIS are on different subnets, then it must be ensured that the CAI Network addresses can be routed between subnets.

The PC with the MNIS requires IPv4 routing enabled. This allows the data message from applications to be internally forwarded to the tunnel adapter of the MNIS. To enable IPv4 routing, the below steps need to be done on the PC with MNIS:

- Using the registry editor of the Windows system, set the `IPEnableRouter` option to "1" (this option is in the `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Services\Tcpip\Parameters`)
- The Windows system service called **Routing and Remote Access** needs to be reconfigured to start automatically when the system starts.

The MNIS needs to be configured to forward data messages from radios to the Application Server. This configuration can be done in the **Advanced/Forwarding Rules** of the MNIS configuration.

4.16.5.4
Mobility Management and Individual Data Transmission

The DDMS, when deployed with MNIS tracks the radios' mobility. The DDMS updates the radios' mobility based on the channel or site, from where the ARS message from the radio is received. The MNIS and any other data application can subscribe with the DDMS for radio mobility information. The DDMS provides radio

mobility information upon subscription, and subsequently when the mobility information gets updated. The DDMS stores the mobility information in persistent memory so that it is available following DDMS or MNIS power cycles. The mobility information is retained even when the radio becomes absent.

Upon power up, the MNIS subscribes with the DDMS to receive the mobility information. Following initial notification, it continues to receive mobility updates from the DDMS. The MNIS uses the radios' mobility information to route the outbound data from the data application. Only individual data messages are routed in this manner.

System	Description
IPSC IP Site Connect	In an IPSC system, the MNIS is aware of the local and wide area channels. If a radio is known to be present on a local channel, then the data message is transmitted only on that local channel. If the radio is known to be present on the wide area channel, then the data message is transmitted on the wide area channel. If the radio is absent, but its mobility information is known based on a previous registration, then the MNIS routes the data message based on the last known mobility information. If the radios' mobility information is not known, then the message is routed to all the channels of the system, except the channels selected as data revert. Sending individual data messages Over-The-Air on all channels wastes bandwidth. Therefore, it is always recommended that the ARS feature is enabled.
CPSS Capacity Plus Single Site	In a Capacity Plus Single Site system, outbound data messages are always routed to the Rest Channel of the repeater. No data messages are routed to the Revert Channels.
CPMS Capacity Plus Multi Site	In a Capacity Plus Multi Site system, a radio's mobility is the site where the radio sends its ARS registration. If the radio's mobility information and site are known by the MNIS, then the data message is routed to the site. If the radio's mobility information is not known, then the data message is routed to an arbitrarily selected site. In both conditions, the data message is transmitted Over-The-Air to at most, two sites. In the following scenario, it is transmitted to only one site: ● If ARS is enabled for site and system change; or ● If ARS is enabled for system change, and the radio is still at the site where it has registered.

If the MNIS is not able to route the message due to a loss of connection with the repeater system, or because of any other erroneous condition, then the data message is dropped and an ICMP message is returned to the data application.

4.16.5.5
Group Messages

Data applications can receive or send group data messages via the MNIS. The MNIS supports group list configuration via its configuration GUI. The groups can be specified in a range to allow a large number of group affiliations. An example would be groups in the range of 1-100. The data messages targeted to the specified groups are sent to the application. The group list can be defined based on the type of system configuration:

- In a conventional system, one group list per slot (1 and 2) can be selected.

System	Description
CPSS Capacity Plus Single Site	In a Capacity Plus Single Site system, one group list can be selected.
CPMS Capacity Plus Multi Site	In a Capacity Plus Multi Site system, one group list per site can be selected.

The group list is also used for routing of outbound group messages from the data application. In a conventional system, if the target group is present only in the group list of slot 1, then the data message is routed to slot 1 only. If the target group is in the group list of slot 1 and slot 2, then the data message is routed to both slots. If the slot is configured as an IPSC local channel, then the group message is routed to all local channels of that slot. If the group is not in any of the group list, then the data message is routed to all the system channels. A group data message is not routed to a channel that is configured as a Data Revert Channel.

System	Description
CPSS Capacity Plus Single Site	In a Capacity Plus Single Site system, the group data message is routed to the Rest Channel.
CPMS Capacity Plus Multi Site	In an Capacity Plus Multi Site system, if the group is a wide area group as provisioned in the Master repeater, then the data message is transmitted at the sites associated with the wide area group. If the group is a local group, then the data message is routed and transmitted at the sites where their group list contains the target group. If the local group is present in multiple group lists, then it gets transmitted at the multiple sites.

4.16.5.6

Data Privacy

The MNIS supports Basic, Enhanced, and AES privacy mechanisms.

When privacy is enabled, the MNIS uses only one transmit key for scrambling the outbound message, this is true for all privacy types. For Basic privacy, this transmit key is also used for descrambling the inbound messages. For Enhanced and AES privacy, all the keys (up to 255) in its key list are used for descrambling the inbound messages.

It is recommended that all radios including the MNIS should have the same privacy settings. If Enhanced and/or AES privacy is being used, then the MNIS should have the transmit key of all the radios and radios should have the outbound key of the MNIS.

4.16.5.6.1
MNIS Data Gateway Key and Key List

Similar to radio, an MNIS Data Gateway can be configured with a **Basic Privacy Key** and/or an **Enhanced** privacy key list, and/or an AES (**Symetric Keys**) privacy key list. Each key list can contain up to 255 keys entered in its corresponding system key list. An MNIS Data Gateway can receive using Basic, Enhanced, AES and No privacy. In other words, it can receive using all privacy types. The MNIS Data Gateway can transmit using Basic, or Enhanced, or AES or No privacy. In other words, it can only transmit with one privacy type.

It is recommended that the MNIS Data Gateway key list contain all privacy keys utilized by radios it communicates with since radios utilize the transmit key of their selected personality when they send data to the MNIS Data Gateway.

4.16.5.6.2
MNIS Data Gateway Transmit Privacy Type and Privacy Key

An MNIS Data Gateway can transmit using Basic, or Enhanced, or AES, or No privacy type. In other words it can only transmit with one privacy type. For Basic privacy, only one **Basic Privacy Key** can be specified in the **Security** option of the MNIS configuration. All keys are hardcoded and only the number of the key from the range 1 – 255 can be selected.

There is no more option to select in the desired system configuration when **Basic** privacy is selected in the **Security Setting**. When in the **Security Setting** the **Enhanced** or AES (**Symmetric Keys**) privacy is chosen, a transmit key (**Security Alias)** from the corresponding key list must be specified. The key list is configurable in the **Security** option of the MNIS configuration.

There is no standard method for the data application to dynamically select the MNIS Data Gateway's transmit privacy key.

4.16.5.6.3
Privacy Reception in the MNIS Data Gateway

There are no configuration options to determine how the MNIS Data Gateway handles the reception of unprotected (clear) or protected (encrypted) calls. An MNIS Data Gateway can receive Basic, Enhanced, AES, and No privacy typed. In other words, it can receive all the privacy types.

If an MNIS Data Gateway receives an unprotected (clear) call it decodes the call normally and forwards the data call to the data application. If an MNIS Data Gateway receives a protected (encrypted) call, and there is a matching key (with matching **Key ID** and privacy type) in its key list, then it decodes the call and forwards the data call to the data application.

4.16.5.7
Considerations for Advanced MNIS Configurations

This section covers in detail a couple of parameters in MNIS configurations.

System	Description
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	In Capacity Plus Single Site and Capacity Plus Multi Site configurations, the MNIS has an “Outbound Data Limit” parameter. This parameter defines the number of data messages that the MNIS can simultaneously transmit, and therefore the maximum number of Trunked Channels that can be busy with data. In Capacity Plus Multi Site mode, the parameter can be configured per site. The parameter does not control the number of inbound data transmissions from the radio. The

System	Description
	configuration ensures that the MNIS does not occupy channels more than specified. It does not control system data loading. See Digital Repeater Loading on page 399 to determine the application data loading that can be supported by the system.
CPMS Capacity Plus Multi Site	In an Capacity Plus Multi Site configuration, the MNIS has an “Individual Data to Registered Site” parameter which can be enabled or disabled. When enabled, the data message is transmitted only at the site where the radio has registered. If the radio roams, then it must re-register at the new site. This parameter should be enabled only when all the radios in the system either do not roam, or have ARS upon system/site change enabled. The enabling of the parameter has a couple of benefits: ● The individual data is treated as a local call, and is therefore faster and does not involve other sites in a call setup. ● The call does not engage two sites. The enabling of this parameter should be carefully considered, as data delivery could be missed when a radio roams, but unable to register immediately after roaming to the new site.

In conventional configurations, the MNIS has a “Conventional Channel Access” parameter that can be set to normal, which is the default setting, or data centric. If the selection is normal, then channel access for application data outbound transmissions follow the channel access rules similar to what the radios use. The repeater introduces a random delay when the channel is busy. The duration of this delay is between 0 – 1.8 seconds. After this delay, if the channel becomes idle, then the data message is transmitted, or another random delay is introduced. This approach is used for collision avoidance when the channel is busy with radio activity. If the selection is data centric, then the random hold-off is not introduced. The repeater transmits the data immediately after the channel becomes free.

4.16.5.8
DDMS Usage by MNIS

The DDMS is required by the MNIS, and operation without DDMS is not recommended.

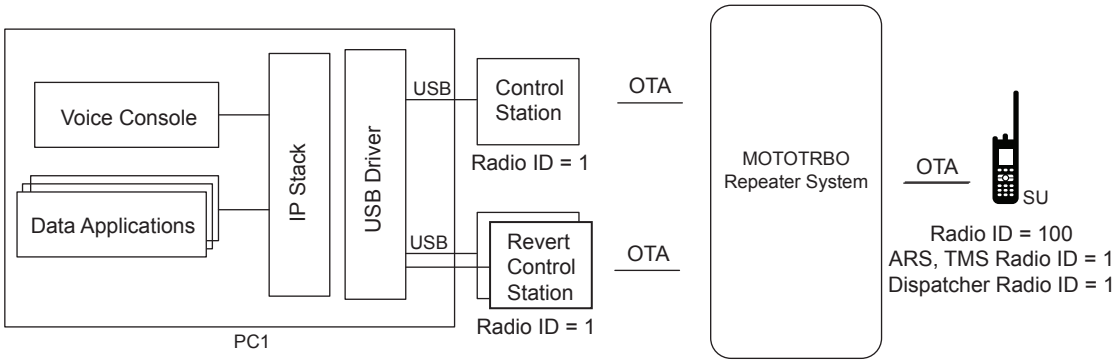
4.16.5.9
Control Station Migration to MNIS

The Control Stations can be replaced by the MNIS in systems where the Control Stations are being used for application data communication. In deployments where the Control Stations are used by voice consoles and data applications, it may still be beneficial to replace the Control Stations and monitor Data Revert Channels. For IPSC or Capacity Plus Multi Site systems, the Data Revert Channels can be converted to local channels to increase revert data throughput, as Control Stations are not required in the coverage range of the local channel.

The Control Stations can be replaced by MNIS without requiring any configuration changes to the fielded radios. Figure 183: System with Control Stations Used by a Voice Console and Data Applications on page 506 depicts a MOTOTRBO system with Control Stations used by a voice console and data applications. The data applications can be migrated to MNIS-based deployment as shown in Figure 184: System with a Control Stations Used by a Voice Console and MNIS Used by Data Applications on page 506. Since the fielded radios are configured with the Control Station Radio ID for the voice console contact and the ARS/TMS contact, the MNIS Application ID should be configured with the same ID to avoid configuration changes to the fielded radios. This can be accomplished by upgrading the Control Station to firmware versions R02.06.10 or

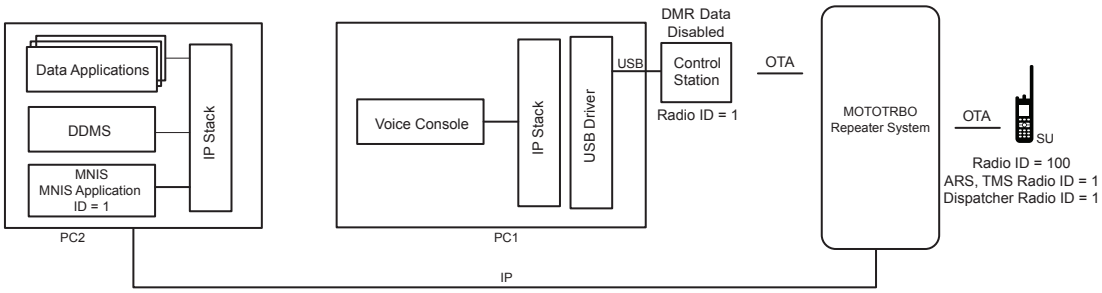
later. Using the CPS, select the **Voice Only** checkbox, which configures the radio being used as a control station to ignore data calls received Over-the-Air. The voice console calls continue to be handled through the Control Station. The data application messages are handled through the MNIS. This option is also supported in firmware versions prior to R01.11.00.

Figure 183: System with Control Stations Used by a Voice Console and Data Applications



In Figure 184: System with a Control Stations Used by a Voice Console and MNIS Used by Data Applications on page 506 two separate PCs are shown for clarity. The deployments can be on the same PC.

Figure 184: System with a Control Stations Used by a Voice Console and MNIS Used by Data Applications



NOTE: The MNIS does not support L2 fragmented data. Ensure that the largest data size [Data Message + IP/UDP Header] transmitted from the radio is less than the Max TX PDU Size configured in the radios. If the largest data sent from the radio is greater than the Max TX PDU Size value in the radio, then the value needs to be reconfigured with a larger Max TX PDU Size.

4.16.5.10

Considerations for the IP Network

A reliable network is important for application data communication reliability. In the event of a network fault, the MNIS could lose connectivity with the entire repeater system, or to some selected system sites. The MNIS is designed to automatically establish the link with the repeaters after the network is restored.

When the MNIS loses connection with a few sites/repeaters, but remains connected with other system sites/repeaters, then the MNIS continues to receive and route data messages from the connected sites/repeaters. Once the connection is restored, then the MNIS automatically resumes receiving and sending data with those sites or repeaters. No user intervention is required. The MOTOTRBO RDAC application can monitor the presence of the MNIS on the network.

The MNIS sends/receives a data message as a single datagram whereby the size is dependent on the message size, either received or sent, to the data application.

IP Datagram Size = Max Message Size + Overhead Size (120 bytes) where:

- Max message size could be the largest message size such as the text message size.
- Overhead size includes IP/UDP headers, protocol header, authentication, and others.
- The overhead does not include any VPN-related overhead.

The bandwidth requirement of the network between the MNIS and the repeater system is not large. The bandwidth required is for link establishment with the repeater system, and for receiving or sending the data messages to and from the radios.

The network bandwidth required by the MNIS is due to the Link Management IP traffic between the MNIS and the repeaters, and the IP traffic associated with the data messages sent and received from the MNIS. The following base values are used when estimating the network bandwidth due to MNIS:

Link Management BW per Repeater Peer = 1 kbps
Max IP BW due to Data Message per Channel = 7.5 kbps
% Data Loading on Voice Channel = 40%

The following sections covers the formula for estimating the network bandwidth by one MNIS.

4.16.5.10.1
Estimation of Link Bandwidth Where MNIS Is Deployed

Total Number of Voice Channels in the System = V

Total Number of Data Revert Channels in the System = D

Total Number of Repeaters in the System = R

Downlink BW (IP traffic from repeater system to MNIS):

- Downlink BW (with Data Revert) = D*7.5 + R*1 kbps
- Downlink BW (without Data Revert) = V*7.5*0.4 + R*1 kbps

Uplink BW (IP traffic from MNIS to repeater system):

- Uplink BW = V*7.5*0.4 + R*1 kbps

4.16.5.10.2
Estimation of Link Bandwidth at Repeater Sites

If the IP link bandwidth at the site is estimated for voice and data streaming to remote sites, then adding bandwidth at the sites is not required. If the IP link bandwidth at the site is not estimated for voice streaming as would be the case with single site, IP Site local channel or Capacity Plus Single Site configurations, then the bandwidth estimate at the site is a follows:

Total Number of Voice Channels at the Site = v

Total Number of Data Channels at the Site = d

Total Number of Repeaters at the Site = r

Uplink BW (IP traffic from repeater site to MNIS):

- Uplink BW (with Data Revert) = d*7.5 + r*1 kbps
- Uplink BW (without Data Revert) = v*7.5*0.4 + r*1 kbps

Downlink BW (IP traffic from MNIS system to repeater site):

- Downlink BW = v*7.5*0.4 + r*1 kbps

There are a few other considerations to take note of:

- An IPSC wide area channel or a local area channel is considered as one channel.

- In Capacity Plus Single Site:
  Total number of voice channels (V or v) = Number of Trunked Repeaters*2.
- In Capacity Plus Multi Site:
  Number of Voice Channels (V) = Number of Trunked Repeaters in System*2
  . Number of Voice Channels per Site (v) = Number of Trunked Repeaters per Site*2.
- The generic formula for MNIS IP bandwidth calculation is:
  BW = BW due to data messages + BW due to Link Management
- In the case of multiple MNIS instances, the IP bandwidth due to data messages gets distributed between them based on data messages received or sent by them. The IP bandwidth due to link management does not get distributed.
- Additional bandwidth must be budgeted when a VPN is used.

4.16.5.10.3
Considerations for Router with Networked Applications

An application that connects with the repeater system utilizes the Link Management procedure. The MNIS, Voice Dispatch Console, and RDAC are examples of applications that connect with the repeater system using this procedure. On the contrary, data applications like Location, Text, and others deployed with MNIS do not connect with the repeater system. To distinguish between them, an application that connects with the repeater system is defined as a networked application.

The repeaters and the networked applications establish connections with each other in the MOTOTRBO system. In deployments where a router/firewall with NAT is required, the router/firewall with hair-pinning support can be also required. The hair-pinning feature allows establishing communication between devices of the system when they are using a WAN side IPv4 address with NAT to communicate with other devices located in the same LAN. For more information about repeater configuration types and hair-pinning requirements, go to Repeater Network Configuration Options in Capacity Plus Single Site and Capacity Plus Multi Site on page 386.

4.16.5.11
MNIS Data Gateway and DDMS Computer Specifications

Table 88: MNIS Data Gateway and DDMS Computer Specifications

Component	Requirements
Operating Systems	Windows Server 2016
	Windows Server 2012 R2
	Windows 10 (64 bit)
	Windows 8.1 (32 and 64 bit)
Memory	MNIS and DDMS: 1 GB and above required by host Operating System
Hard Disk	MNIS and DDMS Prgrammer Install: 5 GB (Program Files & Database)
Software	Running multiple instances of MNIS and DDMS are not supported.

4.17

CSBK Data System Design Considerations

When configuring the CSBK data feature in a system, keep in mind the following items:

- CSBK data does not support Basic, Enhanced Privacy, or any foreseeable privacy features.
- CSBK data does not support confirmed data delivery mode even if the data call confirmed is configured by CPS.
- The CSBK data can only be routed to the PC through a USB connection.
- The ARS and LRRP protocols are enhanced to support CSBK data. Therefore legacy LRRP and ARS Application Server cannot work with the CSBK data feature enabled.
- The location information is compressed into a single CSBK, and recovered at the Control Station or MNIS with the location information of the repeater. IPSC/Capacity Plus Multi Site does not work with a Control Station for location CSBK data, because the Control Station does not know where the location data comes from. However, IPSC/Capacity Plus Multi Site works with the MNIS.
- When cadence 7.5 seconds and 15 seconds are expected, the feature should be enabled and window size set to one or two. Take note that a one-time window is not requested to send the GPS data missed periodic window when the cadence is 7.5 seconds or 15 seconds. This means location updates are not queued during voice calls. Therefore the update success rate gets impacted when the voice loading is high.
- The XCMP device to server raw data must not exceed seven bytes, otherwise the error indication gets broadcasted to the XCMP device.
- The following is a list of limitations for GPS report:
  - The distance between the radio and the repeater (receiving inbound GPS data over the air) must not exceed 130 miles (approximately 209 kilometers).
  - Latitude system error horizontal distance of less than 8 feet (approximately 2.4 meters) is introduced.
  - Longitude system error horizontal distance of less than 6 feet (approximately 1.8 meters) is introduced.
  - Speed-horizontal of 1 knot accuracy, maximum 138 miles (approximately 222 kilometers) per hour, is supported by an Enhanced GPS scheduled channel when GPIO pin status change is not required.
  - Direction-horizontal of 16 cardinal directions, is supported by an Enhanced GPS scheduled channel when GPIO pin status change is not required.
  - Info-Time of minutes and/or seconds, therefore suggested required maximum info age shall not exceed 50 minutes, is supported by an Enhanced GPS scheduled channel.

All radios, repeaters, MNIS, ARS and LRRP applications enabled with the CSBK data feature are backward compatible with radios before R02.30.00. To ease migration, ARS is transmitted as CSBK data when the feature is enabled through CPS per channel. The LRRP server knows if the radios have the capability to transmit the LRRP report as CSBK data through the ARS registration. The LRRP report cannot be transmitted as CSBK data when the channel is not enabled with CSBK data feature. Therefore, if the ARS message does not indicate CSBK data capability, the LRRP server should not send the LRRP request to demand the radio to transmit LRRP report as CSBK data. If such LRRP requests are sent before, the LRRP stop should be sent to the radio to cancel the request. There are a few considerations to take note of when enabling the CSBK data feature:

- ARS: When the feature is enabled by CPS, the radio sends the ARS registration as CSBK, the Control Station, and MNIS sends the ARS registration to the ARS server with optional payload 0x10 0x80 when the ARS CSBK data is received.
- ARS: When the ARS server (DDMS) sends the Device Registration ACK with optional payload 0x10 0x80, the Control Station and MNIS sends the ACK as CSBK data.

- LRRP: When the CSBK data feature is enabled at a channel via CPS and the location request contains a LRRP token for CSBK location feature (0x40, 0x01, 0x41), the LRRP (GPS) message with location data is sent as CSBK.
- LRRP: When the CSBK data feature is enabled at a channel through CPS, the LRRP (GPS) message without location data (such as LRRP triggered answer) is sent as CSBK. If the message cannot be carried in one single CSBK, it is sent as a DMR data packet.

4.18
GPIO Triggered Event Driven and Distance Driven Location Update System Design Considerations

When configuring the GPIO Triggered Event Driven and Distance Driven Location Update in a system, the following rules must be followed:

- To support GPIO Triggered Event Driven Location Update,
  - For portable, the Cable Type should be configured as Generic or Telemetry or Motorola Solutions if the cable is a smart Telemetry cable;
  - For both portable and mobile, the Feature of GPIO Physical Pins should be configured as Generic Input or Telemetry VIO, and if Telemetry VIO is configured, the Action of such VIO should be configured as output command because output command indicates the GPIO as an input pin.
- For Distance Driven Location Update, to avoid triggering the update too often, it is recommended to configure the distance to be 100 meters or larger.
- For GPIO triggered event driven update, the location report cannot be guaranteed if two events are triggered within 200ms.
- The GPIO Triggered Event Driven and Distance Driven Location Update is not sent periodically like the interval triggered GPS update; therefore, the reliability may be a concern and needs to be addressed. Some reliability considerations are as follows:
  - Don’t configure the gap between the updating distances to be too large. If the gap between the updating distances is reasonable, even if some location updates are missed over the air, the location tracking can still have enough updates;
  - At the same time, keep a periodic location update with a long interval, so that the subscriber will not be out of track when it’s not moving or moving slowly;
  - At Non-EGPS Channel, use confirmed GPS update. Note that confirmed data delivery can increase the reliability, but it also increases the time away from the home channel at the same time.

4.19
Customer Fleetmap Development

In a MOTOTRBO system, the system administrator can maximize the system's communication effectiveness by translating their organization's operation requirements into a list of supported features. The result of identifying and formalizing this information is often referred to as fleet mapping.

Fleet mapping can be thought of as:

- Assigning groups to the radios issued to personnel.
- Assigning groups to the dispatcher control positions.
- Assigning groups to channels and slots.
- Defining the feature subsets available to the personnel using the radios and dispatcher control positions.

A fleetmap determines how the radio communications for each user group of an organization is controlled. Through controlling communications between different user groups and between individuals within a group, the organization can manage the radio communications system resources efficiently. Fleet mapping also provides a structured approach to the management of a large number of radio users, and provides the opportunity to plan in advance for expansion or changes within an organization.

Some of the factors that should be considered when creating or planning changes to the fleetmap are:

- Identifying a functional fleetmap design team
- Identifying radio users
- Organizing radio users into groups
- Assigning IDs and aliases
- Determining feature assignments:
  - Private Calls
  - All Call
  - PTT ID and Aliasing
  - Radio Disable
  - Remote Monitor
  - Radio Check
  - Call Alert
  - Emergency Configurations
- Determining channel access requirements
- Determining subscriber programming requirements
- Determining data application access and requirements

4.19.1
Identify a Functional Fleetmap Design Team

To develop a fleetmap, a design team of key representatives from the customer's system managers, technicians, and operators needs to be formed to create effective communications plans for radio users and system operators.

4.19.2
Radio Users Identification

The system administrator needs to do the following to establish a fleetmap:

- Determine the customer's organizational structure from a radio user's perspective
- Consider the needs of portable and mobile radio users
- List all of the potential radio users in a single column on a spreadsheet
- Define the functional groups that use the system
- Group together radio users who need to communicate with each other on a regular basis

Typically, each functional group of radios has different communication requirements. Therefore, each functional group has their own codeplug for their radios that differs from other functional groups.

Table 89: Codeplug Communication Requirements

Codeplug	Functional Group	User Name	Alias	User ID	Talks with	Listens only to
construction.ctb	Construction	John	John	1873	Construction, Transport	Security
	Construction	Bob	Bob	1835	Construction, Transport	Security
	Construction	Rick	Rick	542	Construction, Transport	Security
security.ctb	Security	Al	Al	98	Security, Administrative	-
	Security	Joe	Joe	4762	Security, Administrative	-
administrative.ctb	Administrative	Frank	Frank	6654	Administrative, Security	-
	Administrative	Mike	Mike	19172	Administrative, Security	-
	Administrative	Steve	Steve	78378	Administrative, Security	-
transport.ctb	Transport	Lenny	Lenny	23	Transport, Construction	Security
	Transport	Carl	Carl	2	Transport, Construction	Security

4.19.3
Radio Users Organized into Groups

Once you have identified all of the individual users, associate them with groups. The communication requirements for one group may differ with the requirements of another group. Certain groups may need to communicate with multiple groups, in addition to their primary group. Therefore, identify the individual radios and the corresponding groups that they need to communicate with. Also note that the group organization may be different from the organization's formal reporting structure.

Determine the traffic patterns of the individual users and functional groups, so that channel, slot and group assignments can be associated with each user. Digital Repeater Loading on page 399 should provide information to help decide the distribution of groups, logical channel assignments (slots) and physical channel assignments.

When organizing the MOTOTRBO system, individual users, radios, and groups all have different requirements. Subsequently, they also have different parameters associated with them. Organize the radios, groups and slot assignments in a spreadsheet.

An example is shown in the following figure.

Figure 185: Radio Users Organized into Groups

							Functional group and talkgroup mapping							
							Construction			Security		Administrative	Transport	
							TG ID: 62	TG ID: 54	TG ID: 46	TG ID: 8766	TG ID: 123	TG ID: 99	TG ID: 997	TG ID: 368
							Cement factory	Metal shop	Carpenters	Patrol	Front desk	Admin	Delivery trucks	Cement mixers
							ch 1 - slot 1	ch 2 - slot 1	ch 2 - slot 1	ch 2 - slot 1	ch 1 - slot 1	ch 2 - slot 1	ch 1 - slot 1	ch 2 - slot 1
File codeplug as	Functional group	User name	Alias	User ID	Talks with functional groups	Listens only to functional groups								
construction.ctb	Construction	John	John	1873	Construction, Transport	Security	x							x
	Construction	Bob	Bob	1835	Construction, Transport	Security			x				x	
	Construction	Rick	Rick	542	Construction, Transport	Security	x	x	x					x
security.ctb	Security	Al	Al	98	Security, Administrative	-				x	x	x		
	Security	Joe	Joe	4762	Security, Administrative	-				x	x	x		
administrative.ctb	Administrative	Frank	Frank	6654	Administrative, Security	-					x	x		
	Administrative	Mike	Mike	19172	Administrative, Security	-					x	x		
	Administrative	Steve	Steve	78378	Administrative, Security	-				x	x	x		
transport.ctb	Transport	Kenny	Kenny	23	Transport, Construction	Security		x	x				x	x
	Transport	Carl	Carl	2	Transport, Construction	Security	x							

4.19.3.1

Configuring Groups

In MOTOTRBO systems, capabilities for Group Calls are configured through the subscriber (portable and mobile) CPS. The repeater does not require any specific configuration with respect to groups. There are three interrelated steps in configuring your radios to participate in Group Calls; it is configured through the “Contacts”, “RX Group Lists” and “Channels” menu folders in CPS. While the MOTOTRBO CPS enables great flexibility in configuring your system for Group Calling, one basic procedure is as follows:

Procedure:

1. In the **Contacts** folder, go to the **Digital** folder, and add a call type of **Group Call**.

   The CPS provides a default name and ID.

2. Assign a unique ID between 1 and 16776415, and also rename the Group Call to an intuitive alphanumeric name representative of the user workgroup that ultimately will be using this group, for example, “Maintenance.”

   All Calls created in the **Contacts** folder appear in the **Contacts** menu of the subscriber by name, and the Group name also appears on the radio display when a Group Call is received. In step 4, assign this Group Call, again by name, to the Transmit (TX) “Contact Name” attribute of a channel.

3. In the **RX Group Lists** folder, add a new group list, and then add the Group Call you just created to be a member of the list.

   The group list controls which groups a radio hears when tuned to a selected channel. For example, if members of the Maintenance group should also be able to listen to other groups on the channel,

those other groups would be added to the RX Group List; if members of the Maintenance group should only hear traffic related to their own group, then only the Maintenance group would be added to the group list. The group list should again be renamed to something intuitive; in step 4 assign this group list, by name, to the RX Group List attribute of a channel. In the channels menu, each “zone” can contain up to 16 channels that can be mapped to the 16-position top selector knob of the portable radio or the relative channel number selections on a mobile. Radio users that require more than 16 channels must organize them into multiple folders in CPS, so that they can be accessed as “zones” in the radio menu. Zones, if used, can and should also be given names.

4. In an appropriate folder, create a new digital channel. To fully define the channel, you must assign the appropriate receive and transmit frequencies, and also select the TDMA slot number.
5. Add the group list defined in step 3 to the RX Group List attribute, followed by adding the digital Group Call to the TX Contact Name attribute. Also define the TX Admit Criteria.
6. Rename the channel to something intuitive, and assign it to a knob position.

   The channel name is displayed on the radio whenever it is selected through the top knob on a portable or the up/down channel selection buttons on a mobile.
   If configured as described, radio users are able to place a Group Call simply by selecting the defined channel and pressing PTT. Groups can also be selected from the Contacts menu on display radios, as enabled in step 2. It is also possible to assign a Group Call to a radio programmable button (called a “one touch call” in CPS) so that users can place a Group Call at the touch of a button.

4.19.4
IDs and Aliases Assignments

Each radio, group, and Control Station in the system must have a unique ID number and alias. There should be no duplicate IDs on the system.

4.19.4.1
Radio ID Identification

Radio IDs for a MOTOTRBO system range between 1 and 16776415. The Radio IDs in CPSS are the same as the IDs in CPMS and range from 1 to 65535. There are two approaches to identifying Radio IDs:

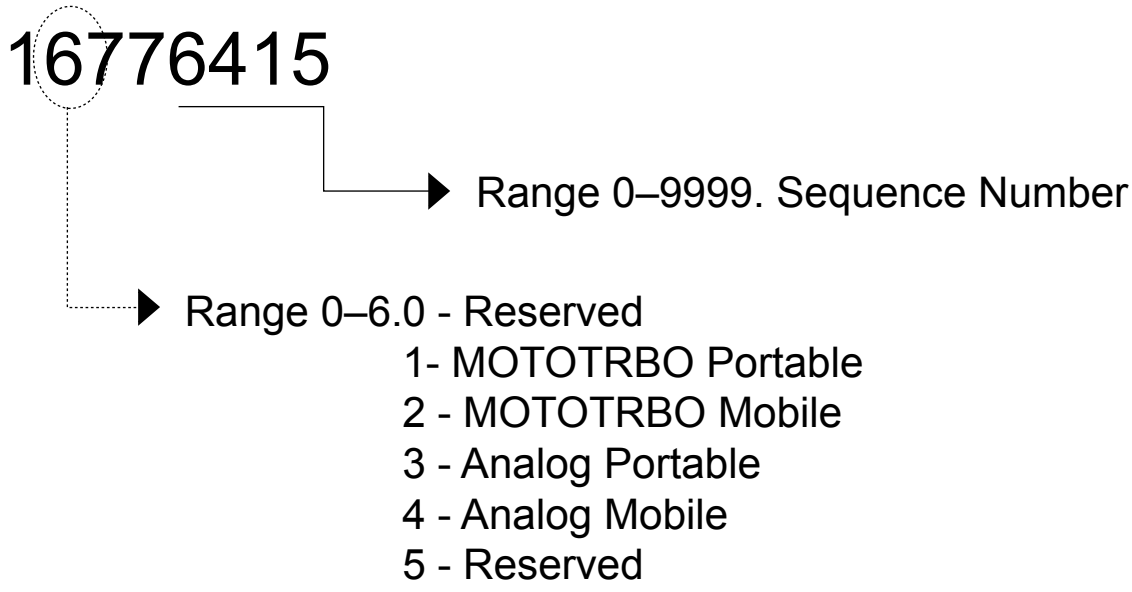
Option A

As a general practice, create contiguous ID ranges, but allow room for future expansion. As an example, a department has a current requirement for 1200 IDs. However, the department may need up to 2000 IDs in 12 months. Assigning the IDs during planning saves future re-programming of radios and subscriber records.

Option B

The Radio ID can be created so that each ID provides certain information about the radio. Each digit in the Radio ID can represent a certain code or radio type.

Figure 186: Radio ID Digits



NOTICE: The Radio IDs in CPSS are the same as the IDs in CPMS and ranges from 1 to 65535.

4.19.4.2

Radio Alias Assignments

You can assign an alias to each radio user. Although anything can be used as an alias, the user's last name is often used. Radios that are assigned to vehicles are often aliased with the vehicle number such as "Cab 35" or "Fire Truck 3." If radios are used by multiple users through different shifts, the job description is often used such as "West Side Guard" or "Cleaning Crew 2."

Since unique names are required, no two radio users should have the same alias. Aliases should be consistent in all radio programming (CPS), and the data applications. Databases are not shared between the various applications. There is no centralized database in MOTOTRBO. Since aliasing is done independently on each device, if the alias and ID do not match in each device in the system, customers may become confused.

An example of a spreadsheet showing a possible Radio ID and alias database is shown below:

Table 90: Examples of Possible Radio ID and Aliases

Functional Group	User Name	Alias	Unit ID	Talks with	Listens only to
Construction	John	John	1873	Construction, Transport	Security
Construction	Bob	Bob	1835	Construction, Transport	Security
Construction	Rick	Rick	542	Construction, Transport	Security
Security	Al	Al	98	Security, Administrative	-

Functional Group	User Name	Alias	Unit ID	Talks with	Listens only to
Security	Joe	Joe	4762	Security, Administrative	-
Administrative	Frank	Frank	6654	Administrative, Security	-
Administrative	Mike	Mike	19172	Administrative, Security	-
Administrative	Steve	Steve	78378	Administrative, Security	-
Transport	Lenny	Lenny	23	Transport, Construction	Security
Transport	Carl	Carl	2	Transport, Construction	Security

4.19.4.3
Group ID Identifications

Group IDs for a MOTOTRBO system range between 1 and 16776415. The same approach that is used to identify Radio IDs can be used for Group IDs. Group IDs are not centrally maintained or managed in a MOTOTRBO system. It is up to the system administrator to document the Group designation. Note that these IDs must match those entered in other radios and data applications in order for the system to operate correctly.

NOTE: The Talkgroup IDs in CPSS are the same as the IDs in CPMS and ranges from 1 to 254. The Talkgroup ID of 255 is reserved for “All Call”.

The Talkgroup IDs in CPSS are the same as the IDs in CPMS and ranges from 1 to 254. The Talkgroup ID of 255 is reserved for “All Call”.

4.19.4.4
Group Alias Assignments

The groups should also be consistent throughout the system. Display radios and data applications identify groups by alias. Groups should be named with an alias the customer can easily understand. Highly abstract names often cause confusion.

When assigning aliases, consider character and subscriber limitations. Some radio models may allow more or fewer characters than the data applications. Since aliasing is done independently in each device, if the alias and ID do not match in each device in the system, customers may become confused. The following figure is an example:

Figure 187: Example of Mismatched Aliasing

Functional group and talkgroup mapping							
Construction			Security		Administrative	Transport	
TG ID: 62	TG ID: 54	TG ID: 46	TG ID: 8766	TG ID: 123	TG ID: 99	TG ID: 997	TG ID: 368
Cement factory	Metal shop	Carpenters	Patrol	Front desk	Admin	Delivery trucks	Cement mixers
ch 1 - slot 1	ch 2 - slot 1	ch 2 - slot 1	ch 2 - slot 1	ch 1 - slot 1	ch 2 - slot 1	ch 1 - slot 1	ch 2 - slot 1

4.19.5
Determine Which Channel Operates in Repeater Mode or Direct Mode/Dual Capacity Direct Mode

Repeater mode enables unit-to-unit communications using the repeater. Direct mode/dual capacity direct mode enables unit-to-unit communications without using the repeater. Each channel on the radio is programmed to be either a direct mode channel, dual capacity direct mode or a repeater mode channel through the CPS.

Channels defined as Repeater channels in the CPS can be toggled to operate in Talkaround mode through user selection from the menu or a programmable button. When this happens, the transmit frequency is set equal to the receive frequency, and this channel effectively performs like a Direct Mode channel.

If a 12.5 kHz RF channel is used for dual capacity direct mode, both timeslots are provisioned for 6.25e direct mode only. Similar to repeater mode, 6.25e channels are configured via CPS to operate in either timeslot 1 or timeslot 2, and color code (0-14) can be provisioned differently in each timeslot. The full range of radio IDs and talkgroup IDs are available for use in 6.25e direct mode (dual capacity direct mode).

4.19.6
Supervisor Radios Feature

Supervisor radios are not defined in the CPS by any specific “Supervisor” option. Instead they are subscribers that have supervisory options enabled. Supervisor radios are responsible for acknowledging Emergency Calls and alarms, and also perform administrative duties such as remote monitor and selective radio inhibit. Some features should only be allowed to users that can use them responsibly.

4.19.7
Configuring the Private Calls Feature

In MOTOTRBO systems, capabilities for Private Calls are configured through the subscriber (portable and mobile) CPS. The repeater does not require any specific configuration with respect to Private Calls. While the MOTOTRBO CPS enables great flexibility in configuring your system for Private Calling, one basic procedure is as follows:

Procedure:

1. Program every MOTOTRBO radio in a system with an assigned a unique radio ID in the CPS.
   a. Go to the **General Settings** menu.
   b. In the **Radio ID** field, enter the radio ID.

2. In the **Contacts** folder, go to the **Digital** folder, and add a call type of **Private Call**.

   The CPS provides a default name and ID; assign the actual radio ID of the radio that is to be privately called to this field.

3. Rename the call to an intuitive alphanumeric name (representative of the radio to be addressed).

   All Calls created in the “Contacts” folder appear in the “Contacts” menu of the subscriber by name, and this name also appears on the radio display when a Private Call is received. If configured as described, radio users are able to make Private Calls by selecting the Private Call, by name, from the radio’s Contacts menu. In addition, similar to assigning a Group Call to a channel as described, it is also possible to assign a Private Call to the TX Contact Name attribute of a channel, so that users can place Private Calls by making the appropriate channel selection through the top knob on a portable or up/down channel select buttons on a mobile. It is also possible to assign a Private Call to a radio programmable button (called a “one touch call” in CPS) so that users can place a Private Call at the touch of a button. These latter two methods are the only methods for non-display radios to place Private Calls.
   A radio can, in practice, receive a Private Call from any other radio that is available on the channel, regardless of whether the receiving radio has created a CPS Private Call entry for that radio. The receiving radio displays the radio ID of the calling radio, rather than an alphanumeric alias. Similarly, a radio can place a Private Call to any other radio by utilizing the “manual dialing” option in the radio’s menu; however, the user must know the Radio ID of the called party.

4.19.8
Configuring the All Call Feature

In MOTOTRBO systems, capabilities for All Calls are configured through the subscriber (portable and mobile) CPS. The repeater does not require any specific configuration with respect to All Calls. While the MOTOTRBO CPS enables great flexibility in configuring a system for All Calls, one basic procedure is as follows:

Procedure:

1. In the **Contacts** folder, go to the **Digital** folder, and add a call type of **All Call**.

   The CPS provides a default name.

2. Rename the call to an intuitive alphanumeric name representative of the All Call feature.

   All Calls created in the **Contacts** folder appear in the “Contacts” menu of the subscriber by name. If configured as described, a user would initiate an All Call by selecting the call, by name, from the radio’s Contacts menu. Additionally, similar to assigning a Group Call to a channel as described, it is possible to assign an All Call to the TX Contact Name attribute of a channel, so that users can place All Calls by making the appropriate channel selection through the top knob on a portable or up/down channel select buttons on a mobile. This is the only method for a non-display radio to place an All Call.

   It is also possible to assign an All Call to a radio programmable button (called a “Number Key Quick Contact Access” in the CPS), so that users can place an All Call at the touch of a button. However, this method to initiate an All Call, is only supported on the display portable radios and through a keypad microphone with the alphanumeric display mobiles.

   Since All Calls are monitored by everyone on a slot, it is suggested that only supervisors be granted the ability to transmit All Calls.

4.19.9
Radio Disable Feature

In MOTOTRBO systems, Radio Disable is configured in the portable and mobile radio CPS. To allow a radio the ability to initiate this function, this option must be enabled in the CPS **Menu** settings. To permit (or prevent) a given radio from decoding and responding to this command, this option must be configured in the CPS **Signaling Systems** settings.

Since the ability to disable a user could be misused, it is suggested that only supervisors be granted the ability to initiate a Radio Disable.

4.19.10
Remote Monitor Feature

In MOTOTRBO systems, Remote Monitor is configured in the portable and mobile radio CPS. To allow a radio the ability to initiate this function, this option must be enabled in the CPS **Menu** settings. To permit (or prevent) a given radio from decoding and responding to this command, this option must be configured in the CPS **Signaling Systems** settings.

If a radio is configured to decode the remote monitor command, the duration that the target radio transmits after receiving a Remote Monitor command can be set in the CPS **Signaling Systems** settings of the target radio.

Since the ability to remotely monitor a user could be misused, it is suggested that only supervisors be granted the ability to initiate a Remote Monitor.

4.19.11
Radio Check Feature

In MOTOTRBO systems, Radio Check is configured in the portable and mobile radio CPS. To allow a radio the ability to initiate this function, this option must be enabled in the CPS **Menu** settings. All MOTOTRBO radios decode and respond to a Radio Check.

4.19.12
Call Alert Feature

In MOTOTRBO systems, Call Alert is configured in the portable and mobile radio CPS. To allow a radio the ability to initiate this function, this option must be enabled in the CPS **Menu** settings. All MOTOTRBO radios decode and respond to a Call Alert.

4.19.13
RX Only Feature

In MOTOTRBO, a radio can be configured as a receive only (RX Only) device and does not transmit. The RX Only mode of operation is useful when a radio user monitors the radio communication, or in hospitals where RF transmission is harmful.

System	Description
CPSS Capacity Plus Single Site	In Capacity Plus Single Site, Revert Control Stations should be configured as “RX Only” radios, only if the data messages are transported Over-The-Air as unconfirmed data messages. For confirmed data messages, an RX Only Revert Control Station does not send acknowledgement and a radio sends the same data message multiple times. Multiple

System	Description
	transmissions waste the air bandwidth and cause the server to receive duplicate messages.

4.19.14
Remote Voice Dekey Feature

In MOTOTRBO systems, Remote Voice Dekey is configured in the portable and mobile radio CPS. If used in a repeater system, the repeater does not require any specific configuration with respect to Remote Voice Dekey. However, the repeater requires the use of Transmit Interrupt capable software. To allow a radio the ability to initiate this function, this feature must be enabled through the CPS. Only MOTOTRBO radios provisioned with the ability to be interrupted can dekey in response to the Remote Voice Dekey command.

The Remote Voice Dekey feature can be used in direct, talkaround, or repeater modes of operation.

The Remote Voice Dekey feature is capable of remotely dekeying group voice calls and private voice calls; Emergency Calls and non-Emergency Calls; and can be used regardless of whether the initiating radio is a member of the call being remotely dekeyed. Since it is possible for this feature to remotely dekey a call that the radio is not unmuted to, the radio user may not be aware of the nature of the call that is being remotely dekeyed. Accordingly, it is recommended that this feature be enabled only in supervisor radios and the radio users be trained on the proper use of the Remote Voice Dekey feature.

The Remote Voice Dekey feature is not capable of remotely dekeying All Calls or non-voice (data or control) calls.

4.19.15
Emergency Handling Configuration

Configuring a communication system (like MOTOTRBO) to handle emergency situations requires some up front design. In emergency situations, it is ideal that when a user initiates an emergency, the user is immediately routed to someone who can handle his emergency situation. The previous sections have addressed some basic feature descriptions of how emergency can operate.

This section outlines in detail how to program the numerous devices in the system in order to meet the needs of a customer’s emergency needs and also provide some guidance on choosing the available options. It is recommended to review the sections in Digital Emergency on page 95 for emergency explanations.

It is important when creating an emergency handling plan to understand the customer’s existing emergency procedures. An interview with a representative in charge of emergency operations is usually required to fully understand the process. This information acts as a base for selecting a configuration.

4.19.15.1
Emergency Handling User Roles

The first step is identifying a user's participation in the emergency handling plan. There are three major roles to identify: Emergency Initiator, monitoring Supervisor, and Acknowledging Supervisor.

An Emergency Initiator is a user that does not necessarily have any responsibility for handling emergencies, but is expected, at some point to have an emergency that needs handling. This user’s radio is configured with either an emergency button or an external switch to initiate an emergency. The radio needs to be programmed on how to contact a Supervisor based on the selected configuration. Alternatively, this radio can be programmed to give a non-persistent indication (display and/or audio) that the current call is an Emergency Call. This indicates to the user that he should avoid interfering with the call taking place. The majority of users in a system will be considered Emergency Initiators.

A monitoring Supervisor is a user that needs to know when an emergency occurs, but is not the individual identified to handle and acknowledge emergencies. This user's radio provides an indication that an Emergency Alarm has been received and provide an indication that an Emergency Call is taking place. This user does not transmit an acknowledgment to the Emergency Alarm. The Emergency Alarm is persistent on the monitoring Supervisor's radio until manually cleared. Duplicate attempts of the same Emergency Alarm do not restart the Emergency indication. There can be multiple monitoring Supervisors per group. A monitoring Supervisor may also be an Emergency Initiator.

An Acknowledging Supervisor is the user specifically identified to respond to received emergency situations. This user's radio provides an indication that an Emergency Alarm has been received, and provides an indication that an Emergency Call is taking place. In addition to the indications, this user's radio is responsible for transmitting an acknowledgment to the Emergency Initiator. Until the Emergency Initiator receives the acknowledgment, Acknowledging Supervisor's radio continues to transmit its emergency alarm messages, until the Acknowledging Supervisor takes action to stop or the radio exhausts the number of programmed retries. It is important to note that the Acknowledging Supervisor's radio (not the user) sends the acknowledgment, when it receives the Emergency Alarm. Reception of an emergency alarm acknowledgment only guarantees that the radio received the message, not the user. Because it is the responsibility of the Acknowledging Supervisor to stop the Emergency Initiator's retries, duplicate attempts of the same Emergency Alarm restarts the emergency indication if cleared. It is highly recommended that there only be one Acknowledging Supervisor per group and slot. If there is more than one, acknowledgment messages may interfere with each other when transmitting, and cause a delay in acknowledging the Emergency Initiator. An Acknowledging Supervisor may also be an Emergency Initiator.

These MOTOTRBO radios are configured to operate in each role by setting a few options using the CPS, as described in the following table. These options are configurable per channel, and therefore per Group, Frequency and Slot. This means that a user can play a different role depending on the channel he has selected. He may be an Acknowledging Supervisor for one Group, but only an Emergency Initiator on another. The selected Digital System references a group of parameters used, when a user initiates an emergency. A radio programmed with a Digital Emergency System of None is not able to initiate an emergency on that channel. The parameters contained within the digital system are discussed in detail later.

Table 91: CPS Option per Channel

Emergency Handling Role	Digital Emergency System	Emergency Alarm Indication	Emergency Alarm Ack	Emergency Call Indication
Emergency Initiator	Selected	Disabled	Disabled	Optionally Enabled
monitoring Supervisor	Selected Or None	Enabled	Disabled	Enabled
Acknowledging Supervisor	Selected Or None	Enabled	Enabled	Enabled

By identifying the roles in the customer's organization, it should start to become clear how they handle emergencies at a high level. If there are numerous supervisors, it is important to note which groups these supervisors monitor, as there may be more than one supervisor that monitors multiple or all the groups. This is key to deciding on an emergency handling strategy.

4.19.15.2
Emergency Handling Strategies

There are two major strategies to handle emergency situations: Tactical or Centralized.

A Tactical emergency handling strategy is when the Emergency Initiators transmit their emergency alarm and call on the channel, group and slot they are currently selected on. This assumes that there is an Acknowledging Supervisor that is monitoring that same channel, group or slot. This means that each group

is required to have a designated supervisor whose responsibility is to handle emergency situations. Because emergency alarms do not traverse slots or channels, there would need to be one (and only one) supervisor designated for each group on every channel and slot. Multiple monitoring Supervisors could be configured to monitor for emergency alarms without sending acknowledgements to stop the Emergency Initiator's retries. It is also very important to note that because users are generally mobile it is possible that the Acknowledging Supervisor becomes unavailable, busy, changes channels, or roams out of range of the system. If this happens, Emergency Initiators may go unacknowledged.

In a system with a small number of users and groups, a Tactical strategy is often the easiest method to implement. When the number of users, groups, and channels grow, the required number of Acknowledging Supervisor also grows. It quickly becomes difficult to guarantee the multiple assigned Acknowledging Supervisors are actively monitoring their assigned groups. It is also often not cost effective to have numerous designated Acknowledging Supervisors handling emergency situations.

In order to operate Tactically, the Emergency Initiator must be on a channel that is configured with a Digital Emergency System, and has its **Emergency Revert Channel** set to **Selected** in the CPS. Since this is set on a per channel basis, a radio could be configured to operate differently based on the selected channel.

A Centralized emergency strategy is when the Emergency Initiators transmit their emergency alarm and call on a dedicated channel, group or slot. This strategy is often referred to as a "revert" strategy. This strategy assumes that there is one dedicated Acknowledging Supervisor whose job is to handle the emergencies of all users in the system, and that the Emergency Initiators automatically change or "revert" to the channel the Acknowledging Supervisor is operating on to process their emergency. Because this Acknowledging Supervisor's role is only to monitor for emergencies, it becomes easier to manage his availability. Further steps can be taken to guarantee the availability of the Acknowledging Supervisor. It is a good idea to locate the Acknowledging Supervisor's radio in a good RF coverage area of the system, so not to go out of range. Having a designated RF channel and slot that is specifically used for managing emergencies, lowers the possibility of encountering a busy system when there is heavy emergency traffic.

In larger systems the Acknowledging Supervisor's role in a centralized configuration is often referred to as a Dispatcher. It is not expected that this Acknowledging Supervisor leave their location and actually resolve the emergency. Their role is to contact and dispatch other resources to handle the emergency that was reported. The Acknowledging Supervisor is able to switch channels to dispatch assistance to the Emergency Initiator, and then switch back to the emergency channel.

In some cases multiple Centralized configurations may be required. This is often needed when the number of users becomes too much for one Acknowledging Supervisor to handle, or if the customer's organization is broken into multiple organizations that have their own Acknowledging Supervisor. This may also be required if a system contains multiple repeaters with non-overlapping RF coverage. While operating on one site, a radio may not be in range of another site, therefore if the radio were to revert to the other site to process an emergency, the radio may not be in the coverage range of the repeater to complete the transmission. In this scenario, it is recommended that an Acknowledging Supervisor be designated for each RF coverage range. This would require a radio to be configured to revert to channels within RF coverage of the selected channel.

In order to revert to a Centralized channel, the Emergency Initiator must select the channel that is configured with a Digital Emergency System, and has its Emergency Revert Channel set to the designated Emergency Channel in the CPS. Since this is configured on a per channel basis, a radio could be configured to operate differently based on the selected channel. There are 32 Digital Emergency Systems available. This means that one radio can be configured to revert to 32 different channels, depending on the configuration of the Digital Emergency System that is assigned to the selected channel.

It is not recommended that a Centralized emergency strategy be implemented using Emergency Initiators operating Tactically and one Acknowledging Supervisor scanning multiple channels. When multiple emergencies occur simultaneously it is more effective for the Emergency Initiators to come to the Acknowledging Supervisor rather the Acknowledging Supervisor searching for the Emergency Initiators.

4.19.15.3
Acknowledgement of Supervisors in Emergency

The emergency strategy of the Acknowledging Supervisor should be considered. Since this user is the one identified to handle emergencies, who should they attempt to contact if there is an emergency. In a tactical environment, the user may only need to change or possible “revert” to another channel to contact another Acknowledging Supervisor. In a centralized configuration with multiple dispatchers, one Acknowledging Supervisor dispatcher could be configured to revert to the other Acknowledging Supervisor dispatcher. If there is no other individual to contact, the Acknowledging Supervisor may simply wish to operate tactically, and transmit the emergency on the selected channel so that the monitoring Supervisors can be contacted.

4.19.15.4
Extended Emergency Call Hang Time

The MOTOTRBO repeater reserves the channel for a short duration after a voice transmission. By default the call hang time associated with an emergency is slightly larger than those for Group Calls and Private Calls. The repeater can be configured to extend the call hang time for Emergency Calls even longer to provide an additional opportunity for the Emergency Initiator or Emergency Acknowledger to communicate without competing with other users.

4.19.15.5
Emergency Revert and GPS/Data Revert Considerations

During registration with the Location Server the radio receives a periodic location update request and an emergency location update request. When the radio enters the emergency state, it attempts to transmit the emergency location update response on a specific channel. The transmission channel of this message is defined by the radio’s Emergency Mode (Emergency Alarm, Emergency Alarm with Call or Emergency Alarm with Voice to Follow) and its GPS Transmission Channel (Selected or Revert). Understanding which channel is used for the Emergency Location Update is important, as a Control Station is required on that channel to enable the reception of the message by the Application Server. For more information on emergency handling, see Emergency Handling Strategies on page 521.

The following sections define how Emergency Revert and GPS Revert interact when the Emergency Revert Channel contains a GPS Revert Channel and the radio received a Emergency Location Update Request on the Selected Channel. These are sample scenarios intended to aid in understanding the interactions.

The following sections use a direct mode configuration to simplify the diagrams, though they can also be applied to repeater mode. The radio initiating the emergency has been configured with the following channels; GROUP1, LOCATION 1, EMERGENCY and LOCATION2. The TX/RX frequency, the GPS Transmission Channel and the Emergency Revert Channel for each of the four configured channels are listed in the following table.

Table 92: Emergency Revert and GPS/Data Revert Considerations

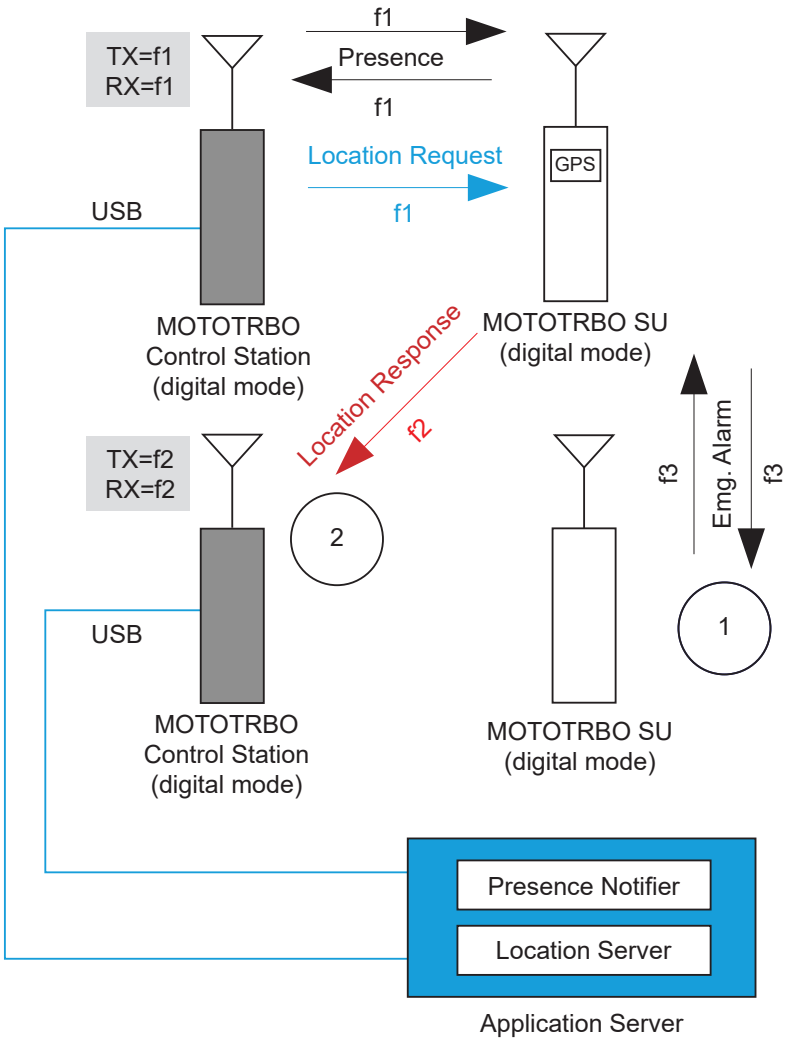
	GROUP 1	LOCATION 1	EMERGENCY	LOCATION 2
Transmit/Receive Frequencies	F1	F2	F3	F4
GPS Transmission Channel	LOCATION 1	None	LOCATION 2	None
Emergency Revert Channel	EMERGENCY	None	None	None

4.19.15.5.1
Emergency Alarm

Figure 188: Emergency Alarm and GPS Revert Interaction Diagram on page 524 illustrates the channels used when an emergency is initiated and the radio is configured for Emergency Alarm Only with an Emergency Revert Channel and the Emergency Revert Channel is configured with a GPS Revert Channel.

NOTE: The channels are defined in Table 92: Emergency Revert and GPS/Data Revert Considerations on page 523.

Figure 188: Emergency Alarm and GPS Revert Interaction Diagram



The following describes the sequence of events.

1. The radio switches from the Selected Channel, f1, to the Emergency Revert Channel, f3. From here the radio transmits the Emergency Alarm and waits for the acknowledgment. While waiting for the acknowledgment, the Emergency Location Update is held in queue.
2. Once the acknowledgment is received the radio switches back to the selected channel, f1, and transmits the Emergency Location Update.

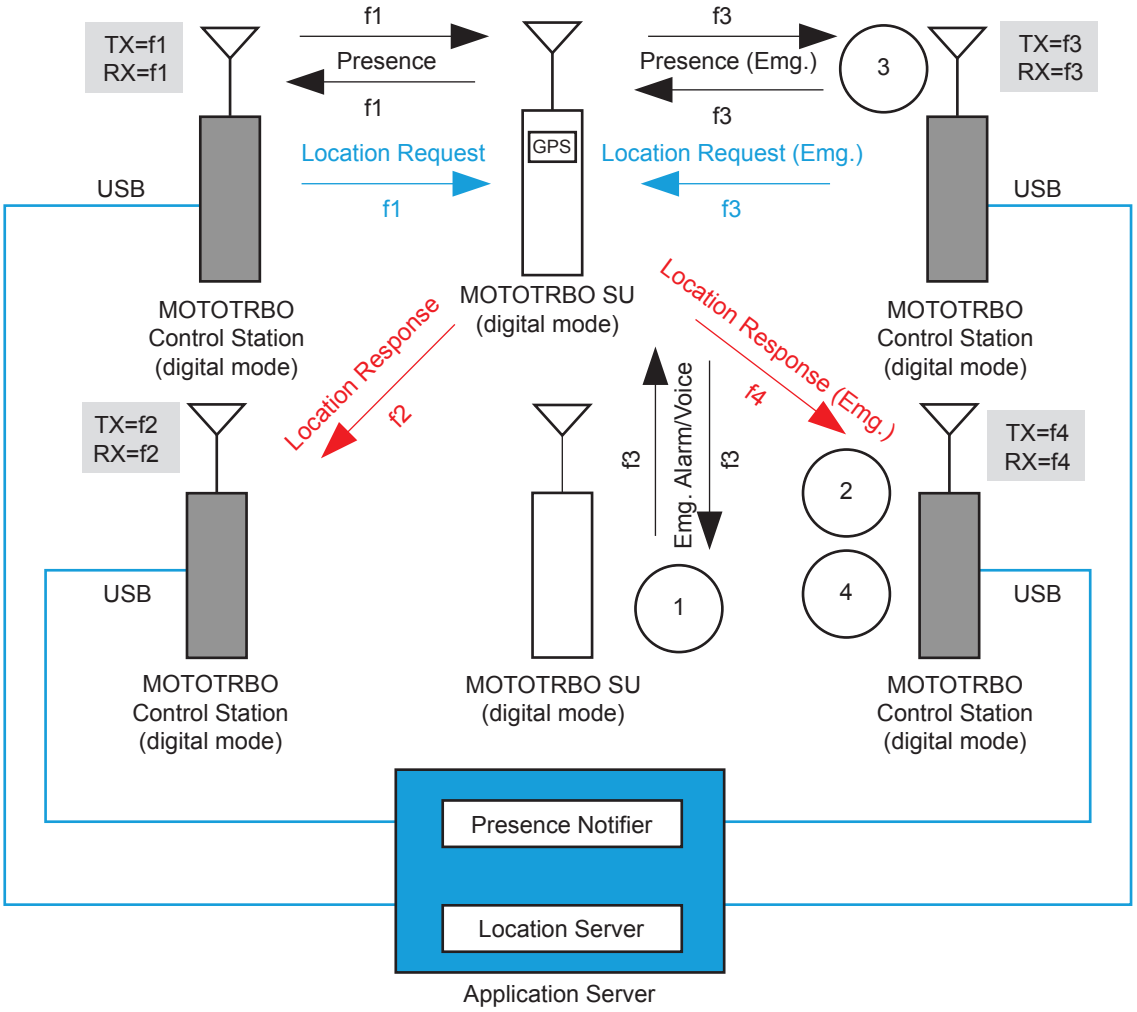
Therefore, in this scenario the GPS Revert Channel associated with the Emergency Revert Channel has no impact on the channel used to transmit the Emergency Location Update.

4.19.15.5.2

Emergency Alarm and Call

Figure 189: Emergency Alarm and Call and GPS Interaction Diagram on page 525 illustrates the channels used when an emergency is initiated and the radio is configured for Emergency Alarm and Call with an Emergency Revert Channel and the Emergency Revert Channel is configured with a GPS Revert Channel.

Figure 189: Emergency Alarm and Call and GPS Interaction Diagram



NOTE: The channels are defined in Table 92: Emergency Revert and GPS/Data Revert Considerations on page 523.

The following describes the sequence of events.

1. The radio switches from the Selected Channel, f1, to the Emergency Revert Channel, f3. From here the radio transmits the Emergency Alarm and waits for the acknowledgment. While waiting for the acknowledgment, the Emergency Location Update is held in queue.
2. Once the acknowledgment is received, the radio switches to the Emergency Revert's GPS Revert Channel, f4, and then transmits the Emergency Location Update.
3. After this transmission, the radio switches to the Emergency Revert Channel, f3, and while not being involved in voice calls, it registers.

   NOTE: This requires the Emergency Revert Channel to be ARS enabled.

4. After registration, periodic location updates are sent on the Emergency Revert's GPS Revert Channel, f4, until the emergency is cleared.

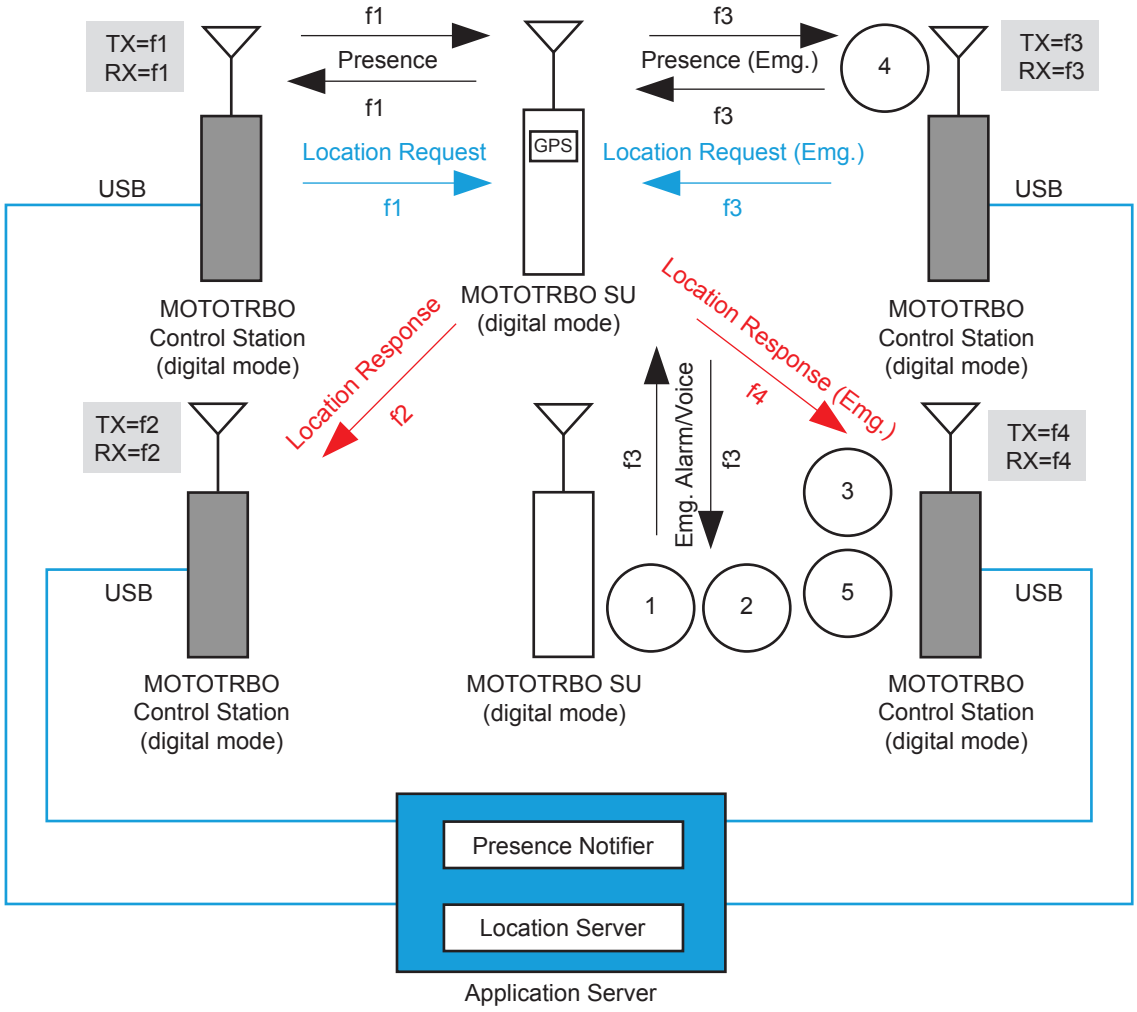
This configuration in Figure 189: Emergency Alarm and Call and GPS Interaction Diagram on page 525 is useful when a system needs to simultaneously support multiple Emergency Calls from multiple groups on a single Emergency Revert Channel. The placement of Emergency Calls on the Emergency Revert Channel and the location updates on a different channel significantly increases both emergency voice throughput and Location Update throughput while in the emergency state. It should be noted that changing the Emergency's GPS Transmission Channel to either the Selected Channel, f1, or the Emergency Revert Channel, f3, removes one Control Station from the system. The actual configuration selected depends on actual customer requirements.

4.19.15.5.3

Emergency Alarm with Voice to Follow

Figure 190: Emergency Alarm with Voice to Follow and GPS Revert Interaction Diagram on page 526 illustrates the channels used when an emergency is initiated and the radio is configured for Emergency Alarm with Voice to Follow with an Emergency Revert Channel and the Emergency Revert Channel is configured with a GPS Revert Channel.

Figure 190: Emergency Alarm with Voice to Follow and GPS Revert Interaction Diagram



NOTE: The channels are defined in Table 92: Emergency Revert and GPS/Data Revert Considerations on page 523.

The following describes the sequence of events.

1. The radio switches from the Selected Channel, f1, to the Emergency Revert Channel, f3, and then transmits one Emergency Alarm.
2. The radio remains on the Emergency Revert Channel, f3, and initiates an emergency voice call. During the emergency voice call the Emergency Location Update is held in queue.
3. Once the emergency voice call ends, the radio switches to the Emergency Revert's GPS Revert Channel, f4, and transmits the Emergency Location Update.
4. After this transmission, the radio switches to the Emergency Revert Channel, f3, and while not being involved in voice calls, it registers.

   NOTE: This requires the Emergency Revert Channel to be ARS enabled.

5. After registration, periodic location updates are sent on the Emergency Revert's GPS Revert Channel, f4, until the emergency is cleared.

This configuration in Figure 190: Emergency Alarm with Voice to Follow and GPS Revert Interaction Diagram on page 526 is useful when a system requires to simultaneously support multiple Emergency Calls from multiple groups on a single Emergency Revert Channel. The placement of Emergency Calls on the Emergency Revert Channel and the location updates on a different channel significantly increases both emergency voice throughput and Location Update throughput while in the emergency state. Changing the Emergency's GPS Transmission Channel to either the Selected Channel, f1, or the Emergency Revert Channel, f3, removes one Control Station from the system. The actual configuration selected depends on actual customer requirements.

4.19.16
Channel Access Configuration

Channel access methods must be specified in the radio's codeplug for each channel through the CPS, that is the TX (Transmit) parameters for each defined channel contains an Admit Criteria option that must be set to one of the three possible values described.

- Always,
- Channel Free, or
- Color Code Free.

An Admit Criteria of Always is sometimes referred to as "impolite channel access". An Admit Criteria of Channel Free is referred to as "polite to all". Finally, an Admit Criteria of Color Code Free is referred to as "Polite to own color code". In polite mode, the radio does not transmit on a channel if there is any activity detected on that channel. In impolite mode, the radio transmits on a channel regardless of any activity on that channel. When operating in impolite mode a radio user causes RF contention if there is another call on the same slot currently in progress. See MOTOTRBO Channel Access on page 83.

Radio users provisioned for polite operation press their PTT to determine if they can transmit or not. A Talk Permit Tone or Talk Denial Tone indicates if they have been granted or denied access. Impolite users are allowed to transmit regardless if the channel is busy or idle, although they would still require to wake the repeater.

The LED busy indication on the radios represents the presence of RF activity on the selected channel and is not specific to the digital slot currently being monitored. Therefore, if the LED indicates no RF activity on the channel, the radio user can be sure their slot is idle. However, if the LED indicates the presence of RF activity on the channel, the radio user does not know if their slot is actually idle or busy. If the radio users transmit when the LED indicates a busy channel, there is a chance their transmission may collide with another transmission. Care should be taken since RF collisions in digital mode most likely results in both transmissions not reaching their intended target. Therefore, it is highly recommend that only well trained and disciplined radio users are configured to have impolite channel access.

4.19.17
Zones and Channel Knob Programming

The MOTOTRBO radio is capable of being programmed with up to 160 channels. Each radio has a 16-position selector knob/switch, in which various channels and call types can be programmed. In order to maximize the programming capability of the radio, the concept of “zones” is introduced.

Zones can be created on the radio through the channels menu of the CPS. A “zone” can contain up to 16 channels that are mapped to the 16-position top selector knob of the portable radio or the channel number selector on a mobile. Radio users that require more than 16 channels must organize them into multiple zones in the CPS, so that they can be accessed as “zones” in the radio menu.

From the radio menu, the user can navigate to the “zones” icon, select it, and switch to a different zone. When in the different zone, the 16-position selector knob/switch is now programmed with that zone’s channels and call types. It is recommended that the Zone should be given aliases that can be understood by the end user.

4.20
Base Station Identifications (BSI) Setting Considerations

Base Station Identification (BSI), sometimes referred to as CWID, is used to identify the licensee operating a repeater or base station. Some form of station identification is usually necessary to comply with the requirements of the local radio regulatory authority.

The transmission time of the Base Station ID (BSI) is proportional to the number of characters in the BSI. To improve channel efficiency, it is recommended to keep the BSI length short. The content of the BSI needs approval from regulatory bodies (for example, FCC in USA). Regulatory bodies and their regulations may vary from nation to nation, thus customers are required to understand their own national laws and regulations while selecting BSI characters and its length.

BSI is available on the MOTOTRBO repeater when configured for analog or digital mode. In both modes, BSI is generated using a sinusoidal tone modulated on an FM carrier. The station transmits the configured Morse code alphanumeric sequence when one of two configured BSI timers has expired. The Exclusive BSI Timer is named TX Interval in CPS and the Mixed with Audio Timer is named Mix Mode Timer in CPS. The goal of these two timers is to minimize the impact to the ongoing traffic while still being compliant with regulatory authorities.

TX Interval is used to configure an “Exclusive BSI” which is sent the next time the repeater de-keys. The Mix Mode Timer is used to configure a “Mixed with Audio” which is mixed with the analog audio on the channel. Mixed with Audio BSI is only utilized when configured for analog operation. Mixing BSI with digital audio is not supported in MOTOTRBO.

When the Exclusive BSI Timer expires, the repeater transmits BSI the next time the repeater de-keys. This allows the BSI to be transmitted without disrupting on going voice, which is ideal. Furthermore, if the Exclusive BSI Timer expires while the repeater is not active (no subscriber activity) the repeater does not wake up and send BSI. Instead, it waits until the next transmission occurs and then transmits BSI upon de-key. BSI is only required during times of activity. Note that Exclusive BSI is interruptible in analog mode if the repeater receives a radio transmission. If interrupted, the BSI is attempted again at the next dekey. Also, whenever the repeater is forced to de-key due to a Time Out Timer expiring, it takes the opportunity to transmit an Exclusive BSI. Exclusive BSI is non-interruptible in digital and Dynamic Mixed modes.

When the “Mixed with Audio” BSI Timer expires, the repeater performs the BSI mixed with the on going audio on the channel. It is very important to note that there is a two minute hold-off timer when the repeater first keys up. The purpose of this additional hold-off timer is to make sure that the BSI is not mixed with audio immediately after being de-keyed for a long duration. This delay gives the repeater a chance to transmit the exclusive BSI before interrupting the audio.

Both the Exclusive BSI Timer and the Mixed with Audio Timer are reset after completion of a BSI transmission.

It is recommended that the Exclusive BSI Timer (TX Interval) is set at 75% of the regulatory authority's required BSI period and the Mixed with Audio BSI (Mix Mode Timer) is set at 95% of the regulatory authority's required BSI period. This way, the repeater begins attempting to send the BSI exclusively well before the required time. This interrupts the voice with mixed BSI as it gets closer to the required period if it has not found an opportunity to perform BSI exclusively.

BSI can be completely disabled by setting both the Exclusive BSI Timer and the Mixed with Audio BSI Timer to 255 in the CPS. It is not a valid configuration to disable the Exclusive BSI and only have the Mixed with Audio BSI enabled. This results in only Mixed with Audio BSI being sent in scenarios where the repeater is keyed for two minutes.

If the Exclusive BSI Timer is enabled, and the Mixed with Audio BSI is disabled, it is possible that during periods of heavy use, the BSI will not be generated within the configured time period. For , it is recommended that the Mixed with Audio BSI is enabled at all times.

Since Mixed with Audio does not operate in digital mode or in Dynamic Mixed Mode, it is possible that during extended periods of high activity the repeater never has a chance to de-key, and would therefore never have a chance to send BSI. This is more likely on a highly loaded GPS only repeater. This should be combated by lowering the traffic on the channel or by lowering the subscriber inactivity timer (SIT) in the repeater. This de-keys the repeater quicker between transmissions and provide a higher chance of de-key and therefore a higher chance of sending Exclusive BSI in the desired time frame.

Since Exclusive BSI is interruptible in analog mode, a situation may arise where extended periods of high activity may cause the repeater to continually dekey, attempt BSI and then be interrupted by another inbound transmission. The dekeying and re-keying of the repeater causes the hold off timer to be reset and the Mixed with Audio BSI is never triggered unless a particular transmission lasts over two minutes. In this case, it is recommended that the hangtime be increased so that the repeater does not dekey between every transmission. If this period of high activity occurs longer than two minutes, the Mixed with Audio occurs, otherwise the Exclusive BSI occurs during a period of decreased traffic load.

It may not be desirable to enable Mixed with Audio BSI with the use of analog data (i.e. MDC or VRM data). The mixing of the BSI with the analog signaling may most likely cause the signaling to become corrupted.

4.21
GPS Revert Considerations (For Single Repeater and IP Site Connect only)

GPS revert, when used correctly, can significantly improve the integrated voice and location data performance of a system.

To maximize location throughput while minimizing missed data (text, telemetry, and others) and voice transmissions, there are a number of factors that must be considered:

- Non-location update traffic should not be transmitted on the GPS Revert Channel when attempting to maximize the Location load on the GPS Revert Channel.
- Avoid adding the GPS Revert Channel into the Scan List if the location load is high, as scanning radios often land on this channel and qualify traffic that is not for them. This can slow down scanning.
- While in repeater mode, avoid placing the alternate slot associated with GPS Revert Channel into the Scan List if the location load is high. Scanning radios often land on this channel to qualify traffic that is not for them. This can slow down scanning.

- For single site mode, the Revert Channel must be set to “Selected” on the radio used as the Control Station.

  NOTE: For IP Site Connect mode, the Revert Channel must be set to “Selected” on the radio used as the Control Station.
- It is not recommended to use a portable as a Control Station, but if a portable is used as a Control Station then battery saver mode should be disabled since the Location Update messages are not preceded with preambles.
- Voice, data or control messages that are sent to an radio on the GPS Revert Channel are not received. The radio is only on the GPS Revert Channel to transmit location updates and it DOES NOT qualify activity on this channel.
- If group data is to be supported on a system, the inclusion of preambles should be added to minimize the occurrence of the group data message being missed while an radio is on the GPS Revert Channel.
- Avoid situations where a large number of subscribers are powered on in a relatively short period of time as this causes a flood of registration messages that impacts the voice quality of service on the Selected Channel during the registration process. GPS Revert and Loading on page 411 for recommendations on minimizing impact when using Motorola Solutions applications.
- In order to minimize users from inadvertently changing a radio to the GPS Revert Channel, it is recommended that the GPS Revert Channel(s) is placed in a different zone than the primary voice and data channel(s).

4.22 Enhanced GPS Revert Considerations

The following is a summarized list of items to keep in mind when configuring the Enhanced GPS feature in a system:

- All GPS and raw data messages from the option board and non-IP peripheral devices are not supported over the Enhanced GPS Revert Channel for one-time and periodic transmissions.
- If a repeater slot configured as “Enhanced GPS Revert” is power cycled, the subscriber’s GPS updates scheduling begin again because the scheduling information is not stored in the repeater’s memory.
- The window size on all repeaters and subscribers should match.
- GPS data must be configured as “unconfirmed” on the GPS Revert Channel on the radio.
- Enhanced GPS only requires to be enabled on the Enhanced GPS Revert Channel of the radio, and not on the Home channel. However, if header compression is planned for use, then this feature needs to be enabled on the Home channel instead.
- For single site mode, the Revert Channel must be set to “Selected” on the radio used as the Control Station.

System	Description
IPSC IP Site Connect	For IP Site Connect mode, the Revert Channel must be set to “Selected” on the radio used as the Control Station.

- Only Enhanced GPS-configured subscribers can work on the Enhanced GPS Revert Channel. This feature do not support the following configurations:
  - Legacy revert repeaters working with Enhanced GPS Revert subscribers

  - Legacy subscribers working with Enhanced GPS Revert repeaters
  - Legacy repeaters working with Enhanced GPS Revert repeaters in IP Site Connect mode
- An application making a periodic request with the Enhanced GPS feature should only make a request with a cadence of 0.5, 1, 2, 4, and 8 minutes. When the window size is 1 or 2 with the CSBK data feature enabled, the application should only make a request with a cadence of 7.5, 15, 30, 60 and 120 seconds. If the cadence is different, the subscriber responds with a LRRP error message “PROTOCOL_ELEMENT _NOT_SUPPORTED”. This is also valid for persistent requests.
- A radio can only have one periodic request at a time. If “Persistent Storage” is enabled on the radio, the user must send a Triggered-Location-Stop-Request from the application before sending a new periodic request. If the user needs to change the application, then the user should either delete all requests from the Persistent Storage through the CPS or ensure that a Triggered-Location-Stop-Request is sent from the first application before a new periodic request is sent by the new application.
- The ARS initialization delay feature is recommended if a customer plans to use Enhanced GPS in a system that has many subscribers powering on at the same time and all of them need ARS. This helps to reduce ARS collisions at power up. More details in ARS Initialization Delay on page 126.
- If CWID is enabled, no GPS updates will be sent out while CWID is being transmitted. The user can choose to disable CWID via the CPS if needed.
- If there are free windows available in a system, these may be used by the repeater to go into hibernate mode (no transmission from repeater). Chances of hibernation could be increased by: .
  - Using CPS configuration to reserve more one-time windows by decreasing "Periodic Window Reservation(%)" parameter to 60% or 45%.
  - Enabling CPS configuration "Shared Channel Frequency" to allocate windows for GPS data in a cumulative manner at the beginning of a data frame. It reduces data transfer overhead (number of wake up and hibernate actions) thus increasing the possibility of channel utilization. However, this leads to more channel collision when the subscribers send window requests and delay in handling GPS data.

    NOTE: Default configuration "Shared Channel Frequency" disabled causes that allocated windows are spread through the whole data frame to handle GPS data as soon as possible.
  - Using CPS configuration “Window Size” to reduce window size to 1 or 2 with the number of subscribers and GPS update rate unchanged. It causes an increase of free windows available in a system.

    NOTE: To avoid uplink collision, when the window size is 1 or 2 with CSBK data feature enabled, disable the "Shared Channel Frequency" CPS configuration on the EGPS channels.
- The CSBK data feature is recommended when high system throughput is required. Refer to Table 16: The System Throughput on page 125. However, there are some limitations to this feature.

4.22.1
Single Site Mode

In Single Site Conventional mode, all location responses are sent over the repeater slot configured as Enhanced GPS revert.

The following three configurations are possible:

- **One slot configured as Enhanced GPS Revert and another slot for voice and data:** In this configuration, only location responses are sent over the Enhanced GPS Revert Channel. Voice, text messages, ARS, and other data are sent over the other slot.
- **Both slots configured for Enhanced GPS Revert:** This configuration is recommended if the number of subscribers sending location updates exceeds the capacity of one Enhanced GPS slot. In this case, a second repeater would be needed to support voice, text messages, ARS and other data.

- **Alternative slot configured for Enhanced GPS Revert:** This configures the alternative slot (that is, the other slot) for enhanced GPS transmission instead of using a data revert channel on a different repeater. Because the subscriber is using the alternative slot of the same repeater as the GPS Revert Channel, it does not need to spend a lot of time (in sync) switching between different repeaters. This configuration can minimize audio holes, and the subscriber can even send GPS update while receiving voice calls. It also allows GPS data transmission in either CSBK data or packet data format. However, CSBK data results in a smaller audio hole (~60ms or less) owing to its single burst format. This configuration is recommended to be used with the CSBK data format.

4.22.2
Capacity Plus Single Site and Capacity Plus Multi Site Modes

CPSM In Capacity Plus Single Site and Capacity Plus Multi Site modes, all location responses and ARS registration messages are sent over the repeater slot configured as Enhanced GPS Revert.

A data revert repeater can be configured for Enhanced GPS revert and the following two configurations are possible through the CPS:

- **One slot configured as Enhanced GPS Revert and another slot for Data Revert:** In this configuration, GPS and ARS registration data are sent over the slot configured as Enhanced GPS revert. All other data and voice either goes on the Data Revert slot or on the Trunked Channels.
- **Both slots configured for Enhanced GPS Revert:** This configuration is recommended if the number of subscribers sending location updates exceeds the capacity of the Enhanced GPS throughput of one slot. In this configuration, a separate data revert repeater or trunked repeaters can be used for other data such as voice, text messages, and server bound data.

4.22.3
IP Site Connect Mode

IPSC

In IP Site Connect mode, GPS updates are routed on the slot configured as wide area Enhanced GPS revert slot.

Three configurations are possible through the CPS for a wide area Enhanced GPS Revert system:

- **One slot configured as Enhanced GPS Revert and another slot for voice and data:** In this configuration, one slot of all the peers in the network is configured for Enhanced GPS operation while the other slot can be used for voice, ARS, text messages, and all other server data.
- **Both slots configured for Enhanced GPS Revert:** This configuration is recommended if the number of subscribers sending location updates exceeds the capacity of the Enhanced GPS throughput of one slot. In this configuration, the entire IP Site Connect system is used for sending location updates only.
- **Alternative slot configured for Enhanced GPS Revert:** This configures the alternative slot (that is, the other slot) of the same repeater for enhanced GPS transmission instead of using a data Revert Channel on a different repeater. This configuration can be applied to both local channels or wide area channels. Because the subscriber is using the alternative slot of the same repeater as the GPS Revert Channel, it does not need to spend a lot of time (in sync) switching between different repeaters. This configuration can minimize audio holes, and the subscriber can even send GPS update while receiving voice calls. It also allows GPS data transmission in either CSBK data or packet data format. However, CSBK data

results in a smaller audio hole (~60ms or less) owing to its single burst format. This configuration is recommended to be used with the CSBK data format.

4.22.3.1
Other Considerations

IPSC

Only one repeater in the wide area Enhanced GPS Revert system should select a value for **Period Window Reservation** in the CPS. All other repeaters should choose a value of **None** for this field. If the inter-repeater communication delay is more than 60 milliseconds, then the window size should exceed seven.

4.23
Enhanced Channel Access Consideration

The Enhanced Channel Access (ECA) feature is a channel access procedure in which a call initiating radio transmits a channel access request and listens on the channel to determine the status of the request. The radio continues with the transmission of the call only when access to the channel is obtained. Only one of the requesting radios can obtain channel access to proceed with the call transmission. The ECA provides the ability to reserve a channel Over-The-Air for one of the call initiating radios, and provide exclusive access to that radio for a short duration.

Enhanced Channel Access is a Motorola Solutions proprietary feature and is not defined in the DMR standard.

NOTE: ECA is applicable only in repeater mode in Single Site Conventional mode of operation.

System	Description
IPSC IP Site Connect	It is applicable only in repeater mode in IP Site Connect mode of operation.
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	ECA is not required in Capacity Plus Single Site or Capacity Plus Multi Site modes because their call startup processes implicitly included ECA.

4.23.1
Enhanced Channel Access Advantages

- It improves voice/data call success rate by minimizing Over-The-Air call collisions due to multiple radios keying up within close proximity.
- It prevents call transmission when the radio is out of inbound range (but within the outbound range) and provides correct call status indication to the user.
- It improves the GPS data success rate on the GPS Revert Channel by minimizing collisions.
- Prioritized channel access for an initiating radio to proceed with a call, among other radios.

4.23.2

Enhanced Channel Access Limitations

Enhanced Channel Access is configurable on the radio and can be enabled or disabled on a conventional digital channel and GPS/Data Revert Channel.

When enabled in the radio, the repeater supports ECA on conventional digital channels. However, the repeater does not support this feature on Enhanced GPS and DMM channels.

System	Description
IPSC IP Site Connect	Enhanced Channel Access is configurable on the radio and can be enabled or disabled on a IPSC LACs, IPSC WACs. When enabled in the radio, the repeater supports ECA on IPSC LACs, IPSC WACs. However, the repeater does not support this feature on Enhanced GPS and DMM channels.
CPSM Capacity Plus Single Site and Capacity Plus Multi Site	ECA is built into Capacity Plus Trunked Channels and is not configurable by the user. This feature is disabled and not required when the Enhanced GPS feature is enabled on the channel because each radio transmits during an assigned time window. When enabled in the radio, the repeater supports ECA on Capacity Plus Data Revert Channels. However, the repeater does not support this feature on Enhanced GPS and DMM channels.

When enabled, ECA is applicable only to polite transmissions initiated by the radio user. If the Admit Criteria in the radio is configured as Channel Free or Color Code Free, the radio applies the ECA procedure when a voice call is initiated. If the Admit Criteria is configured as Always, the ECA procedure is not applied. Data and CSBK calls are always polite transmissions, regardless of the configured Admit Criteria. Therefore, ECA is applied during call transmission if the feature is enabled. However, this slightly increases the system/voice access times for voice calls and latency for data, CSBK calls.

System	Description
IPSC IP Site Connect	When a radio auto roams to a new site in an IPSC system configuration, the radio applies the ECA configuration from the roamed channel and the Admit Criteria from the selected channel.

For phone calls occurring in all system configurations, ECA is enabled by default to achieve optimum performance. It is also recommended to enable ECA on all radios accessing the channel to derive maximum benefit from the feature.

NOTE: For a correct and reliable operation, it is strongly recommended to upgrade the repeater firmware version to R01.08.00 or later, before initiating calls with the ECA feature enabled on the radio.

4.24

Failure Preparedness – Direct Mode Fallback (Talkaround)

NOTE: Occasionally, Talkaround mode is incorrectly referred to as “direct mode”, but they are different. Direct mode is a mode of operation in a system environment whereby no repeaters are present. Talkaround mode is direct radio-to-radio communication for systems that primarily use a repeater but occasionally communicate without a repeater.

A repeater channel is defined by having different receive and transmit frequencies, and any channel that is programmed with the CPS to have different receive and transmit frequencies are considered to be a repeater channel and the MOTOTRBO radio expects a repeater operating on that channel. The radio user receives an access-denied tone if there is no repeater available or if the radio is out of range of the repeater. Channels defined as repeater channels in CPS can be modified to operate in Talkaround mode through user selection from the menu or a programmable button. When a repeater channel is thus modified to operate in Talkaround mode, the transmit frequency is set equal to the receive frequency, and it effectively becomes a direct mode channel. The system now performs similarly to the direct mode topologies we have previously described.

4.25

Failure Preparedness – Uninterrupted Power Supplies (Battery Backup)

To determine the UPS capacity, follow these simple steps:

Procedure:

1. List all equipment to be protected by the UPS on a worksheet.
2. Read the nameplate data on each of the devices listed. Write down the voltage and amperage for each device.
3. Multiply the voltage by the amperage of each device to calculate the Volt/Amps (VA).

   Some equipment, such as PC power supplies, may be marked with a power consumption measured in Watts.
4. Convert Watts to VA by dividing Watts by 0.65 (for a power factor of 0.65), or multiply by 1.54.

   The power factor refers to the relationship between the apparent power (volt-amps) required by the device and the actual power (watts) produced by the device.
5. Total the VA for all devices designated to protect with the UPS and enter it in the “Subtotal” field.
6. Multiply the subtotal found in step 5 by 0.25 and enter it as the “Growth Factor”.

   This number takes into account room for future growth. This growth factor allows for a 5% rate of growth for each year over a five-year period.
7. Add the “Growth Factor” to the “Subtotal” to get the “Required VA”.
8. Select the appropriate UPS model by choosing a model that has a VA rating at least as large as the “Required VA” that was calculated.

4.26
Dynamic Mixed Mode System Design Considerations

During Dynamic Mixed Mode (DMM) operation, the repeater dynamically switches between and digital modes to transmit and digital calls. It is only supported in Single Site Conventional mode. A Dynamic Mixed Mode channel is a programmable channel in the repeater and the channel can be added using the CPS.

To support the DMM feature in the repeater, the following design rules have been laid out.

- Once a call type (or digital) has been qualified, the repeater does not attempt to qualify another call type until the current call is complete, including the call hang time hang and channel hang time. For digital calls, the hang time needs to be expired on both logical channels. call type includes an Over-The-Air call or any operation (PTT, pin knockdown) on the 4-wire Repeater Interface (ARI) trying to access the repeater.
- Console device(s) are supported only when the repeater has not qualified an Over-The-Air digital call. An audible alert (channel busy tone) is generated over the speaker and Rx audio pins on the 4-wire repeater interface to indicate that the channel is busy and that the console access has been denied.
- Only PL (DPL/TPL) squelch type repeat is supported in MOTOTRBO repeater as CSQ repeat is not supported. However, if the receive squelch type is configured to CSQ, the received audio is sent over the Rx audio accessory pin for community repeater operation.
- To ensure proper Dynamic Mixed Mode operation, only exclusive CWID transmission is supported in MOTOTRBO repeater operating in Dynamic Mixed Mode, while mixed CWID is not supported in order to be compliant with the digital mode of operation. Furthermore, the exclusive CWID transmission cannot be interrupted by either Over-The-Air or repeater accessory PTT transmission.

4.26.1
Configuring Considerations for a Dynamic Mixed Mode System

A few repeater and subscriber configuration recommendations have been laid out to ensure proper Dynamic Mixed Mode (DMM) system operation.

Procedure:

1. For analog repeater operation, configure the Rx and Tx squelch types as PL (TPL or DPL) in the repeater.

   The Dynamic Mixed Mode repeater does not repeat if Rx squelch is configured as CSQ.
2. Configure the Tx and Rx squelch types as PL (TPL or DPL) in both legacy analog and MOTOTRBO radios.

   If Rx squelch type is configured as CSQ, the radios unmute to digital transmission and play out digital noise.
3. Configure the admit criteria of both analog and digital radios to be polite to each other.

   MOTOTRBO radio configuration recommendations are provided in the table below. For legacy analog radios, it is recommended to configure the polite rule as Busy Channel Lockout on Wrong PL code.
4. If MOTOTRBO radios need to communicate on their digital channels with the legacy analog radios or with MOTOTRBO radios on analog channels, the digital channels can be configured to scan for analog channels by way of scanning DPL or TPL.

Scanning may result in an initial audio truncation and the truncation depends on the number of scan members in the Scan List. To prevent loss of digital data transmission, it is recommended to configure the preamble duration as per the recommendations listed in Scan Considerations on page 156.

5. It is recommended to have a digital channel as the home channel and add the analog channels to the Scan List.

   This is because the scanning radios can receive data messages only on the home channel.

6. Priority sampling and channel marking CPS configurations are recommended to be disabled in Dynamic Mixed Mode system.

   See Priority Sampling on page 155 and Channel Marking on page 155 for more details.

Result: Some of the CPS configuration recommendations are listed in the following table.

Table 93: Dynamic Mixed Mode System CPS Configuration Recommendations

Repeater Configuration	Description
Channel	Add a new DMM channel and program the parameters in that channel.
Repeater Type	Configure this to Single Site. IP Site Master and IP Site Peer configurations are not supported in Dynamic Mixed Mode system.
SIT	Configure SIT so that the channel hang time (SIT – Group/Private/Emergency Call Hang time) is as small as possible. This allows users to get almost immediate channel access once a digital call ends. Channel Hang Time = SIT – Call Hang Time When SIT = 7 seconds and Group Call hang time = 5 seconds, Channel hang time = 2 seconds for that group voice call. When SIT = 7 seconds and Private Call hang time = 4 seconds, Channel hang time = 3 seconds for that private voice call.
Rx Squelch, Tx Squelch	Configure this to TPL or DPL for non-community repeater operation. Received audio is repeated out. OR Configure this to CSQ for community repeater operation. Received audio is not repeated out. The audio is instead sent over the Rx audio accessory pin.
Strip PL	Check this box to ensure that PL is not added to CWID.
TX Preamble Duration	This duration depends on the number of scan members in the Scan List. See Scanning and Preamble on page 157 for more details. If the radios are required to scan analog channels, then it is recommended that the digital channels scan as few in number of analog channels as possible.
Rx Squelch Type	Configure this to TPL or DPL. If configured for CSQ, the radios unmute to all digital transmissions and play digital noise.
Tx Squelch Type	Configure this to TPL or DPL. Repeater does not repeat if there is no PL in its received signal.
Admit Criteria	Configure analog channel Admit Criteria to “Correct PL”. See Polite to Other Analog System Operation on page 85 for more details. Configure Digital channel Admit Criteria to “Channel Free”.

Repeater Configuration	Description
	See Polite to All Operation on page 84 for more details.
Priority Scanning	Disable priority scanning on all scan members in the Scan List.
PL Type (in Scan List)	It is recommended to configure this to Non-Priority channel so that PL decoding is performed on non-priority Scan List member channels.
Channel Marker (in Scan List)	Disable channel marker.
Talkback	Check this box to allow the radio to talk back on the channel it unmuted during the scan.
Tx Designated Channel	Choose “Selected” or one of the configured scan members as needed. However, it is not recommended to configure the “Last Active Channel”.
Hang Time	Configure this value to as small as possible so that the radios can start scanning immediately.
Digital Hang Time	In a DMM system, the repeater reserves the channel for digital calls till the end of SIT + 1 second. Since no analog calls are allowed until then, it is recommended to configure this to SIT + 1 second.
RSSI Threshold	Adjust this value based on the RF interference level. See MOTOTRBO Channel Access on page 83 for a more detailed description of this field.

4.26.2
Distribution Considerations in a Dynamic Mixed Mode System

A digital transmission may occupy a repeater's physical channel for twice as long as an analog transmission since there are two logical digital channels on each physical channel and transmissions may occur on each logical channel one after another. With a relatively small number of digital radios in Dynamic Mixed Mode system, it is recommended to configure digital radios to operate on only one logical channel during migration to provide fair channel access between and digital transmissions.

As more digital radios start replacing the analog radios, distribute some of the digital radios to use the other logical channel. It is important to note that heavy users of one category (analog or digital) occupies the channel longer than the users in the other category when they are in a polite system configuration.

It is recommended to keep digital channel hang time to the minimum, or as low as possible, to allow fair channel access between analog and digital calls. However, with a smaller channel hang time, the system access time for digital calls may increase due to the fact that the radios need to wake up the repeater before calls.

4.27
Advanced Over-The-Air Radio Programming Configurations

The configuration software has some basic deployment options for OTAP. The Radio Management (RM) application works the same regardless of the underlying system architecture. There are no settings within the application for the specific system configuration, besides those to be programmed into the radios. This section highlights some special system configurations and some considerations that should be taken when using them. Unless specifically noted, these configurations can be used with or without a DDMS, with or without a remote RM Client, and up to 16 Control Stations.

4.27.1
MOTOTRBO Network Interface Service (MNIS) Configuration

The MNIS must be configured with all the following parameters:

- Confirmed data enabled
- UDP header compression disabled
- All voice privacy keys utilized in the system
- Unique MNIS Application ID

Failure to properly set these parameters could result in diminished coverage, longer delivery and retrieval times, or no communication at all. These settings apply to all system types.

UDP header compression increases the number of lower-layer headers, which decreases reliability. The decrease in reliability is not worth the benefits of the compression in the case of large messages.

The MNIS Application ID plays a Radio ID role and should not duplicate the Radio ID of another device in the system. The MNIS uses the MNIS Application ID to monitor and transmit on the radio network and it is similar to the Radio ID of the Control Station.

4.27.2
Control Station Configuration

The Control Station must be configured with the appropriate system type parameters for the channel or system being monitored.

Additionally, the Control Stations connected to the RM Server and RM Device Programmer must be configured with all the following parameters:

- Confirmed data enabled
- UDP header compression disabled
- All voice privacy keys utilized in the system
- Unique Radio ID
- ECA enabled

Failure to properly set these parameters could result in diminished coverage, longer delivery and retrieval times, or no communication at all. These settings apply to all system types.

UDP header compression increases the number of lower layer headers, which decreases reliability. The decrease in reliability is not worth the benefits of the compression in case of large messages. ECA minimizes the impact of voice transmissions colliding with OTAP data. It is suggested that ECA is enabled on all radios within the system if OTAP is utilized.

In some configurations, the multiple Control Stations used by RM may have matching radio IDs. However, their radio ID should not match that of another radio in the field.

It is recommended to use next generation MOTOTRBO mobiles (R02.10.00 or later) as RM Control Stations, since they assure minimal impact to the radio system performance during Over-The-Air transmissions. Older MOTOTRBO mobiles, when used as control stations, do not have the ability to prioritize voice over data traffic.

A static, persistent route is required in the PC so that messages are routed out of the Control Station and not out of any other network interface.

4.27.3

Conventional Configurations

There is little difference between the basic deployments in conventional system types such as direct mode (12.5 or 6.25e), single site repeater, and IP Site Connect. The only settings that are different are the system specific parameters of the Control Station or MNIS. The following are three basic Control Station examples.

Figure 191: Multi-Channel RM Application with Control Stations in Direct Mode

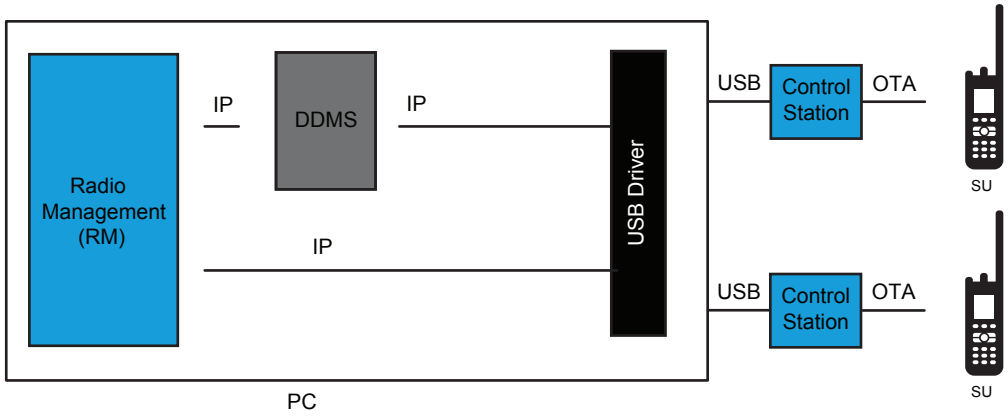


Figure 192: Multi-Channel RM Application with Control Stations in Single Site Repeater Mode

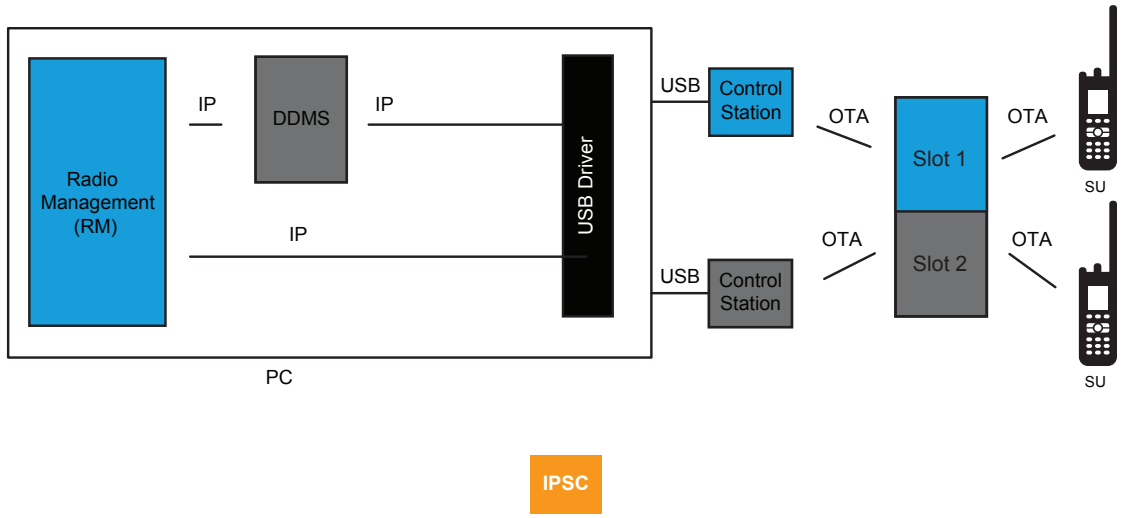
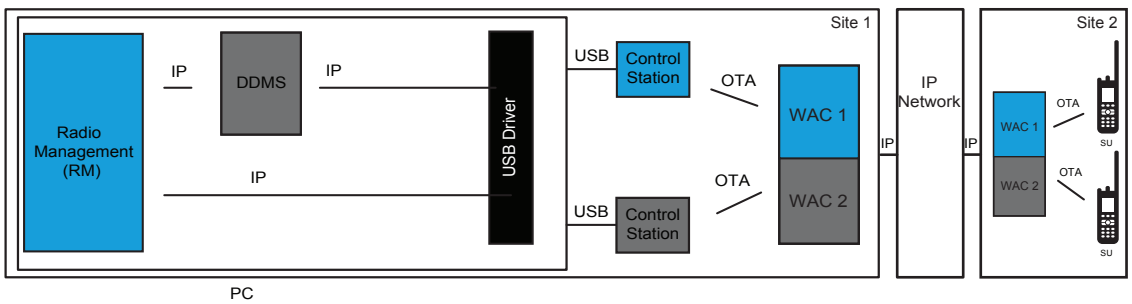


Figure 193: Multi-Channel RM Application with Control Stations in IP Site Connect Mode

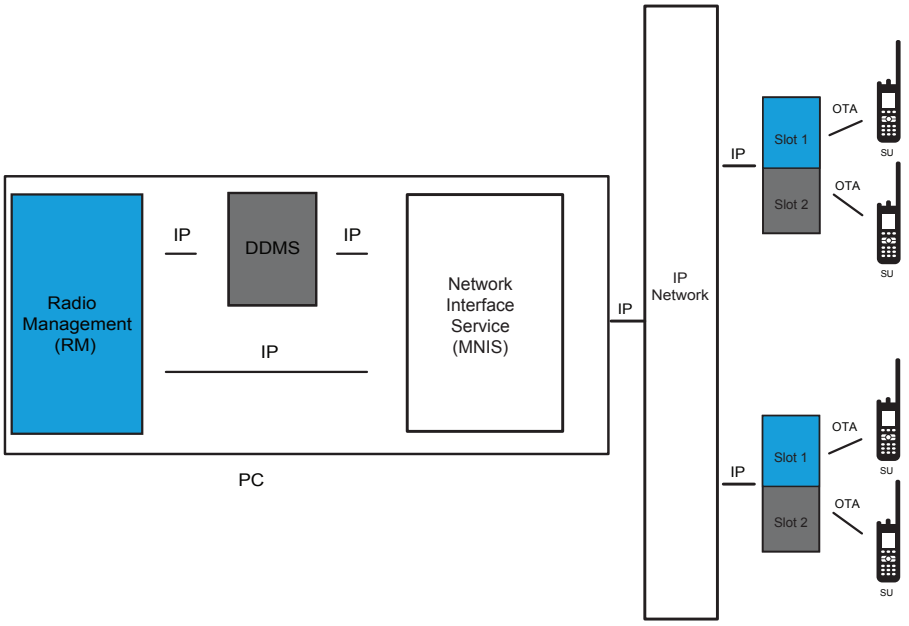


System	Description
IPSC IP Site Connect	When deploying the MNIS, single site repeater and IP Site Connect configurations are generally the same. The MNIS can connect to eight conventional systems. This means eight IP Site Connect systems (each with numerous sites), or eight Single Site repeaters, or any combination of IP Site Connect systems and Single Site repeaters that total up to eight. Unlike the Control Station deployment, the PC that contains the MNIS, DDMS, and RM application do not need to be within RF coverage of any repeaters.

In Figure 194: Multi-Channel RM Application with MNIS in Single Site or IP Site Connect Mode on page 541, the two repeaters shown could be two single site repeaters, or two sites of one IP Site Connect system.

IPSC

Figure 194: Multi-Channel RM Application with MNIS in Single Site or IP Site Connect Mode



Radios are capable of manually changing between channels that are monitored by Control Stations or the MNIS during an active Over-The-Air session.

System	Description
IPSC IP Site Connect	Radios can also roam between sites of an IP Site Connect system during an active Over-The-Air session.

If radios move to channels not monitored by Control Stations or the MNIS, the Over-The-Air operation stops. When the radio returns to the monitored channel, and registers its presence, the Over-The-Air operation starts again.

4.27.3.1

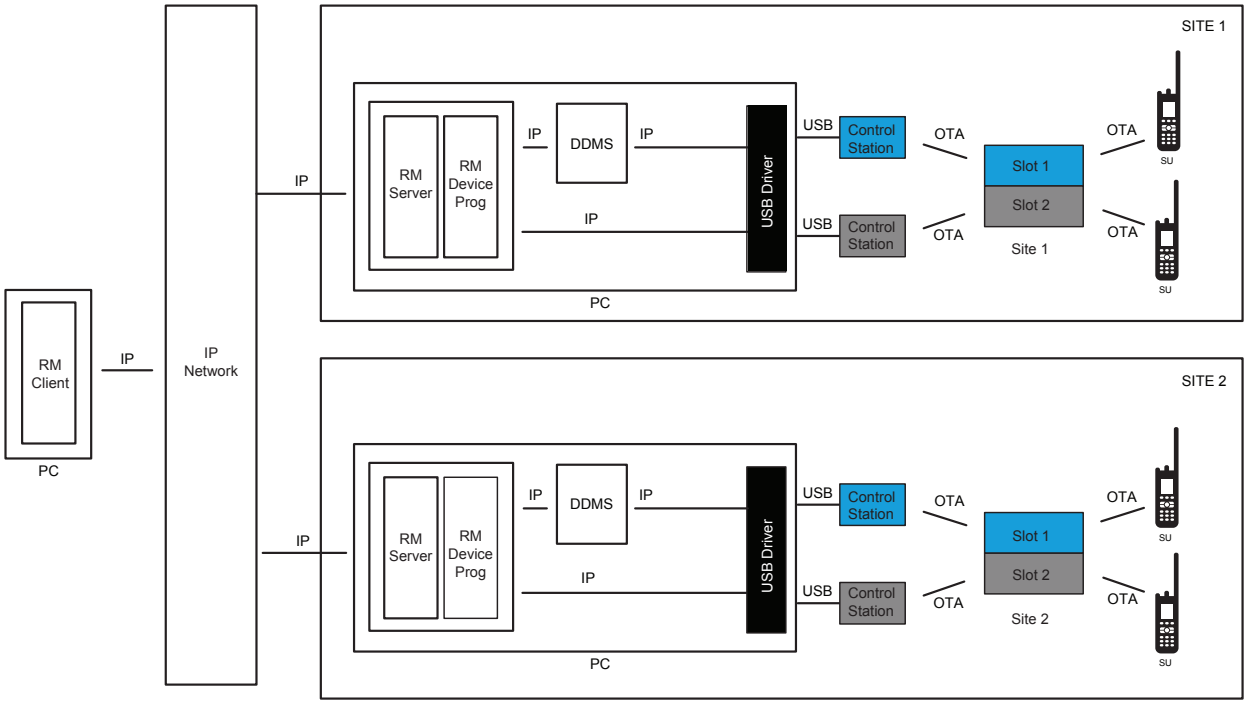
RF Isolated Single Site Repeaters

To communicate with single site repeaters that are not within RF coverage of each other, multiple PCs with Control Stations must be set up, or set up one PC with the MNIS. Depending on RF coverage, one PC may be within RF coverage of multiple sites. In that scenario, more Control Stations can be connected.

A remote RM Client can be used from a centralized location to contact both RM Servers.

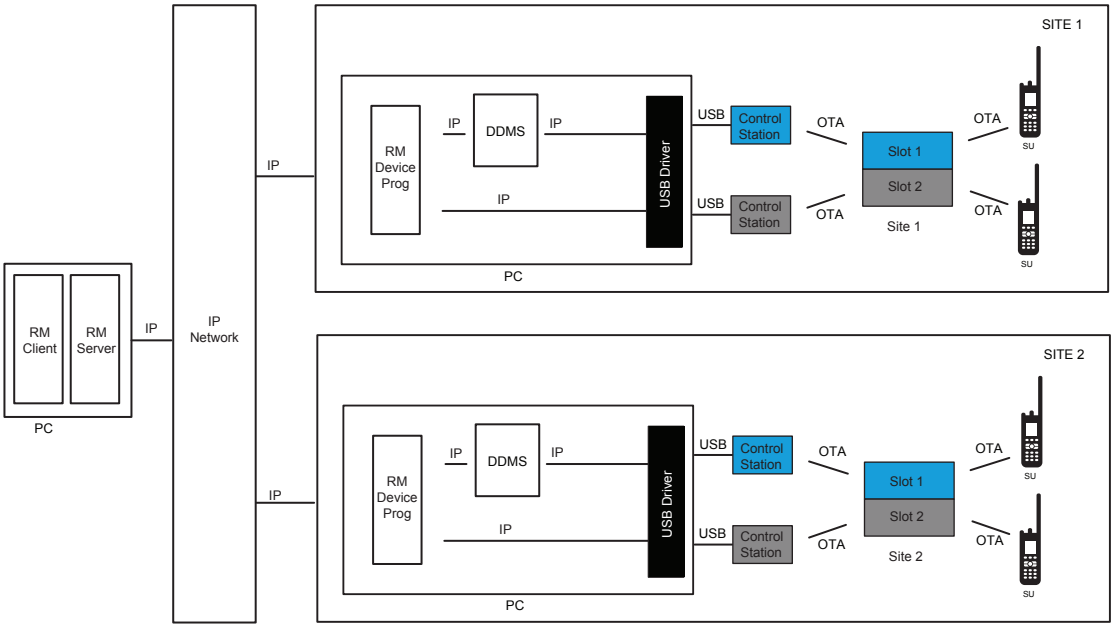
NOTE: It is important to note that one radio should not be configured in more than one RM Server. Therefore if there are radios that move from one site to another, monitored by a different RM Server, RM Device Programmer and Control Stations, they must only be populated in one of the RM Servers. Radios that do move between sites that are monitored by different RM Servers/Device Programmers can only be contacted when they are on the channel monitored by their RM Server. There is a DDMS on both PCs.

Figure 195: RM Application with Control Stations Covering RF Isolated Single Site Repeaters



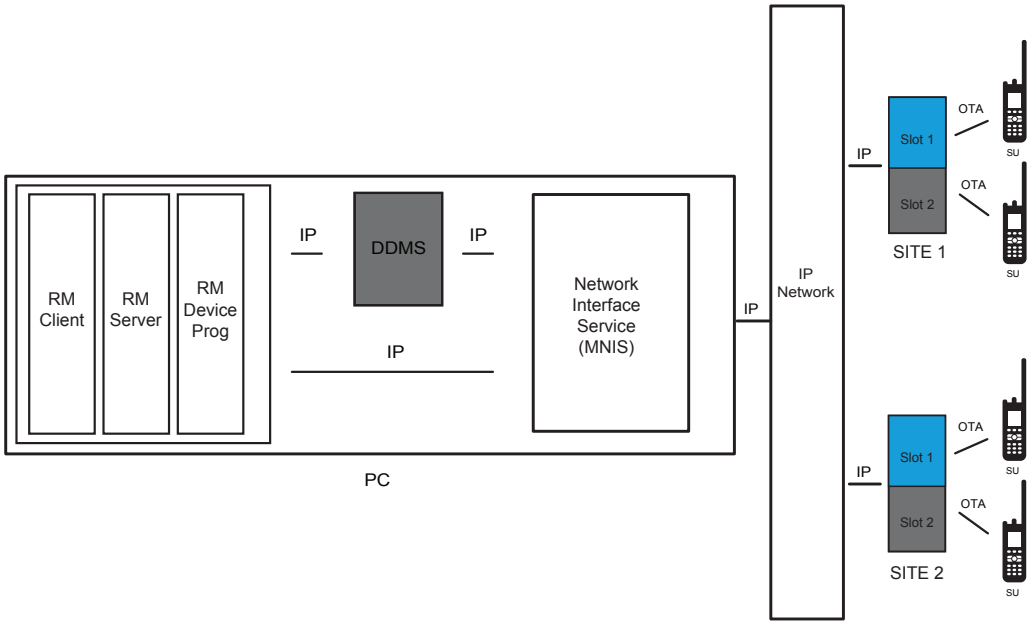
A Remote Device Programmer configuration can be utilized if a centralized RM Server is required, as shown in Figure 196: RM Application with Control Stations Covering RF Isolated Single Site Repeaters Using Remote RM Device Programmers on page 543. This configuration requires a stable, direct network connection between the RM Device Programmers and the RM Server.

Figure 196: RM Application with Control Stations Covering RF Isolated Single Site Repeaters Using Remote RM Device Programmers



When deploying the MNIS, communicating with single site repeaters that are not within RF coverage of each other is much simpler. The MNIS can connect to eight conventional systems. The RM Client can be remote from the RM Server, and the RM Server can be remote from the RM Device Programmer(s). Since the MNIS can be remote from the system, all RM subcomponents can be installed on the same PC at a remote location.

Figure 197: RM Application with MNIS Covering RF Isolated Single Site Repeaters



4.27.3.2

Local Channel Support on IP Site Connect

IPSC

On IP Site Connect systems that have local area channels at some of the sites, there are a couple of configuration options available.

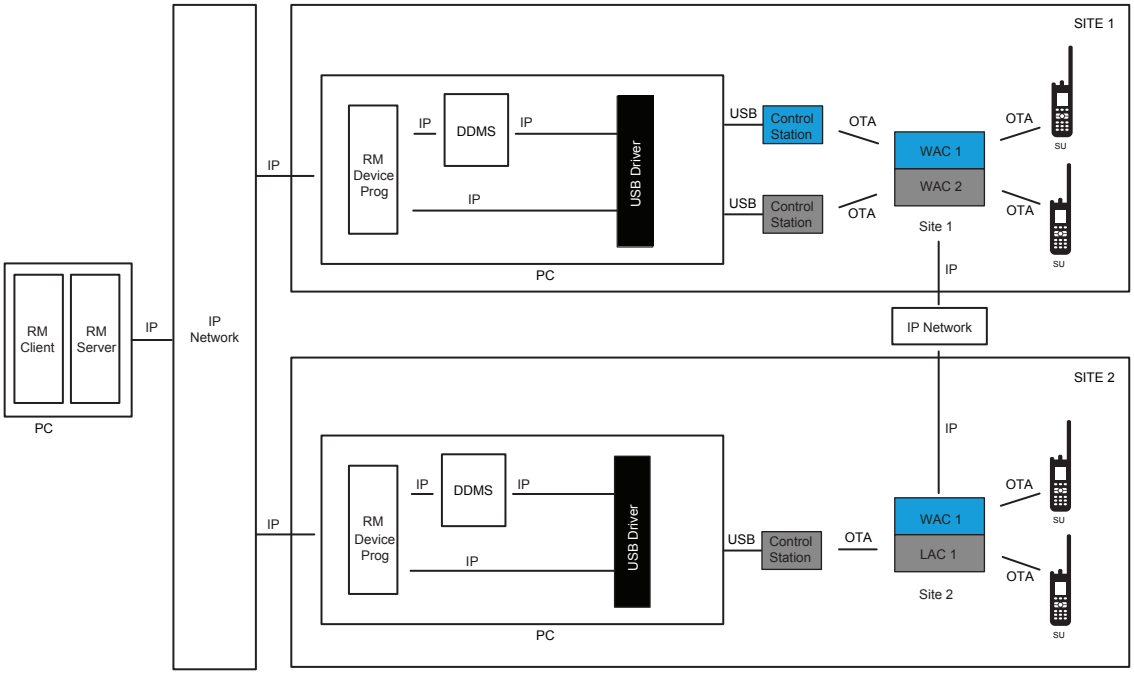
If the radios usually operate on the wide area channels, and infrequently change to the local channels, it may be easiest to have the Radio Management (RM) and Control Stations at one site monitoring the wide area channels only.

In this case, radios can only be programmed Over-the-Air when they become present on the wide area channel monitored by the Control Stations. When they are on the local channels, they are considered absent.

If some of the radios always remain on the local channels, then it is necessary to have Control Stations monitoring them in order for the RM to contact the radios on that channel. Depending on RF coverage of each site and the location of the RM and Control Stations, all sites may not be reachable via RF from one location. Therefore a second PC with Control Stations must be set up within RF coverage of the local channels of other sites.

A Remote Device Programmer configuration can be utilized as shown in Figure 198: RM Application with Control Stations in IP Site Connect Mode Covering Local Channels with Remote RM Device Programmers on page 544. A stable, direct network connection between the RM Device Programmers and the RM Server is required.

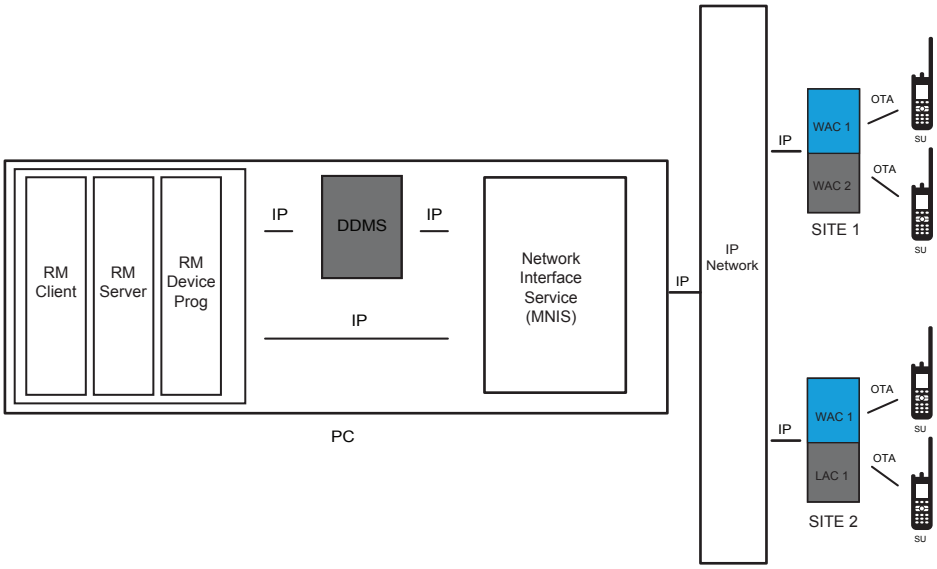
Figure 198: RM Application with Control Stations in IP Site Connect Mode Covering Local Channels with Remote RM Device Programmers



When deploying the MNIS, communicating with local channels of an IP Site Connect system is much simpler. One MNIS can communicate with the wide area and local area channels over the IP network. Therefore, there is no need for a second computer to cover the local channels.

The RM Client can be remote from the RM Server, and the RM Server can be remote from the RM Device Programmer. Since the MNIS can be remote from the system, all RM subcomponents can be installed on the same PC at a remote location.

Figure 199: RM Application with MNIS in IP Site Connect Mode Covering Local Channels



4.27.3.3

Dynamic Mixed Mode (DMM)

The Radio Management (RM) can configure radios Over-the-Air that are operating in digital mode on a DMM system. There are some limitations on performance. For example, when operating in DMM, analog voice transmissions do not have priority while an Over-the-Air operation is occurring. Once an Over-the-Air operation has started in digital mode, the repeater is kept in digital mode for its duration. This means an analog transmission cannot gain access to the system and receives a busy indication for the duration of the operation.

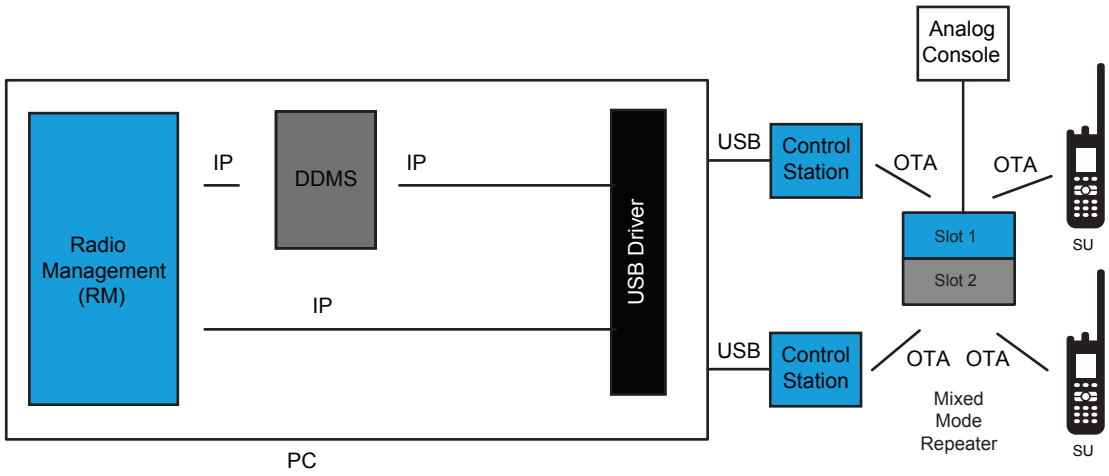
To mitigate this, a pacing option can be set within the RM Device Programmer so that there are times of idle between each delivery or retrieval. The pacing duration is suggested to be greater than five minutes. This may provide the analog radio an opportunity to see an idle channel more often. It is recommended that Over-the-Air configurations occur during non-peak hours, especially when operating on a DMM system.

During an analog or digital voice transmission, the RM Application data is queued in the Control Station.

The MNIS does not support communication with repeaters operating in Dynamic Mixed Mode (DMM).

NOTE: Because some radios may be scanning while operating in DMM, the data preamble on the Control Station may need to be increased to reach the target radios. This increases the size of the data messages Over-the-Air, hence the overall time taken to perform an operation may increase. Follow the standard rules for setting the preamble duration versus the number of scan members.

Figure 200: RM Application in Dynamic Mixed Mode



4.27.4

Capacity Plus Single Site Trunking Configurations

CPSS

Four configurations with Control Stations are available with Capacity Plus Single Site. The major difference between the configurations is how Presence services are handled.

The configurations are:

- Trunked Control Station without Presence
- Trunked Control Station with Presence
- Control Stations with Presence and no Data Revert repeaters
- Control Stations with Presence and Data Revert repeaters

The following MNIS configurations are available for CPSS:

- MNIS without Presence
- MNIS with Presence and no Data Revert repeaters
- MNIS with Presence and Data Revert repeaters

4.27.4.1

Trunked Control Station Without Presence

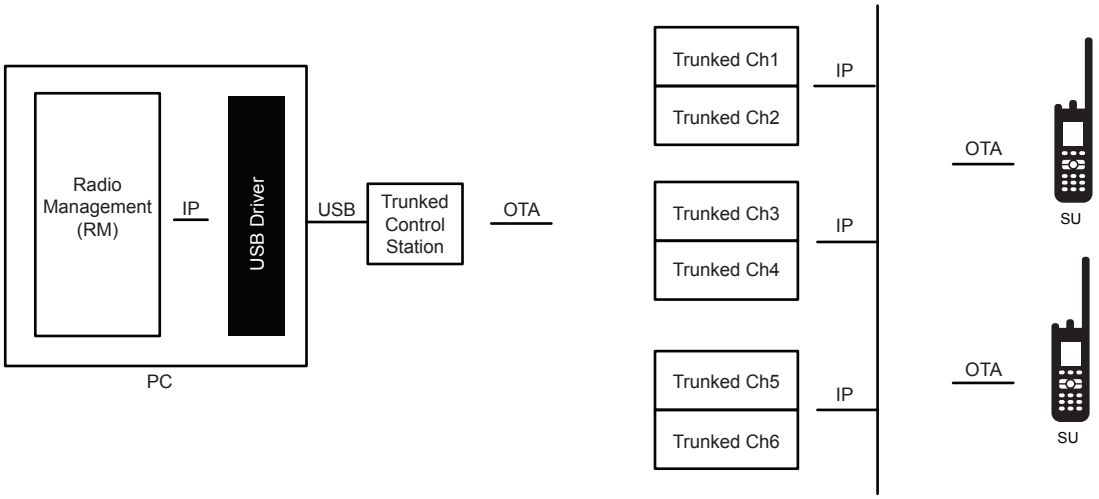
CPSS

The simplest trunking configuration does not utilize Presence at all. Without a DDMS, the RM attempts to contact each radio one by one, regardless if they are present on the system or not. Although this is not optimized, it requires the least amount of infrastructure.

Only one Trunking Control Station is required in this configuration. Since the RM sends one message at a time, there is no need for multiple Control Stations. Therefore, loading on a CPSS system is usually not an issue.

A persistent static route is required in the PC so that messages are routed out of the Trunking Control Station and not out of any other network interface.

Figure 201: RM Application in a Capacity Plus Single Site with no DDMS and Trunked Control Station



4.27.4.2

Trunked Control Station with Presence

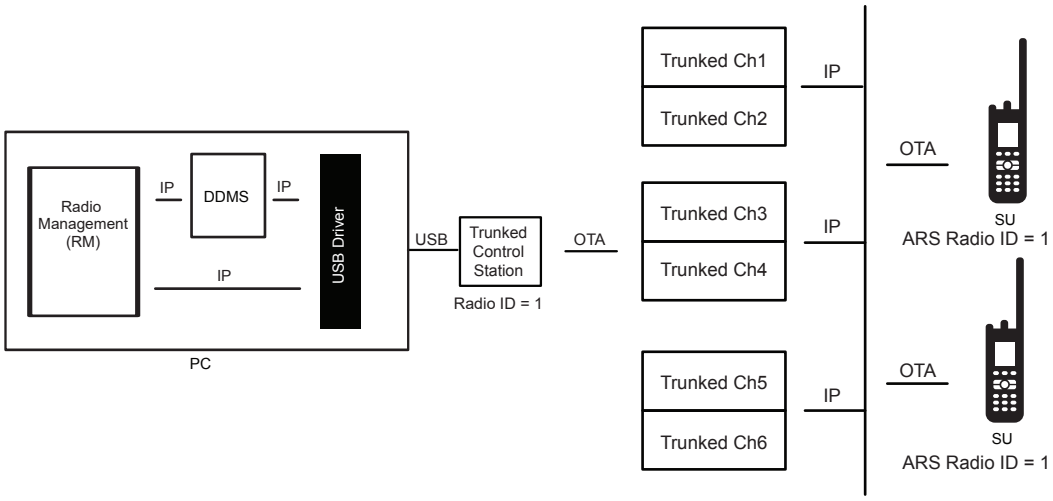
CPSS

This configuration is the same as the previous, but utilizes Presence and a DDMS. The upside to this is that only one Control Station is required and that the RM-only attempts radios that are present.

The down side is the ability to receive Presence registration messages effectively. For example, if two radios power on within a short period of time, both attempt to deliver their Presence registration messages to the same Trunked Control Station, but only one is successful at a time. The unsuccessful radio tries again and eventually becomes successful. As the number of radios that simultaneously register grows, this configuration could lead to a slower registration time. If this becomes a problem, consider increasing the radio's ARS Initialization Delay timer on the Presence registrations. This further distributes the registration attempts.

Therefore, this configuration is more optimized in performing Over-the-Air configurations but less optimized in the Presence registration process.

Figure 202: RM Application in a Capacity Plus Single Site System with a DDMS and Trunked Control Station



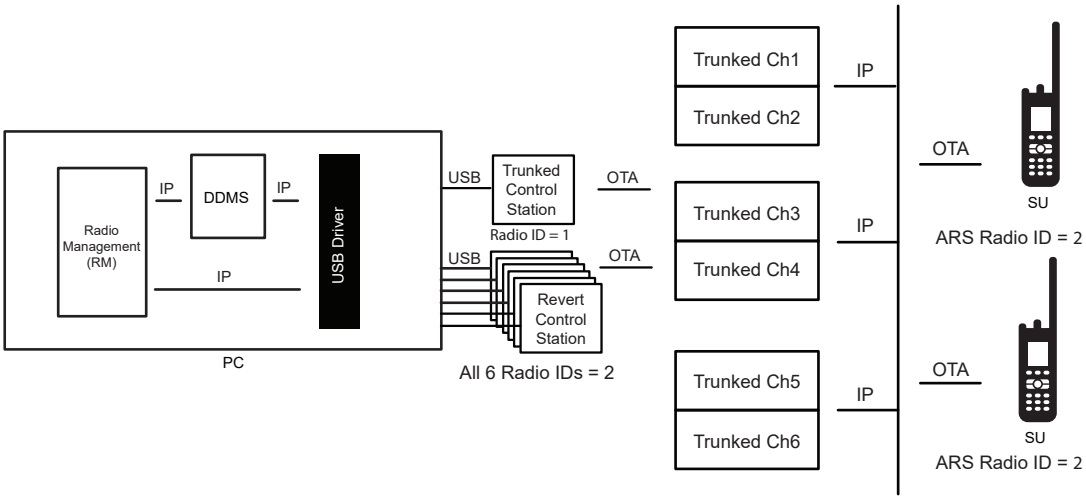
4.27.4.3

Control Stations with Presence and No Data Revert Repeaters

CPSS

To further optimize the reception of simultaneous Presence registrations, Data Revert Control Stations could be installed for every Trunked Channel in a system for the sole purpose of receiving simultaneous Presence registration messages. Outgoing Radio Management application messages are sent through a single Trunked Control Station using a static route in the PC. The Data Revert Control Station's Radio ID should match the ARS Radio ID programmed in the radios and the Trunked Control Station would have a unique Radio ID. Although this configuration is optimized for Presence registration, substantial additional hardware is required.

Figure 203: RM Application in a Capacity Plus Single Site System with a DDMS, no Data Revert Channels, and Control Stations



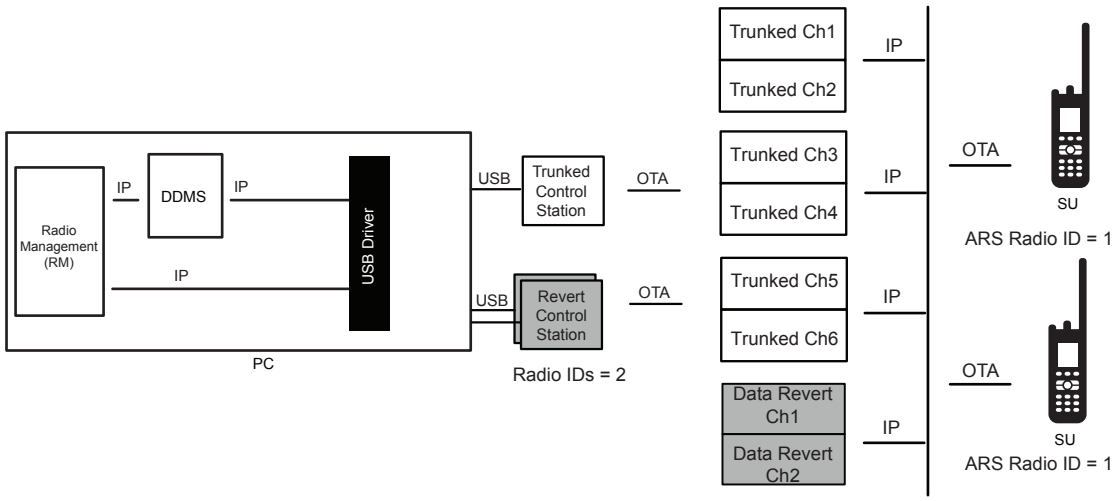
4.27.4.4
Control Stations with Presence and Data Revert Repeaters

CPSS

The RM application operates with Control Stations on Capacity Plus Single Site systems that have existing Data Revert Channels, but it is important to note that the OTAP data is not sent on the Revert Channel. It is expected that the Data Revert Channels exist for other data applications. It is assumed that since OTAP happens rarely, a dedicated Data Revert Channel is unlikely. Recall that no other Over-the-Air data application is supported on the PC with the RM Server and RM Device Programmer.

In this configuration, the Presence registration messages are sent to the Data Revert Channels, while the OTAP data is sent on the Trunked Channels. This configuration only requires Revert Control Stations to monitor the Revert Channels, therefore drastically reducing the number of required Control Stations. There needs to be one Trunked Control Station for the OTAP data. Outgoing RM messages are sent through a single Trunked Control Station. A static route is required on the PC. The Revert Control Stations would have the ARS Radio ID programmed in the radios and the Trunked Control Station would have a unique Radio ID.

Figure 204: RM Application in a Capacity Plus System with a DDMS, Data Revert Channels, and Control Stations

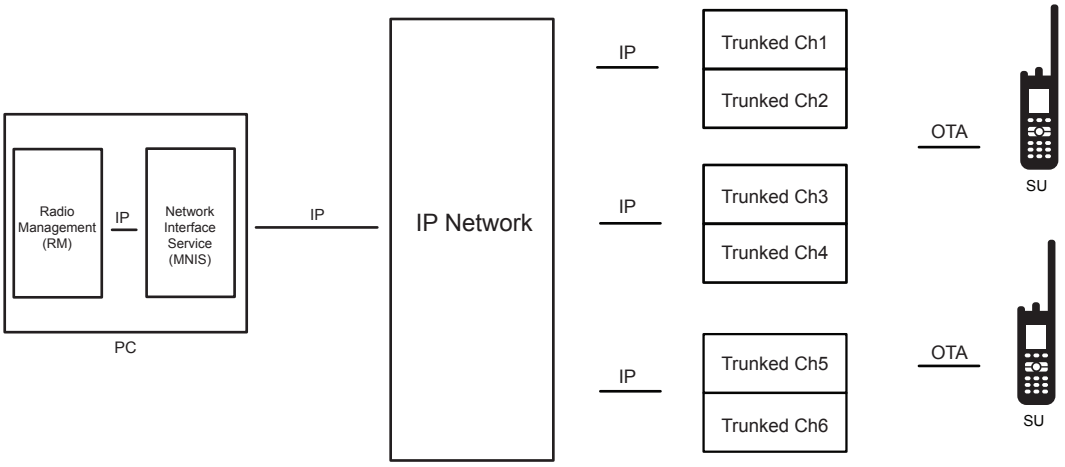


4.27.4.5
MNIS without Presence (DDMS)

CPSS

The simplest trunking configuration does not utilize Presence at all. Without a DDMS, the RM attempts to contact each radio one by one, regardless if they are present on the system or not. Although this is not optimized, it is the simplest configuration.

Figure 205: RM Application in a Capacity Plus Single Site System with an MNIS



4.27.4.6

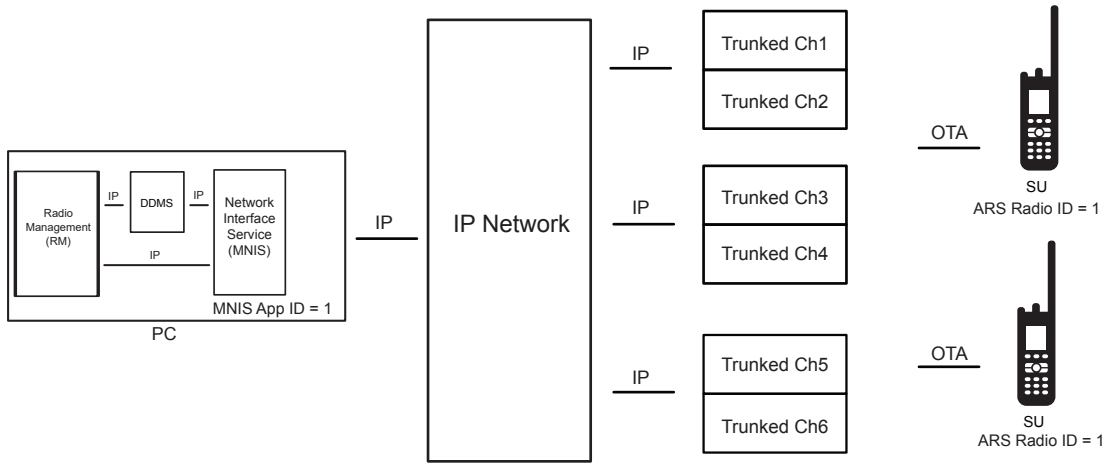
MNIS with Presence and No Data Revert

CPSS

This configuration is the same as the previous one, but utilizes Presence and a DDMS. The MNIS does not have the disadvantages of the Control Station configuration when it comes to the ability to receive Presence registration messages effectively. The MNIS can receive all Presence registration messages, even if numerous messages are sent to it on different Trunked Channels at the same time. Recall that the Control Station configuration requires a Control Station monitoring every Trunked Channel to accomplish this. Therefore, the use of the MNIS in this configuration can drastically decrease cost and complexity.

The MNIS Application ID should match the ARS Radio ID in the radio. Therefore all ARS messages are targeted towards and received by the MNIS.

Figure 206: RM Application in a Capacity Plus System with an MNIS and a DDMS



4.27.4.7
MNIS with Presence (DDMS) and Data Revert

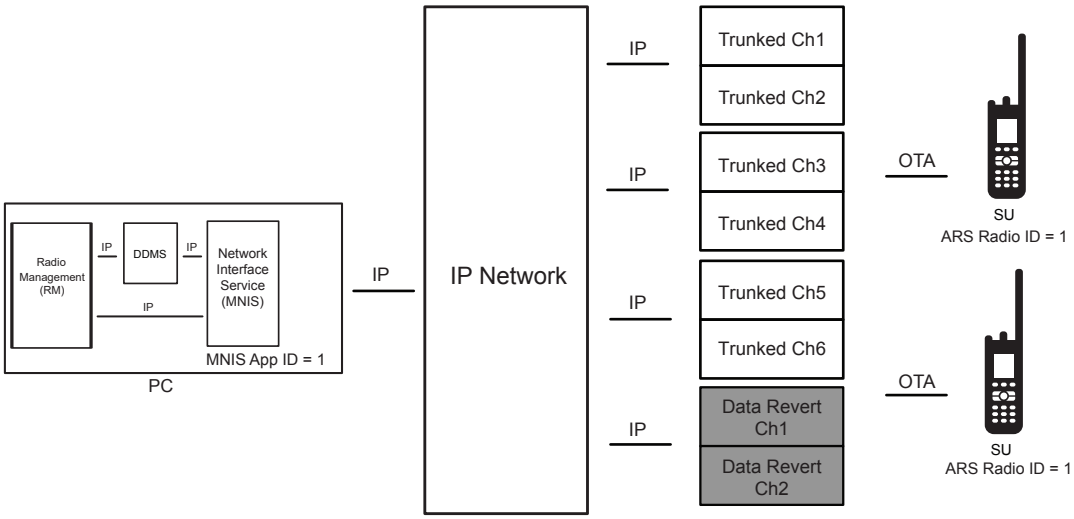
CPSS

The RM application operates with the MNIS on Capacity Plus Single Site systems that have existing Data Revert Channels, but it is important to note that the OTAP data is not sent on the Revert Channel. It is expected that the Data Revert Channels exist for other data applications. It is assumed that since OTAP happens rarely, a dedicated Data Revert Channel is unlikely.

In this configuration, the Presence registration messages are sent to the Data Revert Channels, while the OTAP data is sent on the Trunked Channels. The MNIS can receive and send OTAP messages on the Trunked Channels and the Presence registrations on the Data Revert Channels without additional equipment.

As previously mentioned, it is expected that the Data Revert Channels in this configuration exist for other data applications. See Coexistence with Third-Party Data Applications on page 553 for more details.

Figure 207: RM Application in a Capacity Plus Single Site System with an MNIS, a DDMS, and Data Revert Channels



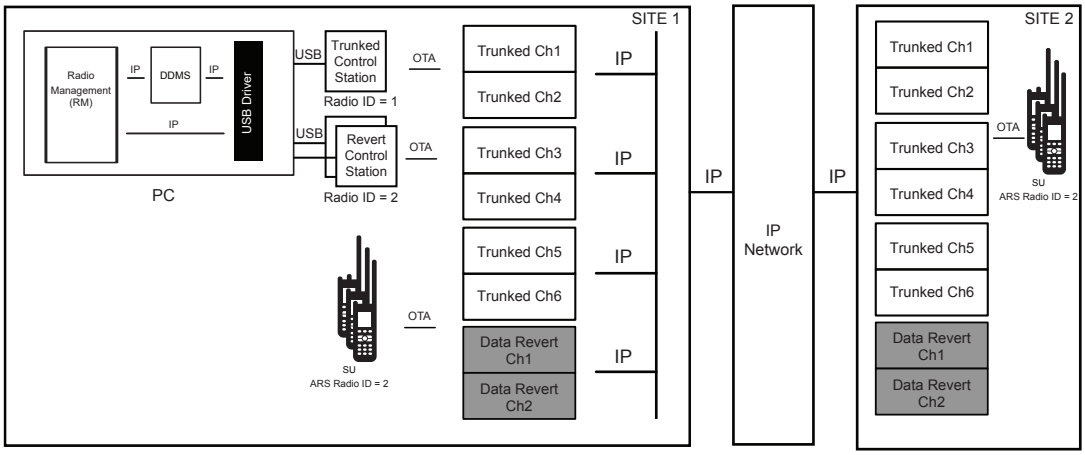
4.27.5
Capacity Plus Multi Site Trunking Configurations

CPMS

There is a small difference in the basic deployments between Capacity Plus Single Site and Capacity Plus Multi Site. As in conventional, the RM itself is unaware the underlying architecture.

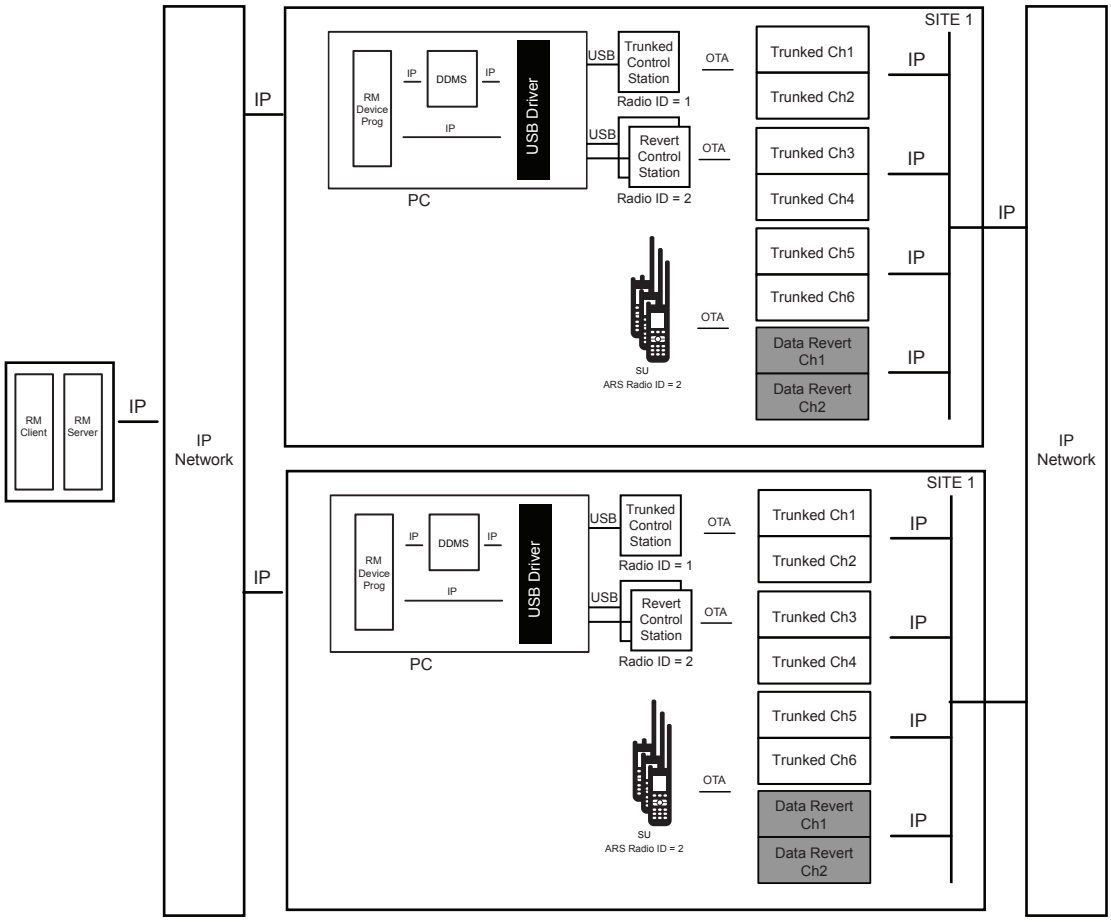
Therefore, all previous Capacity Plus Single Site configurations for the RM are also supported in Capacity Plus Multi Site. This is primarily true because individual data is always sent to a wide area. If utilizing wide-area Data Revert Channels, the RM Server, RM Device Programmer, and Control Stations only need to be within the coverage of one of the sites. Radios send their Presence registration to the Data Revert Channels, which in turn routes the data back to the site where the Data Revert Control Stations are monitoring.

Figure 208: RM Application with Control Stations in a Capacity Plus Multi Site System with Presence (DDMS) and Wide-Area Data Revert Channels



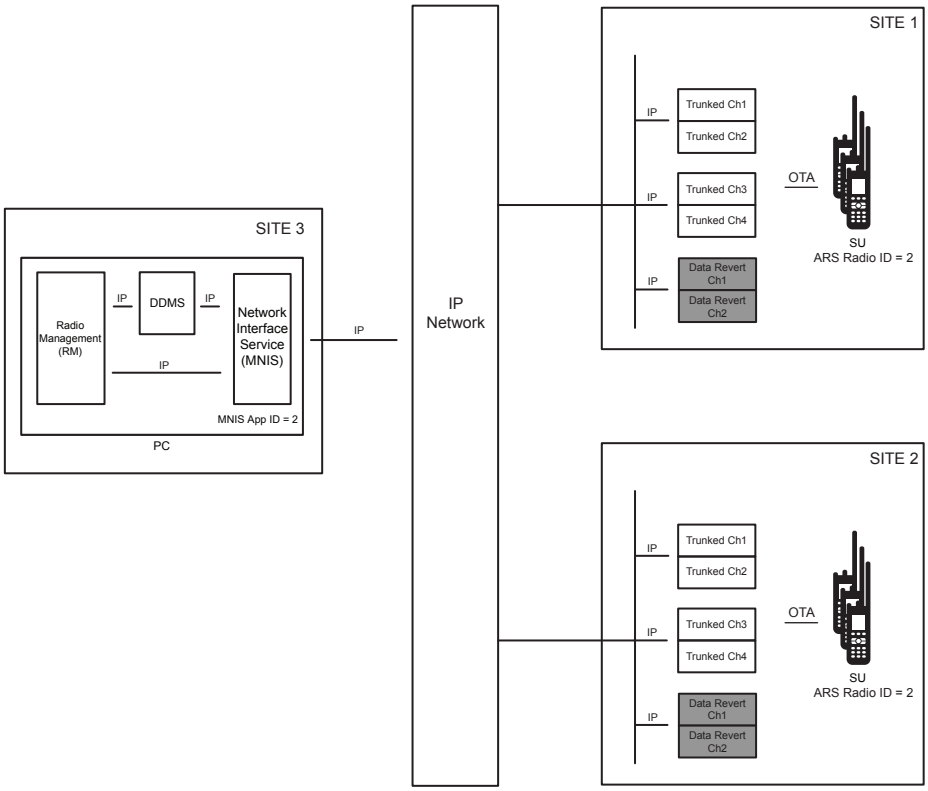
If utilizing local area Data Revert Channels at one or more sites, there must be a separate RM Device Programmer and Control Stations set up within RF coverage of that site. It requires a stable, direct network connection between the RM Device Programmers and the RM Server.

Figure 209: RM Application with Control Stations in a Capacity Plus Multi Site System with Presence (DDMS) and Local Area Data Revert Channels



If utilizing the MNIS with wide or local area Data Revert Channels, the RM Application (Client, Server, and Device Programmer) can all be remote from other Capacity Plus Multi Site sites. The OTAP data is routed to the appropriate site over the IP network. Radios send their presence registration on the Data Revert Channels (wide or local), which in turn routes the data back to the MNIS over the IP network.

Figure 210: RM Application with MNIS in a Capacity Plus Multi Site System with Presence and Wide or Local Area Data Revert Channels



4.27.6
Coexistence with Third-Party Data Applications

OTAP is supported on systems that have third-party data applications, but there are some special considerations and configurations required.

There are three combinations supported:

- RM and Third-Party Data Application with Control Stations
- RM and Third-Party Data Application with MNIS
- RM with MNIS and Third-Party Data Application with Control Stations

The following sections describe the three different combinations.

4.27.6.1
RM and Third-Party Data Application with Control Stations

It is important to understand that although supported on the same system, the RM Device Programmer are not supported on the same computer as a third-party data application when using Control Stations.

If a third-party data application utilizes a different message routing strategy than what is used by the RM, message delivery may become unreliable if on the same computer. Therefore, the RM Device Programmer

should be installed on a different computer with a different set of Control Stations than another third-party data application utilizing Control Stations.

Even if on different computers, a system level conflict may still remain. The RM application can utilize the ARS messages sent by the radios to track presence and mobility. These messages are sent from the radios to the Control Stations associated with the RM. The ARS messages are used to keep track of which radios are present and which channel they are present on.

If the third-party data application does not utilize the ARS, then the radios can be programmed to send their ARS messages to the RM Control Stations and no additional considerations are required.

If the third-party data application utilizes the ARS, then the radios must remain programmed to send their ARS messages to the Control Stations connected to the third-party data application. In order for the RM to also receive the ARS messages, the Control Stations associated with the RM must be programmed with an ARS Monitor ID that matches the Radio ID of the third-party data application's Control Stations. Additionally, the DDMS used by the RM must have the "Passive" option enabled. A section below describes the passive presence and the ARS monitoring ID configuration further.

If operating RM without presence and a DDMS, a configuration utilizing passive presence is not required.

4.27.6.2

RM with MNIS and Third-Party Data Application with Control Stations

The MNIS should not be installed on a computer that also contains Control Stations. These two methods have conflicting routing methods. Therefore, the Radio Management (RM) Device Programmer and MNIS should be installed on a different computer than another third-party data application utilizing Control Stations.

Even if on different computers, a system level conflict may still remain. The RM application can utilize the ARS messages sent by the radios to track presence and mobility. These messages are sent from the radios to the MNIS associated with the RM. The ARS messages are used by the DDMS to keep track of which radios are present and which channel they are present on.

If the third-party data application does not utilize ARS, then the radios can be programmed to send their ARS messages to the RM MNIS and no additional considerations are required.

If the third-party data application utilizes ARS, then the radios must remain programmed to send their ARS messages to the Control Stations connected to the third-party data application. In order for the RM to also receive the ARS messages, the MNIS associated with the RM must be programmed with an ARS Monitor ID that matches the Radio ID of the third-party data application's Control Stations. Additionally, the DDMS used by the RM must have the **Passive** option enabled. A section below describes the passive presence and the ARS monitoring ID configuration further.

If operating RM without presence and a DDMS, a configuration utilizing passive presence is not required.

4.27.6.3

RM and Third-Party Data Application with MNIS

The Radio Management (RM) application and a third-party data application may reside on the same computer if they both utilize the MNIS and DDMS. The radios can be programmed to send their ARS messages to the shared MNIS and tracked by the shared DDMS and no additional considerations are required. Check with the third-party data application vendor on whether they support MNIS and DDMS.

There are many third-party data applications available for MOTOTRBO. These applications may utilize resources on the computer that conflicts with RM. If a conflict between a third-party data application and RM is discovered, or if the third-party data application vendor has requirements above cohabitation with other applications, the applications can be installed on different computers, each with their own MNIS, but they will need to share a DDMS. Both MNIS installations would be configured to reference one DDMS installed on one of the computers. These computers must be in communication via an IP network. The radios would

be programmed to send their ARS messages to the MNIS that is on the same computer as the DDMS. The DDMS shares the presence and mobility with both MNIS instances.

4.27.6.4

Passive Presence and ARS Monitor ID Configuration

In order for the Radio Management to utilize the ARS on a system that has a third-party data application that also utilizes the ARS with Control Stations, a passive presence configuration must be utilized. This configuration essentially allows the RM to passively monitor the ARS messages sent by the radio to the third-party data application without interfering. The preceding RM and Third-Party Data Application with MNIS on page 554 section describes when this configuration may be required.

When using a passive presence configuration, the Control Stations and MNIS associated with the RM are programmed with an ARS Monitor ID that matches the Radio ID of the third-party data application's Control Stations. Additionally, the DDMS used by RM is configured with a "Passive" option.

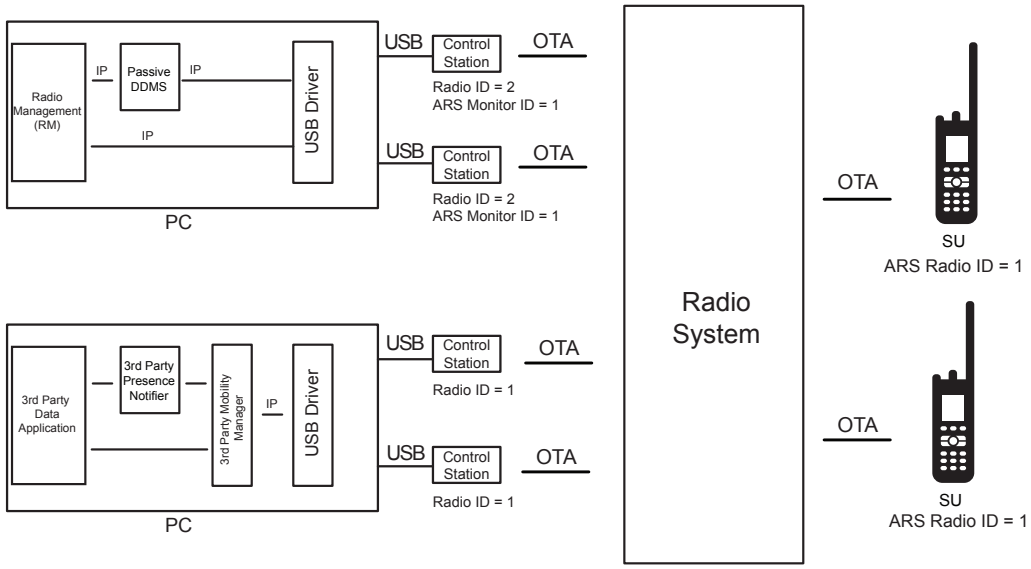
A Control Station or MNIS with an ARS monitoring ID monitors the selected channel for ARS messages targeted towards the specified Radio ID. When an ARS message is received, the message is forwarded, but is not acknowledged Over-the-Air. This ensures there are no Over-Tthe-Air collisions with the acknowledgments sent by the third-party data application's Control Stations. Control Stations and MNISs with an ARS monitoring ID continue to transmit and receive normally on their own programmed rRadio ID and aApplication ID. The rRadio IDs of the Control Stations or the aApplication ID of the MNIS used by the RM must be different than the third-party data application's cControl sStations.

When the DDMS is configured with the "Passive" option enabled, it continues to monitor for incoming ARS messages and notifies its watchers, but does not acknowledge the incoming messages. This ensures there are no Over-Tthe-Air collisions with the acknowledgments sent by the third-party presence application.

NOTE: It is important to note that not only are the RM Control Stations not acknowledging the incoming ARS messages; they are not sending negative acknowledgements or selective retry requests either. This means that if a message is not successfully received by the RM Control Stations, the radio is not aware of it. This limitation can be mitigated by placing the RM Control Stations in a location with similar RF conditions as the third-party data application Control Stations.

The following figure shows a Control Station passive pPresence configuration in a conventional system with a third-party data application.

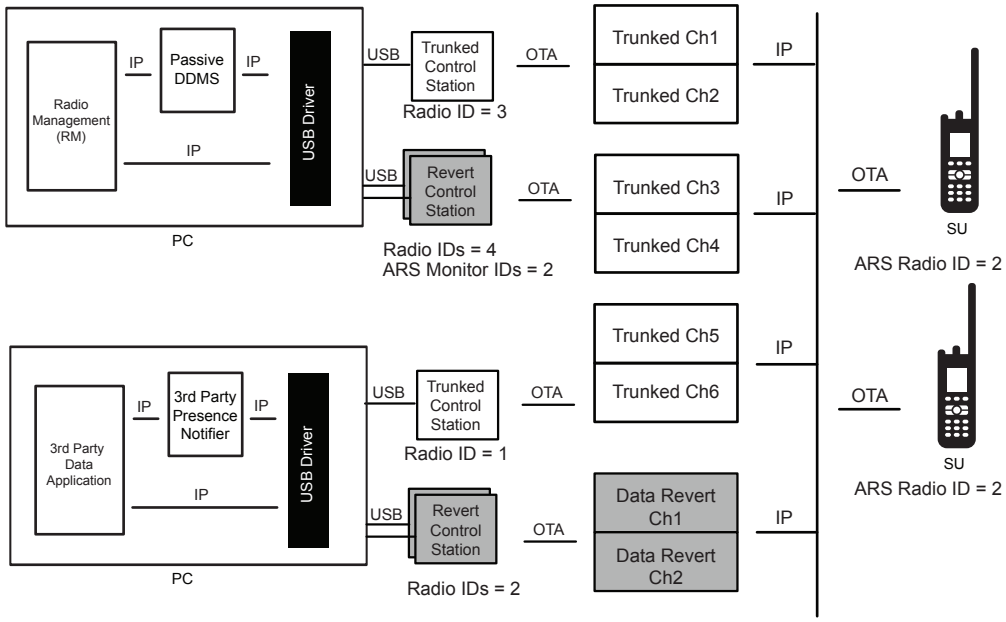
Figure 211: RM Application with Control Stations and Passive Presence Configuration with Third-Party Data Application



The following figure shows a Control Station passive presence configuration in a Capacity Plus Single Site system with dData Revert and a third-party data application.

NOTE: Only the Control Stations used for monitoring automatic registration messages on the Revert Channels require an ARS Monitor ID.

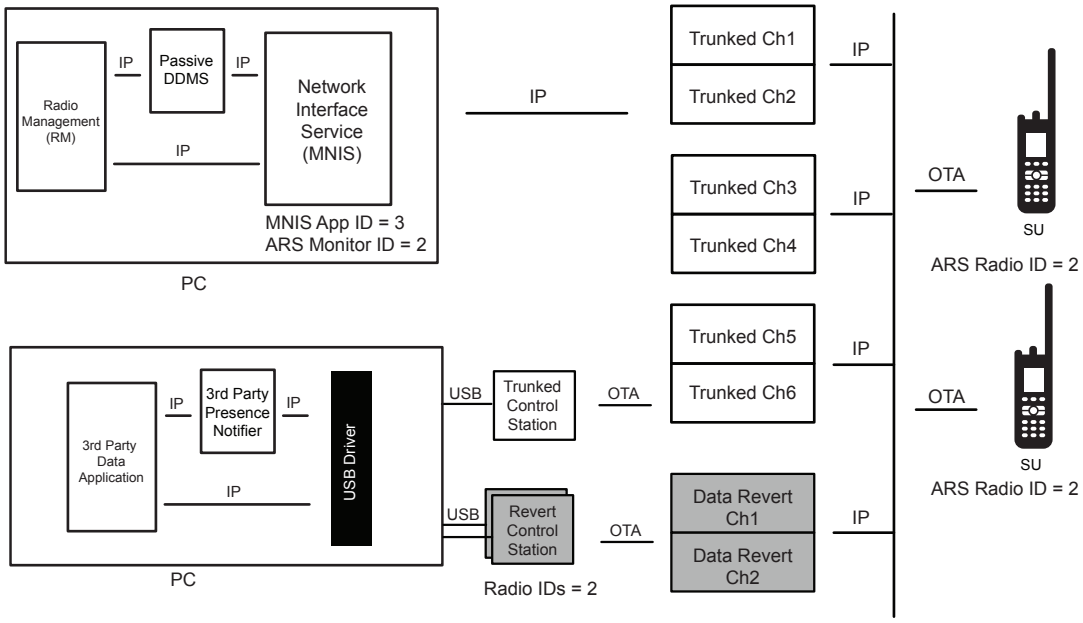
Figure 212: RM Application with Control Stations and Passive Presence Configuration with Third-Party Data Application on a Capacity Plus Single Site Data Revert Configuration



The following figure shows a passive presence configuration in a Capacity Plus Single Site system with Data Revert where the RM is utilizing the MNIS and the third-party data application is using Control Stations. The basic operation is the same as the Control Station configuration shown in Figure 212: RM Application with

Control Stations and Passive Presence Configuration with Third-Party Data Application on a Capacity Plus Single Site Data Revert Configuration on page 556.

Figure 213: RM Application with MNIS and Passive Presence Configuration with Third-Party Data Application on a Capacity Plus Single Site Data Revert Configuration



4.28

Over-The-Air Authentication Key Management

Over-the-Air programming of a radio requires the system administrator to provide an authentication key that matches the authentication key programmed in the radio. The provided authentication key must match the authentication key in the radio prior to performing the first Over-the-Air operation. This ensures that only a validated RM is communicating with a customer's radio. This also ensures that RM is communicating with validated radios.

The initial authentication key (the key ID and key value) must be programmed in the radio via wired CPS prior to the first Over-the-Air operation. The authentication key is set within RM the first time when the archive is imported. It can also be entered manually if an archive is not available.

The authentication key can be changed Over-the-Air if the current authentication key in the radio is known. The system administrator only needs to update the current authentication key in the RM to the new authentication key and deliver and switchover the configuration. The RM utilizes the current authentication key to authenticate the session, and then updates the radio's authentication key with the new authentication key. The new authentication key becomes the current authentication key once successfully switched over.

If the current authentication key in the radio is unknown, it can only be updated through wired CPS. Once updated, the archive should be imported into RM so that the authentication key updated in the radio becomes the current authentication key in RM.

4.29
Over-The-Air Privacy Key Management

OTAP utilizes the standard data service privacy methods: AES, Enhanced, and Basic. It is recommended that privacy be enabled in the system if performing OTAP.

The encryption/decryption is performed at the Control Station or the MNIS and at the end radio. The Control Station and the MNIS can be configured for either Basic, or Enhanced privacy and/or AES. Therefore a channel must only contain radios that all have Basic privacy or all have Enhanced privacy if utilizing OTAP.

NOTE: The Control Station or the MNIS used for OTAP must contain all the privacy keys within all the radios. The radios must contain the privacy key used for transmitting by the Control Station or the MNIS.

The privacy keys are used for both voice and data and can be different per radio. Since the Control Station and the MNIS communicate with many radios, they must contain all keys utilized on the designated channel for conventional or on the system in trunking. If OTAP is utilized through a Control Station, a single conventional channel or a trunking system is limited to the number of Enhanced privacy keys and AES keys that can be contained within one Control Station (which is 16 keys for Enhanced privacy and 16 keys for AES). Since the MNIS supports a large number of Enhanced privacy keys (255) and AES keys (255), this limitation is not present if the MNIS is utilized.

Additionally, all radios must contain the key the Control Station or MNIS is using for transmitting. There is no specific OTAP privacy key. The key designated for the selected channel is used for transmitting OTAP data.

4.29.1
Updating the Privacy Keys in the System

Over-the-Air programming of privacy keys is supported. They can be updated within the RM and delivered to the radios, just like any other parameter. Although performing a key change on a system requires additional considerations to be taken since the keys are also contained within the Control Stations or MNIS used to deliver the keys to the radios.

The old and new keys must be in the Control Stations or MNIS if communication with the radios is required while transitioning. For example, if the radio registers its presence after it has switched over; the Control Station or MNIS is not able to receive the message if it does not have the new key. This can be resolved by either provisioning the new keys into the MNIS or into the receive list of the Control Stations (but still transmitting on the old key), or by suppressing ARS after the switchover. Keeping the old and new keys in the Control Station limits the number of usable keys in the system to half of what the Control Station can hold (16/2=8). The MNIS supports a large number of keys (255); therefore this limitation is not present if the MNIS is utilized. Since there is only one Basic privacy key per radio, it is not possible to contain both the old and new Basic privacy keys.

NOTE: At a minimum, the privacy keys must be updated in the Control Station or MNIS after successfully delivering all the radio’s keys Over-the-Air, or future Over-the-Air operations to the updated radios are not successful.

In order to program the Control Stations connected to the RM Device Programmer, the RM Device Programmer can be temporarily configured via a wired connection. This option can be found in the settings of the RM Device Programmer. The MNIS keys can be updated through the user interface.

Finally, since the new keys are delivered using the old keys, if it is believed that the old keys have been compromised, wired CPS should be used to update the keys in the radios.

4.30
Performance of Over-The-Air Programming

The performance of OTAP is commonly broken into two categories: performance in regard to time to complete an Over-the-Air operation and the impact of the Over-the-Air operation on other system services.

4.30.1
Time to Complete Over-the-Air Operations

There are three major Over-the-Air operations in RM: retrieval, delivery, and switchover. The time it takes to perform any of these operations is highly dependent on the details of the operation itself and the environment of the system.

The time to deliver or retrieve a new configuration is dependent on the following conditions:

- size of the configuration update
- number of radios being processed
- system loading
- RF environment

Because of these numerous dependencies, it may be difficult for the system administrator to exactly determine the time it takes to perform an operation Over-The-Air. However, if some typical configurations and conditions are considered, then some typical times can be predicted that allow the system administrator to plan their time to some level of accuracy.

4.30.1.1
Size of the Configuration Update

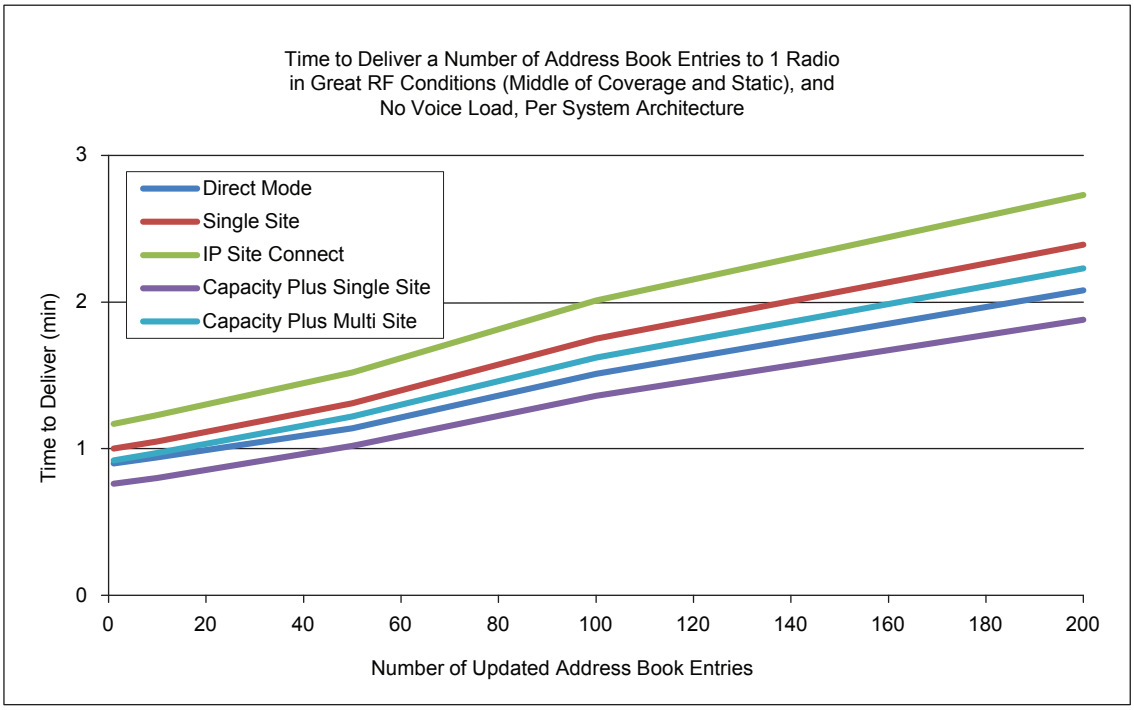
The first thing to understand is the relationship between the amount of configuration change and the amount of time it takes to transfer that change. Many items can be changed within the radio configuration, and each type of item changed has a different impact on the amount of data that needs to be transferred. There is generally no need to understand the entire relationship, but rather to simply understand the impact of a large change and small change.

Only the differences between the Radio Management configuration and the radio configuration are transferred Over-the-Air. It is always recommended that a radio be read on the wire first so that only updates need to be transferred Over-the-Air. Retrieving an entire configuration Over-the-Air or delivering a completely new template to a radio Over-the-Air takes the largest amount of time.

The following figure provides some guidance between the number of address book entries updated or added and the time it takes to deliver them to one radio in great RF conditions with no voice occurring on the channel or system. Great RF conditions are defined as middle of RF coverage and a stationary radio.

NOTE: Retrieval times are slightly shorter than delivery times in general, but for planning purposes we are only showing delivery times.

Figure 214: Time to Deliver a Number of Address Book Entries to One Radio



4.30.1.2

Number of Radios Being Processed

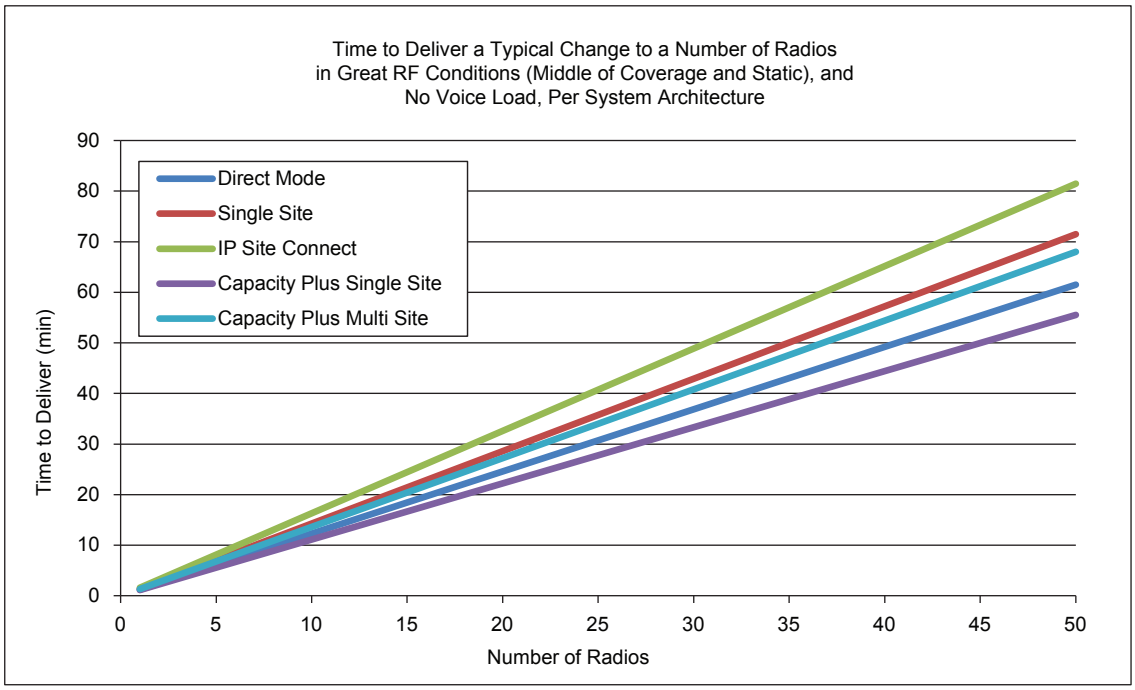
The more radios are updated, the longer the operation takes to complete. The previous chart shows how long delivery to a single radio takes to complete depending on the update size. This value must be multiplied by the number of radios being updated.

The following figure shows the time that it takes to update numerous radios with a “typical update”. The following items are considered typical updates:

- 5 text message strings updates
- 2 privacy key updates
- 25 address book updates
- 1 channel update
- 2 scan list updates
- 1 receive group update

For reference, this typical update size is equivalent to the size of around 50 address book updates in the following figure. As can be seen, the overall time quickly adds up when performing operations on a large number of radios.

Figure 215: Time to Deliver a Typical Change to a Number of Radios



As a rule of thumb, on an idle system, in optimal RF conditions, around 35-45 radios can get a typical update in an hour. This rate may vary depending on the system architecture type. This of course assumes that all radios are present on the channel or system when the operation is scheduled. If a radio is not present, the operation continues to run until the radio becomes present, or the operation is canceled by the system administrator.

4.30.1.3

System Loading and RF Environment

It is always recommended to schedule Over-The-Air operations during times of low voice traffic and when the radios are stationary and in great RF coverage. However, it is recognized that this is not always possible.

The RM) shares the channel with voice and other data services. Therefore if voice traffic loading is high at the time an Over-The-Air operation is scheduled, there is less bandwidth available for RM. Therefore the time to deliver increases as the RM waits for the voice to end.

In addition, if some of the target radios are in poor RF conditions, data delivery times can be longer due to the need to retry any failed messages. Radios that are moving are affected more than those that are stationary, therefore radios that are in vehicles or carried by hand while walking experience longer delivery times. These conditions are always present, but become noticeable when sending many large data messages.

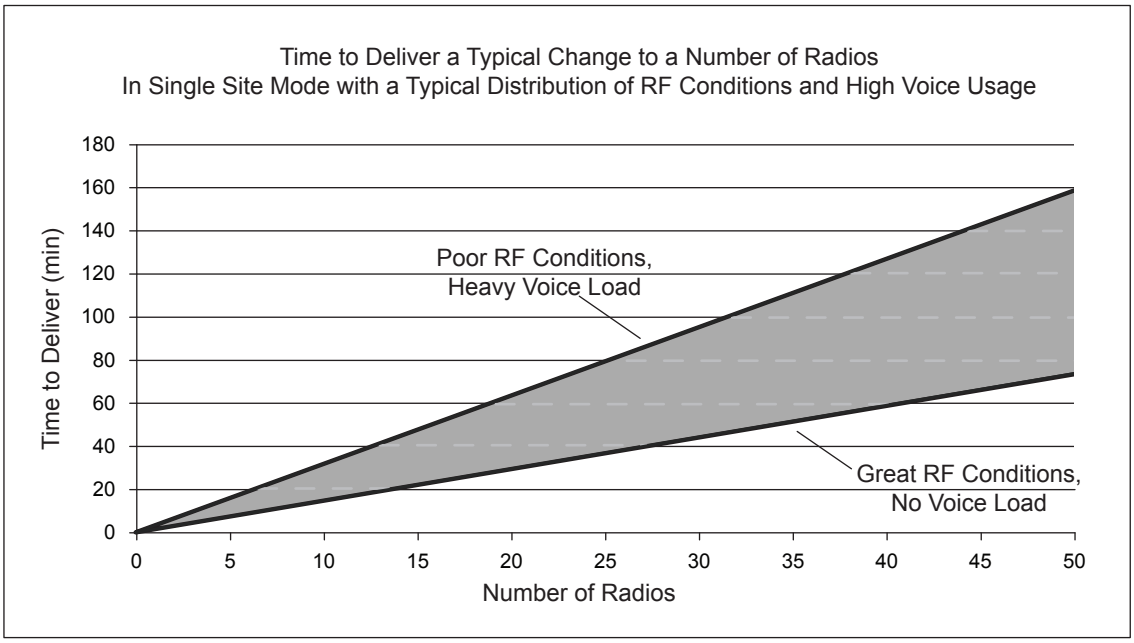
Figure 216: Time to Deliver a Typical Change to Many Radios in Single Site Mode on page 562 provides some expectations on delivery times for a typical change on a single site repeater channel with typical RF conditions and high voice usage.

The bottom of the thick line is the baseline time if all radios were in great RF conditions, stationary and there was little voice (from Figure 215: Time to Deliver a Typical Change to a Number of Radios on page 561). The remaining part of the line is the estimated amount of time with an expected distribution of RF conditions for each radio. The majority of the scenarios are towards the bottom and the less likely scenarios are towards the top.

Note that this chart does not represent the worst case scenario since it is unlikely that all radios are in the worst conditions. This is the expected distribution (thickness of line) for all conventional architectures

including direct mode, single site, and IP Site Connect. See Figure 215: Time to Deliver a Typical Change to a Number of Radios on page 561 for the estimated baseline in great RF conditions, stationary and with little voice.

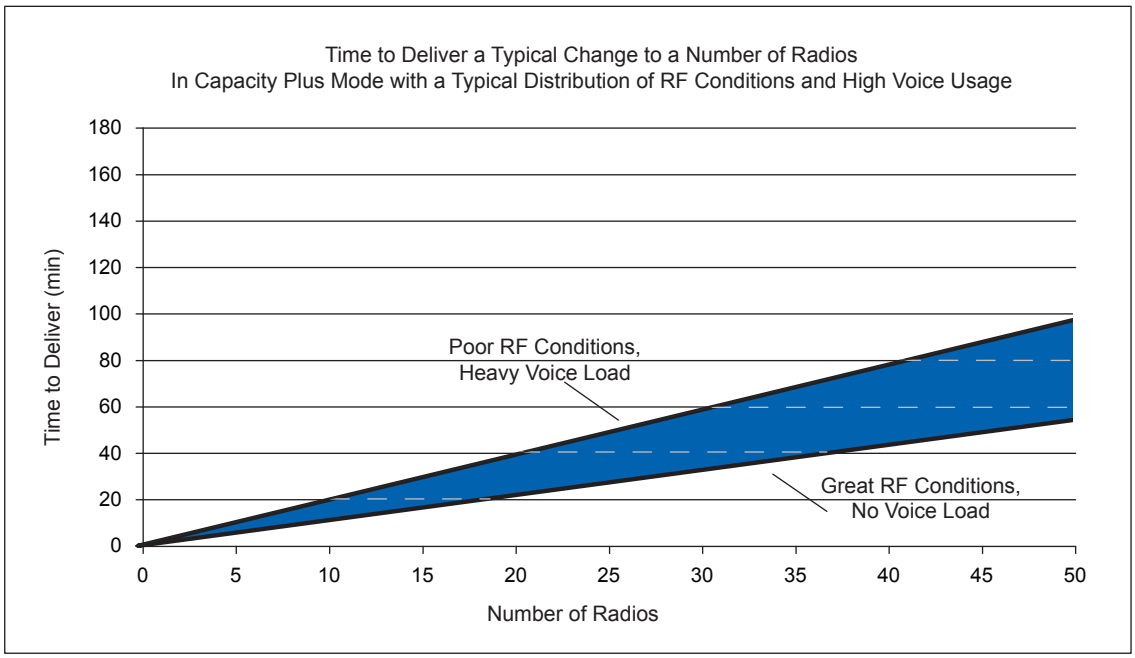
Figure 216: Time to Deliver a Typical Change to Many Radios in Single Site Mode



CPSM

Figure 217: Time to Deliver a Typical Change to Many Radios in Capacity Plus Mode on page 563 provides some expectations on delivery times for a typical change on a Capacity Plus system with typical RF conditions and high voice usage. Note this is the expected distribution (thickness of the line) for all trunking architectures including Capacity Plus Single Site and Capacity Plus Multi Site. See the previous charts for the estimated baseline (bottom of the line) in great RF conditions, stationary and with little voice.

Figure 217: Time to Deliver a Typical Change to Many Radios in Capacity Plus Mode



4.30.2

Performance Impact on Other Services

Performing an RM retrieval, delivery, or switchover Over-the-Air can have an impact on other services on the channel or system.

The three major impacts to consider are:

- Voice access time during an Over-the-Air operation
- Voice downtime during a switchover
- Data downtime during a switchover

4.30.2.1

Voice Access Time During an Over-The-Air Operation

As previously mentioned, it is always recommended to schedule Over-The-Air operations during times of low voice traffic and when the radios are stationary and in great RF coverage. But it is recognized that this is not always possible. In conventional modes, it has been established that voice traffic has an impact on the time it takes to perform Radio Management (RM) Over-The-Air operations, but these operations also have an impact on voice traffic

NOTE: Radios with software versions prior to R02.10.00 do not have access to the channel during an ongoing RM Over-The-Air operation. They most likely receives a talk prohibit tone, since the channel is busy processing data. All radios, regardless of software version, attempting confirmed private calls on a conventional channel while OTAP is occurring experience a low success rate. This is not just the radio being configured, but rather all radios on the conventional channel. To mitigate this, a pacing option can be set within the RM Device Programmer so that there are times of idle between each delivery or retrieval. The pacing duration is suggested to be greater than five minutes.

Radios with software version R02.10.00 and later access the channel and temporarily interrupt ongoing RM Over-The-Air operations. This interruption procedure causes an increase to voice access time by on average of 1.5 seconds, and worst case 3.5 seconds. While waiting for the procedure to complete, the radio user

hears a wait tone, followed by a talk permit tone. Display models also provide an indication of when high volumes of data are occurring on the channel they are selected on. This notifies them that an update is occurring on the system and that their channel access may be slower than normal. This is not just the radio being configured, but rather all radios on the conventional channel.

Voice access time for all radios is not affected during an RM Over-The-Air operation in Capacity Plus Single Site or Capacity Plus Multi Site systems as each transmission occurs on its own channel. However, the radio currently being configured Over-The-Air experiences the increase to voice access time.

4.30.2.2

Voice Downtime During a Switchover

When the radio applies a delivered configuration, the radio must reset to apply the changes. While resetting the radio it is not able to transmit or receive voice Over-the-Air. A reset after a switchover typically causes voice downtime for a single radio in the range of 20–22 seconds.

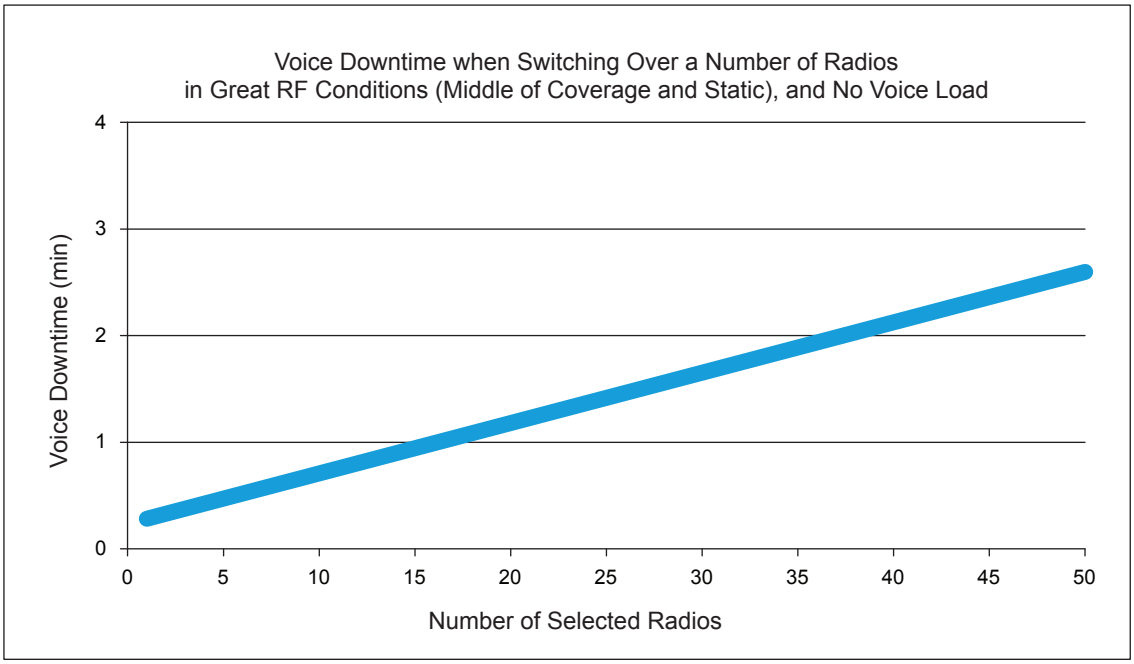
If multiple radios are being switched over, and critical communication parameters are being updated, voice downtime occurs on the system from when the first radio starts its reset to when the last radio finishes its reset. During this time, there may be a mismatch in communication parameters across radios and therefore communication may be disrupted.

If using a non-zero switchover timer, the voice downtime can be as long as the switchover timer itself since some users may choose to delay their switchover.

When performing a delivery with switchover, each radio is switched over as the delivery occurs, therefore the voice downtime can be as long as it takes to deliver to all radios. See the charts in previous sections.

To minimize voice downtime, it is recommended to deliver the configurations, and then schedule an independent switchover with a zero value switchover timer and ARS suppression enabled. Other deliveries or retrievals should not be scheduled to occur at the same time as a switchover. This may cause a delivery to occur in between the switchovers, which increases the overall downtime. The following figure provides some expectations on how long the voice downtime is when in great RF conditions and no voice load in that scenario. This assumes all radios are present. Note that in poor RF conditions and in the presence of voice, these times can increase.

Figure 218: Voice Downtime when Switching Over a Number of Radios



4.30.2.3
Data Downtime During a Switchover

When the radio applies a delivered configuration, the radio must reset to apply the changes. The impact on a system with a third-party data application should be carefully considered.

It is difficult to predict the impact of an Over-the-Air configuration on every third-party data application in the market. It is recommended that a small scale test, with a few controlled radios, is run to understand the recovery process for a specific third-party data application before performing a configuration change on a large group.

Here are some conditions to consider:

- If features, options, or channels required by the third-party data application within the radio are updated incorrectly, a problem can occur. Be cautious when changing such options.
- If ARS Suppression After Switchover option is selected, and the new configuration causes the radio to be on a different channel, then the routing of a third-party data application that utilizes ARS may lose track of which channel the radio is on. Be careful to only suppress ARS after a switchover if making minor changes that do not affect the currently selected channel.
- Because the radio performs a reset, temporary data could be lost. However, if the ARS Suppression After Switchover option was checked within Radio Management), not only does the radio not send a new ARS message after reset, it also preserves all previous LRRP requests and text message service availability requests for this power cycle. This ensures the radio continues sending GPS messages, and knows where the text message server is located after a switchover. If LRRP is already stored persistently, then it can still be stored after a switchover regardless of the ARS Suppression After Switchover option.
- If the third-party data application's temporary data is lost, then the radio may need to re-register after a switchover to trigger the data application to send new information. If this is the case then the ARS Suppression After Switchover option should be unselected, allowing the radio to send an ARS message after a switchover.
- If the third-party data application sends a large number of data messages to a radio when it registers, one should take caution when switching over many radios at the same time, since this could cause an influx of data messages on the channel. Consider increasing the radio's ARS Initialization Delay timer on the presence registrations. Since this can delay sending the ARS message, it could increase the amount of time before the radio contacts the data application, and therefore increases data downtime.

4.31
Radio Management Computer Specifications

Table 94: Radio Management Computer Specifications

Component	Requirements
Operating Systems	• Windows 10 (32 & 64-bit) • Windows 11 (64 bit)
	• Windows Server 2016 (Essential and Standard) • Windows Server 2019 • Windows Server 2022
Memory	RM Client / RM Server / RM Device Programmer Install: 1 GB and above required by host Operation System

Component	Requirements
	RM Server / RM Device Programmer Install: 1 GB and above required by host Operation System
	RM Client Only Install: RAM required by host Operation System
Hard Disk	RM Client / RM Server / RM Device Programmer Install: 5 GB (Program Files & Database)
	RM Server / RM Device Programmer Install: 5 GB (Program Files & Database)
	RM Client Only Install: 400 MB (Program Files & Archive Files*)
	* More space would be required if saving archive files of your radios and device update packages. Each archive file or device update package varies in size depending on the features of the radio.
Other (All Installs)	USB ports (1 or more depending on system configuration)
	Network Connection
	DVD Drive
Software	Running multiple instances of the RM application on one computer is not recommended.

The MNIS and DDMS do not currently support Windows 8 or Windows Vista.

4.32 Configurable Timers

The following is a list of timers that are used to synchronize communication in the radio system. The values of these timers can be configured through the CPS.

Table 95: Configurable Timers

Timer Name	Description	Notes
TX Preamble Duration	Preamble is a string of bits added in front of a data message or control message (Text Messaging, Location Messaging, Registration, Radio Check, Private Call, and others) before transmission. This preamble prolongs the message in order to reduce the chances of the message being missed by the receiving radio. The Transmit (TX) Preamble Duration sets the duration of the preamble. This duration needs to be increased as the number of scan members increases on the target radio. This value can be increased in all the transmitting radios if scanning radios are often missing data messages. However, a larger preamble occupies the channel longer. Therefore, increasing the Transmit Preamble duration increases the success rate of data received while other radios are scanning, but decreases the amount of data that can be transmitted on the channel. This is a radio-wide feature.	The TX Preamble feature is disabled if the duration is set to 0. This feature is supported in Digital mode only.

Timer Name	Description	Notes
Talkaround Group Call Hang Time	Sets the duration during which a radio talks back to a received call or continues a transmitted call using the previously received or previously transmitted digital Group ID. This hang time is used during a Group Call in Talkaround mode to produce smoother conversation. During this time, other radios can still transmit since the channel is essentially idle. After the hang timer expires, the radio transmits using the Contact Name specified for this channel.	This feature is supported in Digital mode only.
Talkaround Private Call Hang Time	Sets the duration the radio keeps the call setup after the user releases the Push-to-Talk (PTT) button. This is to avoid setting up the call again each time the user presses the PTT to transmit. This hang time is used during a Private Call in Talkaround mode to produce smoother conversation. During this time, other radios can still transmit since the channel is essentially idle.	–
Subscriber Inactivity Timer	The Subscriber Inactivity Timer (SIT) controls how long the repeater continues transmitting with absence of subscriber activity on the uplink. If the repeater is operating on shared-use frequencies, it cannot remain keyed indefinitely for the benefit of broadcasting synchronization signals to radios. The repeater is likely de-keyed most of the time; thereby requiring radios to first activate the repeater (through the uplink frequency) and acquire synchronization (through the downlink frequency) before completing the call setup request and subsequent first transmission. The net result of these extra procedures is increased access time; therefore, it is desirable to avoid these steps, whenever possible. There is a trade-off to minimizing access time by keeping the repeater keyed for as long as practically possible, while complying with the regulations regarding shared-use channels, which essentially require the repeater to de-key when the channel is not in use. This can be balanced with the use of the Subscriber Inactivity Timer. If shared use is not a concern, the SIT can be set to the maximum value. If shared use is a concern, the SIT should be set equal to or slightly longer than the configured call hang timers.	The value of this feature must be equal to or greater than the Hang Time (Group, Private or Emergency – whichever is the longest). This feature is disabled if Repeater Mode is set to Analog.
Group Call Hang Time	Sets the duration the repeater reserves the channel after the end of a Group Call transmission. During this time, only members of the Group that the channel is reserved for can transmit. This produces smoother conversation.	This feature is disabled if Repeater Mode is set to Analog. The value of this feature must be equal to or less

Timer Name	Description	Notes
		than the Subscriber Inactivity Timer value.
Private Call Hang Time	Sets the duration the repeater reserves the channel after the end of a Private Call transmission. During this time, only the individuals involved in the call that the channel is reserved for can transmit. This produces smoother conversation. The user may want to set a longer hang time than the Group Call Hang Time as an individual tends to take a longer time to reply (talkback) in a Private Call.	This feature is disabled if Repeater Mode is set to Analog. The value of this feature must be equal to or less than the Subscriber Inactivity Timer value.
Emergency Call Hang Time	Sets the duration the repeater reserves the channel after the end of an Emergency Call transmission. During this time, only members of the Group that the channel is reserved for can transmit. This produces smoother conversation. The user may want to set the longest hang time as compared to the Private and Group Call Hang Time to reserve the channel long enough to receive an emergency response.	This feature is disabled if Repeater Mode is set to Analog. The value of this feature must be equal to or less than the Subscriber Inactivity Timer value.
Call Hang Time	Sets the duration that the repeater reserves the channel for after the end of an analog call transmission. During this time, only members of the call that the channel is reserved for can transmit. This produces smoother conversation. As this hang timer is shared among all types of analog calls (Group, Private, Emergency and others), the duration should be set following the call type that needs the longest hang time.	This feature is enabled only if Repeater Mode is set to Analog or Dynamic Mixed Mode.
TX Interval	The station will generate a Continuous Wave Identification (CWID, also called BSI) when the repeater has no other repeat audio requests (either analog or digital), or all digital hang time has finished and the programmed transmission interval timer period has expired. This feature should be set to a period shorter than the Mix Mode Timer to allow the station the opportunity to send a CWID at the end of a set of user radio exchanges prior to having to send the ID mixed with analog repeat audio.	–
Mix Mode Timer	The station generates a Continuous Wave Identification (CWID) mixed with analog audio when the repeater is repeating analog signals or is in analog hang time and the programmed mix mode timer has expired. This feature should be set to a period longer than the TX Interval to allow the station the opportunity to send a CWID by itself at the end of a set of user radio exchanges rather than having to send the ID mixed with analog repeat audio.	This feature is disabled by the repeater if the value is set to 255 in Analog mode. This feature is also disabled by the repeater if it is in Digital or in Dynamic Mixed Mode. This feature is not applicable to digital repeater operation as CWID is not

Timer Name	Description	Notes
		generated while digital repeat is in progress.
Pretime	Sets the duration that the radio waits, after a Push-to-Talk (PTT) button press, before it starts transmitting the Motorola Solutions Data Communication (MDC) signaling system data packet (for example, preamble bit sync) and data. When communicating through a repeater system or console, this feature allows the repeater to stabilize before the radio starts transmitting the data. Additionally, this timer gives scanning radios time to land on the channel prior to the reception of MDC data.	This feature is supported in Analog mode only.
Coast Duration	If the carrier signal is lost after Motorola Solutions Data Communication (MDC) signaling data is detected, the radio stays muted for the duration of this timer or until the carrier signal is redetected. Once the carrier signal is redetected, this timer is stopped, and the Data Operated Squelch (DOS) Auto Mute Duration timer begins again. This feature helps to prevent temporary loss of DOS in areas of poor signal strength or signal distortions.	–
Auto Mute Duration	Sets the duration that the radio remains muted when the radio is receiving Motorola Solutions Data Communication (MDC) signaling data to reduce noise from the data reception. The user has to know the size of the data to select a suitable duration. If the duration is too short then some unwanted noise is still heard, and if the duration is too long, it might clip some voice audio. This is normally used on radios that support both voice and data on the same channel.	This feature is supported in Analog mode only.
Fixed Retry Wait Time	Sets the duration that the radio waits before attempting another polite or impolite transmission to transmit signaling data. Configuring the radios with different wait durations increases the probability of accessing the system and reduces the chances of data lost due to collisions.	This feature is supported in Analog mode only.
Time-Out Timer (TOT)	The Time-Out Timer (TOT) is the amount of time that the radio can continuously transmit before transmission is automatically terminated. This feature is used to ensure the channel is not monopolized by any one radio. The user may set smaller time-outs for busier channels. This is a channel-wide feature.	–
Time-Out Timer Rekey Delay	Sets the amount of time that the radio waits on a channel after the Time-Out Timer expires (which stops the radio transmission) before allowing the	–

Timer Name	Description	Notes
	user to transmit again. This is a channel-wide feature.	
Hang Time	This sets the duration that the radio that remains on a landed channel after the end of a transmission during a scan operation. The hang time prevents the radio from resuming scanning until the conclusion of the response to the initial call. The timer starts after the end of a transmission and resets whenever a valid activity is detected on the channel during the hang time.	It is recommended to increase the hang time value if the call hang timer in the radio increases for direct mode operation. In repeater mode operation, it is recommended to keep this value as low as possible to allow the radios to start scanning as soon as the existing analog call ends.
Digital Hang Time	This sets the duration that the radio that remains on a landed digital channel after the end of a transmission during a scan operation. The hang time prevents the radio from resuming scanning until the conclusion of the response to the initial call. The timer starts after the end of a transmission and resets whenever a valid activity is detected on the channel during the hang time.	It is recommended to increase the hang time value if the call hang timer in the radio or repeater increases.
Signaling Hold Time	This sets the amount of time that the radio waits on an analog Scan List channel when a carrier signal of sufficient amplitude is detected on the channel. This pause allows the radio time to decode the analog system signaling data. If the decoded information is incorrect, the radio reverts to scan.	This feature must be equal to or greater than the amount of time it takes the radio to transmit the signaling data packet plus the channel's Signaling Systems Pretime.
		This feature is supported in analog mode only.
Priority Sample Time	This sets the duration that the radio waits, when in a call, before scanning the priority channels. If the call is taking place on a Priority 1 Channel, no scanning takes place. When scanning priority channels, the radio briefly mutes the current transmission. Increasing this interval improves the audio quality of the current transmission as fewer checks are done, but this also increases the chance of the radio missing out priority channel activity.	A priority member must be present in the Scan List.

4.33
MOTOTRBO Link Mode

The designer is able to choose the system capacity, such as the number of Backhaul Sites and Backhaul Chains at each site. The frequencies and roles of the repeater should also be considered when configuring the sites.

4.33.1
System Capacity in MOTOTRBO Link Mode

A MOTOTRBO Link configuration increases the coverage area but reduced the call capacity compare to a single site configuration. The maximum size is nine sites with eight links to connect the adjacent sites of a Backhaul Chain.

In a MOTOTRBO Link configuration, MOTOTRBO supports a maximum of 14 IP Site Connect (IPSC) Backhaul Peer or Backhaul Chains.

NOTE: The Hybrid system with three backhaul chains has been verified.

If you have a standard IPSC system and is adding MOTOTRBO Link Sites to expand the coverage, multiple Wireline applications is supported on the wired IPSC system. If the application is located at any MOTOTRBO Link site, then only one wireline application is supported in the system.

MOTOTRBO also supports one Wireline Phone application per system.

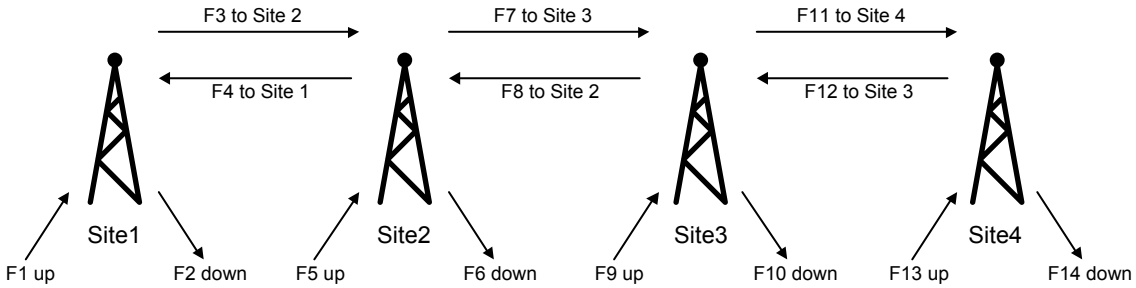
4.33.2
Frequency Considerations in MOTOTRBO Link Mode

The frequencies of repeaters should adhere to the following rules:

- Standard repeater and Link repeater at the same backhaul site must use different frequencies.
- The subscriber radios and Link repeaters can use different frequency bands. The subscriber radios could use Land Mobile Radio (LMR) channels in the UHF frequency band while the Link repeaters could use the VHF frequency band instead.
- The frequencies used by the Link repeaters between neighboring sites must match. That means the Tx frequency of the Link repeater of Site 1 must be the same as the Rx frequency of the Backward Link repeater at Site 2. The Rx frequency of the Link repeater at Site 1 must be same as the Tx frequency of the Forward Link repeater at Site 2.
- Frequencies can be reused if there is no overlapping between backhaul sites. For example, if there is no coverage overlap between Site 1 and Site 4. In the following figure, F1 used by the Standard repeater under Site 1 can be the same as F13 for the Standard repeater at site 4. Also, this rule can be applied on the Link repeaters.

The following figure shows an example of a Dedicated MOTOTRBO Link System with four backhaul sites.

Figure 219: Example of a Dedicated MOTOTRBO Link System with Four Backhaul Sites



4.33.3

Delay in MOTOTRBO Link Mode

The call setup delay and propagation delay in MOTOTRBO Link mode compared to IP Site Connect mode is increased due to the Over-The-Air (OTA) delay introduced by every hop.

For the call types with normal priority, such as Group voice call, the call setup delay is:

- Maximum system (eight hops): 1.5 second
- Smaller system (two hops): 800 ms

For the call types with high priority, such as Emergency call and Wireline Impolite voice call, the call setup delay could be:

- Maximum system (eight hops): 2.2 seconds
- Smaller system (two hops): 1.5 second

The propagation delay for the maximum system with eight hops is 1.2 second. The propagation delay for the smaller system with two hops is about 420 ms. If the call initiator and listener are under the same site, the propagation delay is 60 ms.

4.33.4

Repeater Role in a Dedicated Link Backhaul System Configuration

The following is a listing of the different roles the repeaters perform in a Dedicated Link Backhaul System Configuration.

Standard Repeater

The role of the Standard repeater in a MOTOTRBO Link configuration is essentially the same as a traditional repeater in a conventional single site configuration. The main function of the Standard repeater is to repeat calls received locally Over-The-Air (OTA) or calls received from the Link repeater on the LAN. Standard repeater takes slot synchronization information from Link repeater (it is not the Slot Timing Master).

NOTE: Standard repeater is also referred to as Drop repeater in this document.

Proxy Repeater

The Proxy repeater is a special Standard repeater which is at the origin site and acts as the connectivity bridge between the IP Site Connect WAN and the Digital Mobile Radio (DMR) channel connectivity across the Backhaul Chain. The Proxy repeater also forwards Extended Control and Management Protocol (XCMP) Messages from application peers and maintains presence information for all the repeaters located along the Backhaul Chain. In a Hybrid MOTOTRBO Link configuration, the Proxy repeater is

the IP Site Connect backhaul repeater and may also be a master or a slave peer in an IP Site Connect Backhaul network.

Link Repeater

The role of the Link repeater in a MOTOTRBO Link configuration is unique in that it essentially replaces the wireline connectivity interface with an OTA connectivity interface using a DMR-based protocol. The primary function of the Link repeater is to forward calls received from an adjacent backhaul site's Link repeater to the next site in the backhaul chain.

The following Link repeaters provide slot synchronization and should be the Slot Timing Master:

- Link repeater at Origin site.
- Link repeater at Terminating site
- Forward Link repeater at Interim site (direction from Terminating to Origin site).

The Backward Link Repeater at Interim site (direction from Origin to Terminating site) takes synchronization from the Forward Link Repeater (it is not the Slot Timing Master).

IP Site Connect Backhaul Repeater

The role of the IP Site Connect Backhaul repeater in a Hybrid MOTOTRBO Link configuration is similar to a traditional repeater in a conventional IP Site Connect configuration.

Table 96: Standalone Dedicated-Link Backhaul Configuration

		CPS/RM Options			
Backhaul Rode	Link Mode	Site Type	Repeater Type	Slot Timing Master	IPSC BH Site
Proxy	Dedicated Link	Origin	Standard Repeater	No	No
Drop	Dedicated Link	Interim/Terminating	Standard Repeater	No	No
Link	Dedicated Link	Origin/Interim/Termination	Link Repeater	Yes/No*	No

* Based on Link repeater's site type

Table 97: Hybrid Dedicated-Link Backhaul Configuration

		CPS/RM Options			
Backhaul Rode	Link Mode	Site Type	Repeater Type	Slot Timing Master	IPSC BH Site
Proxy	Dedicated Link	Origin	Standard Repeater	No	Yes
Drop	Dedicated Link	Interim/Terminating	Standard Repeater	No	No
Link	Dedicated Link	Origin/Interim/Termination	Link Repeater	Yes/No*	No
IPSC BH	None	N/A	N/A	N/A	Yes

* Based on Link repeater's site type

4.33.5

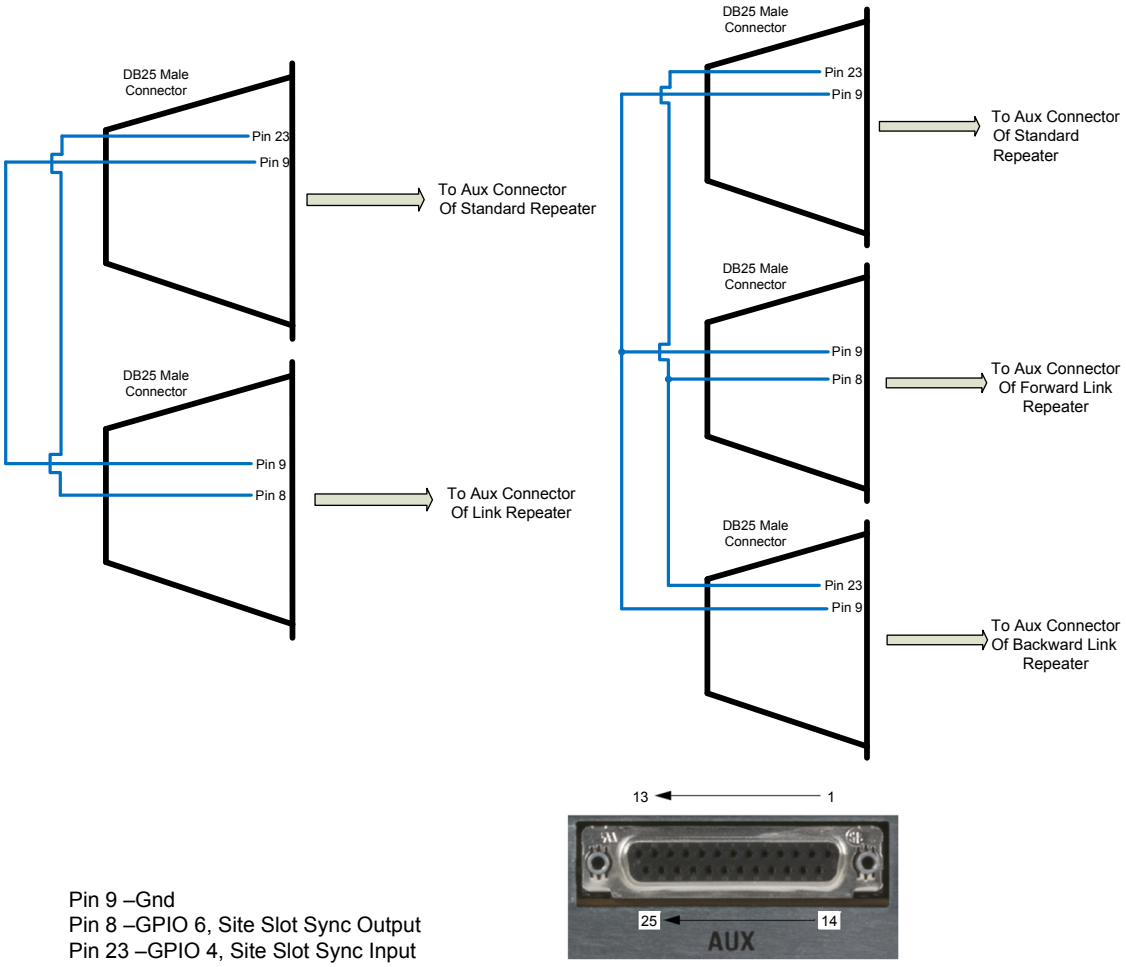
GPIO Pin Configurations

Within a backhaul site, the repeaters synchronize themselves by using GPIO pins on the accessory connector allocated for Slot Synchronization.

The physical connection is through the repeater GPIO connector, with the following pins:

- **DB25_23 - GPIO4:** Site Slot Sync Input -- Slot Timing Master is **No**
- **DB25_8 - GPIO6:** Site Slot Sync Output -- Slot Timing Master is **Yes**

Figure 220: GPIO Pin Configurations



Pin 9 –Gnd
Pin 8 –GPIO 6, Site Slot Sync Output
Pin 23 –GPIO 4, Site Slot Sync Input

4.33.6

Repeater Diagnostics and Control Feature Considerations

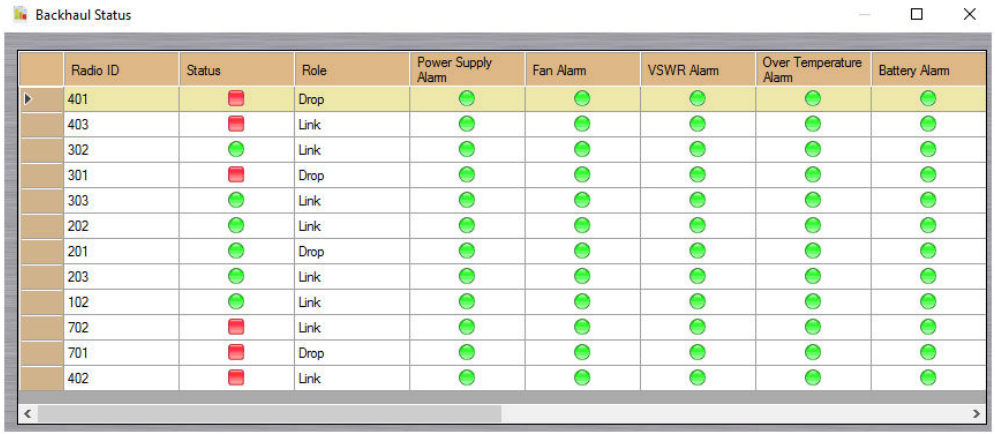
The following are considerations on how the Repeater Diagnostics and Control (RDAC) application supports the following MOTOTRBO Link systems.

In a MOTOTRBO Link system, the RDAC application connects to the Proxy repeater to retrieve the backhaul peer map in one Backhaul Chain, query, and displays the presence and alarm status of its backhaul peers. Remote control commands (such as, repeater enable/disable, power control, and so on) are not supported in a MOTOTRBO Link Chain.

In a Standalone Dedicated MOTOTRBO Link system, the RDAC application chooses the Proxy repeater as the Master peer and configures its IP address and Port number on the RDAC application.

In a Hybrid Dedicated MOTOTRBO Link system, the RDAC application connects to the IP Site Connect backhaul network and chooses the IP Site Connect Master repeater as the Master and configures its IP address and Port number on the RDAC application.

Figure 221: RDAC Backhaul Status



4.33.7

Restricted Access to System Feature Considerations

The following are considerations on how Restricted Access to System (RAS) supports the following MOTOTRBO Link systems.

In a Standalone Dedicated-Link MOTOTRBO Link system, RAS parameters are configured separately on all Drop, Link, and Proxy repeaters.

In a Hybrid Dedicated-Link MOTOTRBO Link system, RAS parameters are configured:

- On all Drop, Link repeaters separately,
- on IP Site Connect backhaul Master peer only (the IP Site Connect backhaul Master repeater is responsible for distributing RAS parameters to all other IP Site Connect backhaul Peer repeaters, including the Proxy repeater).

NOTE: RAS Migration mode is not supported in MOTOTRBO Link configurations. Radio ID Range Check is not applicable to Link repeaters.

4.33.8

Network Application Interface Wireline Interface Feature Considerations

The following are considerations on how the Network Application Interface (NAI) Wireline Interface supports the following MOTOTRBO Link systems.

If the MNIS data or a third-party application connects to one of the backhaul site LANs, the MNIS data or third-party application chooses the Standard repeater as the Master and configures its IP address and User Datagram Protocol (UDP) port number on the MNIS/third party application.

If the MNIS data or third-party application connects to an IP Site Connect backhaul network, the MNIS data or third-party application chooses the IP Site Control Master repeater as the Master and configures its IP address and Port number on the MNIS/third party application.

4.33.9
Continuous Wave Identification Considerations

Analog Continuous Wave Identification (CWID) is supported on both Drop and Link repeaters. The GPIO link master at the terminate site, which is the scheduler, schedules and sends out the CWID of all the repeaters in the backhaul chain. None of the repeaters in the backhaul chain can send the CWID unless triggered by the GPIO link master scheduler.

CWID configuration is set for each repeater within the backhaul chain by using existing configuration using Customer Programming Software (CPS)/Radio Management (RM). All repeaters in the backhaul chain are either configured with CWID enabled or disabled.

It is recommended to configure a similar length of CWID characters for each repeater within the backhaul chain to avoid asynchronous CWID transmission duration. If the length of the CWID characters for each repeater is different, dummy characters could be added to fill the gap.

It is also recommended to configure all the repeaters in MOTOTRBO Link mode with the same CWID transmission interval. The CWID transmission interval should be larger than the Link Beacon Interval. For example, if the Link Beacon Interval is five minutes, the CWID transmission interval could be configured as ten minutes.

IP Site Connect backhaul repeaters send the CWID on their own pace without triggering from the scheduler (same as legacy conventional repeaters).

4.33.10
Failure of the Terminating Site

The terminating site Link repeater serves the role of the system timing Master in the Backhaul Chain. The terminating site Link repeater periodically transmits to the neighboring sites the Keep Alive Beacon CSBK messages while the system is idle in the Backhaul Chain. This synchronizes the timeslot timing and presence information within the Backhaul Chain. In absence of the periodic Keep Alive Beacon CSBK messages between a site and the timing master site, the Slot Sync Master Link repeater concludes that either the Timing Master repeater or the Over-The-Air (OTA) in-between has failed. The Slot Sync Master of this site takes on the system Timing Master role and continues to provide service with available sites.

4.33.11
Failure of the Interim or Origin Site

In absence of the periodic Keep Alive Beacon CSBK messages between the two interim sites, the Backhaul Chain is divided into two independent Backhaul Chains with their own available sites. When the Origin site fails, a Hybrid Backhaul system loses the connectivity between the IP Site Connect backhaul networks and the Backhaul Chain.

4.33.12
Failure of a LAN Switch

A repeater broadcasts “Keep Alive” messages periodically over the LAN to other repeaters at its site. When the LAN fails, a repeater detects the absence of the periodic “Keep Alive” messages. All radios at this site lose the wide area connectivity with other remote sites. However, the Link repeaters are still able to forward calls between their neighbor backhaul sites.

4.33.13
Failure of a MOTOTRBO Link Repeater

A repeater detects the failure of another repeater at its site by the absence of the periodic “Keep Alive” messages from that repeater.

When the failure repeater is a:

Standard Repeater
All radios at this site loses connectivity to the system.

Proxy Repeater
Hybrid Backhaul system loses connectivity between the IP Site Connect Backhaul networks with the Backhaul Chain.

Link Repeater without the Slot Timing Master function
The site loses the call connectivity with its neighbor sites in a backward direction.

Link Repeater with the Slot Timing Master function
The site fails to synchronize slot timing from the Backhaul Chain and loses the call connectivity from the Backhaul Chain eventually.

4.34
Broadcast Calls

A Broadcast Call is an ETSI DMR one-way group call. This type of a call has no hangtime and allows the operator to select a specific group of users to call. It is supported for an Emergency Group Call.

The Network Application Interface (NAI) for third party voice applications supports the Broadcast calls.

The Broadcast calls are supported in the following modes:

- Direct Mode
- Dual Capacity Direct Mode
- Single Site Repeater Mode
- Extended Range Direct Mode
- IP Site Connect Mode

If you are not a part of the Broadcast call, and press the PTT button, the call request is denied by the radio. If the Broadcast call is set to interruptible, the call can be interrupted to support Emergency Voice Interrupt (EVI), Data Over Voice Interrupt (DOVI) and Remote De-Key (RVD), but not Voice Interrupt (VI).

The following call types can be transmitted as a Broadcast call:

- Group call
- Unaddressed call
- Open Voice Channel Mode (OVCM) call

A Broadcast call selection option is available for a group call contact. If this option is not selected the call has hangtime. If the Broadcast call option is selected, the group call has no hangtime.

You can configure a contact group ID as both a Broadcast and a Non-Broadcast call by creating two contacts for the same group ID, where one contact has the Broadcast call option selected and the other not selected. In this scenario the two contacts are associated with different channel positions.

4.34.1
Configuring Broadcast Calls

Use this procedure to enable a Broadcast Call in the Radio Management (RM) application.

Procedure:

1. In the RM application, in the left, navigate to **Set Categories**.
2. Expand the **Configuration** folder.
3. Expand the **Contacts** folder.
4. From the **Contacts** list, click the contact you want to configure.
5. In the right pane, expand the **Digital** section.
6. Select the **OVCM Call** check box.
7. From the **Route Type** drop-down menu, select **Broadcast**.
8. On the top of the right pane, click **Save**.

4.35
Unaddressed Calls

An Unadressed call is an ETSI DMR group call to one of the 16 predefined group IDs. To initiate and/or receive an Unaddressed call, a contact for one of the predefined IDs is required.

The Network Application Interface (NAI) for third party voice applications supports the Unaddressed calls.

The Unaddressed calls are supported in the following modes:

- Direct Mode
- Dual Capacity Direct Mode
- Single Site Repeater Mode
- Extended Range Direct Mode
- IP Site Connect Mode

If the Unaddressed call is set to interruptible, the call can be interrupted to support:

- Emergency Voice Interrupt (EVI)
- Data Over Voice Interrupt (DOVI)
- Remote De-Key (RVD)
- Voice Interrupt (VI)

The Unaddressed call can be configured to be a one-way Broadcast call without hangtime or a two-way Group call with hangtime. Only one Unaddressed Call can be configured per device (subscriber) and many per console.

The allowed ID range for the Unaddressed call contacts is from 16777184 to 16777199.

4.35.1
Configuring Unaddressed Calls

Use this procedure to enable an Unaddressed Call in the Radio Management (RM) application.

Procedure:

1. In the RM application, in the left pane, navigate to **Set Categories**.

2. Expand the **Configuration** folder.
3. Expand the **Contacts** folder.
4. From the **Contacts** list, click the contact you want to configure.
5. In the right pane, expand the **Digital** section.
6. Select the allowed **Call ID** item from 16777184 to 16777199 range.
7. On the top of the right pane, click **Save**.

4.36

Open Voice Channel Mode Calls

An Open Voice Channel Mode (OVCM) is compliant with an ETSI DMR requirements. In OVCM, radios not preconfigured to work in a particular system can both receive and transmit during a group or individual call. The OVCM group call also supports broadcast calls.

The Network Application Interface (NAI) for third party voice applications supports OVCM calls, except for phone calls.

The OVCM calls are supported in the following modes:

- Direct Mode
- Dual Capacity Direct Mode
- Single Site Repeater Mode
- Extended Range Direct Mode
- IP Site Connect Mode

If the OVCM is set to interruptible, the call can be interrupted to support:

- Voice Interrupt (VI)
- Emergency Voice Interrupt (EVI)
- Data Over Voice Interrupt (DOVI)
- Remote De-Key (RVD)

Contact Type (OVCM TX) supports initiating OVCM calls, while Channel Configuration OVCM (OVCM RX) supports participating in an OVCM call. All group and individual contacts can be configured with OVCM TX and OVCM RX enabled or disabled, with disable being the default option. When OVCM TX is enabled for a group or an individual contact, the Subscriber Unit (SU) indicates the call is in OVCM.

The Subscriber Units (SUs) can be configured to allow OVCM RX. In that case, the radio can participate in calls which would otherwise require special preconfiguration. OVCM RX is configurable at the personality level.

Table 98: OVCM CONFIGURABLE PARAMETERS

Tx (Contact Type)	Rx (Channel Configuration)	Expected Behavior
OVCM Tx Enabled	OVCM Rx Enabled	1. Initiates an OVCM call. 2. Receives any OVCM call. 3. Talks back to an OVCM call indicating OVCM.
OVCM Tx Enabled	OVCM Rx Disabled	1. Initiates an OVCM call.

Tx (Contact Type)	Rx (Channel Configuration)	Expected Behavior
		2. Does not receive an OVCM call if not a target group or Subscriber Unit. 3. Receives an OVCM call if a target group or Subscriber Unit (SU). 4. Talks back to an OVCM call indicating OVCM.
OVCM Tx Disabled	OVCM Rx Enabled	1. Does not initiate an OVCM call. 2. Receives any OVCM call. 3. Talks back to an OVCM call indicating OVCM.
OVCM Tx Disabled	OVCM Rx Disabled	1. Does not initiate an OVCM call. 2. Does not receive an OVCM call if not a target group or Subscriber Unit (SU). 3. Receives an OVCM call if a target group or Subscriber Unit (SU). 4. Talks back to an OVCM call indicating OVCM.

4.36.1
Configuring Open Voice Channel Mode Calls in TX Mode

Use this procedure to enable an Open Voice Channel Mode (OVCM) Call in TX Mode in the Radio Management (RM) application.

Procedure:

1. In the RM application, in the left pane, navigate to **Set Categories**.
2. Expand the **Configuration** folder.
3. Expand the **Contacts** folder.
4. From the **Contacts** list, click the contact you want to configure.
5. In the right pane, expand the **Digital** section.
6. Select the **OVCM Call** check box.
7. On the top of the right pane, click **Save**.

4.36.2
Configuring Open Voice Channel Mode Calls in RX Mode

Use this procedure to enable an Open Voice Channel Mode (OVCM) Call in RX Mode in the Radio Management (RM) application.

Procedure:

1. In the RM application, in the left pane, navigate to **Set Categories**.
2. Expand the **Configuration** folder.
3. Expand the **Zone** folder.
4. From the **Zone** list, click the zone you want to configure.

5. From the **Zone Items** section on the right, click the row you want to configure.
6. Select the **OVCM Decode** check box.
7. On the top of the right pane, click **Save**.

Chapter 5

Capacity Plus Network Configurations

5.1 Juniper Infrastructure

5.1.1 Recommended Network Equipment (Juniper)

The following Juniper network equipment is recommended for the MOTOTRBO Systems solution:

- Juniper SRX300 - Services Gateway
- Juniper SRX345 - Services Gateway
- Juniper EX2300-24T - Ethernet Switch

CAUTION: Mixing HP and Juniper equipment is not recommended, since mixed configurations are not verified.

The SRX300 and SRX345 Services Gateways are next-generation networking and security solutions that consolidate security, routing, and switching. They are used to route traffic between the networks at a site. In the case of a multiple site system, they provide Wide Area Network (WAN) connectivity between the sites. For more information, see the Juniper product information for the routers.

Figure 222: Juniper SRX300 Services Gateway Front View

Figure 223: Juniper SRX300 Services Gateway Rear View

For systems with many sites, it is recommended to use SRX345 as a router for the Hub site (the central point of the system, usually with the Master Repeater installed). For High Availability (HA), Juniper SRX can work as a cluster build with two SRX345. In this type of configuration, the two physical devices work as a uniform logical device, where one is active, and the second one is hot standby. In case of master SRX failure, the standby device takes over with minimal traffic disruption. For more information about cluster configuration, see SRX Chassis Cluster Configuration Overview on page 614

Figure 224: Juniper SRX345 Services Gateway Front View

Figure 225: Juniper SRX345 Services Gateway Rear View

Juniper EX2300-24T Ethernet Switch is a managed Ethernet switch with 24 ports of 10/100/100 and 4 SFP ports. The 24 ports of 10/100/1000 are used to connect the Mototrbo Systems devices to the network.

Figure 226: Juniper EX2300-24T Ethernet Switch Front View

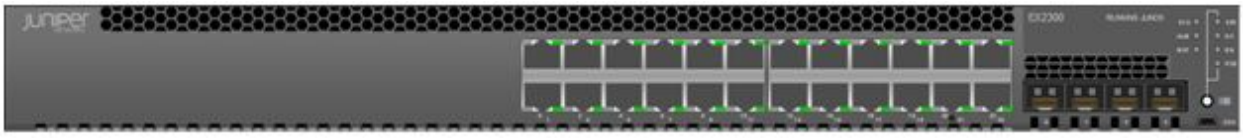


Figure 227: Juniper EX2300-24T Ethernet Switch Rear View

5.1.2

IP Plan for Capacity Plus Single Site and Capacity Plus Multisite Systems

The following section describes the IP plan for the Capacity Plus Single Site and Capacity Plus Multi Site systems. Configuration templates described in the next sections are based on the IP plans described in Capacity Plus Single Site Detailed IP Plan on page 585 and Capacity Plus Multi Site Detailed IP Plan on page 588.

5.1.2.1

CPSS and CPMS Systems LAN Networks

The CPSS and CPMS systems comprise of two IPv4 networks that serve to isolate and manage different types of network traffic:

Radio Network

Radio Network is used mainly for subnets with repeaters. Besides repeaters, it can contain RDAC applications, and technicians service laptop computers exclusively.

Application Network

Application Network hosts all Motorola and non-Motorola applications clients and servers cooperating with MOTOTRBO systems such as: MNIS, RDAC, RM, Dispatch Consoles (TRBOnet, Avtec, SmartPTT).

Besides the networks for the hosts of MOTOTRBO systems, there are subnets for device management and inter-site traffic:

Management Network

Management Network is a subnet for the router management loopback interface. Each router has assigned one IPv4 address with a /32 subnet mask on its `lo0` interface.

WAN Point-to-Point and Point-to-Multipoint

Subnets for WAN are used only in the CPMS systems to address the VPN tunnel interfaces. For Hub-to-Spoke topology, the WAN point-to-point interfaces are in use, so the subnets with /30 subnet mask are required. For AVPN topology, the WAN point-to-multipoint interfaces are in use, so one subnet with /27 subnet mask per system is needed.

5.1.2.2

CPSS and CPMS Systems Site IDs

Subnetworks that belong to the Radio and Application networks are allocated to each site of a CPSS or CPMS system as needed, based on the equipment that is present at a physical location. Repeaters, MNIS, RDAC, and Dispatch Console servers are provisioned with unique Site IDs, Peer IDs, Radio IDs, IPv4 addresses, and UDP ports.

A Site ID must be in the range 1 ≤ siteID ≤ 15. In the CPMS system IP plan, the Site IDs are used as the third octet of an IPv4 address which is intended to be a “user-friendly” indication of the provisioned Site ID. In the proposed IP plan, the Site ID is used to calculate Peer ID and the Peer ID is used to calculate the unique UDP port number for each device in the system. For more information about Site ID, Peer ID, IPv4 address, and UDP port calculation of the CPMS system, see Capacity Plus Multi Site Detailed IP Plan on page 588.

The proposed IP plan for CPSS systems has the same logic but all parameters are already statically assigned by using Site ID equal to “1”. For more information about Site ID, Peer ID, IPv4 address, and UDP port calculation of the CPSS system, see Capacity Plus Single Site Detailed IP Plan on page 585.

NOTE: Not all devices in the system require provisioning of all the above parameters.

5.1.2.3
CPSS and CPMS Systems IP Plan Summary

CPSM

The CPSS and CPMS networks use IPv4 addresses described in *RFC-1918 Address Allocation for Private Internets*. The address space 172.16.0.0/12 includes all IP addresses in the range 172.16.0.0 through 172.31.255.255. Some subnets from this range are used in the IP plan and are presented in the following table using the Classless Inter-Domain Routing (CIDR) notation.

If the WAN provider uses IPv4 addresses in this space, there may be IPv4 address conflicts between the WAN (underlay) and the CPSS or CPMS (overlay) networks, so the IP address scheme may require modification to eliminate this conflict.

An IP plan is one of the most important elements of the designing phase of the CPSS or CPMS systems. It should be adjusted for the IP space already used by the customer. The IP plan should also acommodate the planned number of devices in a deployment, as well as a potential expansion of the system.

The IP plan used by MOTOTRBO configuration templates assumes using VLANs and separation between radio infrastructure and PCs with the application. The RDAC application can optionally be deployed in both networks so in the IP plan it has reserved IPv4 address in both VLANs.

For a high-level summary of the entire CPSS and CPMS systems' IP plan, see Table 99: CPSS and CPMS IP Plan Summary on page 585.

Table 99: CPSS and CPMS IP Plan Summary

IP Space	Network Name
10.16.0.0/16	Radio Network
10.17.0.0/16	Application Network
10.30.0.0/20	WAN Point-to-Multipoint
10.30.16.0/20	Management Network
10.31.0.0/16	WAN Point-to-Point

5.1.2.4
Capacity Plus Single Site Detailed IP Plan

CPSS

In Capacity Plus Single Site systems, the maximum number of repeaters can be 20 so the RDAC Peer ID is moved to 135 and UDP port to 56135. This is the main difference between the CPSS and CPMS systems IP plan logic. (see the following Table 100: Radio Network Subnet IP Assignment in the CPSS IP Plan on page 586 table for a detailed IPv4 address assignment for each required device in the Radio Network). That number of repeaters allows the use of a smaller subnet size in case customers cannot allocate IP subnets with mask /24. The IP subnet with mask /26 has enough space for all devices.

The Application Network uses an IP subnet with mask /27 and it should cover most of the customers' demands for IP address space. Table 101: Application Network Subnet IP Assignment in the CPSS IP Plan on page 587 is a detailed IPv4 address assignment for devices in the Application Network.

Table 100: Radio Network Subnet IP Assignment in the CPSS IP Plan

Radio Network VLAN=10				
IP Address /24	**peerID**	**UDP Port**	**Function**	**Comments**
10.16.1.0	N/A	N/A	IETF-Defined Sub-net Address	N/A
10.16.1.1	N/A	N/A	Router (Default Gateway)	N/A
10.16.1.2	N/A	N/A	Router-1 (VRRP)	Used when router redundancy is used.
10.16.1.3	N/A	N/A	Router-2 (VRRP)	Used when router redundancy is used.
10.16.1.4	N/A	N/A	Ethernet Switch	N/A
10.16.1.5	N/A	N/A	Ethernet Switch (if present)	Used in double switch configuration.
10.16.1.6-7	N/A	N/A	N/A	Reserved for transport devices.
10.16.1.8-14	N/A	N/A	N/A	Reserved for future use.
10.16.1.15	135	56135	RDAC	N/A
10.16.1.16	100	56100	Rest Channel	RID = 00 (Virtual IP Address)
10.16.1.17	101	56101	Repeater #1	RID = 01
10.16.1.18	102	56102	Repeater #2	RID = 02
10.16.1.19	103	56103	Repeater #3	RID = 03
10.16.1.20	104	56104	Repeater #4	RID = 04
10.16.1.21	105	56105	Repeater #5	RID = 05
10.16.1.22	106	56106	Repeater #6	RID = 06
10.16.1.23	107	56107	Repeater #7	RID = 07
10.16.1.24	108	56108	Repeater #8	RID = 08
10.16.1.25	109	56109	Repeater #9	RID = 09
10.16.1.26	110	56110	Repeater #10	RID = 10
10.16.1.27	111	56111	Repeater #11	RID = 11
10.16.1.28	112	56112	Repeater #12	RID = 12
10.16.1.29	113	56113	Repeater #13	RID = 13
10.16.1.30	114	56114	Repeater #14	RID = 14
10.16.1.31	115	56115	Repeater #15	RID = 15
10.16.1.32	116	56116	Repeater #16	RID = 16
10.16.1.33	117	56117	Repeater #17	RID = 17
10.16.1.34	118	56118	Repeater #18	RID = 18
10.16.1.35	119	56119	Repeater #19	RID = 19
10.16.1.36	120	56120	Repeater #20	RID = 20
10.16.1.37-47	N/A	N/A	N/A	Reserved for future use.
10.16.1.48-62	N/A	N/A	DHCP Pool	N/A

Radio Network VLAN=10				
IP Address /24	**peerID**	**UDP Port**	**Function**	**Comments**
10.16.1.63-254	N/A	N/A	N/A	Reserved for future use.
10.16.1.254	N/A	N/A	IETF-Defined Subnet Directed Broadcast	N/A

Table 101: Application Network Subnet IP Assignment in the CPSS IP Plan

Application Network VLAN=30				
IP Address /27	**peerID**	**UDP Port**	**Function**	**Comments**
0.17.1.0	N/A	N/A	IETF-Defined Subnet Address	N/A
10.17.1.1	N/A	N/A	Router (Default Gateway)	N/A
10.17.1.2	N/A	N/A	Router-1 (VRRP)	Used when router redundancy is used.
10.17.1.3	N/A	N/A	Router-2 (VRRP)	Used when router redundancy is used.
10.17.1.4-7	N/A	N/A	N/A	Reserved for transport devices.
10.17.1.8	128	56128	MNIS #1	May additionally host server applications and clients.
10.17.1.9	129	56129	MNIS #2	May additionally host server applications and clients.
10.17.1.10	130	56130	Dispatch Console Server #1	If not co-resident on MNIS.
10.17.1.11	131	56131	Dispatch Console Server #2	If not co-resident on MNIS.
10.17.1.12	N/A	N/A	Dispatch Console Client #1	If not co-resident on MNIS.
10.17.1.13	N/A	N/A	Dispatch Console Client #2	If not co-resident on MNIS.
10.17.1.14	134	N/A	Radio Management Server	If not co-resident on MNIS.
10.17.1.15	135	56135	RDAC	N/A
10.17.1.16	136	56136	Genesis	N/A
10.17.1.17	N/A	4012	BFM	If not co-resident on MNIS.
10.17.1.18	N/A	N/A	Edge Node	N/A
10.17.1.19-23	N/A	N/A	N/A	Reserved for other application hosts.
10.17.1.24-30	N/A	N/A	DHCP Pool	N/A

Application Network VLAN=30				
IP Address /27	**peerID**	**UDP Port**	**Function**	**Comments**
10.17.1.31	N/A	N/A	IETF-Defined Subnet Directed Broadcast	N/A

5.1.2.5

Capacity Plus Multi Site Detailed IP Plan

CPMS

Table 102: Radio Network Subnet IP Assignment in the CPMS IP Plan on page 588 presents a detailed IPv4 address assignment for each required device in the Radio Network. The IP plan allows the use of a smaller subnet size, in case customers cannot allocate IP subnets with mask /24. The IP subnet with mask /26 has enough space for all devices. When a DHCP server is not required, the subnet can be shrunk to /27.
The Application Network uses an IP subnet with mask /27, which should cover most of the customers' demands for IP address space. Table 103: Application Network Subnet IP Assignment in the CPMS IP Plan on page 590 shows a detailed IPv4 address assignment for devices in the Application Network.

The following tables follow common rules, where Site ID is used to create unique IP subnets for each site and Peer IDs for each device. The unique UDP port assignment rule employing Peer ID is useful during system diagnostics in case of problems, especially during packet capture analysis.

The formula for Peer ID consists of two elements, Site ID (one or two digits) and RID (Repeater ID), or statically assigned two digits number.

The formula for UDP port number is a sum of Peer ID and 56000.

Table 102: Radio Network Subnet IP Assignment in the CPMS IP Plan

Radio Network VLAN=10				
1 ≤ siteID ≤ 15				
IP Address /24	**peerID**	**UDP Port**	**Function**	**Comments**
10.16.*<siteID>*.0	N/A	N/A	IETF-Defined Subnet Address	N/A
10.16.*<siteID>*.1	N/A	N/A	Router (Default Gateway)	N/A
10.16.*<siteID>*.2	N/A	N/A	Router-1 (VRRP)	Used when router redundancy is used.
10.16.*<siteID>*.3	N/A	N/A	Router-2 (VRRP)	Used when router redundancy is used
10.16.*<siteID>*.4	N/A	N/A	Ethernet Switch	N/A
10.16.*<siteID>*.5	N/A	N/A	Ethernet Switch (if present)	Used in sites with double switch configuration.
10.16.*<siteID>*.6-7	N/A	N/A	N/A	Reserved for transport devices.
10.16.*<siteID>*.8-14	N/A	N/A	N/A	Reserved for future use.

Radio Network VLAN=10				
1 ≤ siteID ≤ 15				
IP Address /24	**peerID**	**UDP Port**	**Function**	**Comments**
10.16.<siteID>.15	[siteID][15]	56000+ [peerID]	RDAC	N/A
10.16.<siteID>.16	[siteID][RID]	56000+ [peerID]	Rest Channel	RID = 00 (Virtual IP Address)
10.16.<siteID>.17	[siteID][RID]	56000+ [peerID]	Repeater #1	RID = 01
10.16.<siteID>.18	[siteID][RID]	56000+ [peerID]	Repeater #2	RID = 02
10.16.<siteID>.19	[siteID][RID]	56000+ [peerID]	Repeater #3	RID = 03
10.16.<siteID>.20	[siteID][RID]	56000+ [peerID]	Repeater #4	RID = 04
10.16.<siteID>.21	[siteID][RID]	56000+ [peerID]	Repeater #5	RID = 05
10.16.<siteID>.22	[siteID][RID]	56000+ [peerID]	Repeater #6	RID = 06
10.16.<siteID>.23	[siteID][RID]	56000+ [peerID]	Repeater #7	RID = 07
10.16.<siteID>.24	[siteID][RID]	56000+ [peerID]	Repeater #8	RID = 08
10.16.<siteID>.25	[siteID][RID]	56000+ [peerID]	Repeater #9	RID = 09
10.16.<siteID>.26	[siteID][RID]	56000+ [peerID]	Repeater #10	RID = 10
10.16.<siteID>.27	[siteID][RID]	56000+ [peerID]	Repeater #11	RID = 11
10.16.<siteID>.28	[siteID][RID]	56000+ [peerID]	Repeater #12	RID = 12
10.16.<siteID>.29	[siteID][RID]	56000+ [peerID]	Repeater #13*	RID = 13*
10.16.<siteID>.30-31	N/A	N/A	N/A	Reserved for future use
10.16.<siteID>.32-62	N/A	N/A	DHCP Pool	N/A
10.16.<siteID>.63-254	N/A	N/A	N/A	Reserved for future use
10.16.<siteID>.254	N/A	N/A	IETF-Defined Subnet Directed Broadcast	N/A

*Only in use for dedicated Master configured as Data Revert repeater without RF-related activities.

Table 103: Application Network Subnet IP Assignment in the CPMS IP Plan

Application Network VLAN=30				
1 ≤ siteID ≤ 15				
IP Address /27	**peerID**	**UDP Port**	**Function**	**Comments**
10.17.*<siteID>*.0	N/A	N/A	IETF-Defined Subnet Address	N/A
10.17.*<siteID>*.1	N/A	N/A	Router (Default Gateway)	N/A
10.17.*<siteID>*.2	N/A	N/A	Router-1 (VRRP)	Used when router redundancy is used
10.17.*<siteID>*.3	N/A	N/A	Router-2 (VRRP)	Used when router redundancy is used
10.17.*<siteID>*.4-7	N/A	N/A	N/A	Reserved for transport devices.
10.17.*<siteID>*.8	[siteID][18]	56000+ [peerID]	MNIS #1	May additionally host server applications and clients
10.17.*<siteID>*.9	[siteID][19]	56000+ [peerID]	MNIS #2	May additionally host server applications and clients
10.17.*<siteID>*.10	[siteID][20]	56000+ [peerID]	Dispatch Console Server #1	If not co-resident on MNIS
10.17.*<siteID>*.11	[siteID][21]	56000+ [peerID]	Dispatch Console Server #2	If not co-resident on MNIS
10.17.*<siteID>*.12	N/A	N/A	Dispatch Console Client #1	If not co-resident on MNIS
10.17.*<siteID>*.13	N/A	N/A	Dispatch Console Client #2	If not co-resident on MNIS
10.17.*<siteID>*.14	[siteID][24]	N/A	Radio Management Server	If not co-resident on MNIS
10.17.*<siteID>*.15	[siteID][25]	56000+ [peerID]	RDAC	N/A
10.17.*<siteID>*.16	[siteID][26]	56000+ [peerID]	Genesis	N/A
10.17.*<siteID>*.17	N/A	4012 (TCP 58041)	BFM	If not co-resident on MNIS TCP is for client-server communication
10.17.*<siteID>*.18	N/A	N/A	Edge Node	N/A
10.17.*<siteID>*.19-23	N/A	N/A	N/A	Reserved for other application hosts.
10.17.*<siteID>*.24-30	N/A	N/A	DHCP Pool	N/A

Application Network VLAN=30				
1 ≤ siteID ≤ 15				
IP Address /27	**peerID**	**UDP Port**	**Function**	**Comments**
10.17.*<siteID>*.31	N/A	N/A	IETF-Defined Subnet Directed Broadcast	N/A

The following examples show how the formulas should be used.

Example 1:

- Site ID = 2, RID=06
- Peer ID = 206
- UDP port = 56000 + 206 = 56206

Example 2:

- Site ID = 14, RID=09
- Peer ID = 1409
- UDP port = 56000+1409 = 57409

Example 3:

- Site ID = 11, two digits number = [18]
- Peer ID = 1118
- UDP port = 56000+1118 = 57118

Table 104: Example of a Radio Network IP Plan for the Site ID = 15 in the CPMS System

siteID = 15				
Radio Network				
IP Address /24	**peerID**	**UDP Port**	**Function**	**Comments**
10.16.15.0	N/A	N/A	IETF-Defined Subnet Address	N/A
10.16.15.1	N/A	N/A	Router (Default Gateway)	N/A
10.16.15.2	N/A	N/A	Router-1 (VRRP)	Used when router redundancy is used
10.16.15.3	N/A	N/A	Router-2 (VRRP)	Used when router redundancy is used
10.16.15.4	N/A	N/A	Ethernet Switch	N/A
10.16.15.5	N/A	N/A	Ethernet Switch (if present)	Used in sites with double switch configuration
10.16.15.6-7	N/A	N/A	N/A	Reserved for transport devices
10.16.15.8-14	N/A	N/A	N/A	Reserved for future use
10.16.15.15	1515	57515	RDAC	N/A

siteID = 15				
Radio Network				
IP Address /24	**peerID**	**UDP Port**	**Function**	**Comments**
10.16.15.16	1500	57500	Rest Channel	RID = 00 (Virtual IP Address)
10.16.15.17	1501	57501	Repeater #1	RID = 01
10.16.15.18	1502	57502	Repeater #2	RID = 02
10.16.15.19	1503	57503	Repeater #3	RID = 03
10.16.15.20	1504	57504	Repeater #4	RID = 04
10.16.15.21	1505	57505	Repeater #5	RID = 05
10.16.15.22	1506	57506	Repeater #6	RID = 06
10.16.15.23	1507	57507	Repeater #7	RID = 07
10.16.15.24	1508	57508	Repeater #8	RID = 08
10.16.15.25	1509	57509	Repeater #9	RID = 09
10.16.15.26	1510	57510	Repeater #10	RID = 10
10.16.15.27	511	57511	Repeater #11	RID = 11
10.16.15.28	1512	57512	Repeater #12	RID = 12
10.16.15.29	1513	57513	Repeater #13	RID = 13
10.16.15.30-31	N/A	N/A	N/A	Reserved for future use
10.16.15.32-62	N/A	N/A	DHCP Pool	N/A
10.16.15.63-254	N/A	N/A	N/A	Reserved for future use
10.16.15.254	N/A	N/A	IETF-Defined Subnet Directed Broadcast	N/A

Table 105: Example of an Application Network IP Plan for the Site ID = 15 in the CPMS System

Site ID = 15				
Application Network				
IP Address /27	**peerID**	**UDP Port**	**Function**	**Comments**
10.17.15.0	N/A	N/A	IETF-Defined Subnet Address	N/A
10.17.15.1	N/A	N/A	Router (Default Gateway)	N/A
10.17.15.2	N/A	N/A	Router-1 (VRRP)	Used when router redundancy is used
10.17.15.3	N/A	N/A	Router-2 (VRRP)	Used when router redundancy is used
10.17.15.4-7	N/A	N/A	N/A	Reserved for transport devices.

Site ID = 15				
Application Network				
IP Address /27	**peerID**	**UDP Port**	**Function**	**Comments**
10.17.15.8	1518	57518	MNIS #1	May additionally host server applications and clients
10.17.15.9	1519	57519	MNIS #2	May additionally host server applications and clients
10.17.15.10	1520	57520	Dispatch Console Server #1	If not co-resident on MNIS
10.17.15.11	1521	57521	Dispatch Console Server #2	If not co-resident on MNIS
10.17.15.12	N/A	N/A	Dispatch Console Client #1	If not co-resident on MNIS
10.17.15.13	N/A	N/A	Dispatch Console Client #2	If not co-resident on MNIS
10.17.15.14	1524	N/A	Radio Management Server	If not co-resident on MNIS
10.17.15.15	1525	57525	RDAC	N/A
10.17.15.16	1526	57526	Genesis	N/A
10.17.15.17	N/A	4012 (TCP 58041)	BFM	If not co-resident on MNIS, TCP is for client-server communication
10.17.15.18	N/A	N/A	Edge Node	N/A
10.17.15.19-23	N/A	N/A	N/A	Reserved for other application hosts
10.17.15.24-30	N/A	N/A	DHCP Pool	N/A
10.17.15.31	N/A	N/A	IETF-Defined Subnet Directed Broadcast	N/A

5.1.3
Network Topologies

With the introduction of the Juniper devices in the MOTOTRBO systems, the number of possible configuration templates increased. Those templates are divided into different scopes based on topology and used protocols.

- Single Site for Capacity Plus Single Site systems
- Multi-Site for Capacity Plus Multisite systems
  - No Tunnels
  - Static tunnels with Hub-to-Spoke
  - Dynamic tunnels with AVPN
  - NAT

5.1.3.1

Capacity Plus Single Site Topology

CPSS

Single Site configuration is recommended for non-distributed Capacity Plus Single Site (CPSS) systems. From a networking point of view, it can be isolated from any other system, and requires only one site router and one or more switches, depending on how many devices the system requires.

The CPSS can be equipped with Radio Infrastructure, Dispatch Console server, and optionally RDAC and MNIS Data Gateway.

5.1.3.2

Capacity Plus Multi Site Topologies

CPMS

Multi-Site topologies are for the Capacity Plus Multi Site (CPMS) systems. To achieve communication between sites, an IPv4 back-end network that transits all the traffic exchanged by the sites is required. Based on the type of the back-end network devices and requirements, different configurations can be used.

No Tunnels

A topology without tunnels means that all the CPMS system sites are connected to the customer transport network. Moreover, a dynamic routing protocol must be used between site routers and customer network routers. That means that all CPMS network routes are in the customer routers routing table.

For more information about this solution, see No Tunnels Topology Configuration Overview on page 626.

Static Tunnels with Hub-to-Spoke

The use of tunneling has many advantages, for example, an IP addressing scheme for a CPMS system that does not conflict with the customer's current IP plan is easy to implement. Tunnels between sites are set up statically by configuring each one in the SRX routers.

The Hub-to-Spoke concept assumes that the Hub has a VPN tunnel to each Spoke. It means that the traffic between the sites passes entirely through the Hub. The VPN tunnels can be configured by using GRE or IPsec protocol.

For GRE, all the routers' WAN IPv4 addresses must be static. However, when using IPsec for VPN tunnels, Spoke sites routers can have WAN IP addresses assigned dynamically.

For more information about this solution, see Hub-to-Spoke Topology Configuration Overview on page 629.

Dynamic Tunnels with AVPN

From a site-to-site communication point of view, AutoVPN (AVPN) behaves as the Hub-to-Spoke topology. It means that whole traffic is going through the Hub that serves as a single termination point for multiple tunnels to remote sites – Spokes. AVPN allows network administrators to configure a Hub for current and future Spokes. The advantage of the AVPN configuration over Hub-to-Spoke is no configuration changes are required on the Hub when Spoke devices are added or deleted, thus allowing administrators flexibility in managing large-scale network deployments. AVPN uses IPsec protocol to set up VPN tunnels. The Spoke sites routers can have WAN IPv4 addresses assigned dynamically or statically.

For more information about this solution, see Auto VPN Topology Configuration Overview on page 637.

NAT

NAT topology is the topology without tunnels where all sites of the Capacity Plus Multi Site system are usually connected to the WAN network. Each site router has enabled NAT options for incoming and outgoing traffic. Because of that, the network sockets for inter-site communication must be opened on each site router. The whole inter-site traffic is translated to the WAN IPv4 address of the site router and the specific UDP port number. Therefore, all Capacity Plus Multi Site system components must use the static IPv4 addresses. For more information about this solution, see NAT Topology Configuration Overview on page 643.

5.1.4

Types of Configuration Templates

Configuration templates can be divided into those intended for routers, and those intended for switches. Files with additional configuration fragments can enable the expansion of the basic versions. As a result, the total number of configuration files is reduced, while all the options are available for use.

5.1.4.1

Site Router Configurations

The most basic distinction for site routers configuration is based on the number of Ethernet switches in the site. There can be one or more switches on the site. The template configurations assume one or two switches, but adding additional switches does not change the site router configuration (for example, to have three site switches, the second switch must be connected to the first and third switch).

The second distinction for site routers configuration is based on the type of site. The site can play the role of a Hub or a Spoke. This division is true only for tunneling-based Multi Site systems. The following sites can become Spoke sites:

- RF site without a site switch
- RF site with one site switch
- RF site with double site switches

5.1.4.2

Site Switch Configurations

The site can consist of one or two site switches. As in the case of the site routers,several different configuration files are prepared, depending on the type of the site and the number of switches on the site.

For pure RF sites (no additional PC host) with a small number of repeaters, it is possible to deploy only SRX300/345 without a site switch. This configuration is called “Router as a switch”. In this case, Ethernet switching is enabled on the SRX, and all the unused interfaces are assigned to Radio Infrastructure Network VLAN.

By using built-in interfaces, the SRX300 router can connect up to five repeaters, and the SRX345 router can connect up to seven repeaters. When equipped with SFP modules, the SRX300 can have two additional interfaces, while the SRX345 can have eight additional interfaces.

NOTE: When you use “Router as a switch”, device restart is required after the first configuration commit. SRX communicates this after the commit is finished.

5.1.4.3

Add-On Configuration Files

Optional files with specific features or configuration options are available to make the template configurations more flexible and to reduce their number.

These files must be loaded to the device after choosing the basic configuration. For information on how to do this, see Loading the Configuration from a File to the Juniper SRX Router and EX Switch on page 655.

The following are the optional files:

- `SRX345_Addon` adds support for SRX345, as all the site router configuration templates are prepared for SRX300. After committing this file, you must restart the device.
- `*_SEC_Addon` adds security features to the site switch configuration. Those features include port security (limiting the number of MAC addresses that can be learned on a given port), which protects against connecting a different device to the port instead of a legitimate one. The file also adds DHCP snooping, which protects against connecting non-authorized DHCP servers to the ports on the site switch.

5.1.5
SRX Router Configuration Overview

Juniper SRX configuration consists of modules. Each of the modules contains configurations related to various functionalities:

- **system** – login and password configurations,host name, SSH server settings, NTP server settings, and syslog settings
- **security** – Address Book configuration, NAT, Policies, and Zones configurations
- **interfaces** – configurations of each interface
- **routing options** – Router-ID and static routes configuration
- **protocols** – OSPF, LLDP, and MSTP configurations
- **snmp** – SNMP configuration
- **policy-options** – configuration of prefix lists
- **firewall** – configuration of Access List for WAN Interfaces
- **access** – DHCP server settings for LAN networks
- **vlans** – configuration of VLANs

All configuration types for the Juniper devices are based on the configuration files saved in the STANZA format. However, small configuration changes are presented in the set format as in Procedures for Juniper Infrastructure on page 650. You can modify templates in application such as Notepad++. Each section provides embedded configuration fragments with marked items for modification.

5.1.5.1
Management Rules for the Juniper Devices

The management of the Juniper devices within the MOTOTRBO systems is designed based on the system's traffic matrix and it is different depending on what topology is used. For increased security, all Juniper devices in the MOTOTRBO systems allow only SSH connections. In addition, HTTPS access to switches is allowed.

Management rules:

- CPSS **Capacity Plus Single Site**
  - The SSH access to the WAN interface of the site router from the Public Network is allowed (host is defined by the `REMOTE_ACCESS_ADDR`)
  - The SSH connection to and from devices within the `RADIO_NETWORK` and `APPLICATION_NETWORK` is allowed

- The HTTPS (J-WEB) access from RADIO_NETWORK and APPLICATION_NETWORK to all switches is allowed

- CPMS **Capacity Plus Multi Site**
  - **No Tunnels, Hub-to-Spoke, AVPN Topologies**
    - The SSH connection from RADIO_NETWORK and APPLICATION_NETWORK to each network device is allowed
    - The HTTPS (J-WEB) access from RADIO_NETWORK and APPLICATION_NETWORK to all switches is allowed
  - **NAT Topology**
    - The SSH access to the WAN interface of the site router from the Public Network (host defined by the REMOTE_ACCESS_ADDR) is allowed
    - Within the site, the SSH connection from the RADIO_NETWORK and APPLICATION_NETWORK to each network device is allowed
    - Within the site, the HTTPS (J-WEB) access from RADIO_NETWORK and APPLICATION_NETWORK to all switches is allowed

IMPORTANT: SSH access to the SRX routers from RADIO_NETWORK and APPLICATION_NETWORK is allowed only to the SRX routers IP address of the loopback interface.

5.1.5.2

System Module (Router)

Each configuration template for SRX 300/345 routers has the same system modules. There are the following sub-modules:

Login and root-authentication

For security reasons, the configuration templates do not contain credential settings.

IMPORTANT: The **root user** is a built-in account and cannot be deleted. During the MSI configuration templates deployment, you must create the password for the root user. To set up credentials during configuration template deployment, see: Loading the Configuration from a File to the Juniper SRX Router and EX Switch on page 655 and Creating and Modifying Credentials on Juniper EX Switch and SRX Router on page 663.

```
login {
    class super-user-local {
        idle-timeout 10;
        login-alarms;
        permissions all;
    }
    password {
        minimum-length 15;
        change-type character-sets;
        minimum-changes 4;
        minimum-numerics 1;
        minimum-upper-cases 1;
        minimum-lower-cases 1;
        minimum-punctuations 1;
        format sha1;
    }
    message "\n\n\n\tWELCOME IN CAPPLUS SYSTEM\n\n\tUNAUTHORIZED USE OF THIS
```

```
SYSTEM\n\tIS STRICTLY PROHIBITED!\n\tALL LOGINS ARE MONITORED!!\n\n\n";
}
```

Services

Contains the SSH and DHCP server settings. See dhcp-local-server section to check which logical interfaces the DHCP server is running on.

```
services {
    ssh {
        root-login deny;
        no-tcp-forwarding;
        protocol-version v2;
        max-sessions-per-connection 1;
        ciphers [ aes256-ctr aes192-ctr aes128-ctr "aes128-gcm@openssh.com"
"aes256-gcm@openssh.com" ];
        macs [ hmac-sha2-512 hmac-sha2-256 "hmac-sha2-256-etm@openssh.com"
"hmac-sha2-512-etm@openssh.com" ];
        key-exchange [ dh-group14-sha1 group-exchange-sha2 ecdh-sha2-nistp256
ecdh-sha2-nistp384 ecdh-sha2-nistp521 ];
        client-alive-count-max 5;
        client-alive-interval 120;
        connection-limit 10;
        rate-limit 4;
    }
    dhcp-local-server {
        group LAN {
            interface ge-0/0/0.10;
            interface ge-0/0/0.30;
        }
        requested-ip-interface-match;
    }
}
```

Syslog

The default configuration of the event logging module.

System log files are stored locally on the router in the default `/var/log` directory. System log messages are configured to record all users' emergency events. Additionally, all Juniper events with notice severity and authentication or authorization attempts are saved in the messages file.

```
syslog {
    user * {
        any emergency;
    }
    file messages {
        any notice;
        authorization info;
    }
}
```

Processes

A module in which the services of non-used features are disabled.

```
processes {
    app-engine-management-service disable;
    advanced-anti-malware disable;
    application-identification disable;
```

```
    application-security disable;
    idp-policy disable;
    security-intelligence disable;
    utmd disable;
    pppoe disable;
    ppp disable;
    mpls-traceroute disable;
}
```

NTP

Settings for the NTP server and client. The IPv4 address of a loopback interface is the source address for the entire communication with an NTP server.

```
ntp {
    boot-server 101.5.11.10;
    server 101.5.11.10;
}
```

NOTE: Each SRX router in the Hub site is an NTP source for other system devices. To work as an NTP server, it must be synchronized with an external server. SRX router cannot be a standalone NTP server.

NOTE:

- Routers in Hub site:
  - are the NTP source (server) for all the other devices and subsystems in the CPSS and CPMS systems
  - synchronize from designated internal or external NTP server
- Routers in Spoke site – synchronize by using the loopback IPv4 address of the Hub (Hubs) router

Modification of a system module according to your needs

The following example contains embedded configuration fragments with items marked for modification. In this section, only the hostname and NTP settings should be adapted. The boot-server and server fields are set with the IP addresses of the NTP server and it depends on the customer configuration network.

```
system {
    host-name SRX-CPMS-SITE02R1;
    ...
    ntp {
        boot-server 101.5.11.10;
        server 101.5.11.10;
        source-address 10.30.16.2;
    }
}
```

5.1.5.3

Security Module

This module contains the security settings for network traffic. There are the following submodules:

Address Book

The Address book is a collection of addresses and address sets. It is a suite of aliases, referenced in other configuration modules, such as security policies, security zones, and NAT. You can add addresses to address books, or you can use the predefined addresses available in each address book by default.

In MOTOTRBO templates, the address book contains the minimal number of entries required for the configuration. Therefore, when you adapt the template configuration to your needs, applying changes in the address book significantly reduces the number of related changes in the entire configuration. Depending on the selected topology, configuration templates have different entries in the address book.

The address book contains two types of entries: with and without numbers in the name. Entries with a number are grouped as `address-set` and they are referenced only by using the `address-set <name>`. In the example below, a set named `APPLICATION_NETWORK` collects items `APPLICATION_NETWORK_1` `APPLICATION_NETWORK_2`. Entries without a number are always referenced directly – the `RADIO_NETWORK` is an example of such an item.

```
address-book {
    global {
        address RADIO_NETWORK 10.16.1.0/24;
        address APPLICATION_NETWORK_1 10.17.1.0/27;
        address APPLICATION_NETWORK_2 10.17.2.0/27;
        address APPLICATION_NETWORK_3 10.17.3.0/27;
        address APPLICATION_NETWORK_4 10.17.4.0/27;
        address PRIV_NET_CLASS_A 10.0.0.0/8;
        address PRIV_NET_CLASS_B 172.16.0.0/12;
        address PRIV_NET_CLASS_C 192.168.0.0/16;
        address-set APPLICATION_NETWORK {
            address APPLICATION_NETWORK_1;
            address APPLICATION_NETWORK_2;
            address APPLICATION_NETWORK_3;
            address APPLICATION_NETWORK_4;
        }
        address-set PRIV_NETWORK {
            address PRIV_NET_CLASS_A;
            address PRIV_NET_CLASS_B;
            address PRIV_NET_CLASS_C;
        }
    }
}
```

Tabela 106: Description of Address Book Entries

Entries Name	Description
`RADIO_NETWORK`	The Radio Network is mainly for subnets with repeaters. Besides the repeaters, it can contain RDAC applications, and technicians service laptop computers exclusively. In the CPSS IP plan, the subnet 10.16.0.0/16 is reserved for Radio Network.
`APPLICATION_NETWORK`	Application network hosts all Motorola and non-Motorola applications clients and servers cooperating with MOTOTRBO systems such as: MNIS, RDAC, RM, Dispatch Consoles (TRBOnet, Avtec, SmartPTT). Depending on site numbers, there can be a different number of Application Networks. Motorola configuration template example: • `APPLICATION_NETWORK_1 10.17.1.0/27` • `APPLICATION_NETWORK_2 10.17.2.0/27`
`PRIV_NETWORK`	This group collects all private addresses in all classes (RFC 1918): • `PRIV_NET_CLASS_A 10.0.0.0/8` • `PRIV_NET_CLASS_B 172.16.0.0/12`

Entries Name	Description
	• PRIV_NET_CLASS_C 192.168.0.0/16 It is used in policies from the TRUST zone to the UNTRUST zone to block all unnecessary traffic coming from the private subnets to outside of the MOTOTRBO system.

Adaptation of the Address Book to your needs

The following section provides embedded configuration fragments with marked items for modification.

```
address-book {
    global {
        address APPLICATION_NETWORK 10.17.1.0/27;
        address PRIV_NET_CLASS_A 10.0.0.0/8;
        address PRIV_NET_CLASS_B 172.16.0.0/12;
        address PRIV_NET_CLASS_C 192.168.0.0/16;
        address-set PRIV_NETWORK {
            address PRIV_NET_CLASS_A;
            address PRIV_NET_CLASS_B;
            address PRIV_NET_CLASS_C;
        }
    }
}
```

Screen

Screen option at the zone level provides detection and defense mechanisms. It is a mechanism that is used to stop more simplistic attacks, such as SYN and UDP flood. Although these types of attacks are simple in their nature, they can overrun a server or even a firewall. The Screen allows the administrator of an SRX Series product to set up specific thresholds for TCP and UDP sessions. When these thresholds are exceeded, protection mechanisms are enacted to minimize the threat of these attacks. All configurations have the same screen settings:

```
screen {
    ids-option UNTRUST-SCREEN {
        icmp {
            fragment;
            ping-death;
            icmpv6-malformed;
        }
        ip {
            spoofing;
            source-route-option;
            loose-source-route-option;
            strict-source-route-option;
            tear-drop;
            ipv6-malformed-header;
        }
        tcp {
            syn-fin;
            fin-no-ack;
            tcp-no-flag;
            port-scan;
            syn-flood {
                alarm-threshold 1024;
                attack-threshold 200;
                source-threshold 1024;
```

```
                destination-threshold 2048;
                timeout 20;
            }
            land;
        }
        udp {
            flood {
                threshold 200;
            }
            port-scan;
        }
    }
}
```

NAT

Network Address Translation (NAT) is a mechanism to translate the IP address of a computer or group of computers into a single public address when the packets are sent out to the Internet. By translating the IP address, only one IP address is published to the outside network. Since only one IP address is visible to the outside world, NAT provides additional security, and it can only have one public address for the entire network, instead of having multiple IP addresses.

In MOTOTRBO configuration templates, there are two types of NAT: static NAT and dynamic source NAT. Static NAT is dedicated to traffic from the Public network to the LAN network, while source NAT is for traffic initiated from the LAN network to the Public network. Network address translation mechanism is configured for each site except the site where there is no physical switch – the router performs switch functions. Only NAT topology configuration templates have both types of NAT while the rest have only the source NAT.

Source NAT is most commonly used for translating a private IPv4 address to a public IPv4 routable address. Source NAT changes the source address of the packets that pass through the router. The following translations are placed in Motorola configuration templates:

Tabela 107: Capacity Plus Dynamic Source NAT Rules

Name	Source Network	Translation (example)
OUTBAND_NAT	APPLICATION_NETWORK	10.17.1.0/27 -> WAN_ADDR (with port address translation)

Example of source NAT from the configuration templates:

```
nat {
    source {
        rule-set OUTBAND_NAT {
            description "Internet Access for Application Hosts";
            from zone TRUST;
            to zone UNTRUST;
            rule APP_NAT {
                match {
                    source-address-name APPLICATION_NETWORK;
                }
                then {
                    source-nat {
                        interface;
                    }
                }
            }
        }
    }
}
```

Policies

Junos OS allows configuring security policies. They enforce rules for transit traffic, in terms of what traffic can pass through the firewall, and what actions must be executed on the traffic as it passes through the firewall. A security policy is a set of statements that controls traffic from a specified source to a specified destination, by using a specified service. In MOTOTRBO configuration templates, whole policies are prepared in such a way that they do not require an adaptation to the customer's network. Example of `TRUST_POLICY` policy from configuration template:

```
from-zone TRUST to-zone TRUST {
    policy TRUST_POLICY {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
```

`TRUST_POLICY` applies only to the traffic between the networks belonging to the `TRUST` zone. In the configuration templates for the CPSS and CPMS systems, `TRUST` zone contains the `RADIO_NETWORK` and `APPLICATION_NETWORK`. In practice, this means that communication between these networks is not restricted.

All the security policies are based on the Traffic Matrix. The following table presents all allowed and not allowed actions between networks in the Capacity Plus Single Site and Multi Site systems.

Tabela 108: Traffic Matrix for Capacity Plus Single Site

Source	Destination	Action	Description
RADIO NETWORK	RADIO NETWORK	permit	
	APPLICATION NETWORK	permit	
	MANAGEMENT NETWORK*	permit	
	PUBLIC NETWORK	deny	
APPLICATION NETWORK	RADIO NETWORK	permit	
	APPLICATION NETWORK	permit	
	MANAGEMENT NETWORK*	permit	
	PUBLIC NETWORK	permit	Internet Access
REMOTE ACCESS HOST FROM PUBLIC NETWORK	RADIO NETWORK	deny	
	APPLICATION NETWORK	deny	
	MANAGEMENT NETWORK*	deny	
	SITE ROUTER WAN IF	selective	Enabled only: ICMP, SSH

*Management Network contains only the loopback interface with enabled ICMP, SSH, and NTP services.

Tabela 109: Traffic Matrix for Capacity Plus Multi Sites – Except NAT Topology

Source	Destination	Action	Description
RADIO NETWORK	RADIO NETWORK	permit	
	APPLICATION NETWORK	permit	
	MANAGEMENT NETWORK*	permit	
	PUBLIC NETWORK	deny	
APPLICATION NETWORK	RADIO NETWORK	permit	
	APPLICATION NETWORK	permit	
	MANAGEMENT NETWORK*	permit	
	PUBLIC NETWORK	permit	Internet Access**
PUBLIC NETWORK	RADIO NETWORK	deny	
	APPLICATION NETWORK	deny	
	MANAGEMENT NETWORK*	deny	
	SITE ROUTER WAN IF	selective	Enabled only: ICMP

*Management Network contains only the loopback interface with enabled ICMP, SSH, and NTP services.

**For No Tunnels Topology, Internet access is possible only for RM and Dispatch Console server addresses defined in the address book.

Tabela 110: Traffic Matrix for Capacity Plus Multi Sites – NAT Topology

Source	Destination	Action	Description
RADIO NETWORK	RADIO NETWORK	permit	
	APPLICATION NETWORK	permit	
	MANAGEMENT NETWORK*	permit	
	PUBLIC NETWORK	deny	
APPLICATION NETWORK	RADIO NETWORK	permit	
	APPLICATION NETWORK	permit	
	MANAGEMENT NETWORK*	permit	
	PUBLIC NETWORK	permit	Internet Access
REMOTE ACCESS HOST FROM PUBLIC NETWORK	RADIO NETWORK	deny	
	APPLICATION NETWORK	deny	
	MANAGEMENT NETWORK*	deny	
	SITE ROUTER WAN IF	selective	Enabled only: ICMP, SSH

Source	Destination	Action	Description
PUBLIC NETWORK	RADIO NETWORK	selective	Specific TCP and UDP ports opened with static NAT
	APPLICATION NETWORK	selective	
	MANAGEMENT NETWORK*	deny	

*Management Network contains only the loopback interface with enabled ICMP, SSH, and NTP services.

Zones

A security zone is a collection of one or more network segments requiring the regulation of inbound and outbound traffic through policies. Security zones are logical entities, to which one or more interfaces are bound. With many types of Juniper Networks devices, you can define multiple security zones, the exact number of which you determine based on your network needs.

In MOTOTRBO, configuration templates distinguish the following zones depending on the configuration types:

- `TRUST`
- `UNTRUST`
- `MGMT`
- `VPN_TUNNEL`

Zones `TRUST`, `UNTRUST`, and `MGMT` are used in all configuration templates. Zone `VPN_TUNNEL` is used only in Hub-to-Spoke and AVPN configuration templates.

Each zone is equipped with the host-inbound-traffic feature, which enables the protection of the device against attacks launched from systems that are directly or indirectly connected to any of its interfaces. It also enables you to selectively configure the device, so that the administrators can manage it by using certain applications on certain interfaces. You can prohibit the use of other applications on the same or different interfaces of a zone. For example, you can ensure that outsiders do not use the Telnet application from the Internet to log on to the device and connect to your system.

`TRUST` zone is designed for traffic involving devices on the following subnets: `RADIO_NETWORK`, `APPLICATION_NETWORK`. Within the zone DHCP, ping, traceroute, and SNMP services are enabled.

```
security-zone TRUST {
    host-inbound-traffic {
        system-services {
            dhcp;
            ping;
            traceroute;
            snmp;
        }
    }
    interfaces {
        ge-0/0/0.10;
        ge-0/0/0.30;
    }
}
```

`VPN_TUNNEL` zone collects all tunnel logical interfaces. It is used for inter-site traffic. Within the zone, ping, traceroute services, and OSPF routing protocols are enabled. Each tunnel interface must be attached to the `VPN_TUNNEL`.

```
security-zone VPN_TUNNEL {
    host-inbound-traffic {
        system-services {
            ping;
```

```
            traceroute;
        }
        protocols {
            ospf;
        }
    }
    interfaces {
        gr-0/0/0.2;
        gr-0/0/0.3;
        gr-0/0/0.4;
    }
}
```

UNTRUST zone is designed for communication with networks outside the Capacity Plus Single Site or Multi Site systems (Internet), and to establish intra-site communication.

```
security-zone UNTRUST {
    screen UNTRUST-SCREEN;
    host-inbound-traffic {
        system-services {
            ping;
        }
    }
    interfaces {
        ge-0/0/5.0;
    }
}
```

Zone MGMT is the management zone dedicated to the entire administration traffic. This zone is allowed to set up SSH connections to each SRX device. The SRX loopback interface IPv4 address is the NTP server address and belongs to this zone.

```
security-zone MGMT {
    host-inbound-traffic {
        system-services {
            ping;
            ssh;
            ntp;
        }
    }
    interfaces {
        lo0.0;
    }
}
```

5.1.5.4

Interfaces Module (Router)

Interfaces act as doorways, through which traffic enters and exits a device.

Juniper Networks devices support the following interface types:

- Network interfaces – they primarily provide traffic connectivity.
- Services interfaces – they manipulate traffic before it is delivered to its destination.
- Special interfaces – they include management interfaces, the loopback interface, and the discard interface.

In the following sections, only the interfaces used in Motorola configuration templates are presented.

5.1.5.4.1
Network Interfaces

All Juniper Networks devices use network interfaces to physically connect to other devices. A connection takes place along media-specific physical wires through an I/O card (IOC) in the SRX Series Services Gateway. Networking interfaces primarily provide traffic connectivity.

Configuring an interface can define both the physical properties of the link and the logical properties of a logical interface on the link.

In configuration templates, two network interfaces types were used.

Table 111: Examples of Network Interfaces

Interface Name	Description
`ge-0/0/0`	Gigabit Ethernet interface. Physical Interface used for connection to WAN and LAN Networks.
`reth0`	For chassis cluster configurations only, redundant Ethernet interface.
`fab0`	Cluster Fabric Interface is a physical connection between two nodes of a cluster, and it is formed by connecting a pair of Ethernet interfaces back-to-back.

5.1.5.4.2
Services Interfaces

Services interfaces provide specific capabilities for manipulating traffic before it reaches its destination.

To configure services on SRX devices, you configure one or more internal interfaces by specifying slot 0, interface carrier 0, and port 0, for example gr-0/0/0 for GRE.

In MOTOTRBO configuration templates, there are the following services interfaces:

Table 112: Examples of Services Interfaces

Interface Name	Description
`gr-0/0/0`	Configurable Generic Routing Encapsulation (GRE) interface. GRE allows the encapsulation of one routing protocol inside another routing protocol. Packets are routed to this internal interface, where they are first encapsulated with a GRE packet, and then sent. You can create multiple instances of this interface for forwarding encapsulated data to multiple destination addresses, by using the default interface as the parent and creating extensions, for example, `gr-0/0/0.3`, `gr-0/0/0.4`, and so on. The GRE interface is an internal interface only, and it is not associated with a physical interface. It is used only for processing GRE traffic.
`st0`	Secure tunnel interface used for IPSec VPNs. You can create multiple instances of this interface for forwarding encapsulated data by using the default interface as the parent and creating extensions, for example `st0.3`, `st0.4`, and so on.

5.1.5.4.3
Special Interfaces

Special interfaces include management interfaces (primarily intended for accessing the device remotely), the loopback interface (with several uses, depending on the particular Junos OS feature being configured), and the discard interface.

In MOTOTRBO configuration templates, there are the following special interfaces:

Table 113: Examples of Special Interfaces

Interface Name	Description
`lo0`	Loopback interface.

5.1.5.4.4
Logical Interfaces

The logical properties of an interface are the characteristics that do not apply to the physical interface or the wires connected to it.

The logical properties include:

- Protocol families running on the interface (including any protocol-specific MTUs).
- IP address or addresses associated with the interface. A logical interface can be configured with an IPv6 address, IPv4 address, or both. The IP specification requires a unique address on every interface of each system attached to an IP network so that the traffic can be correctly routed. Devices must have a unique IP address for every interface.
- Virtual LAN (VLAN) tagging.
- Any firewall filters or routing policies that are operating on the interface.
- Each logical interface has an additional logical unit identifier, preceded by a period (.)

Table 114: Logical Interfaces

Interface Name	Description
`ge-0/0/0.10`	Logical interface number 10 over physical`ge-0/0/0` interface.
`gr-0/0/0.2`	Logical interface number 2 over GRE `gr-0/0/0` interface.
`irb.30`	Logical interface number 30 over `irb` interface.

An example of an interface configuration:

```
ge-0/0/5 {
    description "WAN Interface";
    unit 0 {
        family inet {
            filter {
                input FILTER_WAN;
            }
            address 101.4.1.18/30;
        }
    }
}
```

The configuration is related to the WAN interface. Physical interface number 5 (`ge-0/0/5`) has logical interface number 0 (`unit 0`) configured with an IPv4 address assigned.

Table 115: Logical Interfaces in Motorola Configuration Templates

Single Switch	Double Switch	Description
`ge-0/0/0.10`	`irb.10`	Radio Network
`ge-0/0/0.30`	`irb.30`	Application Network
`lo0.0`	`lo0.0`	Management Network

NOTE: Integrated Routing and Bridging (IRB) interfaces are used to enable inter-VLAN routing. These logical interfaces work similarly to Layer 3 interfaces, and they should be added to security zones.

In Motorola configuration templates for SRX300/345 devices, the IRB interfaces are used when interface switching is enabled. This type of configuration is required in sites with double switch topology, or when there is no site switch and the SRX works as a site switch.

All interfaces require modifications. The following sections provide embedded configuration fragments with marked items for modification.

LAN Interfaces

Depending on the selected LAN IP network address:

```
ge-0/0/0 {
    description "LAN Interface";
    flexible-vlan-tagging;
    native-vlan-id 1;
    gratuitous-arp-reply;
    unit 10 {
        description "Radio Network";
        vlan-id 10;
        family inet {
            address 10.16.1.1/24;
        }
    }
    unit 30 {
        description "Application Network";
        vlan-id 30;
        family inet {
            address 10.17.1.1/27;
        }
    }
}
```

NOTE: For a double switch configuration, IP addresses must be assigned to `irb` interfaces instead of `ge-0/0/0`. For reference, see Table 115: Logical Interfaces in Motorola Configuration Templates on page 609.

WAN Interfaces

Depending on the underlay network configuration:

```
ge-0/0/5 {
    description "WAN Interface";
    unit 0 {
        family inet {
            filter {
                input FILTER_WAN;
```

```
            }
            address 101.4.1.18/30;
        }
    }
}
```

Loopback Interfaces

According to the IP Plan and depending on the SiteID:

```
lo0 {
    unit 0 {
        description "Management Interface";
        family inet {
            address 10.30.16.1/32;
        }
    }
}
```

5.1.5.5

SNMP Module (Router)

SNMP is used for exchanging management information between the network device and the Genesis GW3. This module is optional and should be used only when the customer is using the GW3 SNMP monitoring system.

NOTE: The SNMP Module is included in the Capacity Plus Single Site and the Capacity Plus Multi Site topologies except the NAT.

Radio and Application Networks are the basic subnets used by the site devices to communicate with the Genesis GW3. Motorola configuration templates include defined user, security mode, SNMP group name, and IPv4 addresses of the Genesis GW3 for trap sending.

Router and switch SNMP credentials must match to the Genesis GW3. The following are the default settings:

```
usm {
    local-engine {
        user MotoUser {
            authentication-none;
            privacy-none;
        }
    }
}
```

For information on adding new users and changing the security settings, see Modifying SNMP Configuration on Juniper EX Switch and SRX Router on page 664.

Adaptation of the SNMP module to your needs

SNMP requires the modification of the targets and the address for trap sending. The following section provides embedded configuration fragments with marked items for modification.

```
snmp {
...
        target-address SNMP_MGMT {
            address 10.17.1.16;
            target-parameters SNMP_V3_PARAMS;
        }
...
...
    trap-options {
```

```
        source-address 10.16.1.1;
    }
}
```

5.1.5.6
Routing-Options and Protocols Modules

This section is used for the static routes and the router-id.

The following section provides embedded configuration fragments with marked items for modification. In MOTOTRBO configuration templates, depending on the site number and WAN configuration, there are the following settings:

```
routing-options {
    static {
        route 0.0.0.0/0 next-hop 101.4.1.5;
    }
    router-id 10.30.16.1;
}
```

A static default route is set to the next-hop in WAN and it must be changed depending on the customer WAN settings.

Router-id value is used in OSPF protocol to identify the routing device from which a packet originated. Configuration templates are using the router loopback address as the router-id.

For information on how to change the WAN IP address and the static route, see: Changing the WAN IP Address (Juniper) on page 665.

Protocols modules are used for settings related to various protocols. In MOTOTRBO configuration templates, the main protocols are OSPF and LLDP.

The OSPF protocol is used as the main routing protocol ensuring communication between the sites. Adding an interface to the OSPF area 0.0.0.0 forces the OSPF process to advertise the IP network configured on this interface. LAN and Loopback interfaces (`lo0`; `ge-0/0/0`; `irb0`) are set as passive. It means that the IP network, including the IP address of the interface, is advertised by the OSPF protocol. On this interface, the OSPF adjacencies are not formed and the hello packets are not sent.

Metrics are calculated using the following formula: **cost = ref-bandwidth/bandwidth**. The default **ref-bandwidth** is **100 Mbps**. Bandwidth depends on the type of interface. For gigabit interfaces, it is 1000 Mbps, and the default OSPF cost is equal to 1.

See the following example of OSPF configuration with a specific metric:

```
protocols {
    ospf {
        area 0.0.0.0 {
            interface lo0.0 {
                passive;
            }
            interface gr-0/0/0.2{
                interface-type p2p;
            }
```

For more details on the OSPF protocol, see the descriptions of the specific configuration type.

The Link Layer Discovery Protocol (LLDP) is an industry-standard, vendor-neutral method to allow networked devices to advertise capabilities, identity, and other information onto a LAN.

In configuration templates dedicated for topology with double switch, the additional protocols and options are added: MSTP, switching mode.

```
l2-learning {
    global-mode switching;
}
mstp {
    configuration-name PCR-MSTP;
    revision-level 1;
    bridge-priority 4k;
    interface SWITCH-PORTS;
}
```

The switching mode option is used for enabling the switching functionalities on SRX Services Gateway.

NOTE: After a change to switching mode, a reboot of the SRX is required.

Multiple Spanning Tree Protocol (MSTP) is required for proper convergence in double switch topology, in which the SRX devices act as a root bridge.

5.1.5.7

Firewall Module

Firewall filters are essential for securing a network and simplifying network management. In Junos OS, it is possible to configure stateless firewall filters to control the incoming and the outgoing packets on the interface and to manipulate packets as necessary.

All MOTOTRBO configuration templates for SRX300/345 contain a firewall filter, except the No Tunnels topology. No Tunnels templates are dedicated to customers who want to deploy the Capacity Plus Multi Site system in their Enterprise Network.

Filter configurations differ, depending on the type of templates. For the CPSS and CPMS NAT templates, `FILTER_WAN` is expanded with the remote access functionality. It allows SSH access from authorized devices located outside of the LAN network to the WAN IPv4 address of the site router. In the policy-options section, the `REMOTE_ACCESS_ADDR` is the public address of the host.

A less secure solution is to access the router from any address in the public network. It is possible by modifying the IP address in the `REMOTE_ACCESS_ADDR prefix-list` to address `0.0.0.0/0`.

The IP address in the `REMOTE_ACCESS_ADDR prefix-list` should be changed according to your needs.

```
policy-options {
    prefix-list REMOTE_ACCESS_ADDR {
        101.3.1.126/32;
    }
}
```

The terms `WAN_ACCESS_TCP` provide access to the WAN interface of the site router.

```
term WAN_ACCESS_TCP {
    from {
        source-prefix-list {
            REMOTE_ACCESS_ADDR;
        }
        protocol [ tcp icmp ];
        destination-port ssh;
    }
```

```
    then accept;
}
```

NOTE: SSH Remote Access to the WAN interface of the router is enabled only in the CPSS and CPMS NAT topology configuration templates.

In addition, each Site (except the 'No Switch') has access to the Internet from the specific subnets (Application Network). The following terms in `FILTER_WAN` are introduced to allow the return traffic:

```
term RETURN_TRAFFIC_TCP {
    from {
        tcp-established;
    }
    then accept;
}
term UDP_FILTER {
    from {
        protocol udp;
    }
    then accept;
}
```

All configuration templates allow pinging the WAN interfaces from the WAN network.

```
term ICMP_FILTER {
    from {
        protocol icmp;
        icmp-type [ echo-request echo-reply unreachable time-exceeded ];
    }
    then accept;
}
```

5.1.5.8
Access Module

Access module provides configuration for DHCP servers for LAN networks.

Radio Network and Application Network have their own DHCP server setup on SRX devices. For details about the ranges of each DHCP server, see IP Plan for Capacity Plus Single Site and Capacity Plus Multisite Systems on page 583.

DHCP settings should be changed according to the selected LAN networks. The following section provides embedded configuration fragments of DHCP configuration for Radio Network with marked items for modification.

```
access {
    address-assignment {
        pool RADIO_POOL {
            family inet {
                network ;
                range RADIO_RANGE {
                    low 10.16.4.32;
                    high 10.16.4.62;
                }
                dhcp-attributes {
                    router {
                        10.16.4.1;
                    }
                }
            }
        }
        pool APP_POOL {
```

```
                family inet {
                    network 10.17.4.0/27;
                    range RADIO_RANGE {
                        low 10.17.4.24;
                        high 10.17.4.30;
                    }
                    dhcp-attributes {
                        router {
                            10.17.4.1;
                        }
                    }
                }
            }
        }
    }
```

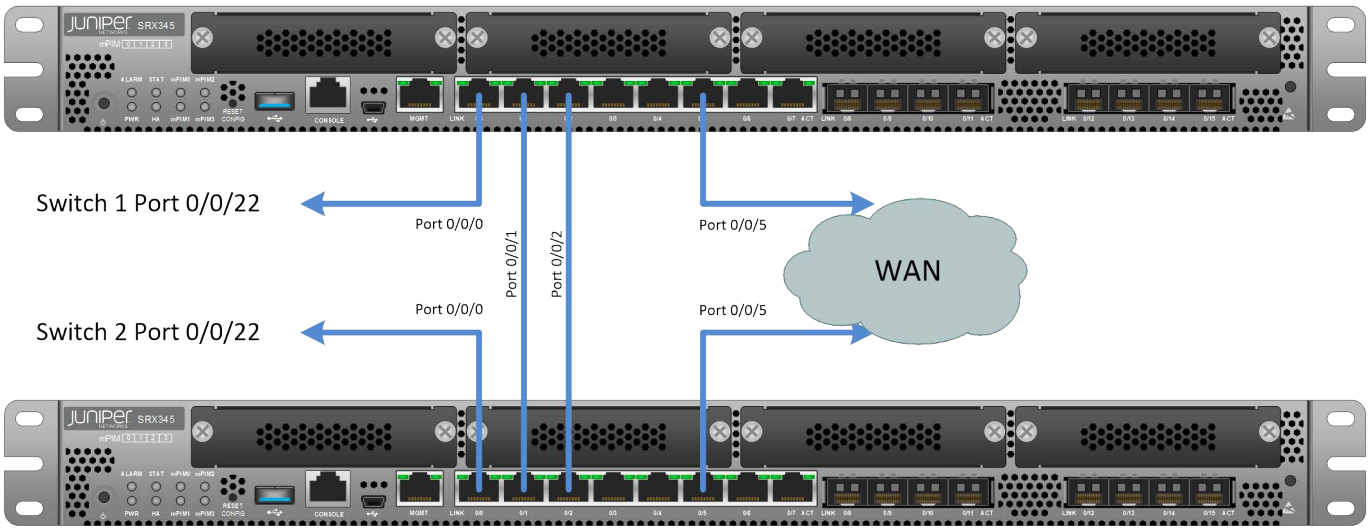
5.1.6

SRX Chassis Cluster Configuration Overview

The Junos OS provides high availability on SRX Series devices by using chassis clustering. SRX Series Services Gateways can be configured to operate in cluster mode, where a pair of devices can be connected and configured to operate as a single node, providing device, interface, and service level redundancy.

Motorola Solutions recommends chassis cluster configuration with at minimum SRX345 Services Gateway hardware.

Figure 228: Juniper SRX345 Chassis Cluster Connection Topology Diagram



All template configurations assume that the chassis cluster is built by using SRX345 devices and that there are two Ethernet switches in the site where the chassis cluster is deployed.

The chassis cluster is deployed in active/passive mode. One device in the cluster is used to route all the traffic, while the other is used only in the event of a failure. In the case of failure, the backup device becomes a master, and it controls all the forwarding. To enable the switchover, chassis cluster ports of the same purpose (LAN, WAN) must be connected to the switch. LAN ports are connected to the site Ethernet switches, but WAN ports are usually connected to the ISP device. If an ISP provides only one port for a customer router, another switch (with at least 3 ports) is required, to ensure that the ISP device is always connected to the SRX chassis cluster. The extra switch must be reliable and powerful enough to handle the site WAN traffic.

Apart from WAN and LAN, direct connections between devices in the chassis cluster are required. For a control link, interfaces `ge-0/0/1` must be connected. For a fabric link, interfaces `ge-0/0/2` must be connected. For reference, see Figure 228: Juniper SRX345 Chassis Cluster Connection Topology Diagram on page 614.

When you create a chassis cluster, the control ports on the respective nodes are connected to form a control plane that synchronizes the configuration and kernel state to facilitate the high availability of interfaces and services.

Similarly, the data plane on the respective nodes is connected over the fabric ports to form a unified data plane. The fabric link allows for the management of cross-node flow processing, and for the management of session redundancy.

NOTE: After the forming of a chassis cluster, Node 1 interface numbers change from `ge-0/x/x` to `ge-5/x/x`.

There are the following prerequisites to form a chassis cluster:

- Both devices must be SRX345.
- If some extension cards are installed in the Mini-PIM slots, both devices must have the same cards in the same slots.
- The software version must be the same on both devices.
- License keys must be the same on both devices.

When all the prerequisites are met and when the Ethernet cables for control and fabric link are connected, then you can continue with the initial configuration to form a chassis cluster. Follow the steps in Preparing SRX345 to Deploy Chassis Cluster on page 659.

After the initial configuration and the reboot of the devices, the chassis cluster is formed. From this point, it can be managed in the same way as a single device.

NOTE:
Chassis cluster Junos OS upgrade must be performed from the node that is Primary at the moment of the upgrade. Follow the steps in Upgrading Juniper OS on SRX Series Chassis Cluster on page 661.

Loading the chassis cluster configuration from a file or changing the current configuration should be performed from the Primary node. For each configuration commit, the configuration must be synchronized with the Secondary Node. Remember that, unlike in a single device, a chassis cluster configuration commit is possible only from the top of the CLI hierarchy. Exiting configuration mode without a commit command causes the loss of all the uncommitted changes.

5.1.7
EX Switch Configuration Overview

Juniper EX switch configuration consists of modules. Each of the modules contains configurations related to the following functionalities:

- **system** – this module contains login and password configurations, hostname, time zone, SSH, NTP and Web server settings, syslog parameters,
- **chassis** –this module contains redundancy configuration (for switch stacking, if exists),
- **interfaces** – this module contains configurations of each interface,
- **snmp** – this module contains SNMP configuration,
- **forwarding-options** – this module contains configuration of packets mirroring sessions, port storm-control parameters,
- **switch-options** – this module contains port security configuration,
- **routing-options** – this module contains static routes configuration,

- **protocols** – this module contains LLDP, IGMP, and MSTP configurations,
- **vlans** – this module contains VLANs configurations.

Management of EX switches is possible through:

- console,
- Out of Band (OOB) Ethernet Management interface me0 (disabled by default in templates),
- The IP address of the IRB interface.

To increase the security of the CPSS and CPM systems, IP access to switches is allowed only by using SSH and HTTPS connections. HTTPS access to Juniper devices is called the J-WEB access. J-WEB interface enables monitoring, configuring, troubleshooting, and managing the switching platform through the Web browser.

5.1.7.1

System Module (Switch)

Each configuration template for the EX2300 switch has the same system modules.

You can distinguish the following sub-modules:

Login and root-authentication

For security reasons, the configuration templates do not contain credential settings.

IMPORTANT: The root user is a built-in account and **cannot** be deleted. During MSI configuration templates deployment, you must create the password for the root user. To set up credentials during configuration template deployment, see Loading the Configuration from a File to the Juniper SRX Router and EX Switch on page 655 and Creating and Modifying Credentials on Juniper EX Switch and SRX Router on page 663.

```
login {
    class super-user-local {
        idle-timeout 10;
        login-alarms;
        permissions all;
    }
    password {
        minimum-length 15;
        change-type character-sets;
        minimum-changes 4;
        minimum-numerics 1;
        minimum-upper-cases 1;
        minimum-lower-cases 1;
        minimum-punctuations 1;
        format sha1;
    }
    message "\n\n\n\tWELCOME IN CAPPLUS SYSTEM\n\n\tUNAUTHORIZED USE OF THIS
SYSTEM\n\tIS STRICTLY PROHIBITED!\n\tALL LOGINS ARE MONITORED!!\n\n\n";
}
```

Services

This module contains the SSH and web server settings. In the web-management section for security reasons, only HTTPS protocol is enabled.

```
services {
    ssh {
        root-login deny;
        no-tcp-forwarding;
```

```
        protocol-version v2;
        max-sessions-per-connection 1;
        ciphers [ aes256-ctr aes192-ctr aes128-ctr "aes128-gcm@openssh.com"
"aes256-gcm@openssh.com" ];
        macs [ hmac-sha2-512 hmac-sha2-256 "hmac-sha2-256-etm@openssh.com"
"hmac-sha2-512-etm@openssh.com" ];
        key-exchange [ dh-group14-sha1 group-exchange-sha2 ecdh-sha2-nistp256
ecdh-sha2-nistp384 ecdh-sha2-nistp521 ];
        client-alive-count-max 5;
        client-alive-interval 120;
        connection-limit 10;
        rate-limit 4;
    }
    web-management {
        https {
            system-generated-certificate;
        }
        session {
            idle-timeout 15;
            session-limit 10;
        }
    }
}
```

Syslog

A default configuration of the event logging module.

System log files are stored locally on the switch in the default `/var/log` directory. System log messages are configured to record all emergency events of the users. All Juniper events with notice severity and authentication or authorization attempts are saved in the messages file. File `interactive-commands` contain all the commands that the user runs by using CLI and J-Web interface.

```
syslog {
    user * {
        any emergency;
    }
    file messages {
        any notice;
        authorization info;
    }
    file interactive-commands {
        interactive-commands any;
    }
}
```

NTP

Configuration of the NTP client.

For the NTP server IP addresses, the Hub routers loopback interface is always used.

```
ntp {
    boot-server 10.30.16.1;
    server 10.30.16.1;
}
```

NOTE: For No Tunnels and NAT Topologies, the IP address of the NTP server is set to the site router's loopback interface.

System

In the **system** section, only the hostname setting should be adapted.

```
system {
    ....
    host-name SRX-CPSS-SITE01SW1;
    ....
}
```

5.1.7.2

Interfaces Module (Switch)

Juniper Networks devices support a variety of interface types. For more information, see Interfaces Module (Router) on page 606.

You can configure the port on the switch as a single port or as an interface range. The interface range works as a template with a set of parameters, to which the ports are attached. When there are multiple ports with almost identical configurations, you can put them to interface range, and only parameters that are different are set under each port. This helps keep the configuration smaller and clearer. Moreover, the name of the interface range is used in other sections of the switch configuration instead of each range member.

In the following example only the description is configured on each port. All other configuration parameters are under `IF-APPLICATIONS` interface range.

```
interface-range IF-APPLICATIONS {
    member ge-0/0/12;
    member ge-0/0/13;
    member ge-0/0/14;
    member ge-0/0/15;
    member ge-0/0/16;
    description "Interfaces for Application Servers";
    unit 0 {
        family ethernet-switching {
            interface-mode access;
            vlan {
                members APP_VLAN;
            }
            storm-control default;
        }
    }
}
```

In the **interfaces** section, only the switch IPv4 interface setting should be adapted.

```
interfaces {
    ...
    irb {
        unit 10 {
            family inet {
                address 10.16.1.4/24;
            }
        }
    }
    ...
}
```

5.1.7.3
SNMP Module (Switch)

SNMP is used to send traps from the network device to the SNMP management application. In MOTOTRBO systems it is usually Genesis GW3.

For more information about SNMP, see SNMP Module (Router) on page 610.

There is one difference between the switch configuration and the router configuration. As the switch has only one IP interface, you do not need to configure a source interface for the SNMP packets.

5.1.7.4
Forwarding Options Module

In the forwarding options, the main feature used by the switch configuration is the analyzer. The analyzer creates a mirror session that copies the traffic from ports configured as the input, to the dedicated destination port configured as the output. This is for diagnostic purposes, in case the traffic analysis is required. In this section, a single port or the alias of interface range can be used.

```
forwarding-options {
    storm-control-profiles default {
        all;
    }
    analyzer {
        inactive: MIRROR-1 {
            input {
                ingress {
                    interface IF-APPLICATIONS;
                    interface IF-REPEATERS;
                    interface ge-0/0/20.0;
                }
                egress {
                    interface IF-APPLICATIONS;
                    interface IF-REPEATERS;
                    interface ge-0/0/20.0;
                }
            }
            output {
                interface ge-0/0/21.0;
            }
        }
    }
}
```

Storm control is a security feature that protects the interfaces against abnormal traffic that can be sent to disrupt normal communication, for example, DoS or DDoS attack.

NOTE: By default, port mirroring is disabled in all switch configuration templates. To enable this option, see Enabling the Port Mirroring on Juniper EX Switch on page 675.

5.1.7.5
Switch Options Module

The switch options exist in the switch configuration only when the port security is in use. When this optional configuration is applied to the switch configuration, then the amount of Ethernet MAC addresses that can be learned on each configured port is limited.

The purpose of that feature is to prevent connecting an unauthorized device to the port.

```
switch-options {
    interface IF-REPEATERS {
        interface-mac-limit {
            1;
            packet-action drop-and-log;
        }
    persistent-learning;
    }
    interface IF-APPLICATIONS {
        interface-mac-limit {
            12;
            packet-action drop-and-log;
        }
    persistent-learning;
    }
    ...
}
```

5.1.7.6
Routing Options Module

The Routing options module in switch configuration is used to set up a static route that creates a default gateway for the switch management traffic.

You must adjust the next-hop IPv4 address each time the template configuration is adapted.

```
routing-options {
    static {
        route 0.0.0.0/0 next-hop 10.16.1.1;
    }
}
```

5.1.7.7
Protocols Module

The protocols module groups the settings for the Multiple Spanning Tree Protocol (MSTP) and the Link Layer Discovery Protocol (LLDP).

MSTP is based on the standard Spanning Tree Protocol (STP). The protocol recognizes the concept of a single Root Bridge, which spans out to a single flood path, blocks the redundant paths to prevent data loops, and re-opens the blocked paths in the event of a primary link failure. In MSTP the convergence time is shorter than in STP and similar to the one in RSTP.

Instead of supporting a flat topology like STP and RSTP, MSTP introduces Regions, where for each Region there is a different set of VLANs. In the current configuration templates, only one Region with all VLANs is in use. In the site, the Root Bridge is determined by using the priority parameter. The SRX router has the highest priority.The first site switch has the second priority, and the second site switch has the third priority. A blocking condition on a port blocks all user traffic on that port. All ports are protected against Root Bridge preemption, except the ports for the router and another site switch.

```
protocols {
    lldp {
        interface all;
    }
    igmp-snooping {
        vlan default;
    }
```

```
    mstp {
        configuration-name PCR-MSTP;
        revision-level 1;
        bridge-priority 8k;
        interface ge-0/0/20 {
            no-root-port;
        }
        interface ge-0/0/22;
        interface ge-0/0/23;
        interface IF-APPLICATIONS {
            edge;
            no-root-port;
        }
        interface IF-REPEATERS {
            edge;
            no-root-port;
        }
    }
}
```

The LLDP is an industry-standard, vendor-neutral method to allow networked devices to advertise capabilities, identity, and other information onto a LAN.

5.1.7.8
VLANs Module

All the VLANs required by the system are configured in the VLANs module.

There is no need to modify this part of the configuration.

```
vlans {
    APP_VLAN {
        description "VLAN Application ";
        vlan-id 30;
    }
    MIRROR_VLAN {
        description "VLAN Mirrored Traffic";
        vlan-id 40;
    }
    RADIO_VLAN {
        description "VLAN Repeaters";
        vlan-id 10;
        l3-interface irb.10;
    }
    UNUSED_VLAN {
        description "VLAN Unused Ports";
        vlan-id 9;
    }
    default {
        description "Default VLAN";
        vlan-id 1;
    }
}
```

When the optional port security feature is loaded to the switch, some VLANs have the DHCP snooping option enabled. DHCP snooping protects against the non-authorized DHCP server connection to access the port on the switch. In the MOTOTRBO systems' configuration templates, only the router built-in DHCP server is allowed.

```
vlans {
    APP_VLAN {
```

```
        forwarding-options {
            dhcp-security;
        }
    }
    RADIO_VLAN {
        forwarding-options {
            dhcp-security;
        }
    }
}
```

5.1.7.9

Juniper EX2300 Switch Port Assignments

The interface ports of the site switch are numbered from 0. It is recommended to connect an interface to a repeater with the next consecutive number, for example: repeater 1 connected to the interface 0, repeater 2 to interfaces 1 etc.

A standardized 24-port Ethernet switch (Juniper EX2300) with either one or two switches deployed at a physical location.

Table 116: Standardized 24-Port Juniper EX2300 Ethernet Switch in CPSS and COMS systems

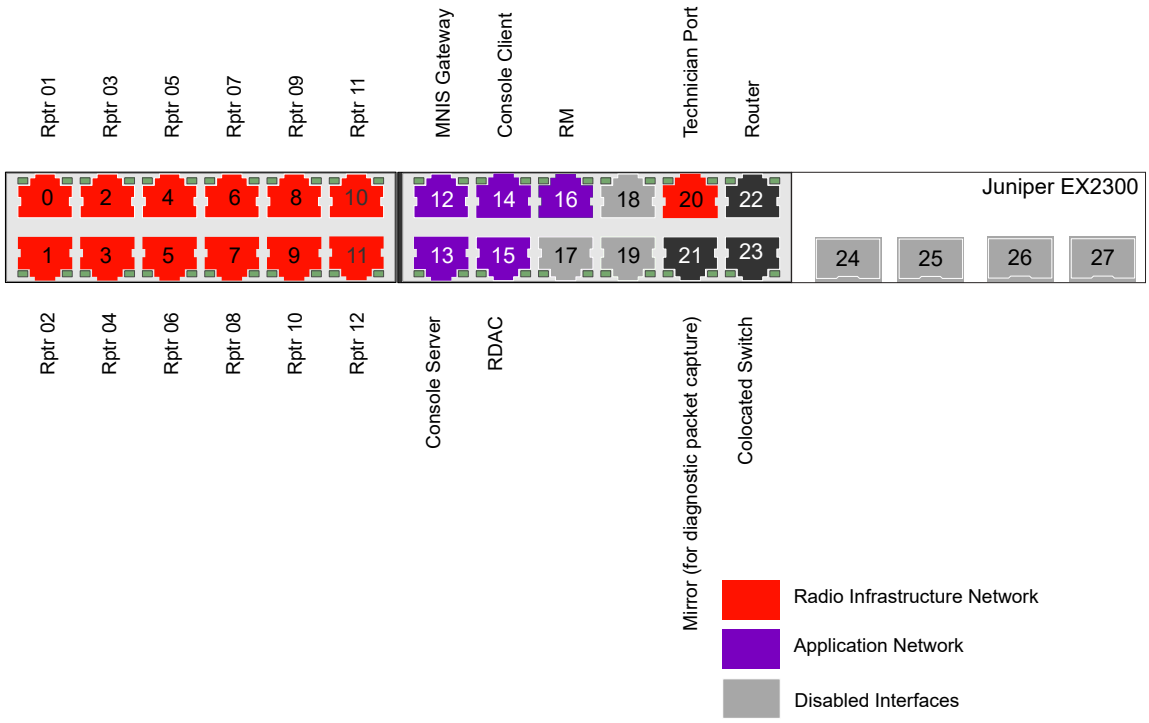
Port Number	Usage	Subnet Type
ge-0/0/0-11	Repeaters	Radio Network
ge-0/0/12	MNIS Data Gateway	Application Network
ge-0/0/13	Dispatch Console Server	Application Network
ge-0/0/14	Dispatch Console Client	Application Network
ge-0/0/15	RDAC	Application Network
ge-0/0/16	RM	Application Network
ge-0/0/17-19	Disabled	Disabled
ge-0/0/20	Technician Service Laptop	Radio Network
ge-0/0/21	Mirror (for diagnostic packet capture)	Mirror VLAN
ge-0/0/22	Router	Trunk
ge-0/0/23	Co-located Switch	Trunk

5.1.7.9.1

Site With a Single Switch

The following figure shows the organization of ports and VLANs of the switch.

Figure 229: Ports and VLANs Assignment on a Juniper EX 2300 Switch in Repeater Site with a Single Switch

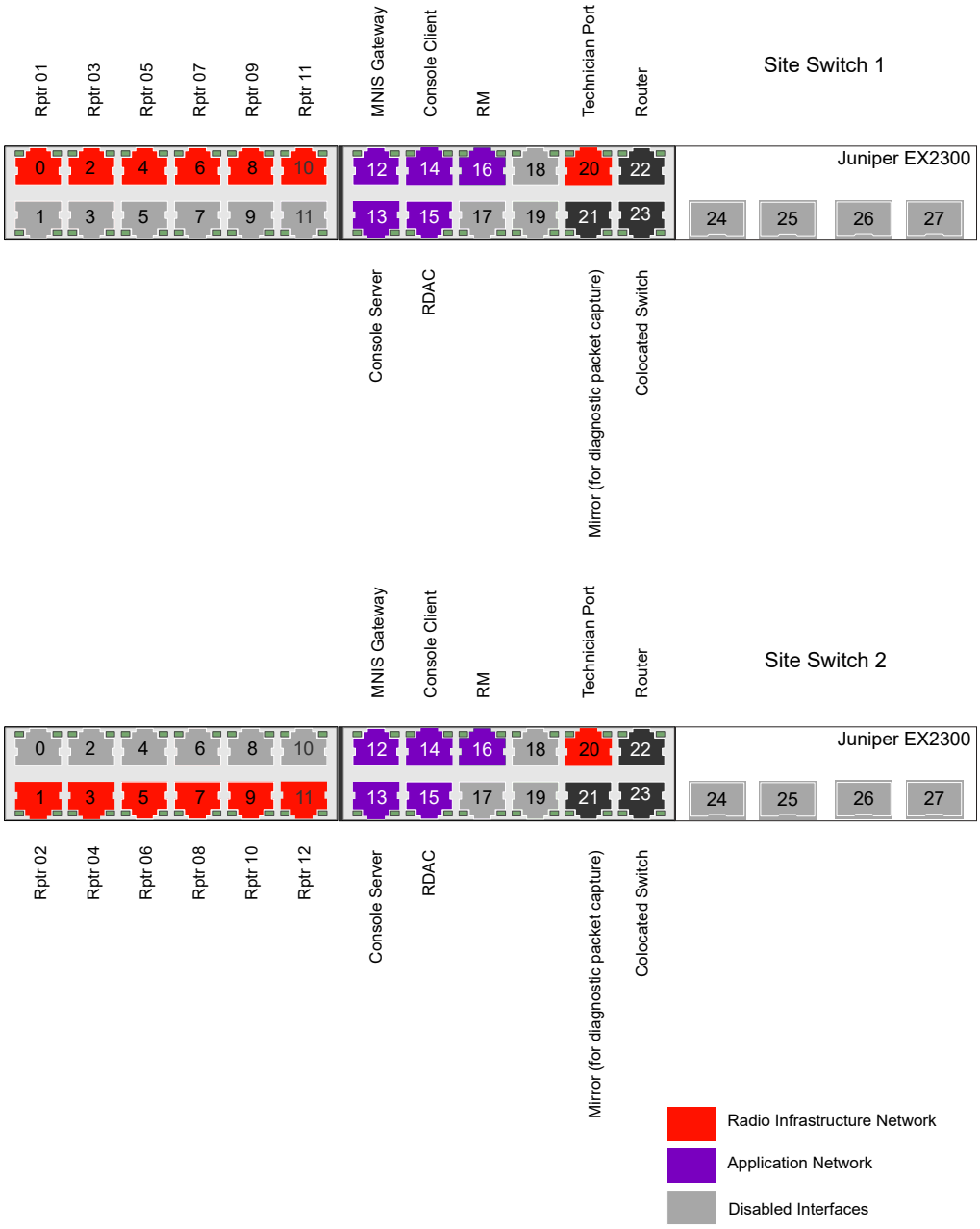


5.1.7.9.2

Site With a Double Switch

In sites with double switches, general guidance is to assign half of the repeaters to one switch and the remaining repeaters to the other switch. The following figure outlines a suggested strategy for assigning repeaters to Ethernet switches at a physical location.

Figure 230: Ports and VLANs Assignment on a Juniper EX 2300 Switch in Repeater Site with a Double Switch



5.1.8

Capacity Plus Single Site Topology Configuration Overview

CPSS

The following are the main assumptions for Capacity Plus Single Site topology templates:

- All entities are connected to one SRX router.
- All IPv4 addresses for transport devices are static (no DHCP IP address assignment for switch or router interfaces).
- All IPv4 addresses are from the Capacity Plus Single Site IP plan, except for routers' WAN interfaces.
- NAT translation is to support connections to access resources on the Internet only from the Application Network.

5.1.8.1

Capacity Plus Single Site Configuration Templates

Depending on the functionality, configuration templates can be divided into the following two types:

- Single Site with one switch
- Single Site with double switch

Depending on the chosen option, there is a single switch or a site switch redundancy. In double switch configuration templates, repeaters can be connected to different switches. In case of a switch failure, some of them remain operational.

The Capacity Site Single Site configuration templates are equipped with the dedicated Application Network to deploy all Motorola and non-Motorola applications clients and servers cooperating with Capacity Plus Single Site system such as: MNIS, RDAC, RM, Dispatch Consoles (TRBOnet, Avtec, SmartPTT).

NOTE: In case of deployment with remote RDAC and/or remote MNIS in the Capacity Plus Single Site system, the site router requires a specific NAT configuration. For details, go to the NAT section in Adaptation of Configuration Templates for NAT Topology on page 644.

Each configuration template is equipped with a WAN interface, which allows connections with external networks. Access to the external network is assured by a static default route. In the case of CPSS topology, the WAN interface is not required.

The CPSS system can be completely isolated, but it has the following consequences:

- NTP server should be located inside the CPSS system.
- Access to the Internet from the Application Network is not possible.

To increase the reliability of the site, you can use an SRX cluster instead of a single router configuration. SRX cluster consists of two identical devices connected to each other. They work and are managed as a single logical device. For more information about SRX cluster options, see SRX Chassis Cluster Configuration Overview on page 614.

5.1.8.2

Adaptation of the SRX Configuration Templates for Capacity Plus Single Site

The following section describes how to adjust the MOTOTRBO configuration templates to your needs. Templates can be modified for example by using Notepad++. Each section provides embedded configuration fragments with marked items for modification.

Almost all of the required changes for CPSS are described in the general section SRX Router Configuration Overview on page 596.

Customer changes require the following configuration parts:

- NTP – see System Module (Router) on page 597.
- Address-book – see Security Module on page 599.
- Interfaces – see Logical Interfaces on page 608.

- Access – see Access Module on page 613.

5.1.9
Capacity Plus Multi Site Configuration Topologies

CPMS

5.1.9.1
No Tunnels Topology Configuration Overview

The MOTOTRBO configuration templates are divided into several types, depending on the network topology. One option is to use dedicated private IP connections as the core network. It can be a private enterprise network, fiber optic, or microwave. It can be a leased or private MPLS network. The main benefit of using such networks is that there is no need to tunnel the Capacity Plus Multi Site inter-site traffic. This option is called the "No Tunnels" topology, and it is based on the OSPF protocol. The following assumptions are fundamental for the configuration templates:

- All IPv4 addresses for the transport devices are static (no DHCP IPv4 address assignment for switch or router interfaces).
- All IPv4 addresses are from the Capacity Plus Multi Site IP plan, except for routers WAN interfaces.
- There is no NAT translation. The traffic forwarded to the Internet must be translated by the customer edge router or firewall.
- None of the site routers have a direct connection to the Internet.
- OSPF routing protocol is used for intersite communication and for connecting with the customer core network.

5.1.9.1.1
No Tunnels Configuration Templates

Configuration templates for the router are created for three sites that use a different number of site switches:

- RF site with co-located Application Network with double site switch (Site01)
- RF site with co-located Application Network with a single site switch (Site02)
- RF site with no physical switch (Site03)

For more information on the assignment of the repeaters to switch ports, see Juniper EX2300 Switch Port Assignments on page 622.

To increase the reliability of the RF site, there is an option to use an SRX cluster instead of a single router configuration. SRX cluster consists of two identical devices connected together, which work and are managed as a single logical device.

For more information on SRX cluster options, see SRX Chassis Cluster Configuration Overview on page 614.

5.1.9.1.2
Adaptation of Configurations Templates for No Tunnels Topology

Site routers configuration templates for No Tunnels topology are similar to other Multi-Site configurations.

For more details on the required adaptations, see SRX Router Configuration Overview on page 596.

The following configuration sections require adjustment:

- Hostname and NTP – see System Module (Router) on page 597.

- Interfaces – see Logical Interfaces on page 608.
- SNMP – see SNMP Module (Router) on page 610.
- Routing-options – see Routing-Options and Protocols Modules on page 611.
- Access – see Access Module on page 613.

The configuration templates for No Tunnels topology are mostly similar to configurations for other topologies, with a number of important differences.

- The address-book in the security section contains multiple aliases of IP addresses or subnets used by the next sections of configuration. That allows changing them in one place, rather than looking for required changes in the entire configuration file.

```
address-book {
    global {
        address RADIO_NETWORK_1 10.16.1.0/24;
        address RADIO_NETWORK_2 10.16.2.0/24;
        address RADIO_NETWORK_3 10.16.3.0/24;
        address APPLICATION_NETWORK_1 10.17.1.0/27;
        address APPLICATION_NETWORK_2 10.17.2.0/27;
        address LOOPBACK_MGMT_NETWORK 10.30.16.0/24;
        address RM_SRV_ADDR 10.17.2.14/32;
        address CONSOLE_SRV_ADDR 10.17.2.10/32;
        address-set RADIO_NETWORK {
            address RADIO_NETWORK_1;
            address RADIO_NETWORK_2;
            address RADIO_NETWORK_3;
        }
        address-set APPLICATION_NETWORK {
            address APPLICATION_NETWORK_1;
            address APPLICATION_NETWORK_2;
        }
        address-set INTERNET_ACCESS {
            address RM_SRV_ADDR;
            address CONSOLE_SRV_ADDR;
        }
    }
}
```

Most entries in the address-book are the same as in the NAT topology templates and can be found in Adaptation of Configuration Templates for NAT Topology on page 644. The following entries are specific to the No Tunnels Topology.

Table 117: Description of Address Book Entries in the No Tunnels Topology

Entries Name	Description
RADIO_NETWORK	The Radio Network exists in all sites of the CPMS system and is mainly for subnets with repeaters. Besides the repeaters, it can contain RDAC applications, and technicians service laptop computers exclusively. In the CPMS IP plan, the subnet 10.16.0.0/16 is reserved for Radio Network.
APPLICATION_NETWORK	Application Network hosts all Motorola and non-Motorola applications clients and servers cooperating with MOTOTRBO systems such as: MNIS, RDAC, RM, Dispatch Consoles (TRBOnet, Avtec, SmartPTT). Depending on site numbers, there can be a different number of Application Networks. Motorola configuration template example:

Entries Name	Description
	○ APPLICATION_NETWORK_1 10.17.1.0/27 ○ APPLICATION_NETWORK_2 10.17.2.0/27
LOOPBACK_MGMT_NETWORK	Management Network where the default value in all configurations is set to: 10.30.16.0/24
RM_SRV_ADDR	This entry reflects the unique address with a 32-bit mask, which is set on the host where the RM application is installed. RM can be deployed only in the Application Network. According to the IP plan for the CPMS system, the IPv4 address for RM depends on the Site ID: ○ RM_SRV_ADDR 10.17.1.14/32
CONSOLE_SRV_ADDR	This entry reflects the unique address with a 32-bit mask, which is set on the host where the Dispatch Console server is installed. It can be deployed only in the Application Network. According to the IP plan for the CPMS system, the IPv4 address for the Dispatch Console server depends on the Site ID: ○ CONSOLE_SRV_ADDR 10.17.1.10/32
INTERNET_ACCESS	It is a set of aliases that require access to the Internet. By default INTERNET_ACCESS set contains the aliases: ○ address RM_SRV_ADDR ○ address CONSOLE_SRV_ADDR

As No Tunnels topology is most often used with customized Capacity Plus Multi Site IP plan, the Infrastructure Networks (RADIO_NETWORK, APPLICATION_NETWORK) can use subnets with IPv4 masks /24, /25, /26, or /27. Not all subnets created by dividing /24 subnets may belong to the Infrastructure Networks, so each used subnet must be explicitly listed in the address-book. This list forms an address-set, named RADIO_NETWORK or APPLICATION_NETWORK and containing all address entries of an Infrastructure Network subnet for each site.

The following is an example of a configuration template with this kind of configuration.

```
address-book {
    global {
        address RADIO_NETWORK_1 10.16.1.0/24;
        address RADIO_NETWORK_2 10.16.2.0/25;
        address RADIO_NETWORK_3 10.16.3.0/26;
        address APPLICATION_NETWORK_1 10.17.1.0/24;
        address APPLICATION_NETWORK_2 10.17.2.0/27;
        address-set RADIO_NETWORK {
            address RADIO_NETWORK_1;
            address RADIO_NETWORK_2;
            address RADIO_NETWORK_3;
        }
        address-set APPLICATION_NETWORK {
            address APPLICATION_NETWORK_1;
            address APPLICATION_NETWORK_2;
        }
    }
}
```

- There is no direct site-to-site connection from the OSPF protocol perspective. Each site router sets adjacency with the transit network router, and it is the source of routing updates. Because of that, the

WAN interface is attached to the OSPF area 0.0.0.0, and the security zone `UNTRUST` has OSPF protocol enabled. Adaptation, while not required, is necessary from the maintenance perspective. You can decide on how to adjust the OSPF configuration if you need the multi-area configuration, or if you use another protocol.
Site switches configuration templates do not require extensive changes. For details on required adaptation, see EX Switch Configuration Overview on page 615.

The following configuration sections require adjustment:

- Hostname – see SRX Router Configuration Overview on page 596.
- Interfaces – see Interfaces Module (Switch) on page 618.
- Routing-options – see Routing Options Module on page 620.

5.1.9.2
Hub-to-Spoke Topology Configuration Overview

CPMS

The Hub-to-Spoke configuration is created for small and medium Capacity Plus Multi Site systems. The Hub site is the central network element of the CPMS system, and every Spoke communicates with it. To connect physical locations, static VPN tunnels are configured in the overlay network between every Spoke and Hub router.

The following are the main assumptions for Hub-to-Spoke topology templates:

- All IPv4 addresses for transport devices are static (there is no DHCP IPv4 address assignment for switch or router interfaces), except for Spokes WAN interfaces.
- Hub router WAN interface IPv4 address must be statically assigned.
- All IP addresses are from the Capacity Plus Multi Site IP plan, except for routers WAN interfaces.
- NAT translation supports connections to access resources on the Internet only from the Application Network.
- OSPF routing protocol is used for inter-site communication.

5.1.9.2.1
Hub-to-Spoke Configuration Templates

The Hub configuration templates for the routers and switches have been categorized as follows:

- Double Switch
  - Router – contains configuration templates for GRE, IPsec,
  - SRX Cluster – contains configuration templates for GRE, IPsec,
  - Switch – contains configuration templates with a double switch in Hub with an optional security add-on.
- Single Switch
  - Router – contains configuration templates for GRE, IPsec,
  - Switch – contains configuration templates with a single switch in Hub with an optional security add-on.

NOTE: Configuration templates for SRX Cluster exist only with Double Switch topology.

The Spoke configuration templates for the routers and switches have been categorized as follows:

- Router – contains configuration templates for GRE, IPsec with static, and IPsec with dynamic WAN IPv4 on Spokes.
- Switch – contains configuration templates with a single or a double switch in Spoke with optional security add-on

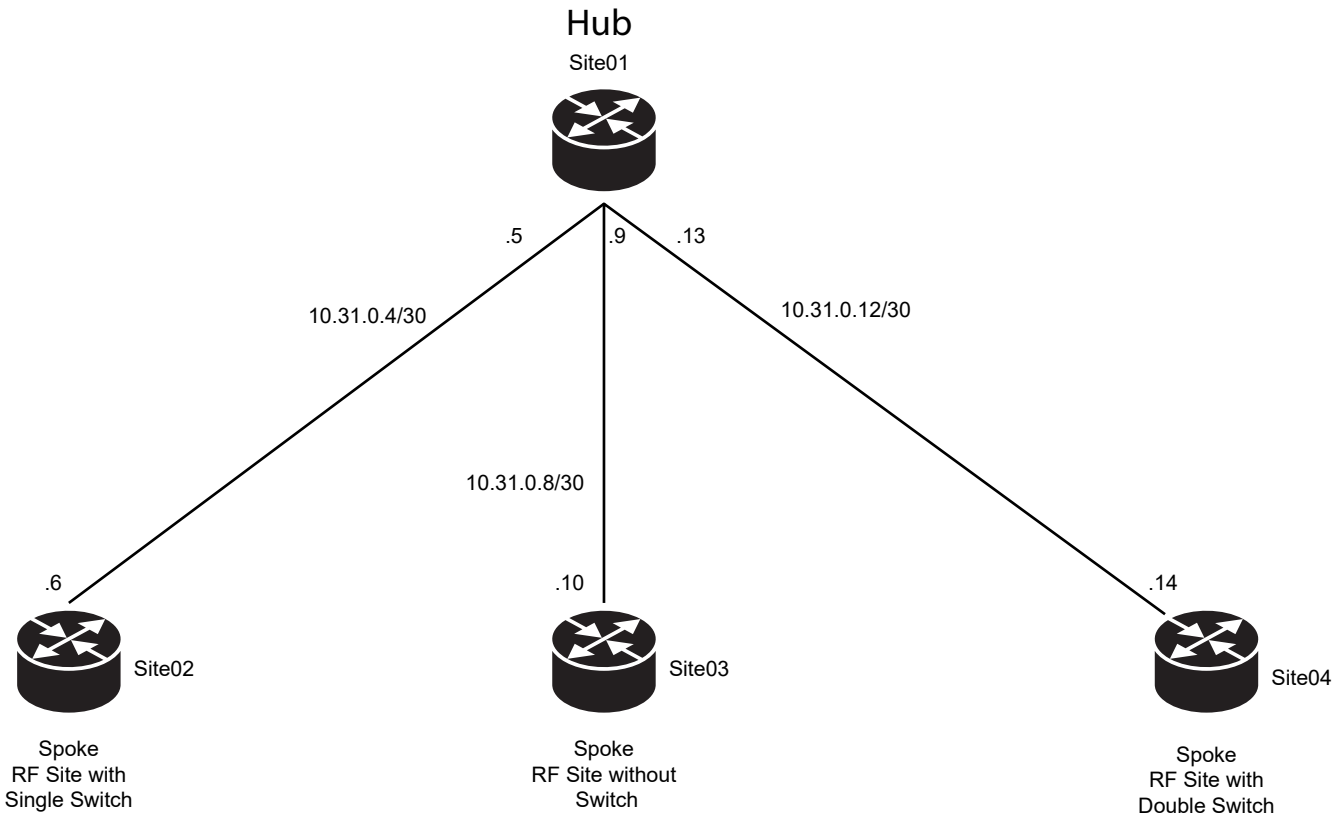
Configuration templates for the Spoke are created for three Spoke sites that use a different site topology:

- RF Site with a single switch (Site02)
- RF Site without a site switch (Site03)
- RF Site with a double switch (Site04)

There is a security add-on for increasing security for each Spoke site switch configuration. This file can be merged into the standard configuration template. For more details, see Add-On Configuration Files on page 595.

The Spokes and the Hub are connected with VPN tunnels. It means that the traffic between sites passes entirely through the Hub. All VPN tunnels are point-to-point. It means that according to the IP plan, the subnets dedicated to the VPN tunnels must have the /30 prefix.

Figure 231: Hub-to-Spoke VPN Overlay Tunnel Network



Hub-to-Spoke configuration templates use the OSPF routing protocols. For the GRE protocol, the interfaces used to create OSPF adjacencies are gr-0/0/0. The GRE tunnel interfaces do not have a built-in mechanism for detecting when a tunnel is down; for this reason each configuration template has enabled keepalive messages to serve as the detection mechanism.

An example of the configuration of the OSPF with GRE protocol:

```
protocols {
    oam {
        gre-tunnel {
            interface gr-0/0/0 {
```

```
                keepalive-time 10;
                hold-time 30;
            }
        }
    }
    ospf {
        area 0.0.0.0 {
            interface lo0.0 {
                passive;
            }
            interface gr-0/0/0.2{
                interface-type p2p;
            }
            interface gr-0/0/0.3 {
                interface-type p2p;
            }
            interface gr-0/0/0.4 {
                interface-type p2p;
            }
            interface ge-0/0/0.10 {
                passive;
            }
            interface ge-0/0/0.30 {
                passive;
            }
        }
        graceful-restart {
            restart-duration 300;
            notify-duration 300;
            no-strict-lsa-checking;
        }
    }
    lldp {
        interface ge-0/0/0;
    }
}
```

For the IPsec protocol, the interfaces used to create OSPF adjacencies are `st0`.

An example of the configuration of OSPF with the IPsec protocol:

```
protocols {
    ospf {
        area 0.0.0.0 {
            interface lo0.0 {
                passive;
            }
            interface st0.2 {
                interface-type p2p;
            }
            interface st0.3 {
                interface-type p2p;
            }
            interface st0.4 {
                interface-type p2p;
            }
            interface ge-0/0/0.10 {
                passive;
            }
            interface ge-0/0/0.30 {
                passive;
            }
        }
```

```
        graceful-restart {
            restart-duration 300;
            notify-duration 300;
            no-strict-lsa-checking;
        }
    }
    lldp {
        interface ge-0/0/0;
    }
}
```

In the GRE and IPsec cases, all OSPF interfaces forming adjacency are set as point-to-point, and they provide a connection between a single source and a single destination (there is only one OSPF adjacency).

In Hub-to-Spoke configuration templates, the OSPF uses the default metrics (the cost is equal to 1).

5.1.9.2.2

Naming Convention in Hub-to-Spoke Topology

Consistency and transparency of network configurations are particularly important during troubleshooting or maintenance sessions. Therefore, MOTOTRBO configuration templates contain unique profile names and interface numbers, making the configuration more transparent and understandable.

IKE Gateways

For IKE gateway profiles, Motorola Solutions recommends the following naming formula: `IKE-GW-<srxROLE>-<SiteID>`

where:

<srxROLE> – can be HUB or SPOKE

```
gateway IKE-GW-SPOKE-2 {
    ike-policy IKE-POL;
    dynamic hostname SRX-CPMS-SITE02R1;
    dead-peer-detection {
        optimized;
        threshold 3;
    }
    external-interface ge-0/0/5.0;
}
gateway IKE-GW-SPOKE-3 {
    ike-policy IKE-POL;
    dynamic hostname SRX-CPMS-SITE03R1;
    dead-peer-detection {
        optimized;
        threshold 3;
    }
    external-interface ge-0/0/5.0;
}
```

`IKE-GW-SPOKE-2` means the IKE profile is used to create the IPsec tunnel towards the Spoke site with SiteID=2

VPN Profiles

Each VPN IPsec tunnel requires an IKE gateway profile and a VPN profile. The IKE gateway configuration is described in the previous section. The naming convention for VPN profiles is similar, it is described by the formula: `IPSEC-VPN-<srxROLE>-<SiteID>`.

NOTE: There is a specific interface (st0.x) and a specific IKE gateway profile bound to each VPN profile.

```
vpn IPSEC-VPN-SPOKE-2 {
    bind-interface st0.2;
    vpn-monitor {
        optimized;
    }
    ike {
        gateway IKE-GW-SPOKE-2;
        idle-time 120;
        ipsec-policy IPSEC-POL;
    }
}
vpn IPSEC-VPN-SPOKE-3 {
    bind-interface st0.3;
    vpn-monitor {
        optimized;
    }
    ike {
        gateway IKE-GW-SPOKE-3;
        idle-time 120;
        ipsec-policy IPSEC-POL;
    }
}
```

`IPSEC-VPN-SPOKE-2` means the VPN profile is used to create the IPsec tunnel towards the Spoke site with SiteID=2

Interfaces

The interface naming convention is used for service interfaces: `gr-0/0/0` and `st0`. The formula is: `unit <SiteID>`

where:

<SiteID> is the value of the SiteID of the opposite endpoint.

Configuration with GRE tunneling:

```
gr-0/0/0 {
    description "Tunnel Interfaces";
    unit 2 {
        tunnel {
            source 101.4.1.6;
            destination 101.4.1.10;
        }
        family inet {
            address 10.31.0.5/30;
        }
    }
    unit 3 {
        tunnel {
            source 101.4.1.6;
            destination 101.4.1.14;
        }
        family inet {
```

```
            address 10.31.0.9/30;
        }
    }
```

According to the formula, `gr-0/0/0 unit 2` is used for the creation of VPN GRE tunnel towards Spoke site with SiteID=2.

Configuration with IPsec tunneling:

```
st0 {
    description "Tunnel Interfaces";
    unit 2 {
        family inet {
            address 10.31.0.5/30;
        }
    }
    unit 3 {
        family inet {
            address 10.31.0.9/30;
        }
    }
```

According to the formula, interface `st0 unit 2` is used for the creation of a VPN IPsec tunnel towards the Spoke site with SiteID=2.

5.1.9.2.3
Adaptation of Configuration Templates for Hub-to-Spoke Topology

The following section provides information on adjusting the MOTOTRBO configuration templates to your needs.

Each section provides embedded configuration fragments, with marked items for modification.

Site routers configuration templates for Hub-to-Spoke topology are similar to the other multi-site configurations. For most of the required adaptations, see SRX Router Configuration Overview on page 596.

The following configuration sections must be adjusted:

- Hostname and NTP – see System Module (Router) on page 597
- Address-book - see Security Module on page 599
- Interfaces - see Logical Interfaces on page 608
- SNMP - see SNMP Module (Router) on page 610
- Routing-options and Protocols - see Routing-Options and Protocols Modules on page 611
- Policy-options - see Firewall Module on page 612
- Access - see Access Module on page 613

Although configuration templates for Hub-to-Spoke topology are very similar to configurations for other topologies, there are some important differences.

Security Module

Motorola configuration templates with IPsec VPN tunneling require an adoption of the additional security section. Remember to reflect the same changes in the Hub and in the Spoke router configurations.

IKE Policy (WAN IP static assignment)

You should modify the pre-shared key in the IKE policy.

```
policy IKE-POL {
    mode aggressive;
    proposals IKE-PROP;
    pre-shared-key ascii-text "$9$HqfzIRSKWxIEds4Zkq/Ctu0I"; ## SECRET-DATA
}
```

The pre-shared key in the template is encrypted. It must be replaced after the configuration load by using the following command from the configuration mode:

`set security ike policy IKE-POL pre-shared-key ascii-text` ***<key>***

where ***<key>*** is the new pre-shared key in clear text format.

IKE Gateway (WAN IP assignment)

The hostname field in the IKE gateway profile for Hub router must match with remote peer hostname. In the Spoke configuration, the hostname parameter must be set as “local-identity”.

Example of the IKE gateway configuration for Hub router that must be adapted:

```
gateway IKE-GW-SPOKE-2 {
    ike-policy IKE-POL;
    dynamic hostname SRX-CPMS-SITE02R1;
    dead-peer-detection {
        optimized;
        threshold 3;
    }
    external-interface ge-0/0/5.0;
}
gateway IKE-GW-SPOKE-3 {
    ike-policy IKE-POL;
    dynamic hostname SRX-CPMS-SITE03R1;
    dead-peer-detection {
        optimized;
        threshold 3;
    }
    external-interface ge-0/0/5.0;
}
```

Example of the IKE gateway configuration for Spoke router that must be adapted:

```
gateway IKE-GW-HUB {
    ike-policy IKE-POL;
    address 101.4.1.6;
    dead-peer-detection {
        optimized;
        threshold 3;
    }
    local-identity hostname SRX-CPMS-SITE02R1;
    external-interface ge-0/0/5.0;
}
```

NOTE: In Spoke IKE gateway configuration remember to modify the address for the `IKE-GW-HUB`. This address depends on the customer’s WAN settings.

IPsec VPN

Although the IPsec section of the Security Module does not require changes of any parameters, for Hub-to-Spoke topology, there must be a configuration for each Spoke site in the Hub site router. That means each Spoke you want to deploy in the CPMS system requires its section in the Hub router configuration for:

- tunnel interface number,
- security zone interface parameters,
- OSPF interface parameters,
- security IKE policy profile (for IPSec),
- security IPsec VPN profile (for IPSec).

Interfaces section: Tunnel Interfaces

The configuration of the tunnel interfaces depends on the type of tunneling protocol. In GRE protocol, the source and destination address of the VPN tunnel (underlay WAN network) must be set in the interface configuration:

- The source IPv4 address specifies the origin of the GRE tunnel (in configuration templates it is the IPv4 address of the local WAN interface).
- The destination address specifies the endpoint of the GRE tunnel (in configuration templates it is the IPv4 address of the other end SRX router's WAN interface).

The items marked in `source` and `destination` mean that the WAN underlay network depends on the local provider.

The items marked in the address stand for the overlay network. According to the IP plan, the overlay networks depend on the connection type and Site ID. For more details, see Capacity Plus Multi Site Detailed IP Plan on page 588.

```
gr-0/0/0 {
    description "Tunnel Interfaces";
    unit 2 {
        tunnel {
            source 101.4.1.6;
            destination 101.4.1.10;
        }
        family inet {
            address 10.31.0.5/30;
        }
    }
    unit 3 {
        tunnel {
            source 101.4.1.6;
            destination 101.4.1.14;
        }
        family inet {
            address 10.31.0.9/30;
        }
    }
    unit 4 {
        tunnel {
            source 101.4.1.6;
            destination 101.4.1.18;
        }
        family inet {
            address 10.31.0.13/30;
        }
```

```
    }
}
```

IPsec protocol requires to set only the local IPv4 address of the overlay network in the interface configuration.

```
st0 {
    description "Tunnel Interfaces";
    unit 2 {
        family inet {
            address 10.31.0.5/30;
        }
    }
    unit 3 {
        family inet {
            address 10.31.0.9/30;
        }
    }
    unit 4 {
        family inet {
            address 10.31.0.13/30;
        }
    }
}
```

Site switches configuration templates do not require many changes to adapt. The required adaptation is described in the general section in EX Switch Configuration Overview on page 615.

The following is a list of configuration sections that must be adjusted:

- Hostname – see SRX Router Configuration Overview on page 596.
- Interfaces – see Interfaces Module (Switch) on page 618.
- Routing-options – see Routing Options Module on page 620.

5.1.9.3
Auto VPN Topology Configuration Overview

5.1.9.3.1
Juniper AVPN Implementation

AutoVPN (AVPN) supports an IPsec VPN aggregator (a Hub) that serves as a single termination point for multiple tunnels to remote sites (Spokes). AVPN allows network administrators to configure a Hub for current and future Spokes. No configuration changes are required on the Hub router when Spoke devices are added or deleted. This provides the administrators with flexibility in managing large-scale network deployments.

AVPN is an extension of static IPsec VPN technology. It uses the same data plane functions such as tunnels, or packet encryption and decryption algorithms. AVPN allows a tunnel interface to be configured with point-to-multipoint mode. The `multipoint` option is configured at the `edit interfaces st0 unit x` hierarchy level on both endpoints.

The AVPN network is a standard Hub-to-Spoke (star) topology, where each Spoke site router has a static VPN tunnel to the Hub site router. All IP traffic from Spoke to Spoke is routed by the Hub.

To set up a VPN tunnel between any site routers by using the AVPN protocol, the routers must detect each other as "trusted" devices. Juniper SRX implementation of AVPN protocol requires Private Key Infrastructure (PKI) for Identity Management. Because of this requirement, before each SRX router can set up a VPN tunnel with any other SRX in the system, it must be equipped with a private certificate signed by the same CA. This is a crucial point of creating the transport network infrastructure for any Capacity Plus Multi Site system when AVPN is in use. For a detailed procedure on how to build a CA and generate certificates for SRX, see Generating Certificates for Juniper SRX Devices on page 667.

Before the deployment of the configured SRX on the site, remember to check the current date and time of the router. If it is wrong, set it manually. Certificates are valid only in the time frame set in the certificate. If the current SRX date and time are outside of this time frame, the router cannot use the certificate to set up a tunnel. Time synchronization with the NTP server does not help, because it communicates with the server over the AVPN tunnel.

The following configurations are not supported with AVPN:

- Policy-based VPNs
- The RIP dynamic routing protocol
- Manual keys and Autokey IKE with preshared keys
- Configuring static next-hop tunnel binding (NHTB) on the Hub for the Spokes
- The group IKE ID user type is not supported with an IP address as the IKE ID.
- When the group IKE ID user type is used, the IKE ID should not overlap with other IKE gateways configured on the same external interface.

5.1.9.3.2
AVPN Configuration Templates

The AVPN configuration is created for CPMS systems of any size. The Hub site is the central network element of the system, and every Spoke connects with it.

To connect physical locations in the overlay network, pseudo-static VPN tunnels are configured between every Spoke and Hub router. Spoke routers may have a statically or dynamically allocated WAN IP address, and the Hub router must have a statically allocated WAN IP address. The tunnels between Hub and Spokes are called pseudo-static because they are set up automatically. They do not expire until one endpoint router goes offline, due to a power outage or underlay network communication disruption.

NOTE: Unlike the AVPN, ADVPN allows IPsec tunnels between Spoke sites. Those tunnels are set up automatically on-demand and removed when not needed. ADVPN creates the on-demand mesh topology: the number of possible VPN tunnels is equal to N*(N–1)/2, where N is the number of routers the ADVPN network consists of. The characteristics of network traffic between devices in Capacity Plus Multi Site systems would cause all dynamic Spoke-to-Spoke tunnels to be established and never removed. For more information about this solution, see "ADVPN Topology Configuration Overview" in the *Installation and Configuration Manual for Capacity Max System*.

The following are the main assumptions for AVPN topology templates:

- All IPv4 addresses for transport devices are static (no DHCP IPv4 address assignment for switch or router interfaces), except for Spokes WAN interfaces.
- The Hub router WAN interface IP address must be statically assigned.
- All IPv4 addresses come from the CPMS IP plan, except for the router's WAN interfaces.
- NAT translation supports connections to access resources on the Internet only from the Application Network.
- The OSPF routing protocol is used for inter-site communication.

The Hub configuration templates for the routers and switches have been categorized as follows:

- Double Switch
  - Router,
  - SRX Cluster,
  - Switch – contains configuration templates with a double switch in Hub with an optional security add-on.
- Single Switch

- Router
- Switch – contains configuration templates with a single switch in Hub with an optional security add-on.

To increase the reliability of the site, you can use an SRX cluster instead of a single router configuration. SRX cluster consists of two identical devices connected to each other. They work and are managed as a single logical device. For more information about SRX cluster options, see SRX Chassis Cluster Configuration Overview on page 614.

NOTE: Configuration templates for SRX Cluster exist only with Double Switch topology.

The Spoke configuration templates for the routers and switches have been categorized as follows:

- Router – contains configuration templates for IPsec with static and IPsec with dynamic WAN IPv4 addresses on Spokes.
- Switch - contains configuration templates with a single or a double switch in Spoke with optional security add-on.

NOTE: Configurations of the Spoke routers with static WAN IPv4 addresses can be mixed with the configurations of the Spoke routers with dynamic WAN IPv4 addresses in the same system. For the Hub router, there is no difference between the Spokes with static or dynamic WAN IPv4 address assignment.

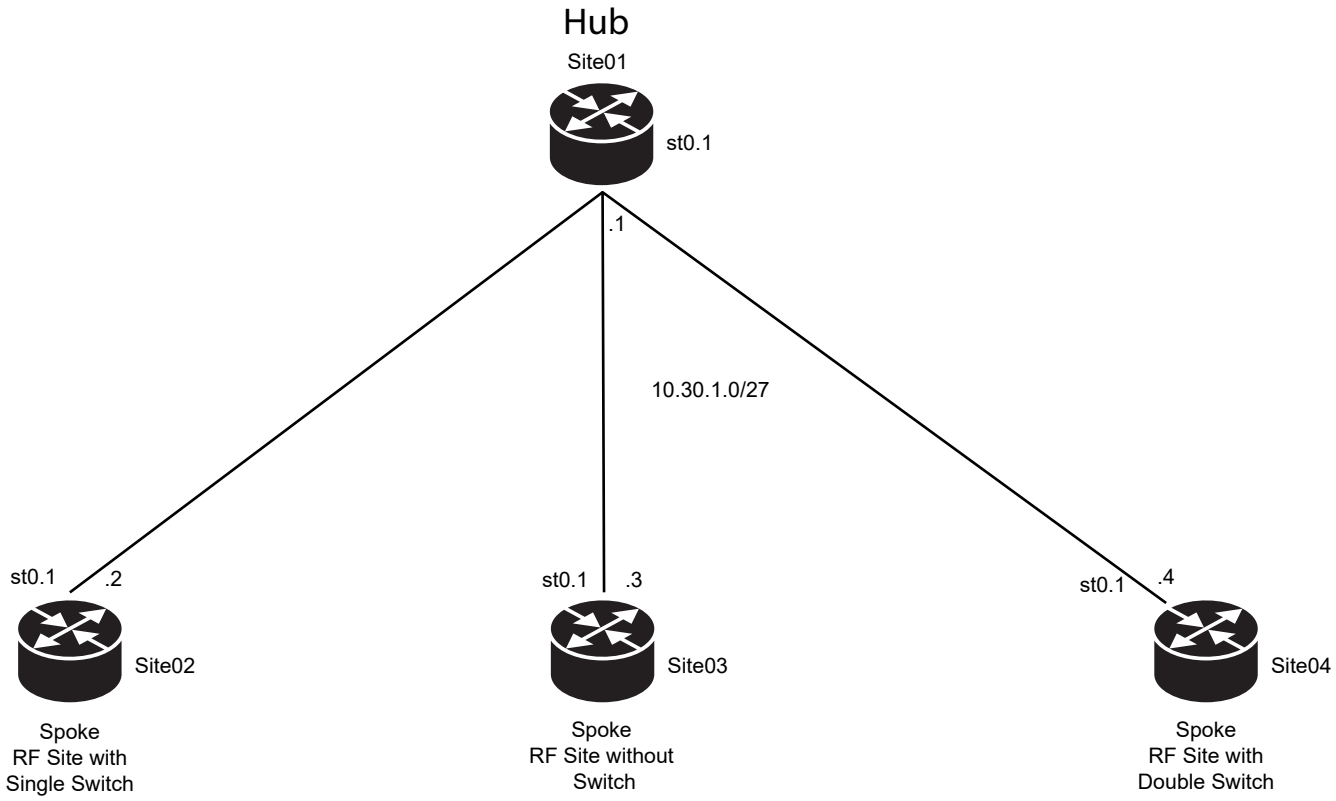
The Spoke configuration templates for routers and switches are created for three sites that use a different site topology:

- RF Site with a single switch (Site02)
- RF Site without a site switch (Site03)
- RF Site with a double switch (Site04)

An additional security add-on increases security for each Spoke site switch configuration. This file can be merged into the standard configuration template. For more details, see Add-On Configuration Files on page 595.

VPN tunnels run between the Spokes and Hub routers. All traffic between sites passes entirely through the Hub. All VPN tunnels are point-to-multipoint. According to the Capacity Plus Multi Site Detailed IP Plan on page 588, the subnets dedicated to the VPN tunnels have the /27 prefix.

Figure 232: AVPN Overlay Tunnel Network Diagram



5.1.9.3.3

Naming Convention in AVPN Topology

The naming conventions are the same as in the Naming Convention in Hub-to-Spoke Topology on page 632.

The difference is that the AVPN Hub router needs only one interface, IKE gateway, and VPN profile for Spokes. The same applies to Spokes, where the site router needs one set of these parameters for the Hub that it is connected to. All tunnel interfaces `st0` have the same number in Hub and Spokes, that is `st0.1`.

5.1.9.3.4

Adaptation of Configuration Templates for AVPN Topology

You need to adjust MOTOTRBO configuration templates to your needs.

Security Module

Configuration templates with AVPN require Identity Management that is covered by two modules: PKI and IKE.

PKI

Adaptation of the PKI configuration is not critical. However, this part must be committed before the Root CA certificate can be imported into the SRX router, as this procedure uses the `ca-profile`" name. For more

details, see Generating Certificates for Juniper SRX Devices on page 667. This part is the same for Hub and for Spoke site routers.

```
pki {
    ca-profile MOTO-CA {
        ca-identity MOTO-CA;
        revocation-check {
            disable;
        }
    }
}
```

NOTE: Each time you remove the `ca-profile` (for any reason, for example during configuration rollback) and commit the configuration, the Root CA certificate is lost and must be loaded again. It is a good practice to keep the certificate file in the user home folder of the SRX flash disk.

IKE

The IKE policy configuration includes the name of the local certificate. In contrast to PKI configuration, this certificate can be imported to SRX before the configuration is committed. This part is the same for Hub and for Spoke site routers.

```
ike {
    policy IKE-POL {
        mode main;
        certificate {
            local-certificate <cert-ID>;
        }
        proposal-set suiteb-gcm-256;
    }
```

The Hub router has only one IKE gateway profile for all the Spokes and those that can be deployed in the future.

In the profile, the other peer certificate is checked. Each time the relationships between two SRX devices must be established, they introduce themselves by using the local certificate.

The following are other peer checks regarding the certificate:

- If it is valid from the date and time point of view
- If it is signed by the common CA
- If it consists of a string configured in the IKE policy profile by the “distinguished-name” parameter (this string must be a continuous fragment)

All the steps are performed in the Identity Management process. When you use template configurations, you must adjust the string in the “distinguished-name” parameter.

The following is an IKE gateway configuration example for a Hub router:

```
gateway IKE-GW-SPOKE {
    ike-policy IKE-POL;
    dynamic {
        distinguished-name {
            wildcard ST=MALOPOLSKA,O=Customer-A;
        }
        ike-user-type group-ike-id;
    }
    dead-peer-detection {
        optimized;
        threshold 3;
    }
    local-identity distinguished-name;
```

```
    external-interface ge-0/0/5.0;
}
```

When you adjust a Spoke router template configuration, only Hub WAN IPv4 address must be adapted.

The following is an IKE gateway configuration example for a Spoke:

```
gateway IKE-GW-HUB {
    ike-policy IKE-POL;
    address 101.4.1.6;
    dead-peer-detection {
        optimized;
        threshold 3;
    }
    local-identity distinguished-name;
    remote-identity distinguished-name;
    external-interface ge-0/0/5.0;
}
```

Interfaces Section: Tunnel Interfaces

The configuration of the tunnel interfaces in AVPN uses only the IPsec protocol and it only requires setting the local address of the overlay network. As AVPN uses a point-to-multipoint interface type, the IPv4 address for each site router belongs to a subnet with /27 prefix. This subnet allows for 30 possible VPN tunnel interfaces (site routers) in one system. The last octet of the IPv4 address is tied to the Site ID. The same rule applies to the loopback interface, so the VPN tunnel and loopback interfaces have IPv4 addresses with the same last octet.

For more information about Site IDs, subnets, and IPv4 addresses.

The following is the interface section configuration example for a Hub router:

```
lo0 {
    unit 0 {
        description "Management Interface";
        family inet {
            address 10.30.16.1/32;
        }
    }
}
st0 {
    description "Tunnel Interfaces";
    unit 1 {
        multipoint;
        family inet {
            address 10.30.0.1/27;
        }
    }
}
```

The following is the interface section configuration example for a Spoke:

```
lo0 {
    unit 0 {
        description "Management Interface";
        family inet {
            address 10.30.16.4/32;
        }
    }
}
st0 {
    description "Tunnel Interfaces";
    unit 1 {
```

```
        multipoint;
        family inet {
            address 10.30.0.4/27;
        }
    }
}
```

Site switches configuration templates do not require many changes to adapt. The required adaptation is described in the general section EX Switch Configuration Overview on page 615.

The following configuration sections must be adjusted:

- Hostname – see SRX Router Configuration Overview on page 596.
- Interfaces – see Interfaces Module (Switch) on page 618
- Routing-options – see Routing Options Module on page 620

5.1.9.4
NAT Topology Configuration Overview

CPMS

The NAT configuration is created for small systems, where each RF Site is connected to a Public network. To connect physical locations together, the Network Address Translation mechanism is configured on each site router.

The following are the main assumptions for NAT topology templates:

- WAN interface IPv4 must be statically assigned.
- All IPv4 addresses for transport devices are static (there is no DHCP IPv4 address assignment for switch or router interfaces).
- All IPv4 addresses are from the Capacity Plus Multi Site IP plan, except for routers WAN interfaces.
- NAT translation is obligatory to support a connection between sites and to access resources on the Internet.

5.1.9.4.1
NAT Configuration Templates

Configuration templates for a router are created for three sites that use a different number of site switches:

- RF site with co-located Application Network with double site switch (Site01)
- RF site with co-located Application Network with a single site switch (Site02)
- RF site with no physical switch (Site03)

To increase security for each Hub and Spoke site switch configuration, a security add-on file can be used. This file can be merged into the standard configuration template. For more details, see Add-On Configuration Files on page 595.

To increase the reliability of the Hub site you can use an SRX cluster instead of a single router configuration. A SRX cluster consists of two identical devices connected together, which work and are managed as a single logical device.

For more information on SRX cluster options, see SRX Chassis Cluster Configuration Overview on page 614.

5.1.9.4.2

Adaptation of Configuration Templates for NAT Topology

Site routers configuration templates for NAT topology are similar to other Multi-Site configurations. For more details on the required adaptations, see the general section SRX Router Configuration Overview on page 596.

The following configuration sections require adjustment:

- Hostname and NTP – see System Module (Router) on page 597
- Security – see Security Module on page 599
- Interfaces – see Logical Interfaces on page 608
- Routing-options – see Routing-Options and Protocols Modules on page 611

  NOTE: In the NAT topology templates in the `routing-options` section there is no `router-id`.

- Access – see Access Module on page 613

Although configuration templates for NAT topology are very similar to configurations for other topologies, there are some important differences.

In the security section, the address-book differs from the other topology templates. In the NAT topology, all inter-site traffic must be translated. Because of this, the address-book contains many aliases of IPv4 addresses or subnets used by the next sections of configuration. That allows changing them in one place, rather than looking for required changes in the entire configuration file.

```
address-book {
    global {
        address RADIO_NETWORK 10.16.1.0/24;
        address APPLICATION_NETWORK 10.17.1.0/27;
        address PRIV_NET_CLASS_A 10.0.0.0/8;
        address PRIV_NET_CLASS_B 172.16.0.0/12;
        address PRIV_NET_CLASS_C 192.168.0.0/16;

        address REST_CHANNEL_ADDR 10.16.1.16/32;
        address RPTR-01_ADDR 10.16.1.17/32;
        address RPTR-02_ADDR 10.16.1.18/32;
        address RPTR-03_ADDR 10.16.1.19/32;
        address RDAC-01_ADDR 10.16.1.15/32;
        address RDAC-02_ADDR 10.17.1.15/32;
        address MNIS-DGW_ADDR 10.17.1.8/32;
        address RM_SRV_ADDR 10.17.1.14/32;
        address GW3_SRV_ADDR 10.17.1.16/32;
        address CONSOLE_SRV_ADDR 10.17.1.10/32;
        address WAN_ADDR 101.4.1.6/32;
        address-set PRIV_NETWORK {
            address PRIV_NET_CLASS_A;
            address PRIV_NET_CLASS_B;
            address PRIV_NET_CLASS_C;
            }
    }
}
```

Table 118: Description of Address Book Entries in the NAT Topology

Entries Name	Description
RADIO_NETWORK	The Radio Network exists in all sites of the CPMS system It is used for subnets with repeaters. Besides the repeaters, it can contain

Entries Name	Description
	RDAC applications, and technicians service laptop computers exclusively. In the CPMS IP plan, the subnet 10.16.0.0/16 is reserved for Radio Network.
APPLICATION_NETWORK	Application Network hosts all Motorola and non-Motorola applications clients and servers cooperating with MOTOTRBO systems such as: MNIS, RDAC, RM, Dispatch Consoles (TRBOnet, Avtec, SmartPTT). Depending on site numbers, there can be a different number of Application Networks. Motorola configuration template example: • APPLICATION_NETWORK_1 10.17.1.0/27 • APPLICATION_NETWORK_2 10.17.2.0/27
WAN_ADDR	This entry reflects the unique address with a 32-bit mask, which is set on the WAN interface. It is used in static NAT configuration for access from the WAN to the LAN network. For more details, see the NAT section.
REST_CHANNEL_ADDR	This entry reflects the unique address with a 32-bit mask, which is configured in the repeaters as the Rest Channel IP address. This address should be common for all repeaters on a site.
RPTR-(01-03)_ADDR	This entry reflects the unique address with a 32-bit mask, which is configured in the repeaters as an Ethernet interface IPv4 address. According to the IP plan, this IPv4 address depends on the Site ID. In the configuration templates for NAT topology each site by default has configured three repeaters (the following is an example for Site ID=1): • RPTR-01_ADDR 10.16.1.17/32 • RPTR-02_ADDR 10.16.1.18/32 • RPTR-03_ADDR 10.16.1.19/32
RDAC-(01-02)_ADDR	This entry reflects the unique IPv4 address with a 32-bit mask belonging to the host where the RDAC application is installed. RDAC can be deployed in the Radio and Application Networks. According to the IP plan, the IPv4 address for RDAC applications depends on the Site ID: • RDAC-01_ADDR 10.16.1.15/32 • RDAC-02_ADDR 10.17.1.15/32
MNIS-DGW_ADDR	This entry reflects the unique address with a 32-bit mask, which is set on the host where the MNIS application is installed. It can be deployed only in the Application Network. According to the IP plan, the IPv4 address for MNIS applications depends on the Site ID: • MNIS-DGW_ADDR 10.17.1.8/32
RM_SRV_ADDR	This entry reflects the unique address with a 32-bit mask, which is set on the host where the RM application is installed. RM can be deployed only in the Application Network. According to the IP plan, the IPv4 address for RM depends on the Site ID: • RM_SRV_ADDR 10.17.1.14/32
GW3_SRV_ADDR	This entry reflects the unique address with a 32-bit mask, which is set on the host where the GW3 application is installed. GW3 can be

Entries Name	Description
	deployed only in the Application Network. According to the IP plan, the IPv4 address for GW3 depends on the Site ID: • GW3_SRV_ADDR 10.17.1.16/32
CONSOLE_SRV_ADDR	This entry reflects the unique address with a 32-bit mask, which is set on the host where the Dispatch Console server is installed. It can be deployed only in the Application Network. According to the IP plan, the IPv4 address for the Dispatch Console server depends on the Site ID: • CONSOLE_SRV_ADDR 10.17.1.10/32 **NOTE:** If the Dispatch Console server is deployed on the same host with the MNIS, then the CONSOLE_SRV_ADDR and MNIS-DGW_ADDR should have the same IPv4 address.
PRIV_NETWORK	This group collects all private addresses in all classes (RFC 1918): • PRIV_NET_CLASS_A 10.0.0.0/8 • PRIV_NET_CLASS_B 172.16.0.0/12 • PRIV_NET_CLASS_C 192.168.0.0/16 It is used in policies from the TRUS zone to the UNTRUST zone to block all unnecessary traffic coming from the private subnets to outside of the CPMS system.

Another important difference in the security section is the nat configuration. In the NAT topology, NAT functions are more extensive, as all inter-site traffic is translated and forwarded through the WAN network. Two types of NAT were used in the configuration templates:

- Source NAT
  Source NAT is the translation of the source IP address of a packet leaving the Juniper Networks device. Source NAT is used to allow hosts with private IPv4 addresses to access a public network.

```
source {
    rule-set OUTBAND_NAT {
        description "Internet Access for Hosts";
        from zone TRUST;
        to zone UNTRUST;
        rule APP_NAT {
            match {
                source-address-name APPLICATION_NETWORK;
            }
            then {
                source-nat {
                    interface;
                }
            }
        }
        rule RADIO_NAT {
            match {
                source-address-name RADIO_NETWORK;
            }
            then {
                source-nat {
                    interface;
                }
            }
```

```
        }
    }
}
```

NOTE: Source NAT does not require any adaptation changes.

- Static NAT
  Static NAT allows connections to be originated from either side of the network, but translation is limited to one-to-one or between blocks of addresses of the same size. The mapping includes destination IPv4 address and destination port number translation in one direction and source IPv4 address and source port number translation in the reverse direction (Reverse NAT).

  NOTE: NAT exposes ports to a port scanner if the router is connected to the Internet. The site NAT implementation should be carefully reviewed, and it should only enable the minimum connections required.

```
static {
    rule-set STATIC_NAT {
        from zone UNTRUST;
        rule REST_CHANNEL {
            description "REST Channel";
            match {
                destination-address-name WAN_ADDR;
                destination-port 56200;
            }
            then {
                static-nat {
                    prefix-name {
                        REST_CHANNEL_ADDR;
                        mapped-port 56200;
                    }
                }
            }
        }
        rule RPTR-01 {
            description "Repeater 01";
            match {
                destination-address-name WAN_ADDR;
                destination-port 56201;
            }
            then {
                static-nat {
                    prefix-name {
                        RPTR-01_ADDR;
                        mapped-port 56201;
                    }
                }
            }
        }
        rule RPTR-02 {
            description "Repeater 02";
            match {
                destination-address-name WAN_ADDR;
                destination-port 56202;
            }
            then {
                static-nat {
                    prefix-name {
                        RPTR-02_ADDR;
                        mapped-port 56202;
                    }
```

```
                }
            }
        }
        rule RPTR-03 {
            description "Repeater 03";
            match {
                destination-address-name WAN_ADDR;
                destination-port 56203;
            }
            then {
                static-nat {
                    prefix-name {
                        RPTR-03_ADDR;
                        mapped-port 56203;
                    }
                }
            }
        }
        rule RDAC_1 {
            description "RDAC Application";
            match {
                destination-address-name WAN_ADDR;
                destination-port 56215;
            }
            then {
                static-nat {
                    prefix-name {
                        RDAC-01_ADDR;
                        mapped-port 56215;
                    }
                }
            }
        }
        rule RDAC_2 {
            description "RDAC Application";
            match {
                destination-address-name WAN_ADDR;
                destination-port 56225;
            }
            then {
                static-nat {
                    prefix-name {
                        RDAC-02_ADDR;
                        mapped-port 56225;
                    }
                }
            }
        }
        rule RM {
            description "Radio Manager";
            match {
                destination-address-name WAN_ADDR;
                destination-port 50000 to 50100;
            }
            then {
                static-nat {
                    prefix-name {
                        RM_SRV_ADDR;
                        mapped-port 50000 to 50100;
                    }
                }
            }
```

```
        }
        rule MNIS_DGW {
            description "MNIS Data Gateway";
            match {
                destination-address-name WAN_ADDR;
                destination-port 56218;
            }
            then {
                static-nat {
                    prefix-name {
                        MNIS-DGW_ADDR;
                        mapped-port 56218;
                    }
                }
            }
        }
        rule GENESIS {
            description "GW3 Application";
            match {
                destination-address-name WAN_ADDR;
                destination-port 56226;
            }
            then {
                static-nat {
                    prefix-name {
                        GW3_SRV_ADDR;
                        mapped-port 56226;
                    }
                }
            }
        }
        rule CONSOLE_SERVER {
            description "Console Server";
            match {
                destination-address-name WAN_ADDR;
                destination-port 56220;
            }
            then {
                static-nat {
                    prefix-name {
                        CONSOLE_SRV_ADDR;
                        mapped-port 56220;
                    }
                }
            }
        }
    }
}
```

The bold port numbers for `destination-port` and `mapped-port` should be adapted by the customer according to the IP plan for the CPMS system and the settings of each system component.

Chapter 6

Capacity Plus Single Site and Multi Site Procedures and Maintenance

6.1 Procedures for Juniper Infrastructure

6.1.1 Loading Basic Configuration with Device Console Port

Perform the following steps to load configuration files by using console port to Juniper EX switch or SRX router.

Prerequisites:
The following hardware is required:

- PC with terminal emulation software (for example PuTTY)
- Console cable for console access to the device

Procedure:

1. Access the device CLI by using the console cable and the terminal emulation software.

   Common settings for terminal emulators:

   ```
   Bits per sec : 9600
   Data bits : 8
   Parity : none
   Stop bits : 1
   Flow control : none
   ```

2. Log on to the device by using the existing username and password. If the device has no user configuration, use the `root` username without a password, then run the `cli` command.

   NOTE: For more information, check the KB16580 and KB11471 by using Juniper Knowledge Base on https://kb.juniper.net/.

3. Enter the configuration mode of the device by using the `configure` command and delete existing configuration by entering `delete`

   - If you configure an EX switch, use the configuration from Configuration of Juniper EX Switch to Allow IP Network Communication on page 651.
   - If you configure an SRX router, use the configuration from Configuration of Juniper SRX Router to Allow IP Network Communication on page 652.

   Step example:

   ```
   motorola@SRX-SITE01R1> configure
   Entering configuration mode


   [edit]
   motorola@SRX-SITE01R1# delete
   This will delete the entire configuration
   ```

```
Delete everything under this level? [yes,no] (no) yes


[edit]
motorola@SRX-SITE01R1#
```

4. Paste the configuration lines to the terminal window.

   NOTE: Do not paste more than 10 lines in one copy/paste action, as the terminal buffer is limited and the copied lines would be truncated.

5. To compare the output with the copied configuration, run `show | display set`
6. After the configuration is loaded, set the password for the "root" user by running the following command:

   ```
   set system  root-authentication plain-text-password
   New password:
   Retype new password:
   ```

   a. Enter the password twice when prompted.

   NOTE: It is not possible to commit the configuration when the username root has no password set

7. To allow access to the device, create a user and password by running the following command:

   ```
   set system login user <username> class super-user-local authentication
   plain-text-password
   New password:
   Retype new password:
   ```

   a. Enter the password twice when prompted.

8. To check correct syntax of the loaded configuration, run `commit check`
9. To activate the new configuration, run `commit and-quit`

6.1.1.1 Configuration of Juniper EX Switch to Allow IP Network Communication

An example of the EX configuration template that allows IP communication with a device.

<parameter> must be replaced with suitable customer information.

```
set system login class super-user-local idle-timeout 10
set system login class super-user-local login-alarms
set system login class super-user-local permissions all
set system login password minimum-length 8
set system login password change-type character-sets
set system login password minimum-changes 2
set system login password format sha1
set system host-name <hostname>
set system auto-snapshot
set system services ssh root-login deny
set system services ssh no-tcp-forwarding
set system services ssh protocol-version v2
set system services ssh max-sessions-per-connection 1
set system services ssh ciphers aes256-ctr
set system services ssh ciphers aes256-cbc
set system services ssh ciphers aes192-ctr
```

```
set system services ssh ciphers aes192-cbc
set system services ssh ciphers aes128-ctr
set system services ssh ciphers aes128-cbc
set system services ssh macs hmac-sha2-512
set system services ssh macs hmac-sha2-256
set system services ssh macs hmac-sha1
set system services ssh macs hmac-sha1-96
set system services ssh key-exchange dh-group1-sha1
set system services ssh key-exchange dh-group14-sha1
set system services ssh key-exchange group-exchange-sha2
set system services ssh key-exchange ecdh-sha2-nistp256
set system services ssh key-exchange ecdh-sha2-nistp384
set system services ssh key-exchange ecdh-sha2-nistp521
set system services ssh client-alive-count-max 5
set system services ssh client-alive-interval 120
set system services ssh connection-limit 10
set system services ssh rate-limit 4
set system services web-management https system-generated-certificate
set system services web-management session idle-timeout 15
set system services web-management session session-limit 10
set interfaces interface-range PORTS unit 0 family ethernet-switching
interface-mode access
set interfaces interface-range PORTS unit 0 family ethernet-switching vlan
members default
set interfaces interface-range PORTS unit 0 family ethernet-switching storm-
control default
set interfaces irb unit 0 family inet address <ip address/prefix>
set forwarding-options storm-control-profiles default all
set vlans default vlan-id 1
set vlans default l3-interface irb.0
```

6.1.1.2

Configuration of Juniper SRX Router to Allow IP Network Communication

Example of the SRX configuration template that allows IP communication with a device.

<parameter> must be replaced with suitable customer information.

```
set system login class super-user-local idle-timeout 10
set system login class super-user-local login-alarms
set system login class super-user-local permissions all
set system login password minimum-length 8
set system login password change-type character-sets
set system login password minimum-changes 2
set system login password format sha1
set system host-name <hostname>
set system time-zone UTC
set system ports console log-out-on-disconnect
set system services ssh root-login deny
set system services ssh no-tcp-forwarding
set system services ssh protocol-version v2
set system services ssh max-sessions-per-connection 1
set system services ssh ciphers aes256-ctr
set system services ssh ciphers aes256-cbc
set system services ssh ciphers aes192-ctr
set system services ssh ciphers aes192-cbc
set system services ssh ciphers aes128-ctr
set system services ssh ciphers aes128-cbc
set system services ssh macs hmac-sha2-512
```

```
set system services ssh macs hmac-sha2-256
set system services ssh macs hmac-sha1
set system services ssh macs hmac-sha1-96
set system services ssh key-exchange dh-group1-sha1
set system services ssh key-exchange dh-group14-sha1
set system services ssh key-exchange group-exchange-sha2
set system services ssh key-exchange ecdh-sha2-nistp256
set system services ssh key-exchange ecdh-sha2-nistp384
set system services ssh key-exchange ecdh-sha2-nistp521
set system services ssh client-alive-count-max 5
set system services ssh client-alive-interval 120
set system services ssh connection-limit 10
set system services ssh rate-limit 4
set system processes app-engine-management-service disable
set system processes advanced-anti-malware disable
set system processes application-identification disable
set system processes application-security disable
set system processes idp-policy disable
set system processes security-intelligence disable
set system processes utmd disable
set security zones security-zone UNTRUST host-inbound-traffic system-services
all
set security zones security-zone UNTRUST host-inbound-traffic protocols all
set security zones security-zone UNTRUST interfaces ge-0/0/5.0
set interfaces ge-0/0/5 unit 0 family inet address <ip address/prefix>
```

6.1.2

Transferring Files to and from Juniper Devices Using SCP Protocol

Perform the following procedure to copy files between PC and SRX router or EX switch by using Secure Copy Protocol (SCP).

Prerequisites:
The following hardware is required:

- PC with SCP client (for example WinSCP)
- Ethernet cable

NOTE: For SRX3xx series routers, the path always starts with `/cf` and it needs to be added in all paths presented in this procedure.

Procedure:

1. Connect the PC to the port of the Juniper device by using Ethernet cable.

   The device interface must allow IP communication to the device. If the device has no configuration, follow the appropriate procedure from Loading Basic Configuration with Device Console Port on page 650.

2. Run the SCP client and open the SCP session by using the management IP address of the device.

   NOTE: When using template configurations, management (SSH, SCP) communication to SRX site routers is allowed only to lo0.0 interface.

3. Log on and upload the file from the PC to the device appropriate folder by using SCP client.

The default path for configuration files is `/var/home/<user_name>/` where ***<user_name>*** is the name of the user used during the login to the device.

NOTE: Do not use this folder for OS upload, as the files are too big for the successful upload to `home` directory. For OS upgrade, upload new image to `/var/tmp/`

4. If you want to backup some files from the device, copy them to the PC.

   NOTE:
   Do **not** log on by using the **root** user. It is a special built-in account, and its home directory has a different path. The files uploaded in such a way are usable only by the **root** user.
   If the connection to the device fails, see Adjusting WinSCP Configuration for Juniper Devices on page 666.

6.1.3
Transferring Files to and from Juniper Devices with the USB Stick

Prerequisites:
The following hardware is required:

- PC with terminal emulation software (for example PuTTY)
- Console cable for console access to the device
- USB stick with FAT32 format

NOTE: For SRX3xx series routers, the path always starts with `/cf` and it needs to be added in all paths presented in this procedure.

Procedure:

1. Access the device CLI by using the console cable and the terminal emulation software.

   Common settings for terminal emulators:

   ```
   Bits per sec : 9600
   Data bits : 8
   Parity : none
   Stop bits : 1
   Flow control : none
   ```

2. Log on to the device by using existing username and password. If the device has no user configuration, use username `root` without a password.

   NOTE: For more information, check the KB16580 and KB11471 by using Juniper Knowledge Base on https://kb.juniper.net/.

3. Enter the shell mode of the device.

   If you use `root` username for login, the current mode is shell.

   If you use another username for login, run `start shell user root` and provide the password for `root` user.

4. To show all the devices with the name starting with “da”, run `ls /dev/da*`

   Example: EX switch output

   ```
   {master:0}
   motorola@SW01> start shell user root
   Password:
   root@SW01:RE:0% ls /dev/da*
   ```

```
/dev/da0         /dev/da0p1       /dev/da0p2
root@SW01:RE:0%
```

Example: SRX router output

```
motorola@SRX-R01> start shell user root
Password:
root@SRX-R01% ls /dev/da*
/dev/da0      /dev/da0s1c   /dev/da0s2c   /dev/da0s3e   /dev/da0s4a
/dev/da0s1    /dev/da0s2    /dev/da0s3    /dev/da0s3f   /dev/da0s4c
/dev/da0s1a   /dev/da0s2a   /dev/da0s3c   /dev/da0s4    /dev/da0s4e
root@SRX-R01%
```

5. Insert USB stick in the USB port.

   On the EX switch, the port is located on the rear panel.

   On the SRX router, the port is located on the front panel.
6. To show all the devices with the name starting with “da”, run `ls /dev/da*` again.
7. Compare both outputs to find the device name of the inserted USB stick.

   Usually, it is “da1s1” for SRX3xx and “da0s1” for SRX1500.
8. To create a new folder, use `mkdir /var/tmp/usb` command.
9. Mount the USB drive to the `/var/tmp/usb` directory by using `mount_msdosfs /dev/da1s1 /var/tmp/usb` or `mount -t msdos /dev/da1s1 /var/tmp/usb` command.
10. To preview all the files in the USB drive, use the command `ls /var/tmp/usb`
11. Copy the required file to or from the USB stick by entering: `cp /<source_path>/<source_file> <destination_path>`

    Step example: `root@SRX-R01% cp /var/tmp/usb/images.tgz /var/tmp`
12. After the file is completely copied, unmount the USB drive by using `umount /var/tmp/usb`, and remove the USB stick from the device.

    NOTE:
    Avoid copying files to `/var/homepath` when you are logged on as `root`.
    If you find any problems with USB stick mounting, check the KB12022 or KB12880 by using Juniper Knowledge Base on https://kb.juniper.net/.

6.1.4
Loading the Configuration from a File to the Juniper SRX Router and EX Switch

Perform the following steps to load configuration from a file on Juniper EX switch or SRX router.

Prerequisites:
The following hardware is required:

- PC with terminal emulation software (for example PuTTY)
- Console cable for console access, or Ethernet cable for IP access to the device

NOTE: For SRX3xx series routers, the path always starts with `/cf` and it needs to be added in all paths presented in this procedure.

Procedure:

1. Access the device CLI by opening SSH session, or by using the console cable and the terminal emulation software.
2. Log on to the device.
3. Enter the configuration mode of the device by using the `configure` command.
4. To override the entire configuration of the device, perform one of the following actions:
   - If the configuration file is in Stanza format, run `load override /<path>/<file>`
   - If the configuration file is in Set format, the old configuration must be deleted before a new one can be loaded. Run the command `delete`, and at the prompt to confirm, enter `yes`, then load a new configuration by entering `load set /<path>/<file>`

   NOTE: When the configuration file is in path `/var/home/<user_name>/`, there is no need to include the path, as this is a default path.
5. After the configuration is loaded, set the password for the "root" user by running the following command:

   ```
   set system  root-authentication plain-text-password
   New password:
   Retype new password:
   ```

   a. Enter the password twice when prompted.

   NOTE: It is not possible to commit the configuration when the username root has no password set.
6. To allow access to the device, create a user and password by running the following command:

   ```
   set system login user <username> class super-user-local authentication
   plain-text-password
   New password:
   Retype new password:
   ```

   a. Enter the password twice when prompted.
7. If you want to load only a fragment of the configuration with changes, or if you want to add some features or parameters, perform one of the following actions:
   - If the file is in Stanza format, enter `load merge /<path>/<file>`
   - If the file is in Set format, enter `load set /<path>/<file>`
8. Once the configuration is loaded to the device, check the correctness of the configuration by entering `commit check`
9. To apply and save the configuration, run `commit and-quit`

6.1.5
Upgrading Juniper OS on the EX2300 Switch

The EX2300 switches contain only 2GB of flash memory, so each upgrade the OS snapshot must be deleted beforehand. It is possible to upgrade the OS to any OS version; however, the switch may lose configuration and, after its restart, boot up with the manufacturer's default configuration. To avoid this, an upgrade path must be followed. The upgrade path is described in the following subchapters.

Perform the following procedure to upgrade the OS on the Juniper EX switch.

NOTE: For double switch topology, you should upgrade both switches to the same OS version before upgrading to the next OS release.

Prerequisites:
The following hardware is required:

- PC with terminal emulation software (for example PuTTY)
- Console cable for console access or Ethernet cable for IP access to the device

Prepare the image file with the supported Juniper OS for EX2300 switch.

Procedure:

1. Access the device CLI by opening SSH session or by using the console cable and the terminal emulation software.
2. To remove all the unnecessary files, enter `request system storage cleanup`

   WARNING: Do not perform this step with the connected USB stick, because the cleanup procedure deletes all the files from the stick.
3. To delete any existing recovery snapshot that is stored on the system, run `request system snapshot delete *`
4. Upload a new OS image file. See Transferring Files to and from Juniper Devices Using SCP Protocol on page 653 or Transferring Files to and from Juniper Devices with the USB Stick on page 654.

   NOTE: Do not perform step 4 before step 2, because the cleanup procedure deletes the uploaded files.
   It is recommended to use the folder `/tmp/` as a path for the OS image upload.
5. Check the time and date of the switch's internal clock by entering `show system uptime`

   If time and date are not current, they must be set either manually or by using the NTP server. Otherwise, the OS upgrade may fail.
6. To install the Juniper OS, enter the following command:

   `request system software add /<path>/<junos-arm-32-version.tgz> no-copy no-validate`

   NOTE: In case of any problem with the OS installation, check the KB31198 by using Juniper Knowledge Base on https://kb.juniper.net/.
7. After successful installation, reboot the system to complete the OS installation process.

   NOTE: After the OS upgrade, the error message may appear after logon to the J-Web interface. This error message appears only if the switch has no access to the Internet. This happens because each OS upgrade loads only the basic version of the J-Web module, and it resets to the default J-Web user preferences.
   To disable the error message, go to **Maintain** → **Update J-Web** menu. Under **Update Preferences**, uncheck **Check for updates automatically on every login**.

6.1.6
Upgrading Juniper OS on the SRX3xx Router

The OS upgrade is possible to any OS version; however, the SRX can lose configuration and, after its restart, boot up with the manufacturer's default configuration. To avoid this, an upgrade path must be followed. The upgrade path is described in the following subchapters.
Perform the following procedure to upgrade the OS on the Juniper SRX router.

Prerequisites:

The following hardware is required:

- PC with terminal emulation software (for example PuTTY)
- Console cable for console access or Ethernet cable for IP access to the device

Prepare the image file with the supported Juniper OS for SRX3xx series router.

Procedure:

1. Access the device CLI by opening the SSH session or by using the console cable and the terminal emulation software.
2. Run the `show system storage detail` command to check the available space on flash. Look for the `/cf/var` path. If Capacity shows less than 50% go to step 4, if more than 50% continue with step 3.

   Step example:

   ```
   motorola@SRX-R01> show system storage detail
   Filesystem  1024-blocks   Used   Avail Capacity Mounted on
   /dev/bo0s3f     2218426 756710 1284242      37%    /cf/var  check this row
   ```

3. To remove all the unnecessary files, run `request system storage cleanup`

   WARNING: Do not run step 3 with the connected USB stick, because the cleanup procedure deletes all the files from the stick.

4. Upload a new OS image file by following the steps in Transferring Files to and from Juniper Devices Using SCP Protocol on page 653 or Transferring Files to and from Juniper Devices with the USB Stick on page 654.

   NOTE: Do not perform step 4 before step 3, because the cleanup procedure deletes the uploaded files.

5. To install the Juniper OS, run the following command:

   ```
   request system software add /var/tmp/<junos-srxsme-version.tgz> no-validate
   ```

6. After successful installation, reboot the system to complete the OS installation process.
7. (Optional) After the device restart with the new OS, run the following command:

   ```
   request system snapshot slice alternate
   ```

   This command copies the current partition of the OS on flash to the alternate one. In case of any problems with the current partition, the device uses the alternate one during the boot process.

   Step example: SRX output before performing step 7:

   ```
   motorola@SRX-R01> show system snapshot media internal
   Information for snapshot on    internal (/dev/da0s1a) (primary)
   Creation date: Feb 24 15:41:34 2020
   JUNOS version on snapshot:
     junos  : 18.2R3-S2.9
   Information for snapshot on    internal (/dev/da0s2a) (backup)
   Creation date: Dec 6 09:48:27 2019
   JUNOS version on snapshot:
     junos  : 18.2R3.4
   ```

6.1.7

Preparing SRX345 to Deploy Chassis Cluster

Perform the following steps to form a chassis cluster by using two SRX345 routers.

NOTE: For more details about chassis cluster requirements, see SRX Chassis Cluster Configuration Overview on page 614.

Prerequisites:
The following hardware is required:

- PC with terminal emulation software (for example PuTTY)
- Console cable for console access to the device
- Two SRX345 routers with exactly the same hardware configuration and the same OS version.

Procedure:

1. Access the device CLI using the console cable and terminal emulation software.

   Common settings for terminal emulators:

   ```
   Bits per sec : 9600
   Data bits : 8
   Parity : none
   Stop bits : 1
   Flow control : none
   ```

2. Log in to each device and perform one of the following actions:
   - If the device has no user configuration, use `root` user without a password, run `cli` and enter the configuration mode by using `configuration` command, then go to step 4.
   - If there is a user configuration, log in by using the existing user name and password.
3. Enter the configuration mode by using `configuration` command, run `delete` and confirm `yes` when prompted.
4. Set the password for `root` user and commit the configuration changes by using the following commands:

   ```
   set system root-authentication plain-text-password
   New password:
   Retype new password:
   commit and-quit
   ```

   NOTE: It is not possible to commit the configuration when the username `root` has no password set.

   Step example: SRX output example for a device with no existing default configuration:

   ```
   motorola@SRX-R01> configure
   motorola@SRX-R01# delete
   This will delete the entire configuration
   Delete everything under this level? [yes,no] (no) yes
   motorola@SRX-R01# set system root-authentication plain-text-password
   New password: <password>
   Retype new password: <password>
   motorola@SRX-R01# commit and-quit
   commit complete
   Exiting configuration mode
   motorola@SRX-R01>
   ```

5. Connect both SRX345 routers by using Ethernet cables. For a control, link connect interfaces ge-0/0/1. For a fabric link, connect interfaces ge-0/0/2, see SRX Chassis Cluster Configuration Overview on page 614.
6. Enable the cluster mode and reboot the devices. On both devices, enter:
   `set chassis cluster cluster-id <cluster-id> node <node-id> reboot`

   The ***<cluster-id>*** is the same on both devices, but the ***<node-id>*** must be different, as one device is node 0, and the other device is node 1. The range for the ***<cluster-id>*** is 0-15. Setting the ***<cluster-id>*** to 0 disables the cluster mode.

   NOTE: This step is performed in operational mode, not with a configure mode command.

   Step example:

   ```
   On device A:
   motorola@SRX-R01> set chassis cluster cluster-id 1 node 0 reboot
   On device B:
   motorola@SRX-R02> set chassis cluster cluster-id 1 node 1 reboot
   ```
7. When both devices boot up, wait up to 5 minutes and log in to one device as a `root` user.
8. Run `cli` command and verify the cluster status with the following command:

   `show chassis cluster interfaces`

   Step example:

   ```
   root% cli
   {primary:node0}
   root> show chassis cluster status
   Cluster ID: 1
   Node   Priority       Status  Preempt  Manual  Monitor-failures

   Redundancy group: 0 , Failover count: 1
   node0         1      primary       no      no          None
   node1         1    secondary       no      no          None
   ```

6.1.8

Loading Configuration from a File on SRX Series Chassis Cluster

Perform the following procedure to load configuration from a file on Juniper SRX Chassis Cluster.

Prerequisites:
The following hardware is required:

- PC with terminal emulation software (for example PuTTY)
- Console cable for console access or Ethernet cable for IP access to the device

For the SRX345 series, use the configuration template file for the SRX345 Chassis Cluster.

WARNING: Using the configuration file for a single SRX3xx router results in failure.

For the SRX1500 series use the configuration template file for the SRX1500 Chassis Cluster.

Procedure:

1. Access the device CLI by opening the SSH session or by using the console cable and terminal emulation software.

2. When using console cable, check the prompt if the node is primary or secondary. If it is secondary node, reconnect the console cable to primary node.

   SSH sessions always connect to the primary node.

   Step example:

   ```
   {primary:node0}
   root@SRX-R01>
   ```

3. To upload the configuration file, follow Transferring Files to and from Juniper Devices Using SCP Protocol on page 653 or Transferring Files to and from Juniper Devices with the USB Stick on page 654.

4. To override the entire configuration of the device, choose one of the following:

   - If the configuration file is in Stanza format, enter `load override /<path>/<file>`
   - If the configuration file is in Set format, the old configuration must be deleted before a new one can be loaded. Run the command `delete` and confirm `yes` when prompted, then run `load set /<path>/<file>` to load a new configuration.

   NOTE: When the configuration file is in path `/var/home/<user_name>/`, there is no need to include the path, as this is a default path.

5. After the configuration is loaded, set the password for the "root" user by running the following command:

   ```
   set system  root-authentication plain-text-password
   New password:
   Retype new password:
   ```

   a. Enter the password twice when prompted.

      NOTE: It is not possible to commit the configuration when the username root has no password set.

6. To allow access to the device, create a user and password by running the following command:

   ```
   set system login user <username> class super-user-local authentication
   plain-text-password
   New password:
   Retype new password:
   ```

7. If you want to load only a fragment of the configuration to change or to add some features or parameters, perform one of the following actions:

   - For the file in Stanza format, enter `load merge /<path>/<file>`.
   - For the file in Set format, enter `load set /<path>/<file>`

8. Once the configuration is loaded to the device, check the correctness of the configuration by running `commit check` command.

9. To apply and save the configuration, run `commit and-quit` command.

6.1.9
Upgrading Juniper OS on SRX Series Chassis Cluster

Perform the following procedure to upgrade OS on the Juniper SRX series chassis cluster.

Prerequisites:
The following hardware is required:

- PC with terminal emulation software (for example PuTTY)
- Console cable for console access or Ethernet cable for IP access to the device

Prepare the image file with the supported Juniper OS for SRX series router.

Procedure:

1. Access the device CLI by opening an SSH session or by using the console cable and terminal emulation software.
2. When using the console cable, check the prompt if the node is primary or secondary. If it is the secondary node, reconnect the console cable to the primary node.

   SSH sessions always connect to the primary node.

   Step example:

   ```
   {primary:node0}
   root@SRX-R01>
   ```

3. Follow the steps in Transferring Files to and from Juniper Devices Using SCP Protocol on page 653 or Transferring Files to and from Juniper Devices with the USB Stick on page 654 to upload the file with the new OS image.
4. Install the new OS by entering the following command:
   a. For SRX345 use:

      ```
      request system software in-service-upgrade <path/os_file_name.tgz> no-validate no-sync
      ```

   b. For SRX1500 use:

      ```
      request system software in-service-upgrade <path/os_file_name.tgz> no-compatibility-check
      ```

5. Wait until the primary node finishes the installation process and restarts.

   NOTE: This is the sequence of the process:
   - The primary node copies the OS image to the secondary node.
   - The primary node installs the new image.
   - The secondary node installs the new image and restarts.
   - When the secondary node is operational, then the primary node restarts.
   - The secondary node takes over and becomes a primary node.
   - After restart, the original primary node becomes a secondary node.

6. Log in again and check if both nodes have the same new OS version.

   Step example: For SRX345:

   ```
   root@SRX-01> show version
   node0:
   --------------------------------------------
   Hostname: SRX-R01
   Model: srx345
   Junos: 19.4R2.6
   JUNOS Software Release [19.4R2.6]

   node1:
   --------------------------------------------
   Hostname: SRX-R02
   Model: srx345
   ```

```
Junos: 19.4R2.6
JUNOS Software Release [19.4R2.6]
```

Step example: For SRX1500

```
root@ SRX-SITE001CR1> show version
node0:
--------------------------------------------
Hostname: SRX-SITE001CR1
Model: srx1500
Junos: 21.4R3-S4.9


node1:
--------------------------------------------
Hostname: SRX-SITE001CR2
Model: srx1500
Junos: 21.4R3-S4.9
```

*The output is truncated.

6.1.10
Creating and Modifying Credentials on Juniper EX Switch and SRX Router

Prerequisites:
The following hardware is required:

- PC with terminal emulation software (for example PuTTY)
- Console cable for console access or Ethernet cable for IP access to the device

Procedure:

1. Access the device CLI by opening an SSH session or by using the console cable and terminal emulation software.
2. Log on to the device and enter the configuration mode of the device by entering `configure`
3. To change the password of an existing user, run the following command and enter the password twice when prompted:

   ```
   set system login user <username> authentication plain-text-password
   New password:
   Retype new password:
   ```

4. To create a new user and password, run the following command, and enter the password twice when prompted:

   ```
   set system login user <username> class super-user-local authentication
   plain-text-password
   New password:
   Retype new password:
   ```

5. To delete an existing user, run the following command:

   ```
   delete system login user <username>
   ```

6. To change the current password for the **root** user, run the following command, and enter the password twice when prompted:

```
set system  root-authentication plain-text-password
New password:
Retype new password:
```

7. After the device configuration is updated, check the correctness of the configuration by entering `commit check`
8. To apply and save the configuration, enter `commit and-quit`

6.1.11
Modifying SNMP Configuration on Juniper EX Switch and SRX Router

Prerequisites:
The following hardware is required:

- PC with terminal emulation software (for example PuTTY)
- Console cable for console access or Ethernet cable for IP access to the device

The exact procedures can be found in the following subsections.

6.1.12
Clearing Persistent MAC Addresses Table on Juniper EX Switch

Perform the following steps to clear the persistent MAC addresses table on Juniper EX switch.

Perform these steps in the following situations:

- After applying a security add-on configuration file.
- When you need to replace a device connected to the switch port on which security features are enabled.

Prerequisites:
The following hardware is required:

- PC with terminal emulation software (for example PuTTY)
- Console cable for console access or Ethernet cable for IP access to the device

Procedure:

1. Access the device CLI by opening SSH session or by using the console cable and terminal emulation software.
2. Log in to the device and run an appropriate command:
   a. After applying a security add-on configuration file, enter the following command:
      `clear ethernet-switching table persistent-learning mac`
   b. After replacing the device connected to the switch port on which security features are enabled, enter the following command:
      `clear ethernet-switching table persistent-learning interface ge-0/0/<x>.0`
      where ***<x>*** is the interface number for which you want to clear the MAC address table.

6.1.13

Changing the WAN IP Address (Juniper)

Procedure:

1. Access the device CLI by opening an SSH session or by using the console cable and terminal emulation software.
2. Log on to the device and enter the appropriate command to check the current WAN IP address:
   a. For SRX3xx router, enter the following command:

      `show configuration interface ge-0/0/5 | display set`

      Step example:

      ```
      motorola@SRX-R01> show configuration interface ge-0/0/5 | display set
      set interfaces ge-0/0/5 unit 0 description "WAN Interface"
      set interfaces ge-0/0/5 unit 0 family inet filter input FILTER_WAN
      set interfaces ge-0/0/5 unit 0 family inet address 10.2.1.42/30
      ```

   b. For SRX345 chassis cluster, enter the following command:

      `show configuration interface reth1 | display set`

      Step example:

      ```
      {primary:node0}
      root@SRX-R01> show configuration interfaces reth1 | display set
      set interfaces reth1 description "Cluster Redundant WAN Interface"
      set interfaces reth1 redundant-ether-options redundancy-group 1
      set interfaces reth1 redundant-ether-options minimum-links 1
      set interfaces reth1 unit 0 description "WAN Interface"
      set interfaces reth1 unit 0 family inet filter input FILTER_WAN
      set interfaces reth1 unit 0 family inet address 10.2.1.6/30
      ```

3. **NOTE:** If WAN interface is not a part of any dynamic routing protocol, then you must update the IP static routes configuration after the change of the WAN IP address.

   To check the current configuration, enter the following command:

   `show configuration routing-options`

   Step example:

   ```
   motorola@SRX-R01> show configuration routing -options | display set
   set routing-options static route 0.0.0.0/0 next-hop 10.2.1.41
   set routing-options router-id 172.30.16.2
   ```

4. Enter the configuration mode by using the `configuration` command and update the WAN IP address by entering the appropriate commands:
   a. For SRX3xx router, enter the following commands:

      ```
      delete interfaces ge-0/0/5  unit 0 family inet address
      <Old_IP_Address/prefix_mask>
      set interfaces ge-0/0/5  unit 0 family inet address <New_IP_Address/
      prefix_mask>
      delete routing-options static route 0.0.0.0/0 next-hop <Old_Nex-
      hope_IP_Address>
      set routing-options static route 0.0.0.0/0 next-hop <New_Nex-
      hope_IP_Address>
      ```

b. For SRX345 chassis cluster, enter the following commands:

```
delete interfaces reth1 unit 0 family inet address <Old_IP_Address/prefix_mask>
set interfaces reth1 unit 0 family inet address <New_IP_Address/prefix_mask>
delete routing-options static route 0.0.0.0/0 next-hop <Old_Nexhope_IP_Address>
set routing-options static route 0.0.0.0/0 next-hop <New_Nexhope_IP_Address>
```

5. After updating the device configuration, check the correctness of the configuration by running the `commit check` command.
6. To apply and save the configuration, run the `commit and-quit` command.

6.1.14

Saving the Rescue Configuration on Juniper Devices

Perform the following steps to save the rescue configuration on Juniper EX switch, SRX router, or SRX345 chassis cluster.

When the current device configuration is a final working configuration, it is recommended to save it in the device special location in case of any configuration problems in the future.

Prerequisites:
The following hardware is required:

- PC with terminal emulation software (for example PuTTY)
- Console cable for console access or Ethernet cable for IP access to the device

Procedure:

1. Access the device CLI by opening SSH session or by using the console cable and terminal emulation software.
2. Log on to the device and enter the following command:

   `request system configuration rescue save`

   CAUTION: Entering this command overrides any older rescue configuration already saved in the device.

   NOTE: If you need to load the rescue configuration, enter the configuration mode and run the following commands:

   ```
   rollback rescue
   commit and-quit
   ```

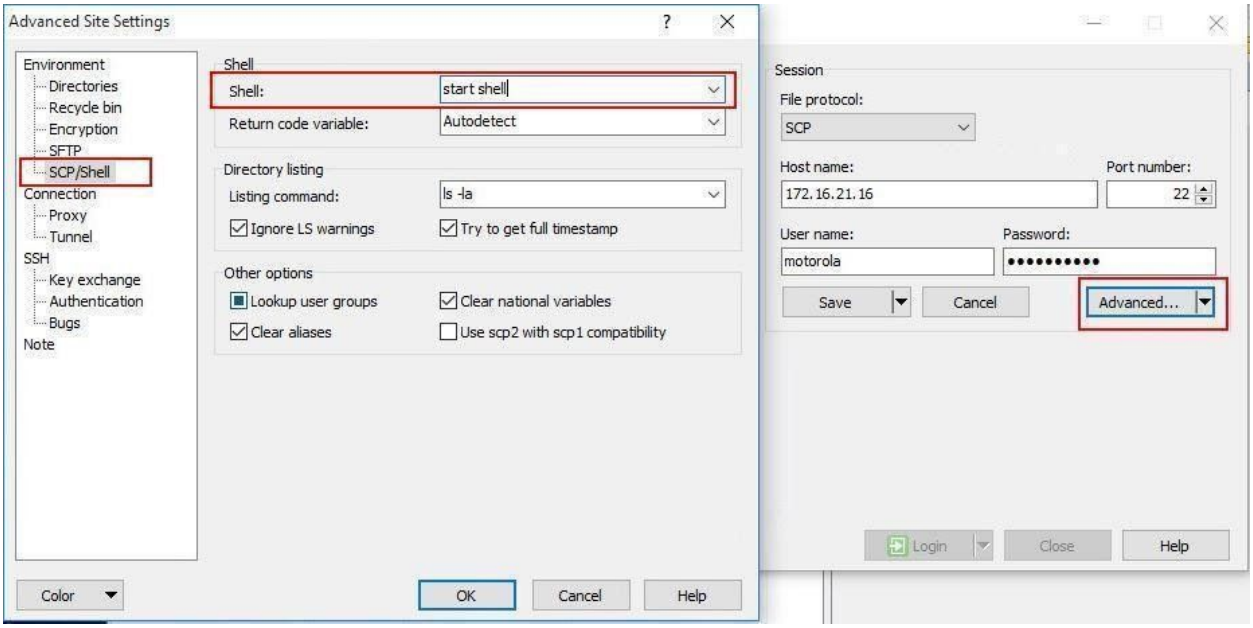
6.1.15

Adjusting WinSCP Configuration for Juniper Devices

Procedure:

To enable logging to a Juniper device by using WinSCP, in the advanced options of device profile configure **start shell**

Figure 233: Start Shell Setting in Advanced Options



6.1.16

Generating Certificates for Juniper SRX Devices

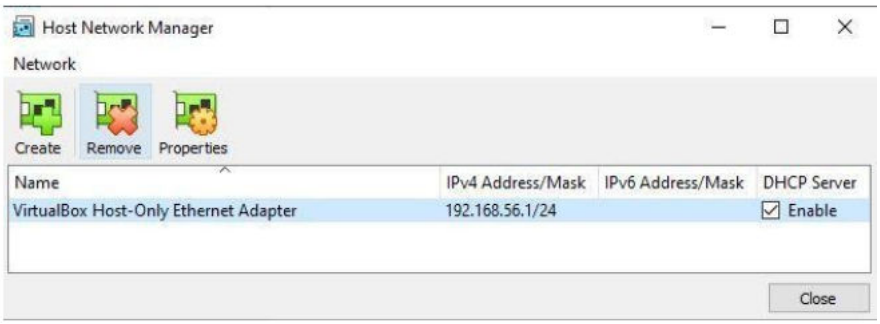
Perform the following procedure to generate certificates for your Juniper SRX devices using a Certificate Authority (CA) server.

Procedure:

1. Download and install VirtualBox application version 6.x from https://download.virtualbox.org/virtualbox.

   The User Manual and the installation file are located in the same folder.
2. Restart the PC before you launch the VirtualBox application.
3. To change the configuration of the network interface that allows communication between the host computer and virtual machines, select **File** → **Host Network Manager** option.

   Figure 234: Host Network Manager



4. Perform one of the following actions:

If...	Then...
If you want to build a new CA server,	perform the following actions: **a.** Create a new Virtual Machine in VirtualBox application. **b.** Install Ubuntu-Linux distribution from an iso file provided by Motorola Solutions. **c.** Prepare the configuration files and generate root certificate.

If...	Then...
If you want to run a precon-figured CA server,	perform the following actions: **a.** To import Ubuntu-Linux distribution from a file provided by Motorola Solutions, select **File** → **Import Virtual Appliance**. The **Appliance settings** window appears. See Figure 235: Appliance Settings Window Visible During Import on page 670. **IMPORTANT:** From the **MAC Address Policy** drop-down list, select **Generate new MAC addresses for all network adapters**. **b.** Start your virtual machine. **c.** Log on to the Linux host by using the VirtualBox console window. The username is `motorola` and the password is `Motorola12` **d.** After providing credentials, the system will force you to change the password for the `motorola` user. The system: ● requires the current password - `Motorola12` ● prompts to enter the new password twice **NOTE:** The new password cannot be the same as the old one. The new password rules: ● at least 10 characters ● at least 1 upper case letter ● at least 1 lower case letter ● at least 1 digit ● at least 3 changes than the old password **e.** From the console prompt, note down the IP address of the Linux host and open the SSH session to this IP address. The IP address is based on the configuration performed in step 3. See Figure 236: Linux Host IP Address on page 671. **f.** Edit `/home/motorola/PCR-CA-01/subalt.txt` file. The default string is `subjectAltName=DNS:customer-a.local`. It can be modified with Fully Qualified Domain Name (FQDN) name or email address reference. For email address, the string pattern is `subjectAltName=email:admin@customer-a.local`. The chosen DNS or email address must match the Juniper SRX configuration.

Figure 235: Appliance Settings Window Visible During Import

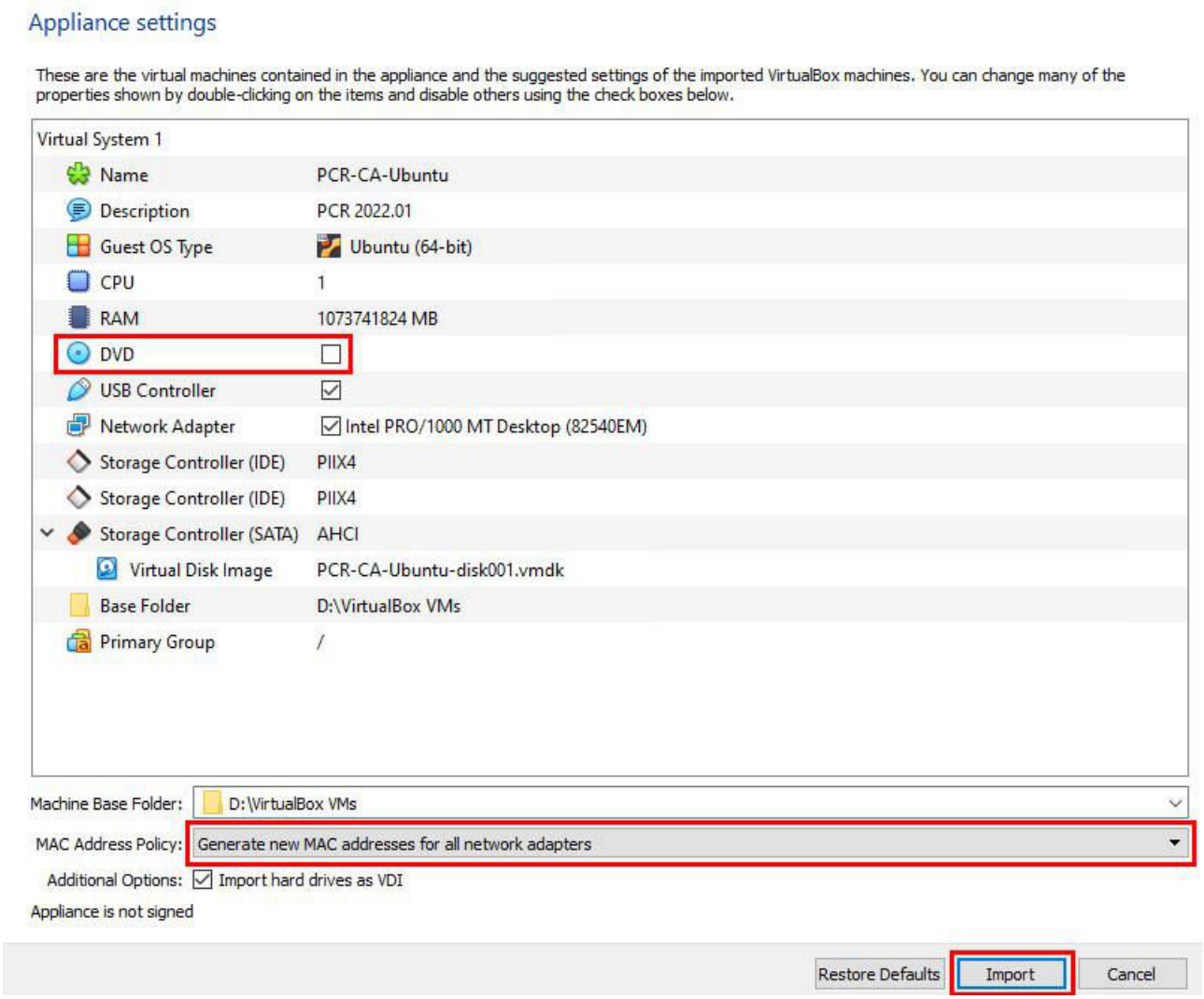
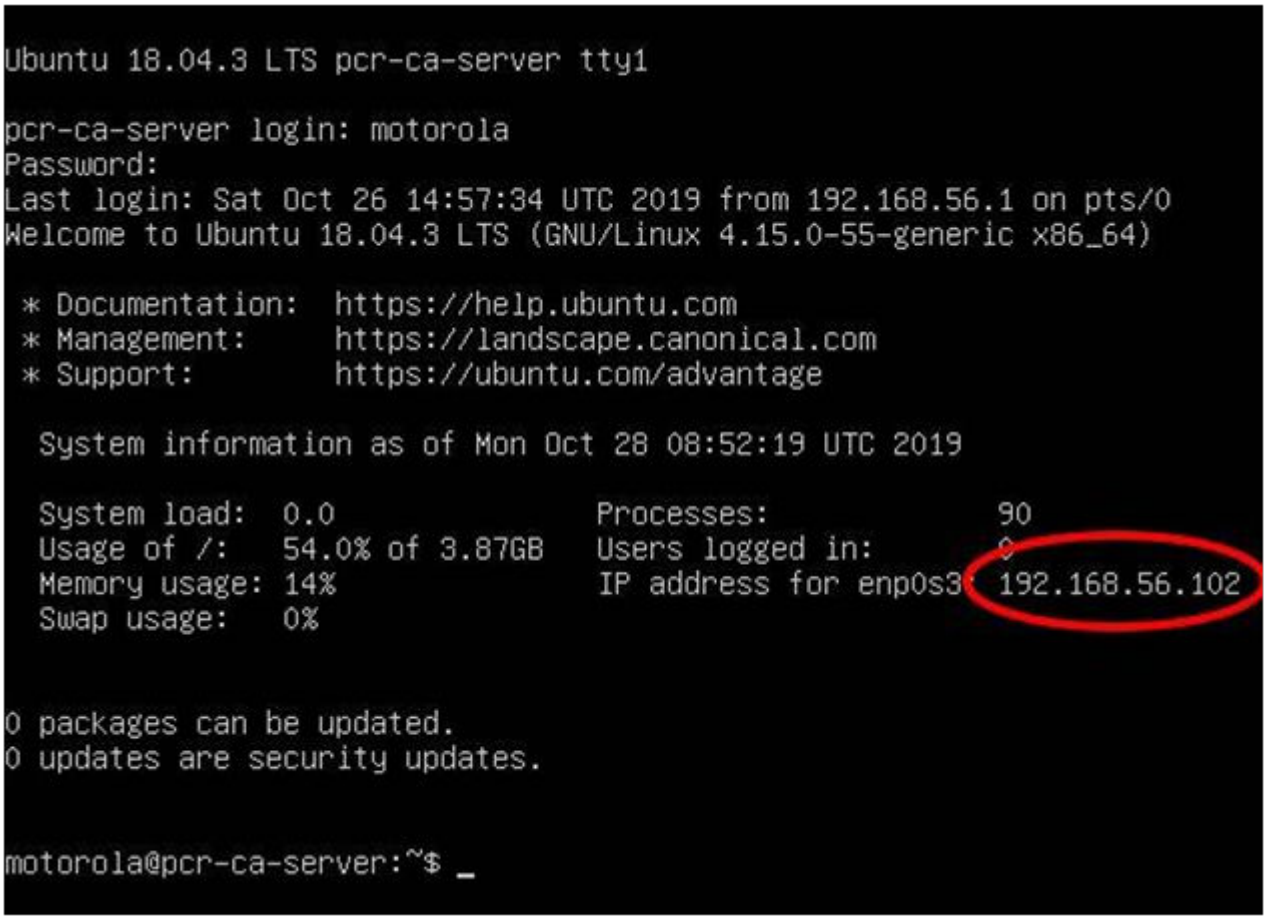


Figure 236: Linux Host IP Address



5. To make a copy of a root CA certificate file from the CA server, download the `cacert.pem` file from the server, using WinSCP tool or a prefered alternative.

   The file is located in `/home/motorola/PCR-CA-01/` folder.

6. For each Juniper SRX device, perform the following actions:

   a. Configure the device to allow network communication to the device.

      For configuration template, see Configuration of Juniper SRX Router to Allow IP Network Communication on page 652.

      NOTE:
      When logging, do not use the `root` username. This is a special build-in account with a different home directory path.

      Alternatively, use USB port to copy files between the device and the CA server.

      For SRX3xx series routers, the path always starts with `/cf` and it needs to be added in all paths presented in this procedure.

   b. In the home directory, create a folder for a local copy of PKI files by entering the following commands:

      i. `start shell`

      ii. `mkdir CA`

      iii. `exit`

   c. Generate private key by entering

`request security pki generate-key-pair type ecdsa size 384 certificate-id` ***<certificate-ID>***
command.

CAUTION: Make sure that ***<certificate-ID>*** string is unique. For example, use `SRX-`***<SN>***`-`***<XX>***, where ***<SN>*** is a serial number of the SRX device, and ***<XX>*** is a subsequent number, in case that more than one certificate for a device is required, as CA does not allow to sign another CSR with the same certificate-ID name.

d. Generate a CSR based on the private key by entering
`request security pki generate-certificate-request certificate-id` ***<certificate-ID>*** `subject "CN=`***<certificate-ID>***`,OU=Base,O=`***<Customer Name>***`,ST=`***<State>***`,C=`***<Country code>***`" domain-name` ***<customer domain name>*** `filename /var/home/`***<user name>***`/CA/`***<certificate-ID>***`.csr`

where `domain-name`***<customer domain name>*** must match the settings from 4.f on page 669

e. Upload ***<certificate-ID>***`.csr` file generated from the SRX device to the CA server.

f. Upload `cacert.pem` file to `/var/home/`***<user name>***`/CA` folder.

g. Configure the profile for root CA certificate by entering the following commands:

i. `configure`

ii. `set security pki ca-profile` ***<root CA name>*** `ca-identity` ***<root CA name>***

iii. `set security pki ca-profile` ***<root CA name>*** `revocation-check disable`

iv. `commit and-quit`

h. Import root CA certificate file by entering
`request security pki ca-certificate load ca-profile` ***<root CA name>***
`filename CA/cacert.pem`

7. Perform the following actions on the CA server:

a. Open SSH session to the CA server.

b. Change folder to `PCR-CA-01` by entering `cd PCR-CA-01`

c. Run
`sudo openssl ca -in` ***<certificate-ID>***`.csr -out certs/`***<certificate-ID>***`.pem -extfile subalt.txt`

The command signs each CSR file and creates the certificate for the SRX device.

d. Copy the signed certificate files from the CA server to each SRX device.

8. To install the signed certificate on each SRX device, run
`request security pki local-certificate load certificate-id` ***<certificate-ID>***
`filename CA/`***<certificate-ID>***`.pem`

9. Check the installed root and device certificates:

a. To check if a correct CA certificate exist, run
`show security pki ca-certificate ca-profile` ***<root CA name>*** `detail`

Step example:

```
Certificate identifier: Ubuntu-CA
  Certificate version: 3
  Serial number: 24530e5e241697bce5c2dfcda870152da2a7d094
  Issuer:
    Organization: PCR-Transport, Organizational unit: PCR-SRX-LAB,
Country: PL,
    State: NON, Locality: Krakow, Common name: PCR-CA
  Subject:
```

```
    Organization: PCR-Transport, Organizational unit: PCR-SRX-LAB,
Country: PL,
    State: NON, Locality: Krakow, Common name: PCR-CA
  Subject string:
    C=PL, ST=NON, L=Krakow, O=PCR-Transport, OU=PCR-SRX-LAB, CN=PCR-CA,
emailAddress=admin@pcr-lab.local
  Validity:
    Not before: 10-26-2019 10:26 UTC
    Not after: 07-14-2034 10:26 UTC
  Public key algorithm: ecdsaEncryption(384 bits)
    04:85:af:a9:e4:aa:ea:12:ef:40:f3:d2:2e:cf:30:75:7a:97:54:88
    f3:c9:2e:73:0c:30:a1:42:e5:b8:cc:9f:c5:b9:3f:0b:e0:76:6f:bb
    9f:c0:9d:6c:97:21:f3:d1:d1:3a:72:3e:4d:42:0a:0a:ad:03:81:94
    d4:fc:03:8a:a7:36:22:12:a4:fe:13:aa:ae:82:eb:d7:e6:7d:cc:72
    24:38:a0:89:de:bc:2b:aa:e5:e2:a9:e5:34:c8:c8:ab:20
  Signature algorithm: ecdsa-with-SHA384
  Fingerprint:
    e5:8d:43:77:63:89:96:71:a3:07:81:5d:bd:51:07:52:ab:ea:69:df (sha1)
    92:8d:43:9a:d0:96:db:04:ce:bf:af:1f:75:8d:98:20 (md5)
```

b. To check if a correct device certificate exists, enter:

`show security pki local-certificate certificate-id` ***<certificate-ID>*** `detail`

Step example:

```
Certificate identifier: SRX-SITE22-ID01
  Certificate version: 3
  Serial number: 00001002
  Issuer:
    Organization: PCR-Transport, Organizational unit: PCR-SRX-LAB,
Country: PL,
    State: NON, Locality: Krakow, Common name: PCR-CA
  Subject:
    Organization: Customer-A, Organizational unit: Base, Country: PL,
    State: NON, Common name: SRX-SITE22-ID01
  Subject string:
    C=PL, ST=NON, O=Customer-A, OU=Base, CN=SRX-SITE22-ID01
  Alternate subject: email empty, customer-a.local, ipv4 empty, ipv6
empty
  Validity:
    Not before: 10-28-2019 15:45 UTC
    Not after: 10-25-2029 15:45 UTC
  Public key algorithm: ecdsaEncryption(384 bits)
    04:05:69:aa:e4:84:c6:91:b4:32:42:85:46:5c:f6:08:e1:01:36:f2
    7a:5d:6b:a4:e4:20:5c:1e:c6:42:1f:85:b0:59:c6:f8:00:29:ee:d4
    00:6e:37:4c:55:b9:b0:9a:d2:60:4a:8a:ee:32:4b:7d:9a:f2:f5:ba
    14:c3:8e:20:2c:9b:02:dd:35:2c:64:09:4f:cb:43:a2:8c:ee:82:fd
    21:bd:07:7d:f9:13:c5:ef:ab:c1:70:38:24:3e:57:f8:1c
  Signature algorithm: ecdsa-with-SHA384
  Fingerprint:
    2d:5a:65:83:77:a0:8d:03:1c:60:cb:b8:c9:51:b6:17:66:e3:78:e4 (sha1)
    48:69:aa:0d:41:ac:0b:23:2c:e1:9e:79:18:16:96:eb (md5)
  Auto-re-enrollment:
```

```
    Status: Disabled
    Next trigger time: Timer not started
```

CAUTION: A device certificate is valid only for the SRX device for which it was requested. It can be installed only once. A certificate installed in the SRX device is saved in a special folder on flash. If the configuration is deleted, the certificate remains valid.
The root CA certificate is bound to the profile in configuration. If this section is deleted from the configuration, the root CA certificate is removed from the installed certificates.

A file with a root certificate used to import remains on flash and can be used again.

6.1.17

Reserving IP Address on DHCP Server in SRX3xx Router

This procedure sets a static IP assignment for a host in the Dynamic Host Configuration Protocol (DHCP) server configuration on Juniper SRX3xx router.

Prerequisites: Ensure the following hardware is available:

- PC with terminal emulation software (such as PuTTY)
- Console cable for console access or Ethernet cable for IP access to the device

Procedure:

1. Access the device CLI by opening Secure Shell (SSH) session or using the console cable and terminal emulation software.
2. Log on to the device.
3. Run the following command:

   ```
   show dhcp server binding
   ```

4. In the output, find the IP-to-MAC address assignment in the VLAN and note the MAC address.

   NOTE: If the output contains more than one assignment, you need to check the host MAC address in another way.

   Step example: : An example of a possible connection (VLAN 30 “Application”):

   ```
   motorola@SRX-SITE1R01> show dhcp server binding
   IP address    Session Id  Hardware address    Expires  State  Interface
   172.20.1.192  1           00:0c:29:a6:e5:5e   86345    BOUND  ge-0/0/0.30
   ```

5. Enter the configuration mode of the device by entering `configure`
6. To set a static IP-to-MAC assignment in DHCP server configuration, enter the following commands:

   ```
   set access address-assignment pool <DHCP_Pool> family inet host
   <Host_Name> hardware-address <Host_MAC_Address>
   set access address-assignment pool <DHCP_Pool> family inet host
   <Host_Name> ip-address
   <Host_IP_Address>
   ```

   where:

   <DHCP_Pool> is the name of the DHCP server pool attached to the IP interface of the SRX router where the host is connected

   <Host_Name> is the name for the host. The name can be anything but it helps identify the host

   <Host_MAC_Address> is a MAC address of the host that is already known or discovered in step 4

<Host_IP_Address> is the IP address to be assigned to the host every time it sends a DHCP request to the server

7. To apply and save the configuration, run `commit and-quit`

   Step example:

   ```
   motorola@SRX-SITE01R01#set access address-assignment pool APP_POOL_1
   family inet host LMR-GW hardware-address 00:0c:29:a6:e5:5e
   motorola@SRX-SITE01R01#set access address-assignment pool APP_POOL_1
   family inet host LMR-GW ip-address 172.20.1.143
   motorola@SRX-SITE01R01# commit and-quit
   configuration check succeeds
   commit complete
   Exiting configuration mode
   ```

8. To clear the old binding from the static IP-to-MAC reservation of the host, run the following command using information from step 4:

   ```
   clear dhcp server binding <Host_Dynamic_IP_Address>
   ```

   Step example:

   ```
   motorola@SRX-SITE01R01> clear dhcp server binding 172.20.1.192
   ```

   IMPORTANT: The current host binding must be cleared. Otherwise it will get the previous dynamically assigned IP address again. Proceed to the next step only after the current host binding is cleared.

9. Force the host to request an IP address from the DHCP server by performing one of the following actions:
   - Restart the host.
   - Restart the Ethernet interface.
   - Disconnect the link.

10. After the host renewed the IP address, check the DHCP server bindings by running the following command:

    ```
    show dhcp server binding
    ```

    Step example:

    ```
    motorola@SRX-SITE01R01> show dhcp server binding
    IP address    Session Id  Hardware address  Expires  State  Interface
    172.20.1.143    2         00:0c:29:a6:e5:5e   85855   BOUND  ge-0/0/0.30
    ```

6.1.18

Enabling the Port Mirroring on Juniper EX Switch

By default, this mirror session exists on the switch but it is disabled not to overload the switch CPU. This session must be disabled after finishing the diagnostic and when the mirrored traffic is no longer needed.

Prerequisites: Ensure you have access to:

- PC with terminal emulation software, for example PuTTY
- Console cable for console access or Ethernet cable for IP access to the device

Procedure:

1. Access the device CLI by opening a Secure Shell (SSH) session or by using the console cable and terminal emulation software.
2. Log on to the device.
3. To check the configuration of the traffic mirror session, run the following command `show configuration forwarding-options analyzer`

   Example:

   ```
   motorola@SRX-SITE01SW1> show configuration forwarding-options analyzer
   inactive: MIRROR-1 {
       input {
           ingress {
               interface IF-APPLICATIONS;
               interface IF-REPEATERS;
               interface ge-0/0/20.0;
           }
           egress {
               interface IF-APPLICATIONS;
               interface IF-REPEATERS;
               interface ge-0/0/20.0;
           }
       }
       output {
           interface ge-0/0/21.0;
       }
   }
   ```

   If there is `inactive:` before `MIRROR-1`, it means this that session is inactive.
4. Optional: Enable the inactive mirror session by entering `configure` and running the `activate forwarding-options analyzer MIRROR-1` command
5. To apply and save the configuration, enter: `commit and-quit`
6. To check the current status of the mirroring session, run the following command `show forwarding-options analyzer`

   Example

   ```
   motorola@SRX-SITE01SW1> show forwarding-options analyzer
     Analyzer name                     : MIRROR-1
     Mirror rate                       : 1
     Maximum packet length             : 0
     State                             : up
     Ingress monitored interfaces      : ge-0/0/20.0
     Egress monitored interfaces       : ge-0/0/20.0
     Output interface                  : ge-0/0/21.0
   ```

   NOTE: Only the active ports from the configured range are displayed.
   If the mirroring session is not needed anymore, you can disable it and apply the configuration.
7. Optional: To disable the active mirror session, preforming the following actions:
   a. Enter the configuration mode by entering `configure`
   b. Run the following command:
      `deactivate forwarding-options analyzer MIRROR-1`
   c. Apply and save the configuration, by running `commit and-quit`

6.2

Maintenance and Troubleshooting for Juniper Infrastructure

CPSM

The maintenance and troubleshooting guide for the Juniper infrastructure in the MOTOTRBO systems are the same as for the Capacity Max system. For more information regarding the Juniper procedures, see “LAN Connection Troubleshooting on a Juniper EX2300 Network Switch” and “Juniper Routers Troubleshooting” in the *Capacity Max System Operations, Troubleshooting, and Maintenance Guide*.

Chapter 7

Sales and Service Support Tools

7.1 Purpose of This Section Testing

This section introduces the standard system layout, identifying each component's role in servicing the system features listed in Module 2. This module is to help the reader understand what devices are needed to support a particular system feature. It will also display the building blocks of the system from a subscriber only system to a mixed mode multi-repeater, data capable system.

7.2 Applications Overview

The three software applications listed below and their associated drivers are available on the CD kit GMVN5141.

Table 119: Applications Overview

Name	Application Overview
Customer Programming Software (CPS)	CPS enables a dealer to program the device's features according to the customer requirements. Navigating around the CPS is now easy and convenient with the addition of a help pane that displays topic-sensitive help instantly without the need to access the online help file.
AirTracer	AirTracer has the ability to capture Over-The-Air digital radio traffic and save the captured data into a file. AirTracer can also retrieve and save internal error logs from MOTOTRBO radios. The saved files can be analyzed by trained Motorola Solutions personnel to suggest improvements in system configurations or to help isolate problems.
Tuner	Tuner is an application to tune and test subscriber and repeater products. Navigating the around the Tuner is now easy and convenient with the addition of a help pane that displays topic-sensitive help instantly without the need to access the online help file.

7.3 Service Equipment

Recommended Test Equipment

The list of equipment contained in the following table includes most of the standard test equipment required for servicing Motorola Solutions portable radios, as well as several unique items designed specifically for servicing this family of radios. The Characteristics column is included so that equivalent equipment can be substituted; however, when no information is provided in this column, the specific Motorola Solutions model listed is either a unique item or no substitution is recommended.

Description	Characteristics	Example	Application
Service Monitor	Can be used as a substitute for items marked with an asterisk (*)	Aeroflex 3920 (www.aeroflex.com), or equivalent	Frequency/deviation meter and signal generator for wide-range troubleshooting and alignment
Digital RMS Multimeter*	100 µV to 300 V 5 Hz to 1 MHz 10 Meg Ohm Impedance	Fluke 179 or equivalent (www.fluke.com)	AC/DC voltage and current measurements. Audio voltage measurements
RF Signal Generator *	100 MHz to 1 GHz -130 dBm to +10 dBm FM Modulation 0 kHz to 10 kHz Audio Frequency 100 Hz to 10 kHz	Agilent N5181A (www.agilent.com), Ramsey RSG1000B (www.ramseyelectronics.com), or equivalent	Receiver measurements
Oscilloscope *	2 Channel 50 MHz Bandwidth 5 mV/div to 20 V/div	Leader LS8050 (www.leaderusa.com), Tektronix TDS1001b (www.tektronix.com), or equivalent	Waveform measurements
Power Meter and Sensor *	5% Accuracy 100 MHz to 500 MHz 50 Watts	Bird 43 Thruline Watt Meter (www.bird-electronic.com) or equivalent	Transmitter power output measurements
RF Millivolt Meter	100 mV to 3 V RF 10 kHz to 1 GHz	Boonton 92EA (www.boonton.com) or equivalent	RF level measurements
Power Supply	0 V to 32 V 0 A to 20 A	B&K Precision 1790 (www.bkprecision.com) or equivalent	Voltage supply

7.4
Documentation

The following section is an overview of documentation and websites provided by Motorola Solutions to support the entire range of products available in the MOTOTRBO system and provide further information about the MOTOTRBO system.

7.4.1
MOTOTRBO Documentation

The following items listed are documentation provided by Motorola Solutions to support the entire range of products available in the MOTOTRBO system.

Table 120: MOTOTRBO Documentation

Motorola Solutions Part Number	Name
GMLN4575D	MOTOTRBO Publications CD
68012003064	DP 4801 / DP 4800 Portable User Guide
68012003065	DP 4801 / DP 4800 Portable Quick Reference Card
68012003066	DP 4601 / DP 4600 Portable User Guide
68012003067	DP 4601 / DP 4600 Portable Quick Reference Card
68012003068	DP 4401 / DP 4400 Portable User Guide
68012003069	DP 4401 / DP 4400 Portable Quick Reference Card
68012003070	DP 4801 / DP 4800 / DP 4601 / DP 4600 / DP 4401 Portable Basic Service Manual
68012003071	DP 4801 / DP 4800 / DP 4601 / DP 4600 / DP 4401 Portable Detailed Service Manual
68012003060	DM 4400 / DM 4401 Mobile User Guide
68012003061	DM 4600 / DM 4601 Mobile User Guide
68012003062	DM 4400 / DM 4401 Mobile Quick Reference Guide
68012003063	DM 4600 / DM 4601 Mobile Quick Reference Guide
68012003037	DM 4400 / DM 4401 / DM 4600 / DM 4601 Mobile Basic Service Manual
68012003036	DM 4400 / DM 4401 / DM 4600 / DM 4601 Mobile Detailed Service Manual
6878362A01	DM 4400 / DM 4401 / DM 4600 / DM 4601 Mobile Installation Manual
6866574D01	DP 340x Quick Reference Guide (Multilingual)
6866574D05	DP 340x User Guide
6866574D02	DP 360x Quick Reference Guide (Multilingual)
6866574D06	DP 360x User Guide
6866574D04	DP 3000 Series Accessory List Leaflet
6866574D35	DP 3000 Series Detailed Service Manual
6866574D29	DP 3000 Series Basic Service Manual

Motorola Solutions Part Number	Name
6866575D33	DM 3000 Series Basic Service Manual
6866575D40	DM 3000 Series Detailed Service Manual
6866575D01	DM 340x Quick Reference Guide (Multilingual)
6866575D05	DM 340x User Guide
6866575D02	DM 360x Quick Reference Guide (Multilingual)
6866575D06	DM 360x User Guide
6866575D04	DM 3000 Series Accessory List Leaflet
6866575D26	DM 3000 Series Installation Manual
6866576D03	DR 3000 Basic Service Manual
6866576D16	DR 3000 Detailed Service Manual
6866576D02	DR 3000 Installation Guide

7.4.2
URL

The URLs listed are websites to provide further information about the MOTOTRBO system.

Table 121: Websites

URL	Name
www.tiaonline.org	TSB-88 – Wireless Communications Systems-Performance in Noise and Interference-Limited Situations, Recommended Methods for Technology-Independent Modeling, Simulation, and Verification
https://mototrbodev.motorolasolutions.com	MOTOTRBO Option Board ADK Development Guide on the MOTODEV Application Developers website.
https://emeaonline.motorolasolutions.com	Motorola Solutions Online website (contains the bandwidth calculation tool for Capacity Plus Multi Site)

Appendix A

Control Station Installation

The Data Revert Channel concept may require careful planning to achieve the expected data message throughput, as described in the loading sections of the MOTOTRBO System Planner. This is especially true as the number of Control Stations in a location is increased to support larger data traffic loads. Poorly designed installations may result in self-inflicted interference. The result of this interference is often corrupted data messages, which increases the number of data message retries. This increase results in an additional load placed on the system.

A.1 Control Stations Configuration Options

The Control Station type is determined by the configuration of the **Data Modem System Type** in the **Control Station** section of the **General/Network** settings in the RM/CPS. There are three available options: **None**, **Digital**, and **Capacity Plus**. When **None** is selected, the radio is not a data modem. When **Digital** is selected, the radio is a Conventional Control Station. When **Capacity Plus** is selected, the radio is a Data Revert Control Station or Trunked Control Station working at Capacity Plus mode. This is a radio-wide feature.

The second configuration step for Control Station is the configuration of the channel on which the Control Station will be listening and receiving data messages. This channel needs to be added in the **Zone** of the **Zone/Channel Assignment** settings in the RM/CPS. When configuring a channel, there are four available options: **Analog**, **Digital**, **Capacity Plus Personality,** and **Capacity Plus Personality (Linked)**. This is a channel-wide feature.

In Table 122: Interaction Between Control Station Modem Type and Channel Type Parameters on page 682 you can find the available combination of those parameters that decide the mode in which the Control Station will be working.

Table 122: Interaction Between Control Station Modem Type and Channel Type Parameters

Data Modem System Type	Channel Type	Control Station Type
Digital	Digital	Conventional
Digital	Capacity Plus Personality*	Invalid
Capacity Plus	Digital	Data Revert
Capacity Plus	Capacity Plus Personality*	Trunked

* Capacity Plus Personality means Capacity Plus Personality or Capacity Plus Personality (Linked).

NOTE: Revert Control Station uses Digital channel type and listens only on one repeater's time slot of the configured frequency, regardless if the repeater is Trunked or Data Revert. In contrast, Trunked Control Station uses Capacity Plus channel type and in the idle state follows with the Rest Channel.

A.2 Data Bearer Service

MOTOTRBO radios support both Unconfirmed and Confirmed Data Bearer Services at Layer 2. The method selected impacts the transmit and receive roles that Revert Control Stations and either primary Control

Stations (Conventional) or Trunked Control Stations (Capacity Plus) play within a system. In turn, these roles can impact the installation.

It should be noted that applications often implement their own confirmations at the application level (Layer 7); therefore the use of the Unconfirmed Data Bearer Service does not require that messages are unconfirmed by the receiving radio.

A.2.1
Unconfirmed Data

When Unconfirmed Data is transmitted, it is transmitted to the receiver once. The receiver checks the integrity of the entire data message (CRC check) and either passes this up to the application (CRC check passes) through the IP layer or discards the data (CRC check fails). The following is an example to highlight the roles played by the Control Stations.

For example, a text message is sent from a text message server to an individual radio in a Capacity Plus system. Here, the text message is routed from the server to a Trunked Control Station. When the Control Station is allowed to transmit the data on the Rest Channel, it is transmitted once. The receiving radio then checks the integrity of the message and if the CRC check passes, the data is passed up to the application. Upon receipt of the text message, the radio's application is required to send an application layer acknowledgment to the server for confirmation. Here, the radio moves to a Data Revert Channel and when allowed, transmits the data once to a Revert Control Station. The receiving Control Station checks the integrity of the message and if the CRC check passes, the data is passed up to the application. If the confirmation is not received by the application on the server, it attempts to retry the message with the same procedure. Therefore, the use of the Unconfirmed Data Bearer Service can be utilized with application layer acknowledgments to provide an end-to-end confirmed data process.

The following is a summary of the transmit and receive roles required of the various Control Stations in the system utilizing Unconfirmed Data.

- Revert Control Station (Conventional and Capacity Plus) – RX Only
- Primary Control Station (Conventional) – TX Only
- Trunked Control Station (Capacity Plus) – TX Only

NOTE: When operating with Unconfirmed Data, the Revert Control Stations may be configured to operate as RX Only.

A.2.2
Confirmed Data

When Confirmed Data is transmitted, it is transmitted to the receiver up to three times. The receiver checks the integrity of each TDMA burst (CRC check) as well as the entire data message (CRC check) and either passes this up to the application (CRC check passes) through the IP layer or responds to the initiating radio that selected bursts or the entire message must be re-sent. Scenarios like retries do not change the TX/RX roles played by the Control Stations. The following describes a first attempt success example.

For example, a text message is sent from a text message server to an individual radio in a Capacity Plus system. Here, the text message is routed from the server to a Trunked Control Station. When the Control Station is allowed to transmit the data on the Rest Channel, it is transmitted. The receiving radio checks the integrity of the bursts and of the message. If the CRC check passes, it transmits a received confirmation burst back to the Trunked Control Station as well as passes the data up to the application. Upon receipt of the text message, the radio's application is required to send an application layer acknowledgment to the server for confirmation. Here, the radio moves to a Data Revert Channel and transmits the data to a Revert Control Station when allowed. The receiving Control Station checks the integrity of the bursts and of the message and if the CRC check passes, it transmits a received confirmation burst back to the radio as well as passes the data up to the application.

The following is a summary of the transmit and receive roles required of the various Control Stations in the system utilizing Confirmed Data.

- Revert Control Station (Conventional and Capacity Plus) – RX and TX
- Primary Control Station (Conventional) – TX and RX
- Trunked Control Station (Capacity Plus) – TX and RX

NOTE: When operating with Confirmed Data, the Revert Control Stations cannot be configured to operate as RX Only.

A.3 Interference

With multiple Control Stations operating in close proximity, it is important to isolate the transmitted signals from the receivers. Typical types of interference to consider are Intermodulation and Desense (Blocking).

A.3.1 Intermodulation

Intermodulation (IM) occurs when two or more off channel signals “mix” in the receiver’s front-end to create a product that falls on the receive channel. This product effectively raises the noise floor of the receiver and dictates a larger received signal to establish an acceptable Signal to Noise Ratio (SNR).

Typical IM protection of the Control Station is around 75 dB. This protection diminishes when one of the interferers is on the adjacent channel. Operating with self-inflicted IM due to frequency selection is not recommended, as TX/RX isolations in excess of 80 dB (depends on interferer level and receiver level) may be required. Adequate frequency planning/selection may resolve this concern.

A.3.2 Desense (Blocking)

Desense or blocking occurs when a very strong off-channel signal begins to saturate the receiver’s front end. This effectively raises the noise floor of the receiver and dictates a larger received signal to establish an acceptable SNR. Typical desense protection of a Control Station is 100 dB. Every installation must take this into consideration when designing the site installation.

A.4 Control Station Installation Considerations

Mitigation techniques require isolating the transmitted signal from the receivers.

There are two general rules for good design:

- Place the receiving Control Station antennas in a location where they receive a strong RF signal from the source.
- Turn down the output power of the transmitting Control Stations to the minimum required power to establish reliable communications.
  A strong receive signal can overcome elevated noise floors without impacting data reliability and turning down the TX power decreases the interfering signals that the receivers must tolerate. These generals rules have only one objective, which is to help achieve acceptable TX/RX isolation within a reasonable budget. However, a stronger receive signal is not always better when IM issues exist. When the issue is caused by third order IM, every one dB of receive path loss degrades the receivers’ sensitivity by one dB and improves IM performance by three dB. Two examples are provided to illustrate this point when IM is not an issue.

50 watts (+47 dBm) of Control Station output power is required, and the typical receiver power level into the Control Station is -115 dBm. The difference between the TX and the RX power is 162 dB. Since the Control Station typically provides 100 dB of blocking protection, 62 dB of TX/RX isolation is required.

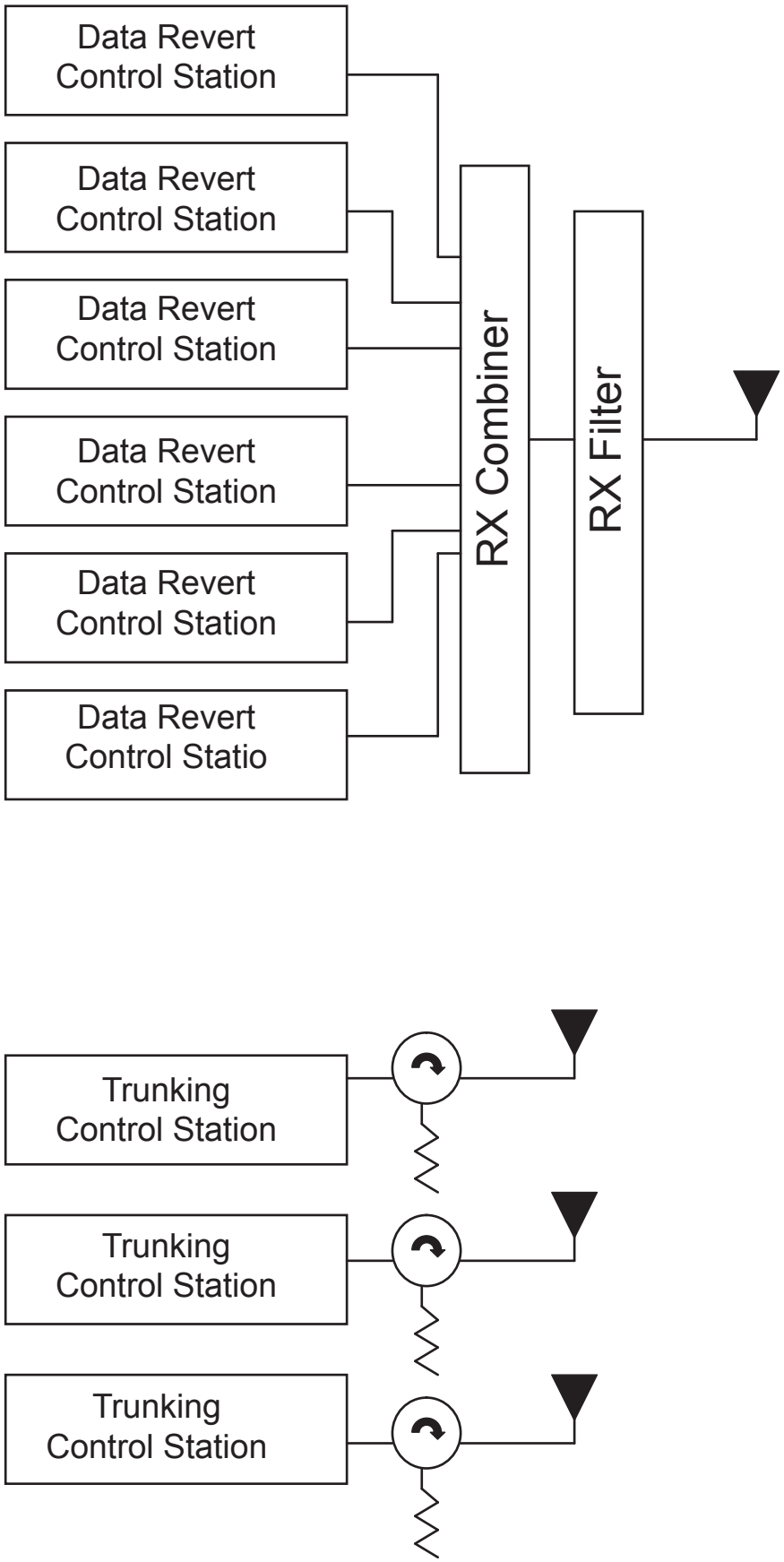
2 watts (+33 dBm) of Control Station output power is required, and the typical receiver power level into the Control Station is -95 dBm. The difference between the TX and the RX power is 128 dB. Since the Control Station typically provides 100 dB of blocking protection, 28 dB of TX/RX isolation is required. This comparatively, is much easier to obtain than in Example 1.

A.4.1
Unconfirmed Data Considerations

The Revert Control Stations only receive and never transmit. Therefore, there are no isolation requirements between these stations. The installation could be as simple as using an individual antenna for each Control Station. The Primary or Trunked Control Stations only transmit and never receive. Therefore, there are no isolation requirements between these stations. The installation could be as simple as using an individual antenna for each Control Station.

However, the Revert and either the Primary or Trunked Control Stations may be in close proximity with each other and there are isolation requirements between these different types of Control Stations. Assuming an IM free frequency plan was selected, the interference to account for is blocking. If the different types of Control Stations must be in close proximity, consider adding an RX bandpass filter to attenuate the TX signals. If an IM free frequency plan is not possible, it is recommended to place circulators on the transmitting Control Stations in order to minimize TX IM. An example of this type of installation is illustrated in the following figure.

Figure 237: Installation of Control Stations for Unconfirmed Data



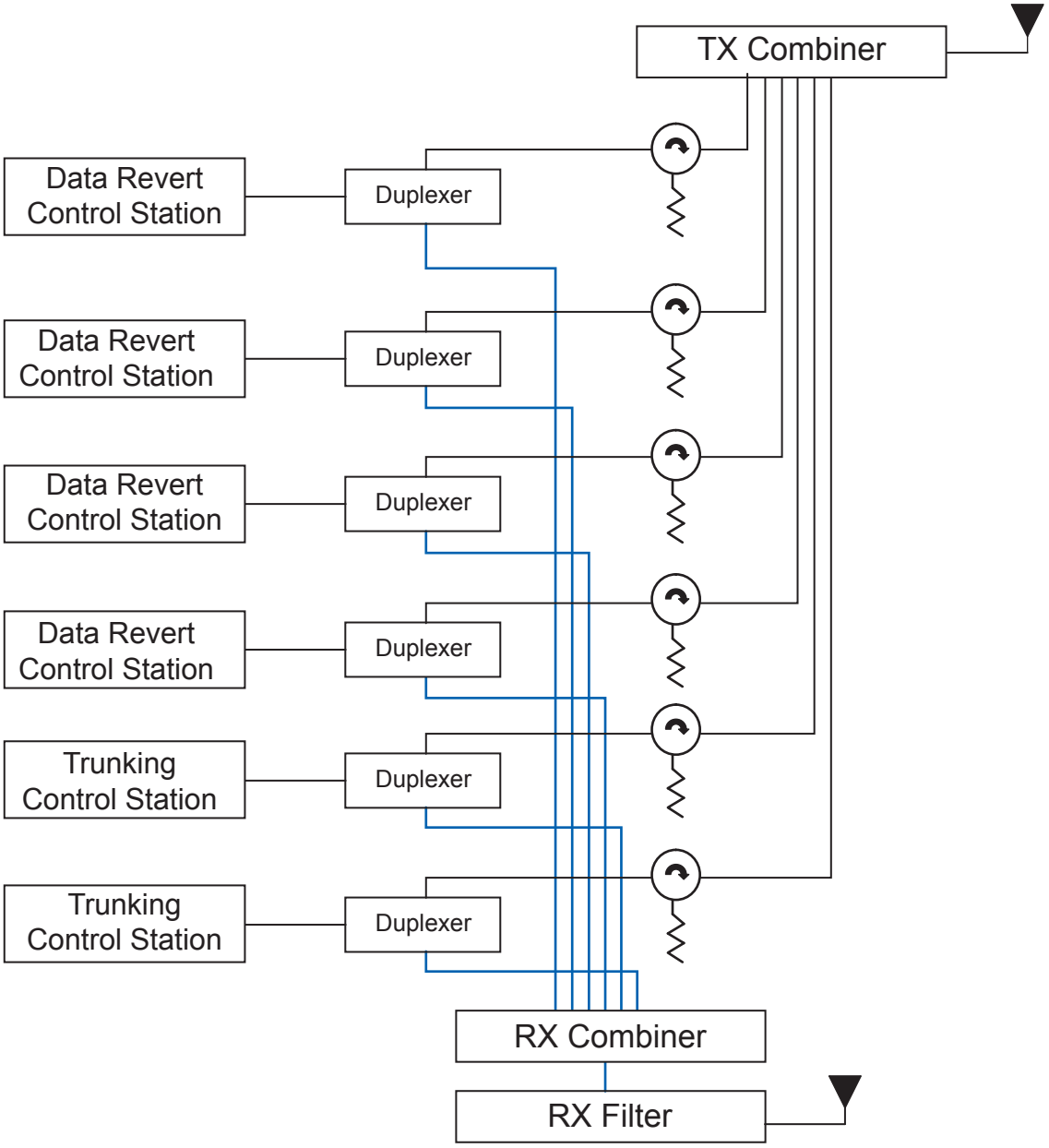
A.4.2

Confirmed Data Considerations

All Control Stations must be both TX and RX. Therefore, there are isolation requirements between all Control Stations and not just different types of Control Stations. Assuming an IM free frequency plan was selected, the interference to design around is blocking. One method is to separate the RX and TX paths of the Revert Control Stations. As these are fixed frequencies, this can be accomplished with a duplexer.

Trunked Control Stations are required to operate on multiple channels and Revert Control Stations are only required to operate on one channel. The properties of the duplexers may differ for the different Control Station types. The same techniques that were applied to Unconfirmed Data can then be applied to Confirmed Data. An example of this type of installation is illustrated in the following figure.

Figure 238: Installation of Control Stations for Confirmed Data



A.4.3

Antenna Separation

One method to provide isolation between the transmitters and the receivers is through antenna separation. The following figures indicate the typical isolation of two dipole antennas when either separated horizontally or vertically.

Figure 239: Horizontal Separation Isolation

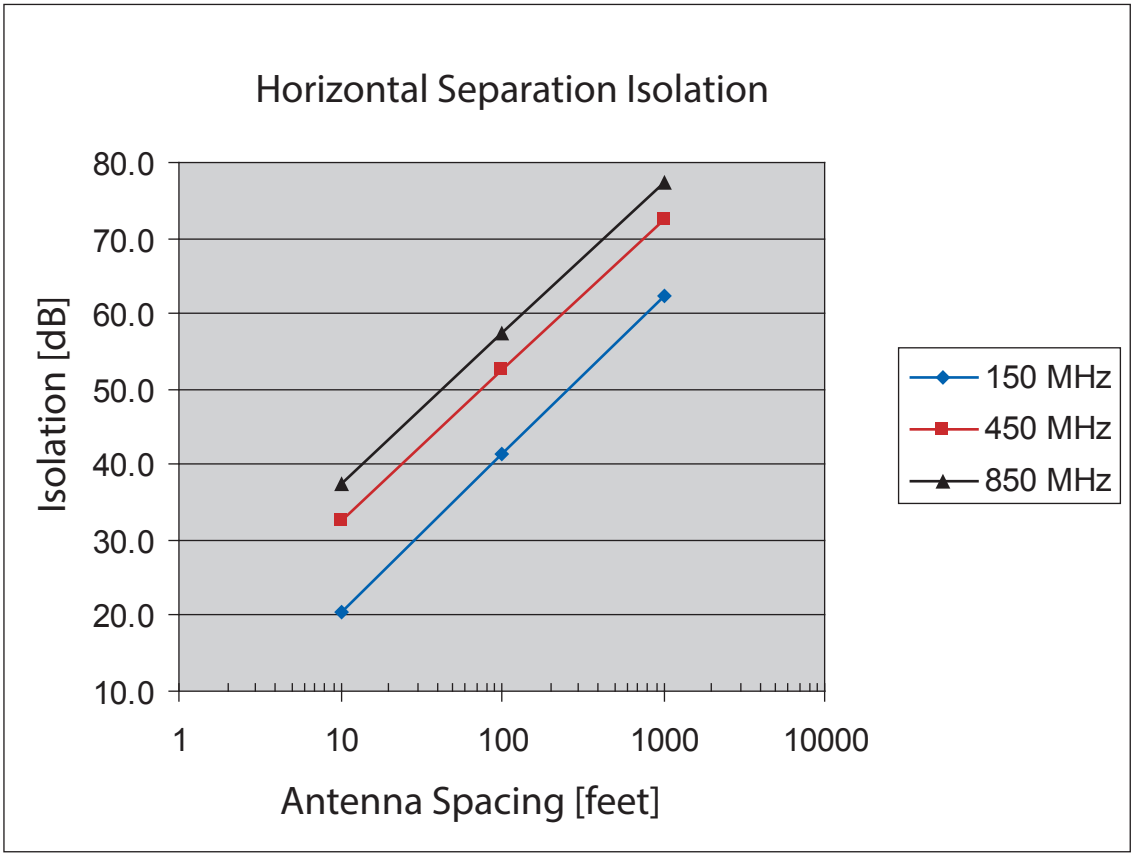
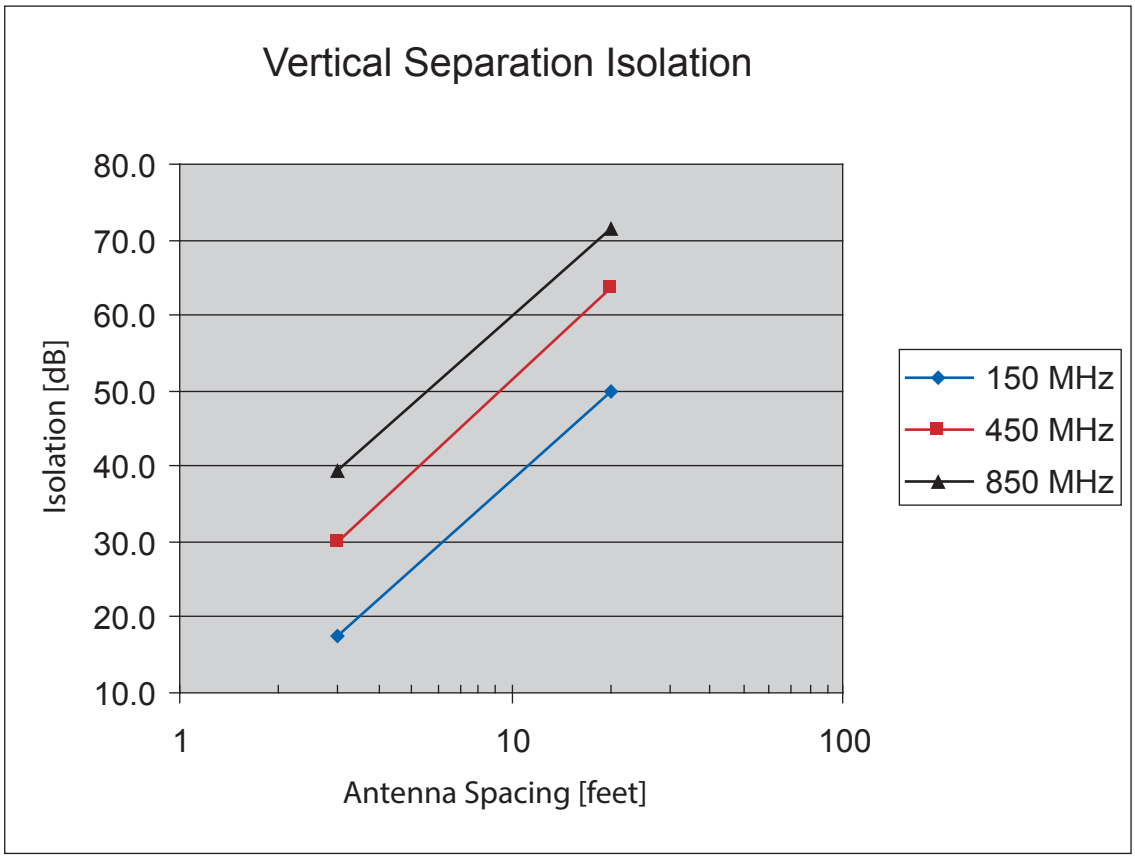



Figure 240: Vertical Separation Isolation