

Data Modem Tethering

Data Modem Tethering Installation Manual

OCTOBER 2023

© 2023 Motorola Solutions, Inc. All Rights Reserved.



MN003449A01-AM

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 non-exclusive, 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 wheellie bin label on the product (or the package in some cases). As defined by the WEEE directive, this crossed-out wheellie 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 centre 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.

© 2023 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.

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
MN003449A01-AA	Initial version of the <i>APX™ Data Modem Tethering Manual</i> .	November 2016
MN003449A01-AB	Updated the manual to include APX Mobile radios.	January 2017
MN003449A01-AC	Updated to include APX Portable radios and Wi-Fi capability	January 2018
MN003449A01-AD	Updated the following sections: <ul style="list-style-type: none">• Motorola Solutions Radios Supported for APX Data Modem Tethering on page 16• Models of Data Routers Supported on page 17• Wi-Fi Configuration for Sierra Wireless Data Modems on page 28• Modem On/Off Button on page 71	May 2019
MN003449A01-AE	Updated the following sections: <ul style="list-style-type: none">• APX Data Modem Tethering Overview on page 16• Motorola Solutions Radios Supported for APX Data Modem Tethering on page 16• Models of Data Routers Supported on page 17• Data Modem Connection Options on page 18• External Data Modem Configuration on page 27• Network Selection on page 70• Modem On/Off Button on page 71• Status Icons on page 78• Table 12: Network Components Required for Broadband on page 80• Figure 66: APX Data Modem Tethering Reference Architecture on page 84• Data Routing That Supports APX Data Modem Tethering on page 86 Added the following content: <ul style="list-style-type: none">• VPN Topologies on page 20• SmartConnect on page 81	December 2019
MN003449A01-AF	Updated the following section: <ul style="list-style-type: none">• Ethernet Configuration on page 22	May 2020
MN003449A01-AG	Updated the following sections: <ul style="list-style-type: none">• Ethernet Configuration on page 22• Broadcast Configuration on page 32	August 2020

Version	Description	Date
	<ul style="list-style-type: none"> • VPN Configuration for MG90 on page 44 <p>Added the following content:</p> <ul style="list-style-type: none"> • WAN Links Friendly Names on page 34 	
MN003449A01-AH	<p>Updated the following sections:</p> <ul style="list-style-type: none"> • Table 3: Motorola Solutions Radios Supported for APX Data Modem Tethering on page 16 • Table 4: Data Modem Supported Interfaces on page 17 • WAN Links Friendly Names on page 34 • Wi-Fi and Ethernet LAN Configuration on page 40 • Port Forwarding Configuration for MG90 on page 43 • VPN Configuration for MG90 on page 44 • Status Icons on page 78 • Architecture That Supports APX Data Modem Tethering on page 83 • Data Routing That Supports APX Data Modem Tethering on page 86 	July 2021
MN003449A01-AJ	<p>Updated the following sections:</p> <ul style="list-style-type: none"> • Motorola Solutions Radios Supported for APX Data Modem Tethering on page 16 • Models of Data Routers Supported on page 17 • Ethernet Configuration on page 22 	August 2021
MN003449A01-AK	<p>Updated the following sections:</p> <ul style="list-style-type: none"> • Broadcast Configuration on page 32 • WAN Links Friendly Names on page 34 • VPN Configuration for MG90 on page 44 • Multiple VPN Configuration on page 46 • Status Icons on page 78 	December 2021
MN003449A01-AL	<p>Added the following sections:</p> <ul style="list-style-type: none"> • Sierra Wireless XR80 and XR90 Modems Configuration on page 46 • Simple Setup on page 46 • Setting Local Area Network (LAN) on page 46 • Configuring the Modem to Use the Bridge on page 47 • Setting Wi-Fi on page 56 • Adding New Users to the Container on page 48 • Enabling Container Usage on page 49 • Adding New Registries on page 50 	August 2023

Version	Description	Date
	<ul style="list-style-type: none">• Creating Images from the Registry on page 51• Container Volume on page 51• Uploading the Container Volume on page 52• Creating the Container Application on page 53• Advanced Setup on page 54• Setting Local Area Network (LAN) on page 55• Configuring the Modem to Use the Bridge on page 55• Setting a Zone on page 57• Setting Monitoring Rules on page 58• Configuring the VPN on page 59• Configuring the Radio to Use the JSON Broadcasts on page 60• Setting the Container to Use MotBridge on page 60• Radio Codeplug Configuration on page 62• Verifying JSON Broadcasts on page 62	
MN003449A01-AM	Updated the following section: Models of Data Routers Supported on page 17	October 2023

Contents

Intellectual Property and Regulatory Notices	2
Contact Us	3
Document History	4
List of Figures	10
List of Tables	12
About APX Data Modem Tethering	13
What Is Covered In This Manual?.....	13
Helpful Background Information.....	13
Related Information.....	13
Chapter 1: Overview of APX Data Modem Tethering	16
1.1 APX Data Modem Tethering Overview.....	16
1.2 Motorola Solutions Radios Supported for APX Data Modem Tethering.....	16
1.3 Models of Data Routers Supported.....	17
1.4 Data Modem Connection Options.....	18
1.5 VPN Topologies.....	20
1.5.1 Site-to-Site Topology.....	20
1.5.2 Remote Access Topology.....	21
1.6 USB Connectivity.....	22
1.7 Ethernet Configuration.....	22
1.8 Supported System Combinations.....	24
1.9 Supported Configurations.....	25
Chapter 2: External Data Modem Configuration	27
2.1 Sierra Wireless (ALEOS) Configuration.....	27
2.1.1 USB Configuration for Sierra Wireless Data Modems.....	27
2.1.2 Telnet Configuration.....	28
2.1.3 Wi-Fi Configuration for Sierra Wireless Data Modems.....	28
2.1.4 Port Forwarding Configuration for Sierra Wireless (ALEOS).....	29
2.1.5 DMZ Usage.....	30
2.1.6 VPN Configuration for Sierra Wireless Modems.....	31
2.2 Sierra Wireless MG90 Configuration.....	32
2.2.1 Broadcast Configuration.....	32
2.2.2 WAN Links Friendly Names.....	34
2.2.3 Cellular WAN Configuration.....	37
2.2.4 Ethernet WAN Configuration.....	38
2.2.5 Wi-Fi and Ethernet LAN Configuration.....	40

2.2.6 Port Forwarding Configuration for MG90.....	43
2.2.7 VPN Configuration for MG90.....	44
2.2.8 Multiple VPN Configuration.....	46
2.3 Sierra Wireless XR80 and XR90 Modems Configuration.....	46
2.3.1 Simple Setup.....	46
2.3.1.1 Setting Local Area Network (LAN).....	46
2.3.1.2 Configuring the Modem to Use the Bridge.....	47
2.3.1.3 Setting Wi-Fi.....	47
2.3.1.4 Adding New Users to the Container.....	48
2.3.1.5 Enabling Container Usage.....	49
2.3.1.6 Adding New Registries.....	50
2.3.1.7 Creating Images from the Registry.....	51
2.3.1.8 Container Volume.....	51
2.3.1.9 Uploading the Container Volume.....	52
2.3.1.10 Creating the Container Application.....	53
2.3.2 Advanced Setup.....	54
2.3.2.1 Setting Local Area Network (LAN).....	55
2.3.2.2 Configuring the Modem to Use the Bridge.....	55
2.3.2.3 Setting Wi-Fi.....	56
2.3.2.4 Setting a Zone.....	57
2.3.2.5 Setting Monitoring Rules.....	58
2.3.2.6 Configuring the VPN.....	59
2.3.2.7 Configuring the Radio to Use the JSON Broadcasts.....	60
2.3.2.8 Setting the Container to Use MotBridge.....	60
2.3.2.9 Radio Codeplug Configuration.....	62
2.3.2.10 Verifying JSON Broadcasts.....	62
2.4 Motorola Solutions VML750 Configuration.....	63
2.4.1 USB Configuration for VML750.....	63
2.4.2 Wi-Fi Configuration for VML750.....	64
2.4.3 Port Forwarding Configuration for VML750.....	66
2.4.4 DMZ Usage.....	67
2.4.5 VPN Configuration for VML750.....	67
Chapter 3: APX Radio User Interface.....	70
3.1 Network Selection.....	70
3.2 Modem On/Off Button.....	71
3.2.1 Turning On the Modem at the Modem Menu Screen.....	74
3.2.2 Turning On the Modem with Modem Button.....	75
3.2.3 Turning Off the Modem Connection.....	76
3.3 Information at the Modem Screen.....	76

3.4 Scenario of Changing from External Router-enabled Channel to External Router-disabled Channel.....	77
3.5 Scenario of Changing from External Router-Enabled Channel to Unprogrammed Channel.....	77
3.6 Scenario of Entering or Exiting Out-of-Range Site.....	77
3.7 Status Icons.....	78
3.8 Types of Data Features Supported By the Radio.....	79
Chapter 4: Agency Applications Network.....	83
4.1 Architecture That Supports APX Data Modem Tethering.....	83
4.2 Data Routing That Supports APX Data Modem Tethering.....	86
4.3 Network Security That Supports APX Data Modem Tethering.....	89
Chapter 5: Implementation of APX Data Modem Tethering.....	91
5.1 APX Radio Data over Broadband Implementation Pre-Planning.....	91
5.2 Expanding a System to Add Broadband for Existing ASTRO 25 Data Services.....	91
5.3 Configuring the Border Router.....	98
5.4 Updating the ACL File.....	102
Chapter 6: Agency Application Network Switches.....	106
6.1 Installing and Configuring X460 Switches.....	106
6.2 Switch Hardware Installation.....	106
6.3 Switch Software: Preparation for Installation/Upgrade.....	106
6.4 General Commands for Working with the Switch.....	108
6.5 Installing XOS and SSH Modules and .XSF on X460 Switch.....	111
6.6 Switch Configuration Backup and Restore.....	116
Chapter 7: APX Data Modem Tethering Troubleshooting.....	117
7.1 Overview of Troubleshooting of APX Data Modem Tethering.....	117
7.1.1 Radio Troubleshooting.....	118
7.1.2 APX Data Modem Tethering Event Logging.....	118
7.1.3 Functional Constraints in the Current Release.....	119
Chapter 8: Recovery of APX Data Modem Tethering.....	120
Chapter 9: Switch Install Log Files.....	121

List of Figures

Figure 1: APX Mobile through the USB.....	18
Figure 2: APX Mobile through the Wi-Fi.....	18
Figure 3: APX Portable through the Wi-Fi.....	19
Figure 4: APX Mobile through the USB Ethernet HUB.....	19
Figure 5: APX Mobile Wired and Six Radios with Wi-Fi Capability.....	19
Figure 6: APX 8500 MP through the Ethernet Faceplate.....	19
Figure 7: Site-to-Site Topology.....	21
Figure 8: Remote Access Topology.....	22
Figure 9: USB Ethernet HUB Cable Assembly.....	23
Figure 10: APX 8500 MP with Ethernet Faceplate.....	24
Figure 11: USB Configuration for Sierra Wireless Data Modems.....	27
Figure 12: Telnet Configuration.....	28
Figure 13: Sierra Wireless Routers Wi-Fi Configuration.....	29
Figure 14: Sierra Wireless Port Forwarding Configuration.....	30
Figure 15: Site-to-Site VPN Configuration.....	32
Figure 16: Status Broadcast Configuration.....	33
Figure 17: Cellular Friendly Name.....	34
Figure 18: Ethernet (Satellite) Friendly Name.....	35
Figure 19: Wi-Fi Friendly Name.....	36
Figure 20: WAN Link Summary.....	36
Figure 21: Cellular WAN Configuration.....	37
Figure 22: Ethernet WAN Configuration.....	39
Figure 23: Ethernet LAN Configuration.....	40
Figure 24: LAN Segment Configuration Window.....	41
Figure 25: Wi-Fi LAN Access Points.....	42
Figure 26: Wi-Fi LAN Access Points Configuration.....	43
Figure 27: MG90 Port Forwarding Configuration.....	44
Figure 28: MG90 VPN Configuration 1.....	45
Figure 29: Configuring LAN.....	47
Figure 30: Configuring SSID.....	48
Figure 31: Create User Configuration.....	49
Figure 32: Users.....	49
Figure 33: Container Usage.....	49
Figure 34: New Registry Configuration.....	50
Figure 35: Registry Access.....	50
Figure 36: Images.....	51

Figure 37: Container Volume.....	53
Figure 38: Container Application Configuration.....	54
Figure 39: Containers Status.....	54
Figure 40: Setting LAN.....	55
Figure 41: Configuring Ethernet 1 and Ethernet 2.....	56
Figure 42: Configuring Ethernet 3.....	56
Figure 43: Configuring LAN.....	57
Figure 44: Configuring SSID.....	57
Figure 45: Setting a Zone.....	58
Figure 46: Monitoring Rules.....	59
Figure 47: IPsec Tunnels.....	60
Figure 48: LAN Segment Configuration for the Container.....	61
Figure 49: Containers Status.....	61
Figure 50: Radio Codeplug Configuration for Using the Modem.....	62
Figure 51: USB Configuration for VML750.....	64
Figure 52: VML750 Wi-Fi Configuration (General).....	65
Figure 53: VML750 Wi-Fi Configuration (AP Basic).....	65
Figure 54: VML750 Wi-Fi Configuration (AP Security).....	66
Figure 55: VML750 Port Forwarding Configuration.....	67
Figure 56: VML750 Remote Access VPN Tunnel Mode Configuration.....	68
Figure 57: VML750 Site-to-Site VPN Tunnel Mode Configuration.....	69
Figure 58: APX Mobile O2 Control Head Programmable Buttons.....	72
Figure 59: APX Mobile O3 Control Head Programmable Buttons.....	72
Figure 60: APX Mobile O5 Control Head Programmable Buttons.....	72
Figure 61: APX Mobile O7 Control Head Programmable Buttons.....	73
Figure 62: APX Mobile O9 Control Head Programmable Buttons.....	73
Figure 63: APX Mobile Keypad Mic Programmable Buttons.....	73
Figure 64: APX Portable Programmable Buttons.....	74
Figure 65: APX Mobile E5 Control Head Programmable Buttons.....	74
Figure 66: APX Data Modem Tethering Reference Architecture.....	84
Figure 67: APX Radio LMR Data Path.....	87
Figure 68: APX Radio Broadband Data Path.....	88
Figure 69: Single APN for Sierra Wireless Router.....	89
Figure 70: Extreme Switch Voucher.....	114

List of Tables

Table 1: Motorola Solutions Documentation.....	13
Table 2: Non-Motorola Solutions Documentation.....	14
Table 3: Motorola Solutions Radios Supported for APX Data Modem Tethering.....	16
Table 4: Data Modem Supported Interfaces.....	17
Table 5: APX Mobile radio to external router cable options.....	22
Table 6: APX Mobile radio to external router cable options.....	23
Table 7: APX 8500 MP with Ethernet Faceplate connectivity.....	24
Table 8: Supported Configurations for APX Data Modem Tethering over Broadband.....	25
Table 9: Network Selection between LMR and a Single Broadband WAN.....	70
Table 10: Network Selection between LMR and a Modem with Cellular and Satellite WANs.....	71
Table 11: MG90.....	78
Table 12: Network Components Required for Broadband.....	80
Table 13: X460 Switch Configuration File Types.....	107
Table 14: Basic Commands for Switch Install, Upgrade, and Backup and Restore.....	108
Table 15: Troubleshooting Instructions for APX Data Modem Tethering.....	117
Table 16: Resources for APX Data Modem Tethering Centralized Logging Configuration.....	118
Table 17: Resources for Recovery of APX Data Modem Tethering.....	120

About APX Data Modem Tethering

The APX™ Data Modem Tethering manual provides descriptions, architecture, and implementation for router tethering services in a converged Broadband/ASTRO network.

What Is Covered In This Manual?

This manual contains the following chapters:

- [Overview of APX Data Modem Tethering on page 16](#) provides an overview of data services, network architecture, implementation, recovery, and troubleshooting information for APX™ Data Modem Tethering.
- [Agency Applications Network on page 83](#) describes the agency architecture used for APX™ Data Modem Tethering solution.
- [Implementation of APX Data Modem Tethering on page 91](#) includes the processes and procedures required to implement APX™ Data Modem Tethering.
- [Agency Application Network Switches on page 106](#) provides information and procedures for installing the Extreme Networks Summit X460 switches.
- [APX Data Modem Tethering Troubleshooting on page 117](#) provides troubleshooting information for the expansion feature that adds the Broadband network capability for APX™ Data Modem Tethering.
- [Recovery of APX Data Modem Tethering on page 120](#) includes information about the recovery of network elements used for the APX™ Data Modem Tethering feature.

Helpful Background Information

Motorola Solutions offers various courses designed to help with learning about the system. For information, go to <http://www.motorolasolutions.com/training>.

Related Information

See the documents in the table for information about the Public Safety LTE network and the ASTRO® 25 system.

Unless otherwise specified, the Motorola Solutions documents listed here are available from Motorola Online at <http://businessonline.motorolasolutions.com>

If you are new to Motorola Online, follow the on-screen instructions to sign up for an account. To access Public Safety LTE infrastructure manuals, select **Resource Center Product Information** → **Manuals** → **Private Broadband Solutions** and select the appropriate release. To access ASTRO® 25 system manuals, select **Resource Center Product Information** → **Manuals** → **Network Infrastructure** and select the appropriate release.

The Resource Center also provides a search function.

Table 1: Motorola Solutions Documentation

Related Information	Purpose
<i>APX User Guide</i>	Provides basic operation of the radio including Over-The-Air Programming and Text Messaging.
<i>ASTRO 25 Advanced Messaging Solution Server Installation Guide</i>	Installation of the Advanced Messaging Solution Server needed for Text Messaging.

Related Information	Purpose
<i>ASTRO 25 Advanced Messaging Solution Server Provisioning Guide</i>	Provisioning of the Advanced Messaging Solution Server needed for Text Messaging.
<i>Enterprise OS Software Reference Guide</i>	Detailed information about commands and syntax needed for configuring the ASTRO 25® System Border Router.
<i>Enterprise OS Software User Guide</i>	Provides information about how to use Enterprise OS (EOS) needed for configuring the ASTRO® 25 System Border Router.
<i>Key Management Facility</i>	Provides descriptive and procedural information about the Key Management Facility (KMF) such as configuration and information. This manual should be used in conjunction with the <i>Secure Communications — System Perspective</i> manual.
<i>KVL 4000 Key Variable Loader ASTRO 25 User Guide</i>	Provides instructions for using the Key Variable Loader (KVL) to create and store encryption keys, and then load them into other Motorola Solutions equipment such as the radio, Mobile VPN Gateway or Key Management Facility.
<i>Mobile VPN Gateway</i>	Provides overviews, installation, and configuration for the Motorola Solutions Mobile VPN Gateway for secure data over LTE.
<i>Motorola Network Router (MNR) S6000 Hardware User Guide</i>	Provides hardware information for the ASTRO® 25 Border Router.
<i>Public Safety LTE System Overview</i>	Provides a detailed description of the overall Public Safety Long Term Evolution (PS LTE) system offering.
<i>Public Safety LTE Disaster Recovery</i>	Contains processes and procedures to support disaster recovery activities for the Public Safety LTE system.
<i>Public Safety LTE Glossary</i>	Contains a list of Public Safety LTE acronyms.
<i>Secure Communications — System Perspective</i>	Provides overviews, configuration, performance, and troubleshooting information for ASTRO® 25 secure voice and data.
<i>Standards and Guidelines for Communication Sites</i>	Provides standards and guidelines to follow when setting up a Motorola Solutions communications site. Also known as the R56 manual. This manual may be purchased on CD 9880384V83 by calling North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
<i>Unified Network Services Software Implementation Guide Unified Network Services Software Installation and Administration Guide</i>	Describes the installation, operation, and technical aspects of the Unified Network Services (UNS) needed for Presence Service and Location Service.
<i>Unified Network Services Configuration Manager User Guide</i>	Provides instructions for the user interface for configuring UNS at the server level including Presence Service and Location Service.

Table 2: Non-Motorola Solutions Documentation

Related Information	Purpose
Extreme X460 (Summit) switch documentation at: http://documentation.extremenetworks.com/summit/downloads/	The Extreme switches are required for the North Routers and South Routers in the Motorola Solutions-defined agency architecture for this solution.

Related Information	Purpose
Extreme XOS Concept Guide at : http://extrcdn.extremenetworks.com/wp-content/uploads/2014/04/ExtremeXOS-15.5-User-Guide.pdf	XOS is the operating system for the Extreme switches.
Fortinet FortiGate documentation at: http://docs.fortinet.com/fortigate/hardware	The Fortinet firewall is required for the LTE path for this solution.

Chapter 1

Overview of APX Data Modem Tethering

This chapter provides an overview of data services, network architecture, implementation, recovery, and troubleshooting information for APX™ Data Modem Tethering.

1.1

APX Data Modem Tethering Overview

APX™ Data Modem Tethering enable users to send and receive broadband data while simultaneously using the Land Mobile Radio (LMR) voice channel.

APX radios operate on LMR networks while simultaneously utilizing an external Motorola Solutions VML750 R3.1 (or later) or a Sierra Wireless router, delivering fast and efficient data operation along with mission critical LMR voice connectivity. Using broadband via an attached external router, the radio transmits and receives data faster than with standard LMR technology. With the radio in separate broadband and LMR modes, users can receive data while simultaneously using the LMR voice channel. A Virtual Private Network (VPN) Gateway is optionally available for secure communication on the Broadband air interface with Motorola Solutions VML or the Sierra Wireless routers.

APX Data Modem Tethering supports the following data services:

- Location
- Presence
- Text Messaging
- Over-The-Air Programming (OTAP) including Firmware download
- Over-The-Air Re-keying (OTAR)
- SmartConnect

For more information see [Types of Data Features Supported By the Radio on page 79](#).

1.2

Motorola Solutions Radios Supported for APX Data Modem Tethering

Table 3: Motorola Solutions Radios Supported for APX Data Modem Tethering

Model	Type	USB	Ethernet HUB	Wi-Fi	Ethernet
APX 1000BN	Portable	✗	✗	✓	✗
APX 1500BN	Mobile	✓	✓	✗	✗
APX 2500BN	Mobile	✓	✓	✓	✗
APX 4500	Mobile	✓	✓	✗	✗
APX 4500BN	Mobile	✓	✓	✓	✗
APX 6000BN	Portable	✗	✗	✓	✗

Model	Type	USB	Ethernet HUB	Wi-Fi	Ethernet
APX 6500	Mobile	✓	✓	✗	✗
APX 6500BN	Mobile	✓	✓	✓	✗
APX 7500	Mobile	✓	✓	✗	✗
APX 8000	Portable	✗	✗	✓	✗
APX 8500	Mobile	✓	✓	✓	✓ ¹
SRX 2200	Portable	✗	✗	✓	✗

The Data Modem Tethering feature on the radio can only be used if:

- They are enabled for Data Modem Tethering.
- Supported versions of system and device software have been installed in the network.
- Transport equipment configuration changes have been made.
- They are enabled for Wi-Fi or are tethered to a modem with an Ethernet cable or a USB Host to Micro USB Device cable (APX Mobiles only).
- Data service and other implementation tasks have been completed. See [Expanding a System to Add Broadband for Existing ASTRO 25 Data Services on page 91](#).
- The modem is enabled from the codeplug in the Data Wide **External Data Modem** tab.

The radios do not automatically detect the release of the system. Therefore, program the radio codeplugs to disable Data Modem Tethering on systems not certified with the solution.

1.3

Models of Data Routers Supported

Table 4: Data Modem Supported Interfaces

Modem	USB	Ethernet HUB	Wi-Fi	VPN	VPN with Clear Bypass	Maximum Radio Connection	Ethernet
Sierra Wireless XR80, XR90	✗	✓	✓	Site-to-Site (required)	✓	7 ²	✓
Sierra Wireless MG90	✗	✓	✓	Site-to-Site (required)	✓	7 ²	✓
Sierra Wireless GX450, MP70, RV55	✓	✗	✓	Site-to-Site (optional)	✓	1	✗

¹ Only applicable to APX 8500 MP.

² One Ethernet and six Wi-Fi connections.

Modem	USB	Ethernet HUB	Wi-Fi	VPN	VPN with Clear Bypass	Maximum Radio Connection	Ethernet
(ALEOS interface)							
VML470	✓	✗	✓	Site-to-Site (required)	✗	7 ³	✗
				Remote-Access (optional)		1	
Generic Modems	✗	✓	✗	Site-to-Site (Optional)	✓	1 ⁴	✗

1.4

Data Modem Connection Options

The availability of USB and Wi-Fi connections presents many options to the user for deploying radios and external routers.

Figure 1: APX Mobile through the USB

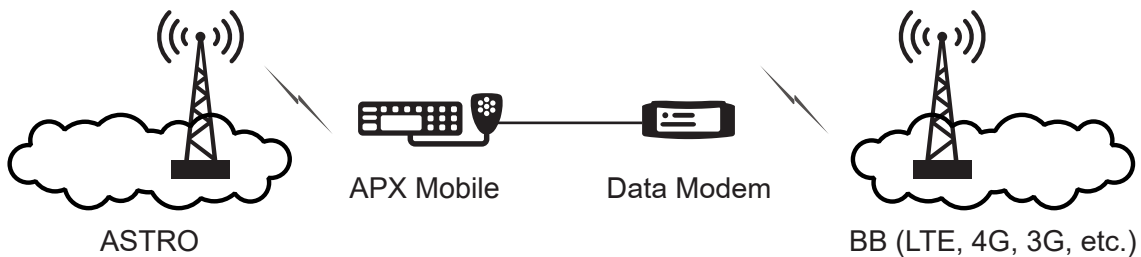
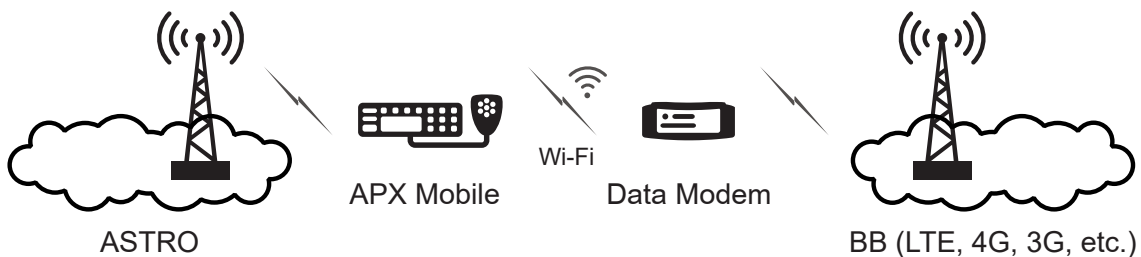


Figure 2: APX Mobile through the Wi-Fi



³ One USB and six Wi-Fi connections.

⁴ Generic Modems are used for SmartConnect only. Smartconnect is only supported on radios that also support Wi-Fi.

Figure 3: APX Portable through the Wi-Fi

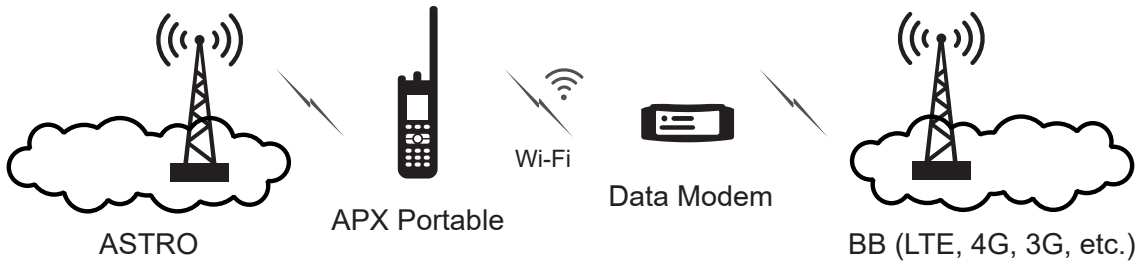


Figure 4: APX Mobile through the USB Ethernet HUB

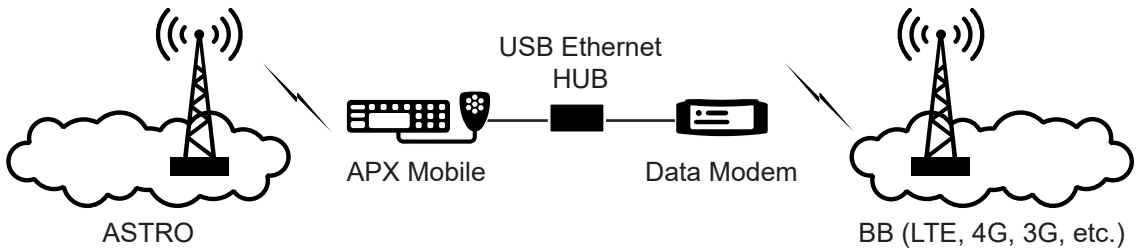


Figure 5: APX Mobile Wired and Six Radios with Wi-Fi Capability

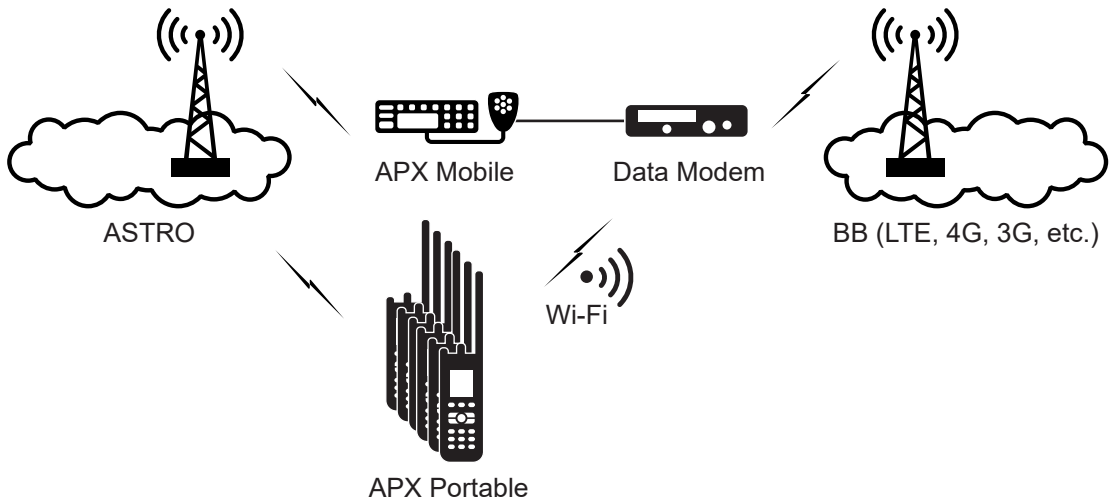
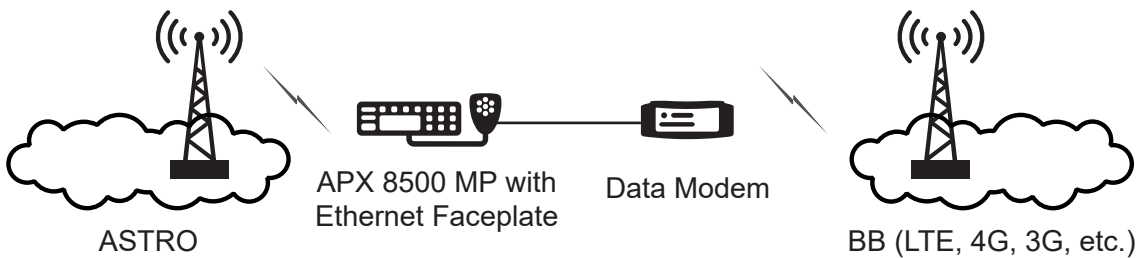


Figure 6: APX 8500 MP through the Ethernet Faceplate



1.5

VPN Topologies

The APX radio utilizes the router's VPN solution when operating in secure mode over the Broadband network.

Selective BYPASS of the VPN tunnel is not supported, so all the incoming and outgoing traffic from the radio is routed through the VPN tunnel if the external router is configured with VPN solution. This solution has been certified to work with Motorola Solutions Mobile VPN Gateway.



NOTE: Smartconnect does not use the VPN tunnel but connects directly to the Microsoft Azure cloud.

1.5.1

Site-to-Site Topology

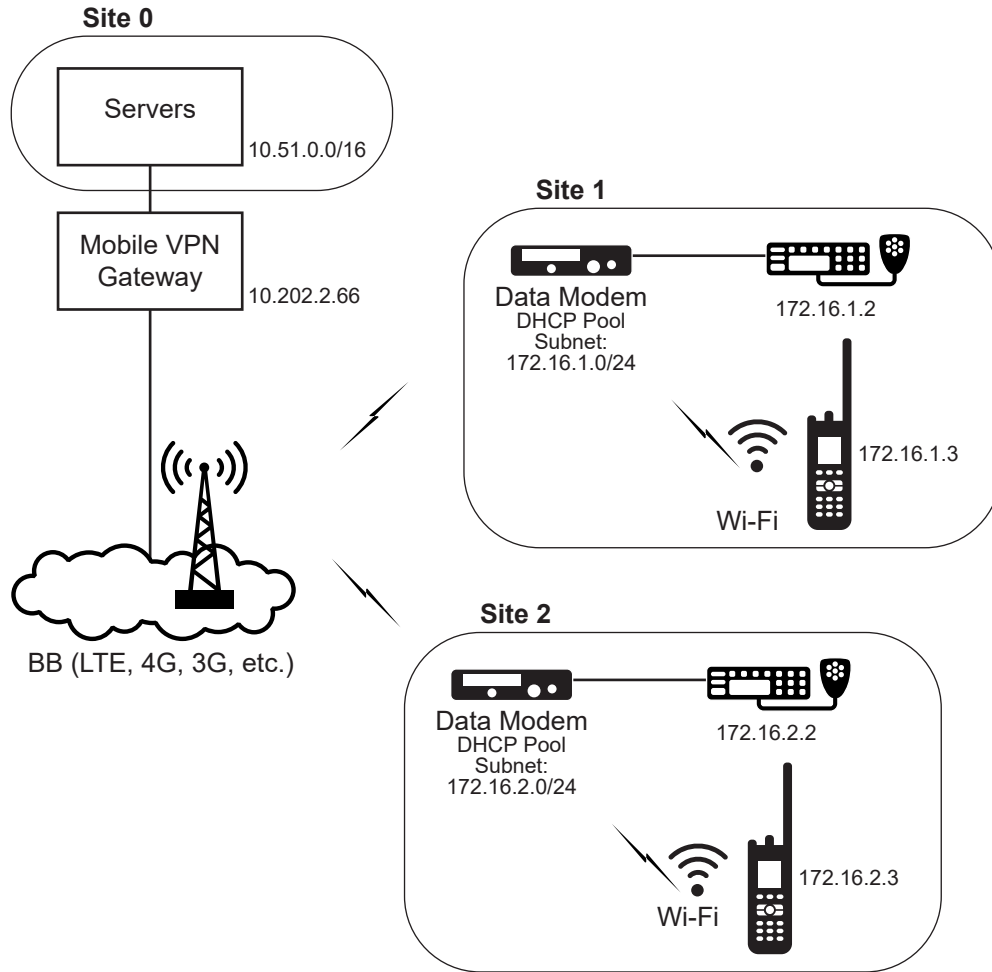
A site-to-site setup is where two (or more) different networks are connected together using one VPN tunnel. In this connection model, devices in one network can reach devices in the other network, and also the other way around.

In this Data Modem Tethering topology, a site is defined as the collection of APX radios that are connected to a single Data Modem. The collection of servers that exist in the CEN (Customer Enterprise Network) defines the other site. The following figure shows that Site 1 and Site 0 form a Site-to-Site VPN tunnel, and a second VPN tunnel is created between Site 2 and Site 0. Take note of the following example of site subnets:

- 10.51.0.0/16 for Site 0
- 172.16.1.0/24 for Site 1
- 172.16.2.0/24 for Site 2

The collection of APX radios at a given site varies from one to seven based on the Data Modem in use and connection method.

Figure 7: Site-to-Site Topology



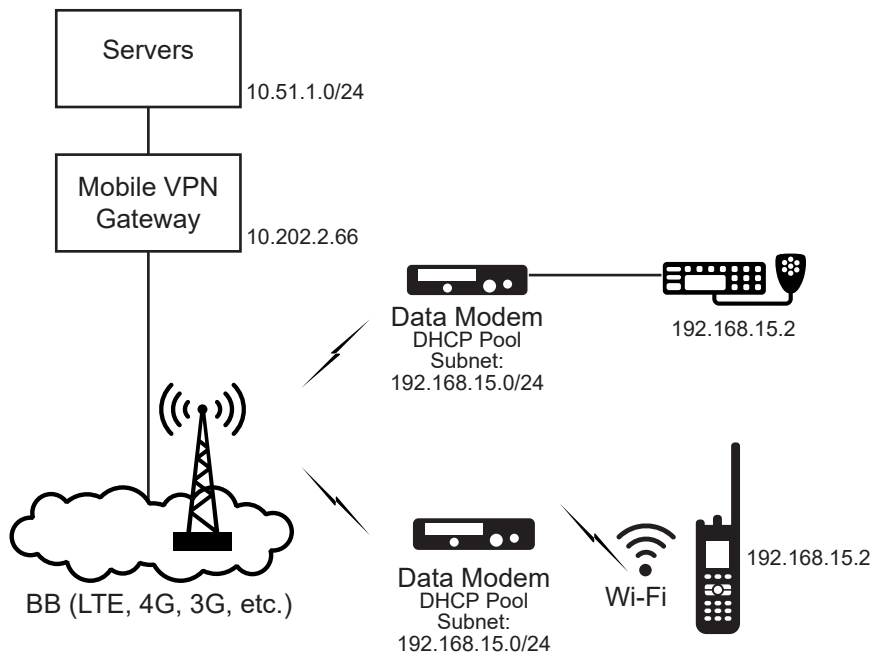
1.5.2

Remote Access Topology

A remote-access VPN allows individual device to establish secure connections with a remote computer network.

In this Data Modem Tethering topology, a single APX radio connects through a data modem to gain remote access to the servers which are hosted in the CEN (Customer Enterprise Network). Take note that a traditional LAN is configured between the Data Modems and the singular radios with the 192.168.15.0/24 subnet.

Figure 8: Remote Access Topology



1.6 USB Connectivity

APX Mobile radio supports a USB Host to Micro USB Device cable to connect to a third party router. The following cable options are available for connecting an APX Mobile radio to an external router:

Table 5: APX Mobile radio to external router cable options

Kit Number	Description
KT000251A02	Cable Assembly, MAP to micro-USB 1.5 m
KT000251A01	Cable Assembly, MAP to micro-USB 4.5 m
KT000252A02	Cable, GCAI to micro-USB

The protocol being used for establishing an IP connection to the third party router is RNDIS and DHCP. The APX radio behaves as RNDIS Host and DHCP Client and the third party router must be setup to be a RNDIS Device and DHCP Server.

1.7 Ethernet Configuration

APX Mobile radio supports a USB Ethernet HUB Cable Assembly to connect to a Sierra Wireless MG90. The APX Mobile radio also supports and Ethernet Faceplate for direct connectivity to the Data Modem.

The following converter box is available for connecting an APX Mobile radio to an external router:

Figure 9: USB Ethernet HUB Cable Assembly

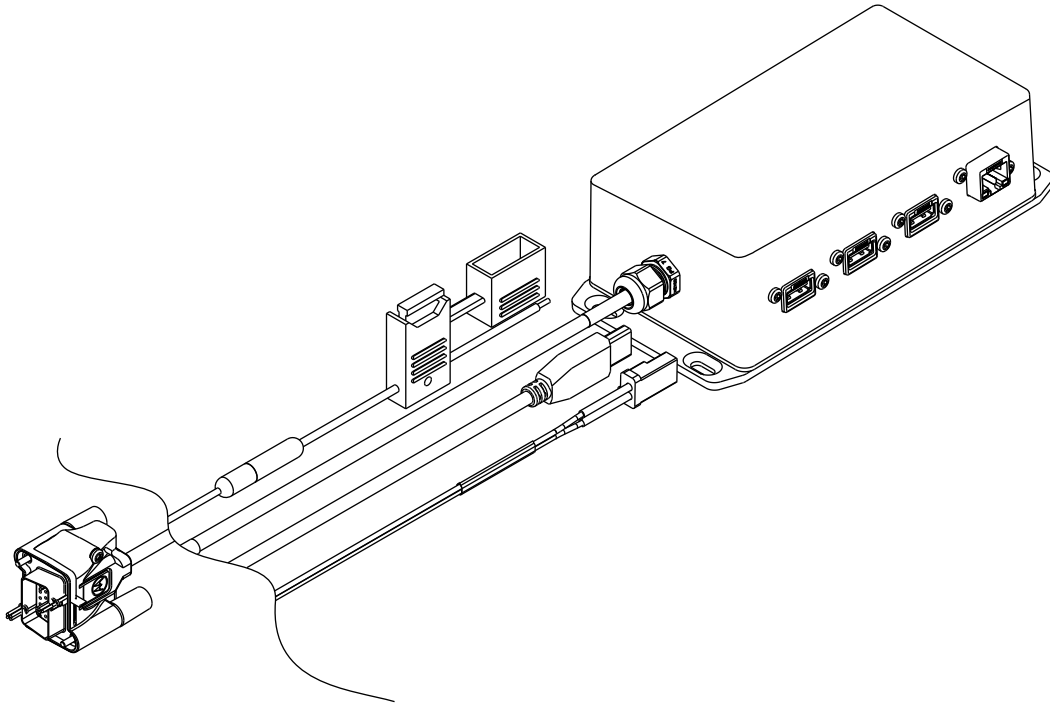


Table 6: APX Mobile radio to external router cable options

Kit Number	Description
KT000259A01	USB Ethernet HUB Cable Assembly

Figure 10: APX 8500 MP with Ethernet Faceplate

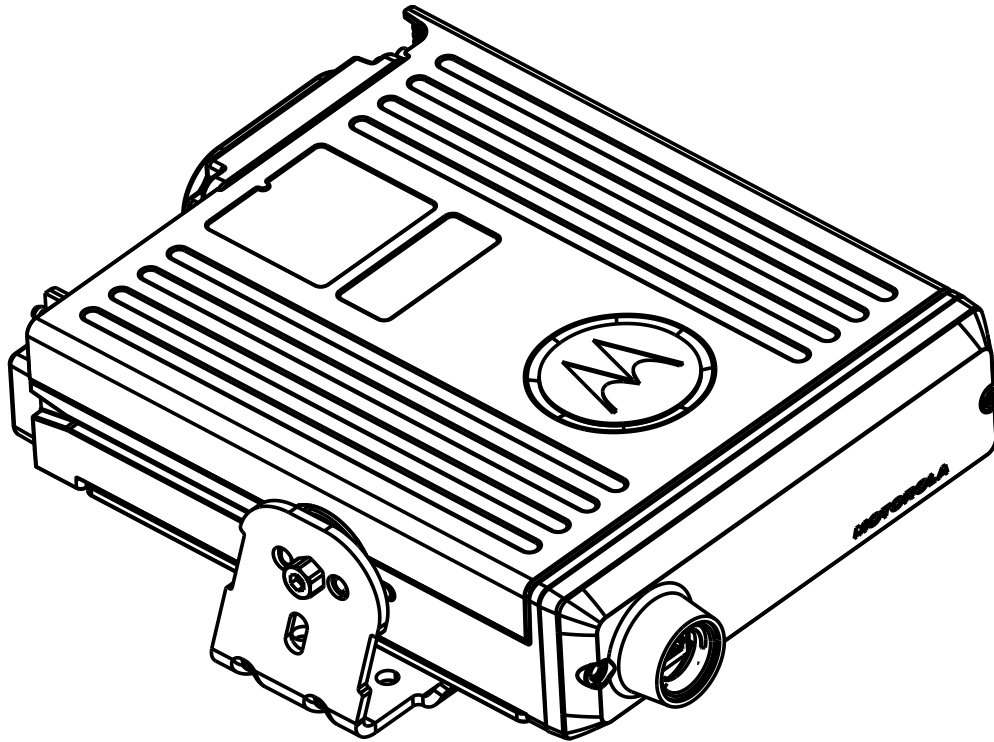


Table 7: APX 8500 MP with Ethernet Faceplate connectivity

Kit Number	Description
HN001998A01	Ethernet Faceplate Retrofit Kit

1.8

Supported System Combinations

The following system combinations are supported for APX® Data Modem Tethering:

- ASTRO and your local LTE or satellite carriers
- Trunked data
- Conventional data
- High Availability data

- ASTRO data encryption (trunked or digital conventional) and Broadband IPsec Virtual Private Network (VPN) encryption

1.9

Supported Configurations

Types of ASTRO Systems Supported

APX Data Modem Tethering supports only ASTRO M core systems including trunked and trunked with digital conventional, and systems with Dynamic System Resilience. M1, M2, and M3 system configurations are supported. ASTRO system frequencies supported are:

- 700/800 MHz (762MHz – 870MHz)
- UHF (380 to 520 MHz)
- VHF (136 to 174 MHz)



NOTE: Broadband cannot be enabled for a personality that supports 700 MHz Land Mobile Radio (LMR) channels. The LMR 700 and 800 MHz RF channel may conflict with some of the broadband bands used by local carriers. Close evaluation of the RF frequencies used in the vehicle is critical to ensure expected operation.

The solution supports ASTRO 7.X system configurations only. Customers on ASTRO 3.X system configurations are required to upgrade to a supported 7.X configuration. Supported 7.X configurations are:

- A7.11
- A7.13 and higher

Types of Broadband Systems Supported

The solution supports tethering an APX radio to a Motorola Solutions VML750 or a Sierra Wireless router. Refer to product documentation for those referenced modems to indicate bands and networks that those specific modems support.

Summary of Supported Configurations

This table shows a summary of the supported configurations and the required network elements.

Table 8: Supported Configurations for APX Data Modem Tethering over Broadband

Supported Configuration for Broadband (LTE, 3G, 2G, etc.)	Fire-walls LTE RAN	Border Routers LMR RNI	Switc hes	KMF	UNS	PDEG	Mobile VPN Gate- way
Fully Clear (Unencrypted), Fully Non-Redundant	1	1	2	none	stand-alone	none	none
Fully Clear, Non-Redundant Radio Network Infrastructures (RNIs), Redundant Applications Network	2	1	4	none	redun-dant	none	none
Fully Clear, Redundant Land Mobile Radio (LMR) RNI, Non-Redundant LTE Radio Access Network (RAN), Re-	2	2	4	none	redun-dant	none	none

Supported Configuration for Broadband (LTE, 3G, 2G, etc.)	Firewalls LTE RAN	Border Routers LMR RNI	Switches	KMF	UNS	PDEG	Mobile VPN Gateway
Redundant Applications Network							
Fully Clear, Non-Redundant LMR RNI, Redundant LTE RAN, Redundant Applications Network	2	1	4	none	redundant	none	none
Fully Clear, Fully Redundant	2	2	4	none	redundant	none	none
Clear LMR, Encrypted LTE, Non-Redundant	1	1	2	stand-alone	stand-alone	none	stand-alone
Clear LMR, Encrypted LTE, Non-Redundant RNI and RAN, Redundant Applications Network	2	1	4	redundant	redundant	none	redundant
Clear LMR, Encrypted LTE, Redundant LMR RNI, Non-Redundant LTE RAN, Redundant Applications Network	2	2	4	redundant	redundant	none	redundant
Clear LMR, Encrypted LTE, Non-Redundant LMR RNI, Redundant LTE RAN, Redundant Applications Network	2	1	4	redundant	redundant	none	redundant
Unencrypted LMR, Encrypted LTE, Fully Redundant	2	2	4	redundant	redundant	none	redundant
Fully Encrypted, Fully Non-Redundant	1	1	2	stand-alone	stand-alone	stand-alone	stand-alone
Fully Encrypted, Non-Redundant RNI and RAN, Redundant Applications Network	2	1	4	redundant	redundant	redundant	redundant
Fully Encrypted, Redundant LMR RNI, Non-Redundant LTE RAN, Redundant Applications Network	2	2	4	redundant	redundant	redundant	redundant
Fully Encrypted, Non-Redundant LMR RNI, Redundant LTE RAN, Redundant Applications Network	2	1	4	redundant	redundant	redundant	redundant
Fully Encrypted, Fully Redundant	2	2	4	redundant	redundant	redundant	redundant

Chapter 2

External Data Modem Configuration

This section describes the configuration of the data modems to support router tethering services.

2.1

Sierra Wireless (ALEOS) Configuration

This section explains the configurations for the Sierra Wireless GX, and MP series modems.

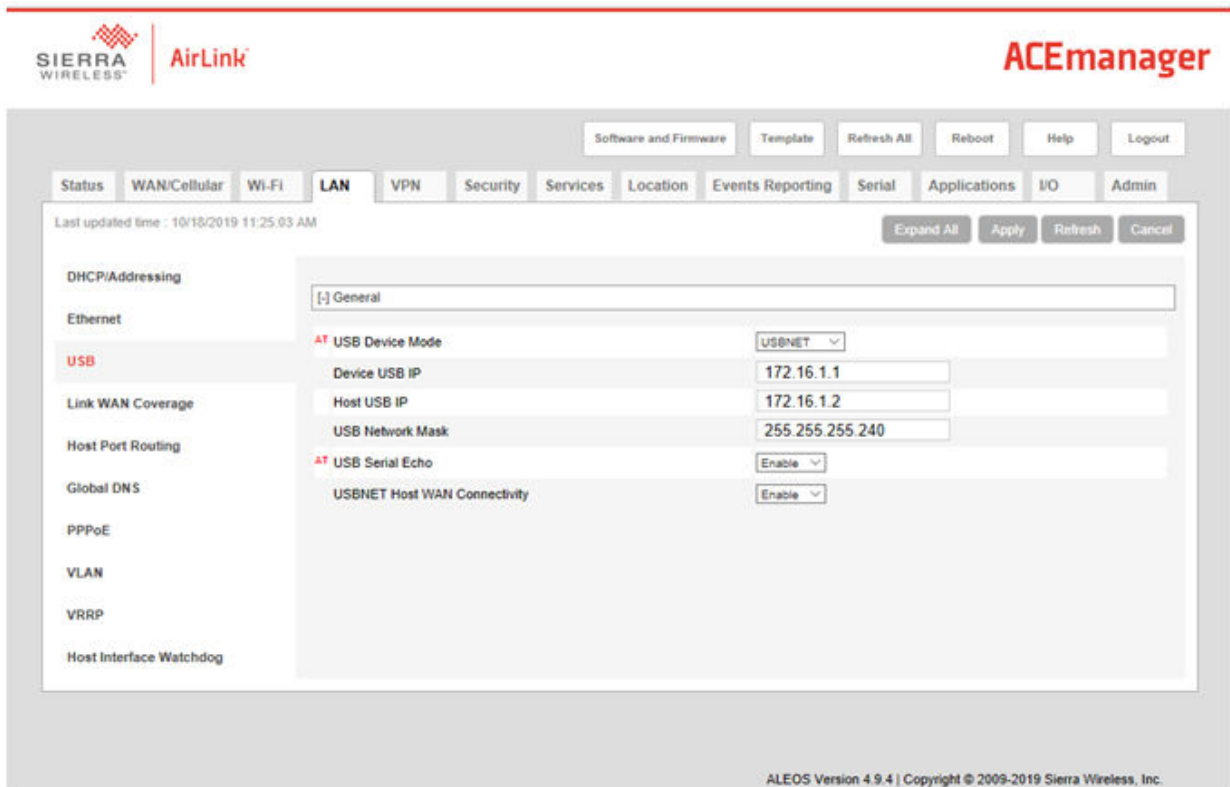
2.1.1

USB Configuration for Sierra Wireless Data Modems

Enable DHCP Server on the router, and ensure that the addresses in the DHCP pool do not conflict with any other subnets configured in the APX Mobile radio codeplug (Serial Link1, CAI, and so on). If the router uses a VPN in Site-to-Site mode to support multiple radios, each router must have a DHCP pool with a unique VPN Configuration.

- Clear Connection: 192.168.15.0/24 safe example DHCP pool for clear.
- VPN Connection (SHOWN): 172.16.1.0/24 example DHCP pool for VPN.

Figure 11: USB Configuration for Sierra Wireless Data Modems



2.1.2

Telnet Configuration

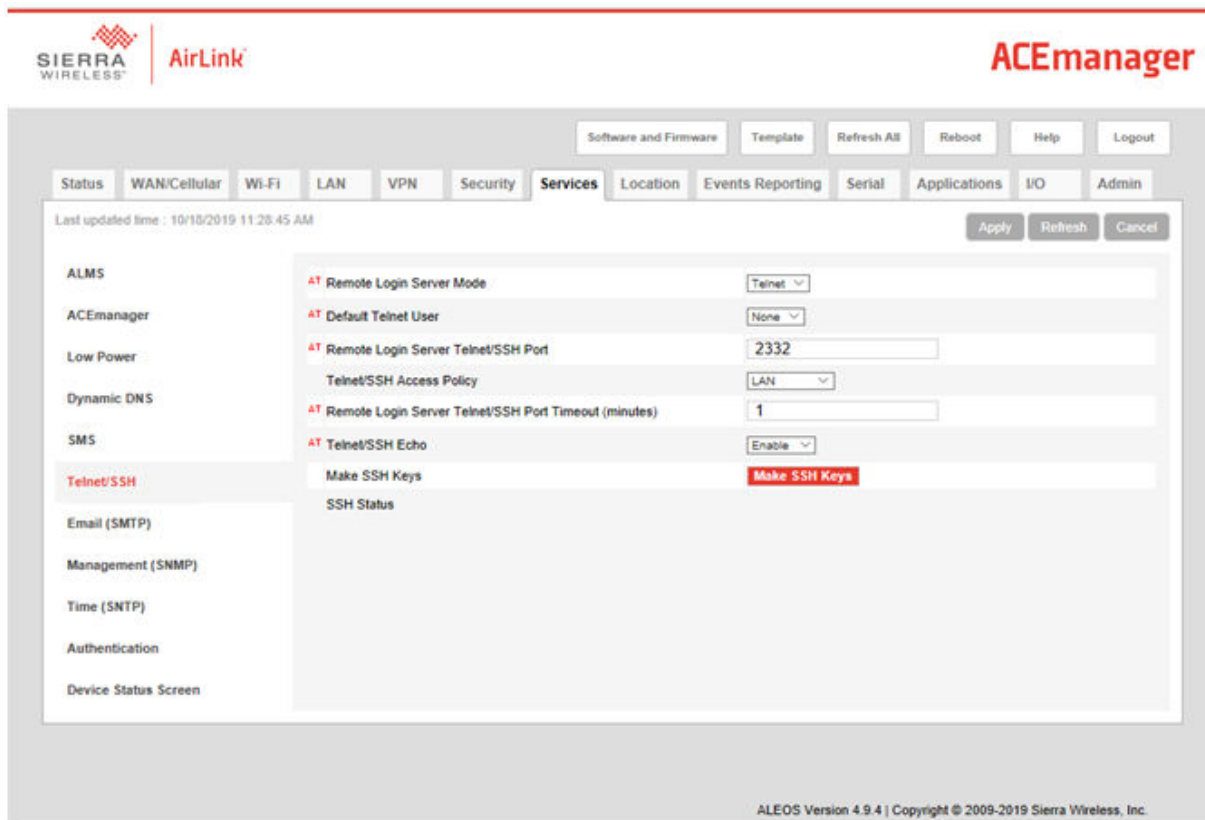
Take note that there is a control layer for transferring router status information between the APX radio and the external router.

Avoid using the following ports for your own applications as these ports are required for Telnet configuration.

Telnet/SSH configuration on the **Services** tab:

- **Remote Login Server Mode** = Telnet
- **Default Telnet User** = None
- **Remote Login Server Telnet/SSH Port** = 2332 (must match the value in the codeplug)
- **Remote Login Server Telnet/SSH Port Timeout (minutes)** = 1 (this settings affects how quickly the APX radio can reconnect to the router following a cable re-connect)

Figure 12: Telnet Configuration



Change Password configuration on the **Admin** tab:

- **User Name** = User
- **Password** = 12345 (Default value. You may change it but it must match the value in the codeplug.)

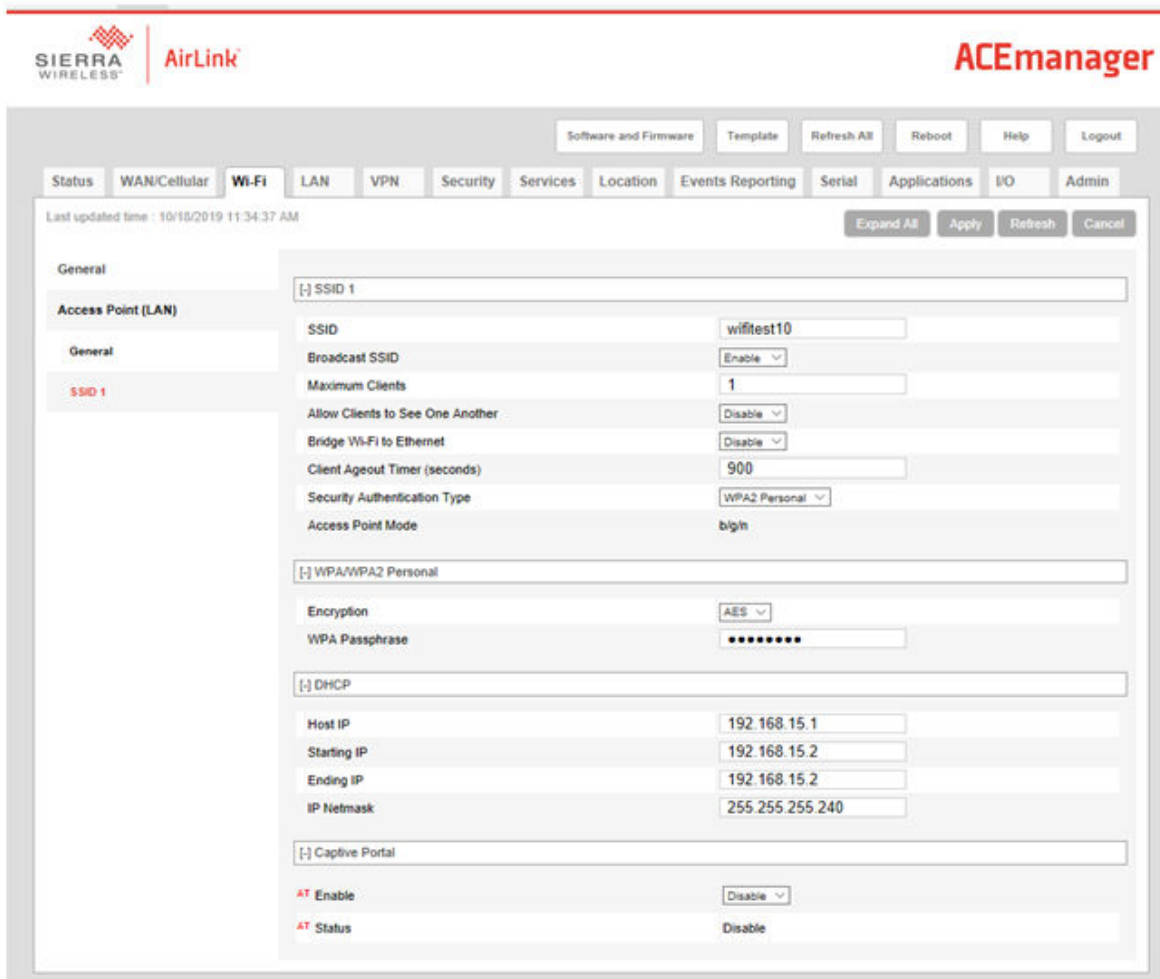
2.1.3

Wi-Fi Configuration for Sierra Wireless Data Modems

The third-party router uses DHCP to assign IP addresses, so DHCP pools must be set up as described in [USB Configuration for Sierra Wireless Data Modems on page 27](#).

- Clear Connection (SHOWN): 192.168.15.0/24 safe example DHCP pool for clear.
- VPN Connection: 172.16.1.0/24 example DHCP pool for VPN.

Figure 13: Sierra Wireless Routers Wi-Fi Configuration



2.1.4

Port Forwarding Configuration for Sierra Wireless (ALEOS)

When the Data Modem Tethering solution is configured to run in a Clear (VPN disabled) configuration, configure port forwarding in the third-party router for unsolicited data requests to arrive at the radio.

The direction of this data is from infrastructure to router to radio and a set of ports need to be forwarded from the router to the radio.

Port Forwarding is a common configuration option in a third party router. The port forwarding entries are usually added to a table that contains the following information:

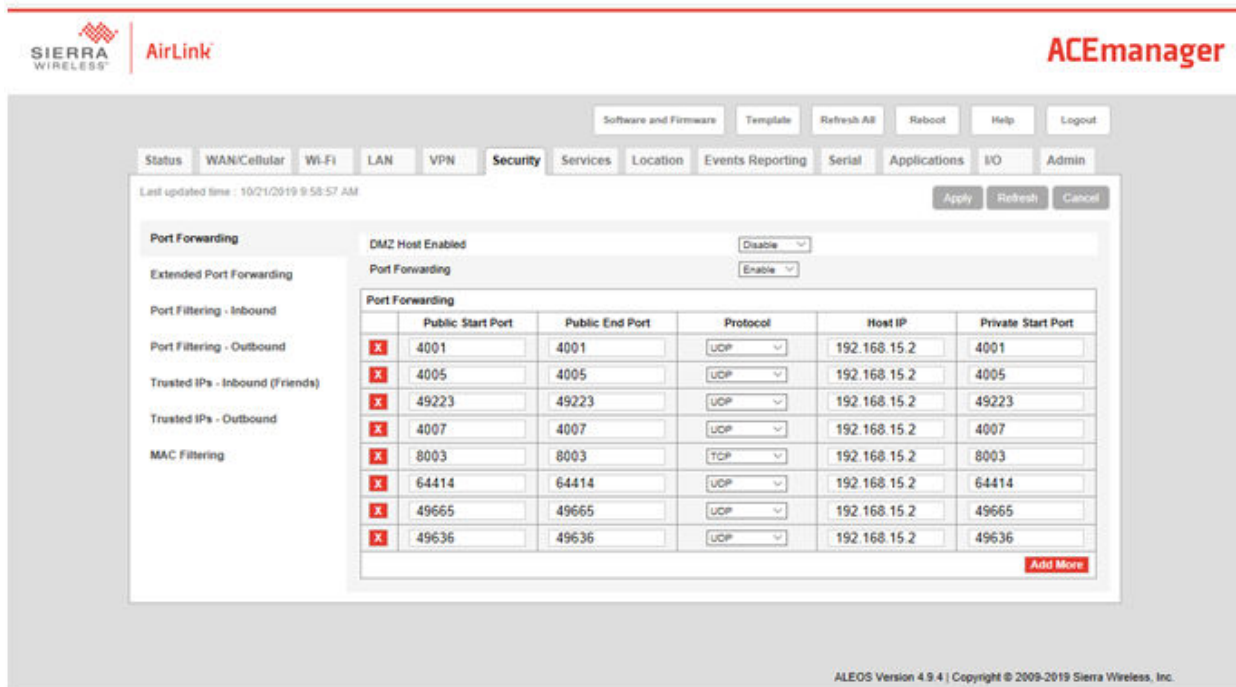
- Public Start Port, Public End Port – This is used to enter a range of ports or a single port. This is port of the data received from the infrastructure to be forwarded to the radio.
- Protocol – third party router manufacturers usually support two protocols: TCP and UDP. Depending of the port being forwarded either TCP or UDP needs to be chosen.

- Host IP – This is the final destination where the data needs to be forwarded. This will be the IP address of the radio obtained using the USB connectivity method. In this field, the customer will need to enter the RNDIS Host IP address assigned to the radio.
- Private Start Port, Private End Port – This is the port used at the final destination. For APX radio data applications, there is no need to convert the public ports to private ports. The same range or single port entered in the Public Start Port, Public End Port fields must be entered here. Note that some manufactures will not have a field called Private End Port.

The following are the application ports used internally by the radio:

- GPS Services (LRRP) – UDP port 4001
- Automatic Registration Services (ARS) – UDP port 4005
- User Authentication Services (UA) – UDP port 49223
- Text Messaging Services (TMS) – UDP port 4007
- Over the Air Programming (OTAP or POP25) – TCP port 8003
- Over the Air Rekeying (OTAR) – UDP 64414 (default) but configurable in the CPS Secure KMF Profile.
- Sensor Request Response Protocol (SRRP) – UDP 49636, plus another port that is configurable in the CPS.

Figure 14: Sierra Wireless Port Forwarding Configuration



2.1.5

DMZ Usage

It is not advisable to use DMZ option on the third-party router when connecting to a radio. The DMZ option selects a local area network as the default route for unsolicited data requests from the infrastructure to the router.

The DMZ option implementation is manufacturer-specific and could invalidate the port forwarding entries added in the steps above. Only advanced users of the router should use the DMZ option with the APX radio.

2.1.6

VPN Configuration for Sierra Wireless Modems

The Sierra Wireless router does not support IKEv2 currently, so only an IKEv1 solution is compatible with the Motorola Solutions Mobile VPN Gateway.

The following are the key fields for the **VPN 1** configuration of the Sierra Wireless data modems on the **VPN** tab. Configure this for the data modems to interoperate with Motorola Solutions Mobile VPN Gateway using the ASTRO Site-to-Site mode.

- **VPN 1 Type** = IPsec Tunnel
- **VPN Gateway Address** = *<Customer Specific Configuration>*
- **Pre-shared Key 1** = *<Customer Specific Configuration>* (must match the PSK in Mobile VPN Gateway configuration)
- **My Identity Type** = IP
- **Peer Identity Type** = IP
- **Negotiation Mode** = Main
- **IKE Encryption Algorithm** = AES-256 (must match the IKE VPN Gateway Config)
- **IKE Authentication Algorithm** = SHA1
- **IKE Key Group** = DH2
- **IKE DPD** = Enabled (recommended to detect when the Mobile VPN Gateway goes down)
- **IKE DPD Interval (seconds)** = 360 (recommended to have client at 6 min and server at 5 min)
- **Local Address Type** = Subnet Address
- **Local Address** = *<Customer Specific Configuration>* (equates to rightsubnet on Mobile VPN Gateway configuration)
- **Local Address - Netmask** = *<Customer Specific Configuration>*
- **Remote Address Type** = Subnet Address
- **Remote Address** = *<Customer Specific Configuration>* (equates to leftsubnet on Mobile VPN Gateway configuration)
- **Remote Address - Netmask** = *<Customer Specific Configuration>*
- **Perfect Forward Security** = Yes
- **IKE Encryption Algorithm** = AES-256 (must match the IKE VPN Gateway Config)
- **IKE Authentication Algorithm** = SHA1
- **IKE Key Group** = DH2

Figure 15: Site-to-Site VPN Configuration

The screenshot displays the configuration page for a Site-to-Site VPN. The interface includes a top navigation bar with buttons for 'Software and Firmware', 'Template', 'Refresh All', 'Reboot', 'Help', and 'Logout'. Below this is a secondary navigation bar with tabs for 'Status', 'WAN/Cellular', 'Wi-Fi', 'LAN', 'VPN', 'Security', 'Services', 'Location', 'Events Reporting', 'Serial', 'Applications', 'I/O', and 'Admin'. The 'VPN' tab is selected, and the page shows a list of VPN configurations on the left, with 'VPN 1' highlighted. The main area displays the configuration for 'VPN 1' under the 'General' tab. The configuration includes fields for 'VPN 1 Type' (IPsec Tunnel), 'VPN 1 Status' (Connected), 'VPN Gateway Address' (10.202.2.66), 'Pre-shared Key 1' (masked), 'My Identity Type' (IP), 'My Identity - IP' (172.31.1.8), 'Peer Identity Type' (IP), 'Peer Identity - IP' (10.202.2.66), 'Negotiation Mode' (Main), 'IKE Encryption Algorithm' (AES-256), 'IKE Authentication Algorithm' (SHA1), 'IKE Key Group' (DH2), 'IKE SA Life Time' (7200), 'IKE DPD' (Enable), 'IKE DPD Interval (seconds)' (360), 'Local Address Type' (Subnet Address), 'Local Address' (172.16.1.0), 'Local Address - Netmask' (255.255.255.240), 'Remote Address Type' (Subnet Address), 'Remote Address' (10.51.0.0), 'Remote Address - Netmask' (255.255.0.0), 'Perfect Forward Secrecy' (Yes), 'IPSec Encryption Algorithm' (AES-256), 'IPSec Authentication Algorithm' (SHA1), 'IPSec Key Group' (DH2), and 'IPSec SA Life Time' (7200). A 'Set VPN Policy' button is also visible.

2.2

Sierra Wireless MG90 Configuration

This section explains the configurations for the MG90 data modem. The MG90 solution is only supported with a VPN. Ensure that the software version of the modem is version 4.3 or later to be fully compatible with the APX radios.

2.2.1

Broadcast Configuration

Part of the MG90 configuration includes configuring JSON broadcasts. These broadcasts are required to provide proper operational status to the APX Mobile.

Specify the following data fields to be included in the broadcasts:

- **Enable** – Must be checked


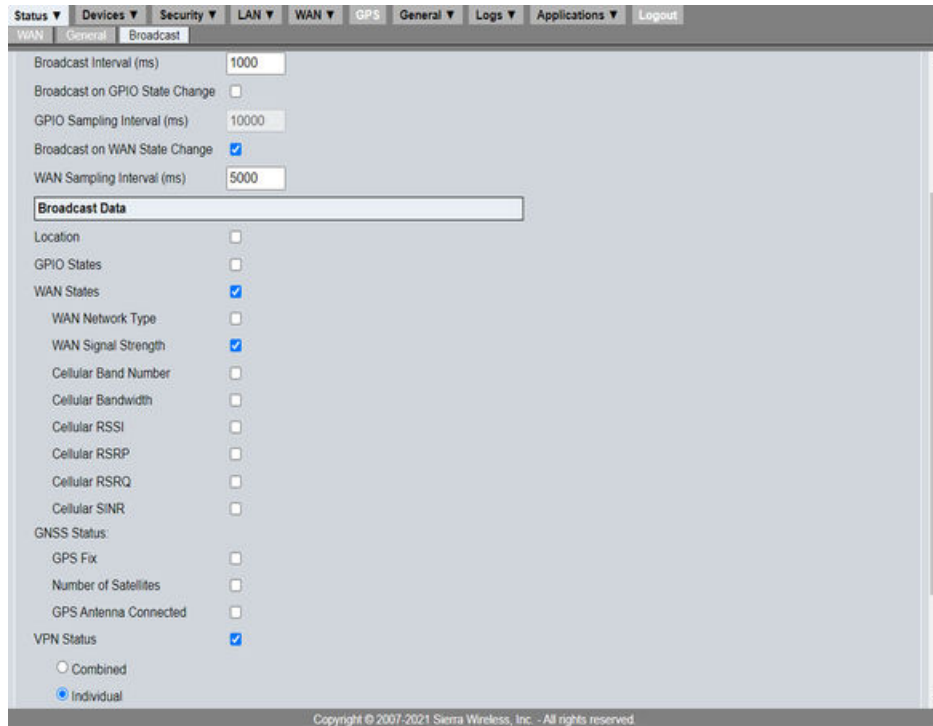
- **Broadcast Port** – Must match the modem port number specified in the radio codeplug
 - **LAN Segments** – Must include a selection for the LAN segment where the APX is connected
 - **Broadcast Interval** – Recommended at 1 second intervals (1000 ms)
 - **WAN Sampling Interval** – Recommended at 1 second intervals (1000 ms)
 - **WAN State** – Must be checked
 - **WAN Signal Strength** – Must be checked
 - **VPN Status** – Must be checked
-  **NOTE: Individual** must be checked to configure multiple VPN (only for MG90 software version 4.3.2 or later)

Figure 16: Status Broadcast Configuration



WAN General Broadcast

Broadcast Interval (ms) 1000

Broadcast on GPIO State Change

GPIO Sampling Interval (ms) 10000

Broadcast on WAN State Change

WAN Sampling Interval (ms) 5000

Broadcast Data

Location

GPIO States

WAN States

WAN Network Type

WAN Signal Strength

Cellular Band Number

Cellular Bandwidth

Cellular RSSI

Cellular RSRP

Cellular RSRQ

Cellular SINR

GNSS Status:

GPS Fix

Number of Satellites

GPS Antenna Connected

VPN Status

Combined

Individual

Copyright © 2007-2021 Sierra Wireless, Inc. - All rights reserved.

2.2.2

WAN Links Friendly Names

The MG90 allows a Friendly Name to be configured for each Wide Area Network (WAN) link.

The WAN friendly name can be set to match the field in CPS (LTE Friendly Name or Satellite Friendly Name) for the radio to differentiate between the LTE and satellite. This configuration allows the radio to use LTE, and to switch to LMR data when LTE is unavailable.

 **NOTE:**

- CPS LTE Friendly Name field can be configured with "*" to enable All WAN Mode. When All WAN Mode is enabled, the radio uses any non-Satellite WAN provided by the MG90 as the highest priority data link. If the active WAN is unavailable, the MG90 waits for another WAN to become active before switching to LMR data. The Satellite WAN is only used when no other broadband or LMR network is available.
- The Friendly Name strings in the MG90 configuration screen and the corresponding fields in the APX radio CPS must be an exact match in order for the APX to use the MG90 WAN Link.

Figure 17: Cellular Friendly Name

Cellular page can be used to configure the Friendly Name of each cellular connection.



Figure 18: Ethernet (Satellite) Friendly Name

Ethernet and Wi-Fi pages can be used to configure the Friendly Name of the Ethernet port used to connect to a satellite modem.

The screenshot displays the 'Local Configuration Interface' for Sierra Wireless AirLink. The interface includes a navigation menu with options like Status, Devices, Security, LAN, WAN, GPS, General, Logs, Applications, and Logout. The 'Ethernet' tab is selected, showing a table of Ethernet ports with columns for Friendly Name, Device Type, Location, Use, Installed, and Actions. The table lists five ports: Panel Ethernet 1, Panel Ethernet 2, APX8500, Panel Ethernet 4, and MSISATWAN. Each port is associated with a 'Device Built-in Ethernet Port' and is currently set to 'LAN' or 'WAN' use. A 'Save' button and a 'Cancel' button are located below the table.

Friendly Name	Device Type	Location	Use	Installed	Actions
<input type="text" value="Panel Ethernet 1"/>	Device Built-in Ethernet Port	Panel Ethernet 1	LAN	<input checked="" type="checkbox"/>	
<input type="text" value="Panel Ethernet 2"/>	Device Built-in Ethernet Port	Panel Ethernet 2	LAN	<input checked="" type="checkbox"/>	
<input type="text" value="APX8500"/>	Device Built-in Ethernet Port	Panel Ethernet 3	LAN	<input checked="" type="checkbox"/>	
<input type="text" value="Panel Ethernet 4"/>	Device Built-in Ethernet Port	Panel Ethernet 4	LAN	<input checked="" type="checkbox"/>	
<input type="text" value="MSISATWAN"/>	Device Built-in Ethernet Port	Panel Ethernet 5	WAN	<input checked="" type="checkbox"/>	

Copyright © 2007-2019 Sierra Wireless, Inc. - All rights reserved.

Figure 19: Wi-Fi Friendly Name

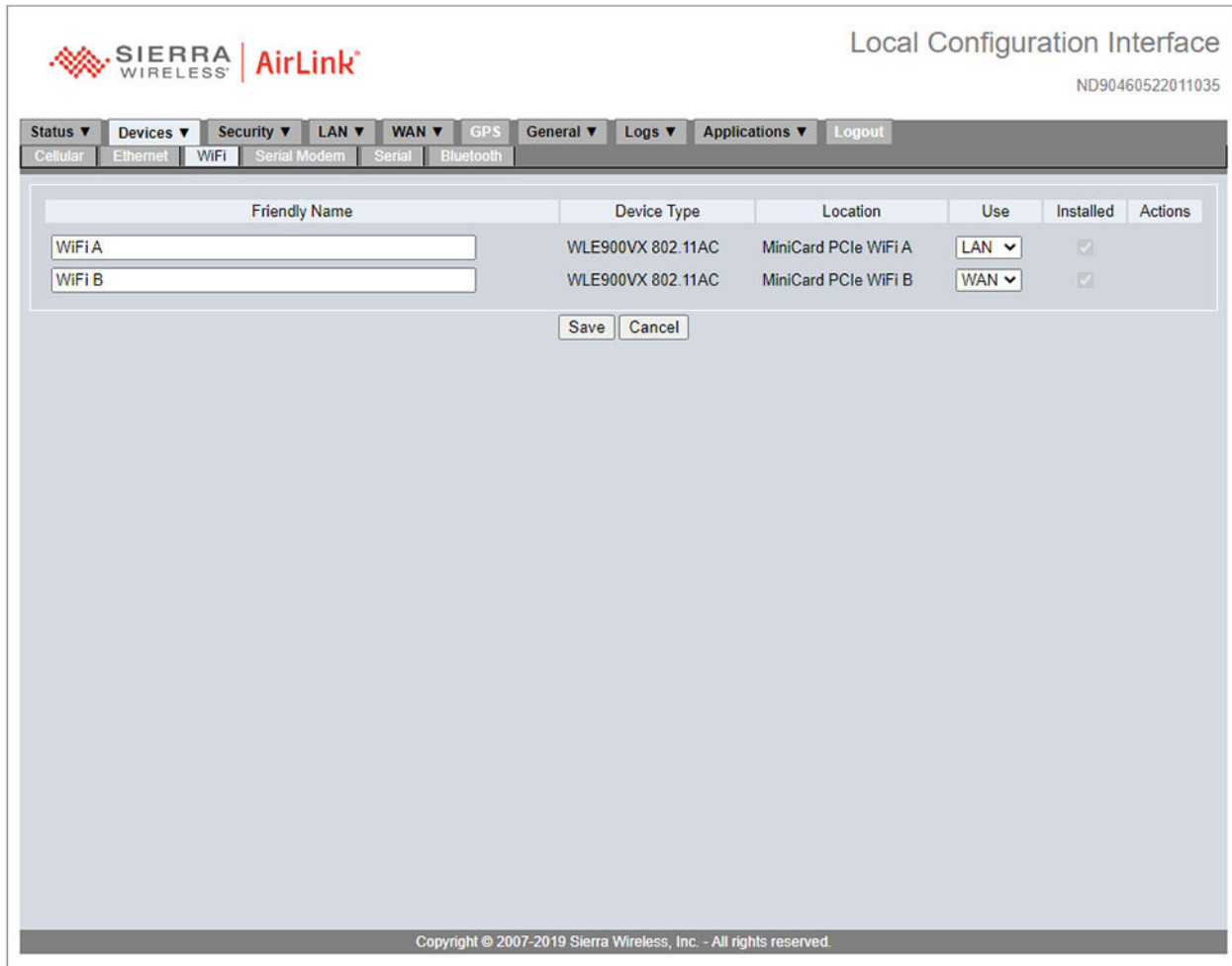
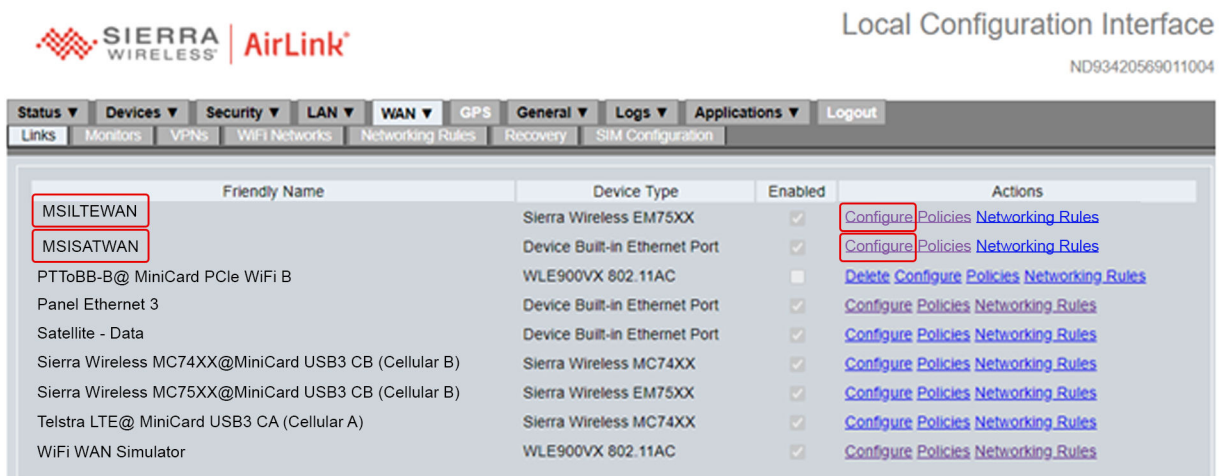


Figure 20: WAN Link Summary

Links page provides a summary of all configured WAN connections. This can be used to verify configured Friendly Names.



2.2.3

Cellular WAN Configuration

The Cellular WAN Link Configuration screen allows you to view and modify connection settings for the MG90's cellular connection.

For more information, refer to *AirLink MG90 Software Configuration Guide*.

Figure 21: Cellular WAN Configuration

The screenshot displays the 'Cellular WAN Link Configuration' interface for a device named '(MSILTEWAN)'. The interface is organized into a grid of settings:

- High Cost Link:**
- MTU Size:** Automatic, Manual
- Masquerade:**
- Masquerade Port Range:** Automatic, Manual. Includes input fields for Minimum Port Number (49152) and Maximum Port Number (65535).
- Automatic DNS:**
- Primary DNS:** [Input field]
- Secondary DNS Servers:** [Input field] comma-separated IP addresses
- Enable Private Zone:**
- Number of Private Zone:** 1
- APN:** vzwinternet
- Signal Strength Filter Length:** 10
- Signal Strength Change Threshold (dBm):** 5
- Use Management Tunnel:**
- Pilot Ping:**
- Monitors:** DefaultMonitor, Fake 1, GSN Ping Monitor, Google Ping Monitor, Sat Ping Monitor
- Monitor Mode:** Success in one monitor keeps the link up
- VPN:** VPN Public
- Connection Method:** Connect One (Random, Round Robin - Alphanumeric Order), Connect All
- Load Balanced:**
- Weight (1-256):** 1
- Split Access:**
- Enable Advanced Module Recovery:**
- Recovery Interval (minutes):** 10
- Advanced Modem Initialization:** ~ Comma separated
- Enable IPV6:**

Buttons for 'Save' and 'Cancel' are located at the bottom right of the configuration area.

2.2.4

Ethernet WAN Configuration

The Ethernet WAN Link Configuration screen allows you to view and modify connection settings for the MG90's ethernet connection.

For more information, refer to *AirLink MG90 Software Configuration Guide*.

Figure 22: Ethernet WAN Configuration

The screenshot displays the 'Ethernet WAN Link Configuration (MSISATWAN)' window. The interface includes a top navigation bar with tabs for Status, Devices, Security, LAN, WAN, GPS, General, Logs, Applications, and Logs. Below this is a sub-menu bar with tabs for Links, Monitors, VPNs, WiFi Networks, Networking Rules, Recovery, and SIM Configuration. The main configuration area is titled 'Ethernet WAN Link Configuration (MSISATWAN)' and contains the following settings:

- High Cost Link:
- Change Default MTU Size:
 - MTU Size: 1500
- Auto Local IP:
- DHCP Assumes Same Network:
- Send Hostname with DHCP: Disabled, Send ESN, Custom
- Local IP Address: [Text Field]
- Network Mask: [Text Field]
- Gateway: [Text Field]
- Masquerade:
 - Masquerade Port Range: Automatic, Manual
 - Minimum Port Number: 49152
 - Maximum Port Number: 65535
- Automatic DNS:
 - Primary DNS: 8.8.8.8
 - Secondary DNS Servers: [Text Field] comma-separated IP addresses
- Enable Private Zone:
 - Number of Private Zone: 1
- Use Management Tunnel:
- Pilot Ping:
- Monitors: DefaultMonitor, Fake 1, GSN Ping Monitor, Google Ping Monitor, Sat Ping Monitor
- Monitor Mode: Success in one monitor keeps the link up
- VPN: VPN Public
 - Connection Method: Connect One (Random, Round Robin - Alphanumeric Order), Connect All
- Load Balanced:
 - Weight (1-256): 1
- Split Access:

At the bottom right, there are 'Save' and 'Cancel' buttons.

2.2.5 Wi-Fi and Ethernet LAN Configuration

The Wi-Fi and Ethernet LAN Link Configuration screen allows you to view and modify connection settings for the MG90's Wi-Fi and Ethernet LAN connection.

For more information, refer to *AirLink MG90 Software Configuration Guide*.

Figure 23: Ethernet LAN Configuration

The wired Ethernet LAN and the Wi-Fi LAN must be in the same network or subnet.

The screenshot displays the 'Local Configuration Interface' for Sierra Wireless AirLink. The interface includes a navigation menu with tabs for Status, Devices, Security, LAN, WAN, GPS, General, Logs, Applications, and Logout. The 'LAN' tab is active, showing a sub-menu with 'Ethernet Links', 'Access Points', 'LAN Segments', 'Virtual LANs', 'Networking Rules', 'LAN Throughput', and 'Captive Portal'. The main content area shows a table of LAN Segments:

Subnet	Friendly Name	Devices	Type	Enabled	Actions
172.22.0.0/24	Default LAN	<ul style="list-style-type: none">WIFI B: WIFI BMSISATWANPanel Ethernet 1Panel Ethernet 2Panel Ethernet 4	WiFi, Ethernet, Ethernet, Ethernet, Ethernet	<input type="checkbox"/> , <input type="checkbox"/> , <input checked="" type="checkbox"/> , <input checked="" type="checkbox"/> , <input checked="" type="checkbox"/>	Configure Networking Rules Default LAN, Default LAN, Default LAN, Default LAN, Default LAN
172.33.1.192/28	Radio	<ul style="list-style-type: none">WIFI A: WIFI AAPX8500	WiFi, Ethernet	<input checked="" type="checkbox"/> , <input checked="" type="checkbox"/>	Configure Networking Rules Radio, Radio

Buttons at the bottom include 'Add New LAN Segment', 'Apply Changes', and 'Cancel'. The footer contains the copyright notice: 'Copyright © 2007-2019 Sierra Wireless, Inc. - All rights reserved.'

In the following example, a LAN segment is configured to contain a DHCP Server on the 172.33.1.192/28 subnet. The LAN segment is assigned to the Ethernet 3 connection and also assigned to the Wi-Fi A LAN connection on the router.


 **NOTE:** The wired and wireless LAN segments to the radio must be assigned to the same subnet.

Figure 24: LAN Segment Configuration Window

The screenshot displays the 'LAN Segment Configuration (Radio)' window within the 'Local Configuration Interface'. The interface includes a navigation menu at the top with options like Status, Devices, Security, LAN, WAN, GPS, General, Logs, Applications, and Logout. Below this is a sub-menu with Ethernet Links, Access Points, LAN Segments, Virtual LANs, Networking Rules, LAN Throughput, and Captive Portal. The main configuration area contains the following fields and options:

Field	Value
Friendly Name	Radio
Default Gateway Address	172.33.1.193
Network Mask	255.255.255.240
Enable DHCP Server	<input checked="" type="checkbox"/>
DHCP Low Address	172.33.1.194
DHCP High Address	172.33.1.206
DHCP Client Lease Time (sec)	28800
Domain search list (comma-separated)	
WINS Servers (comma-separated IP addresses)	
Enable Web Portal	<input type="checkbox"/>
Enable Subnet Management Access	<input checked="" type="checkbox"/>
Isolated	<input type="checkbox"/>
IGMP Snooping	<input type="checkbox"/>
IPv6 Addressing	None

At the bottom of the configuration area are 'Save' and 'Cancel' buttons. The footer of the interface reads: 'Copyright © 2007-2019 Sierra Wireless, Inc. - All rights reserved.'

Figure 25: Wi-Fi LAN Access Points

The screenshot displays the 'Local Configuration Interface' for a Sierra Wireless AirLink device. The interface includes a navigation menu with options like Status, Devices, Security, LAN, WAN, GPS, General, Logs, Applications, and Logout. The 'LAN' menu is expanded to show 'Access Points', 'LAN Segments', 'Virtual LANs', 'Networking Rules', 'LAN Throughput', and 'Captive Portal'. The 'Access Points' section contains a table with two entries:

Device Type	Friendly Name	Actions
WLE900VX 802.11AC	WiFi A	Configure
WLE900VX 802.11AC	WiFi B	Configure

Below the table are 'Save' and 'Cancel' buttons. The footer of the interface reads: 'Copyright © 2007-2019 Sierra Wireless, Inc. - All rights reserved.'

Figure 26: Wi-Fi LAN Access Points Configuration

The screenshot displays the 'Local Configuration Interface' for Sierra Wireless AirLink. The interface is titled 'Access Point Configuration (WiFi)' and is divided into several sections. At the top, there is a navigation menu with tabs for Status, Devices, Security, LAN, WAN, GPS, General, Logs, Applications, and Logout. Below this, there are sub-tabs for Ethernet Links, Access Points, LAN Segments, Virtual LANs, Networking Rules, LAN Throughput, and Captive Portal. The main configuration area is titled '802.11 Configuration' and includes the following settings:

- Enabled:
- Network Type: 802.11a/b/g
- Auto SSID:
- SSID: WiFi
- Broadcast SSID:
- Captive Portal: Not defined
- Channel (Frequency in MHz): 1 (2412)
- Secondary Channel: none
- Enable Multiple Antennas (802.11 n/ac MIMO):
- Channel Width (802.11 ac): 80
- Enable WMM:
- Enable AP Isolation:
- MAC Access Control List: DISABLED
- Encryption: None

Below the 802.11 Configuration section is the 'Virtual BSSIDs' section, which contains three rows for Virtual BSSID 1, 2, and 3. Each row has an 'Enable' checkbox (all are unchecked) and a 'Show/Hide' button. At the bottom of the configuration area, there are 'Save' and 'Cancel' buttons. The footer of the interface reads 'Copyright © 2007-2019 Sierra Wireless, Inc. - All rights reserved.'

2.2.6

Port Forwarding Configuration for MG90

All other applications do not require an internal NATing solution.

Take note that this Network Address Translation (NAT) rule requires the Dynamic Configuration Host Protocol (DHCP) pool to be configured for a size of one so that it is NATing to the correct destination IP.



NOTE: Release version 2020.3 and above does not require NAT entry for Over-The-Air Re-keying (OTAR).

Figure 27: MG90 Port Forwarding Configuration

The screenshot displays the 'Local Configuration Interface' for a Sierra Wireless AirLink device. The interface includes a navigation menu with options like Status, Devices, Security, LAN, WAN, GPS, General, Logs, Applications, and Logout. The 'WAN' menu is expanded to show 'Networking Rules'. The main area is titled 'Port Forwarding Firewall Rule (WAN Global Rules)'. It contains a form with the following fields: Rule Name (OTAR), Source IP (10.51.1.0/24), Destination Port Range (64414 to 64414), Protocol (UDP), Forward to Host (172.16.1.2), and Forward Port Range (4050 to 4050). There are 'Save' and 'Cancel' buttons at the bottom of the form. The footer of the interface reads 'Copyright © 2007-2019 Sierra Wireless, Inc. - All rights reserved.'

2.2.7

VPN Configuration for MG90

Key fields for the VPN configuration is explained in this section.

- **Friendly Name** = Specifies a friendly name for the VPN connection. Please note that there is a corresponding field in the APX CPS for VPN Friendly Name. At this time, the CPS field should be left blank to operate with current MG90 software. This field can be used for MG90 software version 4.3.2 and later.
- **Local Address** = *<Customer Specific Configuration>* (equates to rightsubnet on Mobile VPN Gateway configuration)
- **Local Address - Netmask** = *<Customer Specific Configuration>*
- **Remote Address Type** = Subnet Address
- **Remote Subnets** = *<Customer Specific Configuration>* (equates to leftsubnet on Mobile VPN Gateway configuration)
- **Local Subnets** = Select the previously configured LAN segment (equates to rightsubnet on Mobile VPN Gateway configuration)


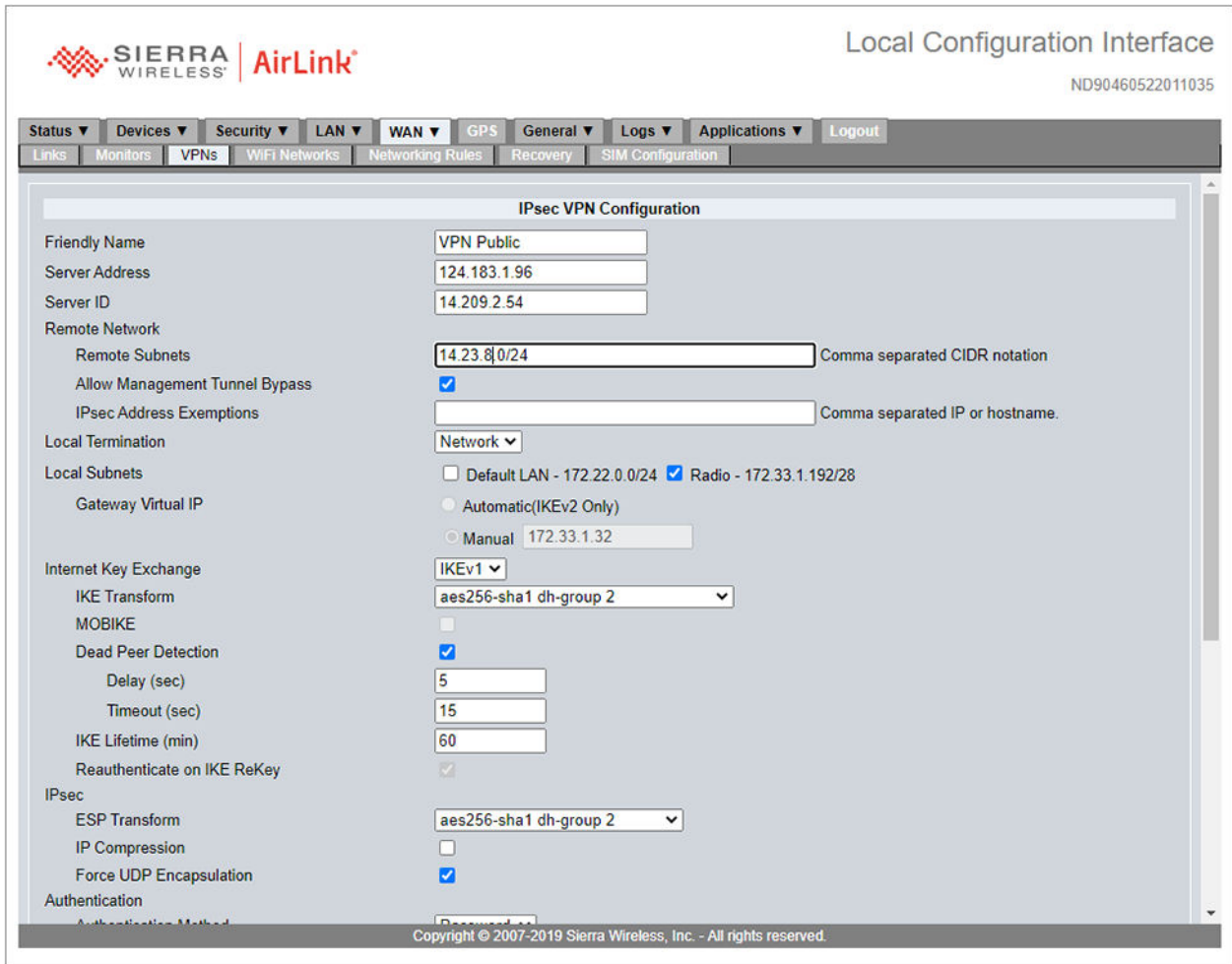
- **Local Termination** = Network
 **NOTE:** Motorola Solutions only supports "Network" configuration (see [Site-to-Site Topology](#) on page 20)
- **IKE Transform** = *<Customer Specific Configuration>* (equates to matching Mobile VPN Gateway configuration)
- **MOBIKE** = *<Customer Specific Configuration>* (equates to matching Mobile VPN Gateway configuration)
- **Dead Peer Detection Timeout (sec)** = 360 (recommended to have client at 6 min and server at 5 min)
- **ESP Transform** = *<Customer Specific Configuration>* (equates to matching Mobile VPN Gateway configuration)

Figure 28: MG90 VPN Configuration 1




The screenshot displays the 'Local Configuration Interface' for an IPsec VPN. The page title is 'Local Configuration Interface' with the ID 'ND90460522011035'. The navigation menu includes Status, Devices, Security, LAN, WAN, GPS, General, Logs, Applications, and Logout. The 'WAN' tab is active, showing 'IPsec VPN Configuration'.

Configuration details include:

- Friendly Name:** VPN Public
- Server Address:** 124.183.1.96
- Server ID:** 14.209.2.54
- Remote Network:** Remote Subnets: 14.23.8/0/24 (Comma separated CIDR notation); Allow Management Tunnel Bypass:
- Local Termination:** Network (dropdown)
- Local Subnets:** Default LAN - 172.22.0.0/24; Radio - 172.33.1.192/28
- Gateway Virtual IP:** Automatic(IKEv2 Only); Manual: 172.33.1.32
- Internet Key Exchange:** IKEv1 (dropdown); IKE Transform: aes256-sha1 dh-group 2 (dropdown)
- MOBIKE:**
- Dead Peer Detection:** ; Delay (sec): 5; Timeout (sec): 15; IKE Lifetime (min): 60
- Reauthenticate on IKE ReKey:**
- IPsec:** ESP Transform: aes256-sha1 dh-group 2 (dropdown); IP Compression: ; Force UDP Encapsulation:
- Authentication:** Authentication Method: (dropdown)

Copyright © 2007-2019 Sierra Wireless, Inc. - All rights reserved.

 **NOTE:** When using any version of MG90 software prior to 4.3.2, The MG90 can ONLY be configured with a single VPN connection, as the radio cannot discern between which VPN is connected if more than one exists. Having multiple VPN connections result in potentially sending customer data in the clear if the wrong VPN is connected.

To attach a VPN to a WAN connection, on the WAN configuration page, make sure to check the box associated with the VPN Friendly Name you set up. See [Figure 22: Ethernet WAN Configuration](#) on page 39.

2.2.8

Multiple VPN Configuration

To connect multiple VPNs on a single WAN, the following are required:

- The MG90 must have software version 4.3.2 or later.
- All of the VPNs must be setup with Internet Key Exchange value of IKEv2.
- In the MG90 broadcast setup, VPN Status must be set to Individual (see [Broadcast Configuration on page 32](#)).

2.3

Sierra Wireless XR80 and XR90 Modems Configuration

This section explains the configurations for the XR80 and XR90 modems. The configuration includes the ability to operate with all supported data tethered features, and SmartConnect.

2.3.1

Simple Setup

To use the XR80 and XR90 modems, you need to connect your modem and install the SIM card. When the modem powers on, connect your computer to the modem. Log on to the modem using the modem IP address.




NOTE: The default IP address is 192.168.1.1, while the default username is admin and the password is on a sticker on the modem. Reset your modem to restore it to the factory default settings if needed.

2.3.1.1

Setting Local Area Network (LAN)


Procedure:

1. Go to **Networking** → **Zones**.
2. At the **LAN Segments** field, select **Default-LAN**.
 **NOTE:** The Default-LAN IP gateway address is 192.168.1.1
3. At the **Start Address** field, enter: 192.168.1.100.
4. At the **End Address** field, enter: 192.168.1.299.

2.3.1.2

Configuring the Modem to Use the Bridge

Your Local Area Network (LAN) settings remain the same as the configurations are already set for using the default LAN.

 **NOTE:** In the following example, Ethernet 1, Ethernet 2, and XP1 Ethernet are used to connect the computer and the radio. Meanwhile, Ethernet 3 is used for the satellite WAN connection. Depending on the need, XP2 Ethernet can serve as the WAN or LAN connection. The XP2 Ethernet is only available on the XR90 modem.

Procedure:

1. Go to **Hardware Interfaces** → **Ethernet Interfaces**.
2. At the **Configuration** field, select **Default**.

2.3.1.3

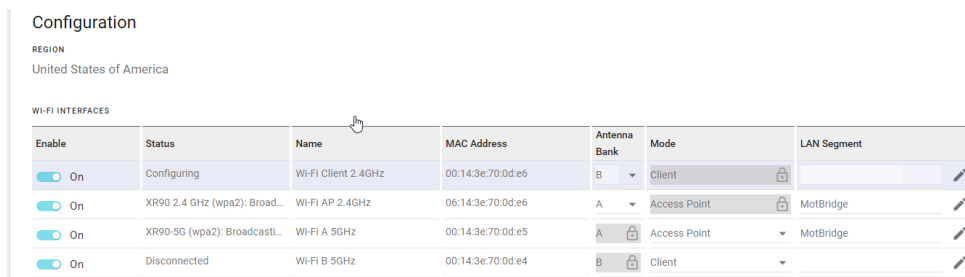
Setting Wi-Fi

The XR80 modem has one bank of Wi-Fi while the XR90 modem has two.

Procedure:

1. Go to **Hardware Interfaces** → **Wi-Fi Interfaces** → **Configuration**.
- Local Area Network (LAN) Configuration*
2. To edit the **Configuration** field, select the **Pen** icon.
 3. Enable the 2.4 GHz and 5 GHz interfaces.
 4. At the **Mode** field, select **Access Point**.
 5. At the **LAN Segment** field, use one of the following options:
 - To perform Simple Setup, select **Default-LAN**.
 - To perform Advanced Setup, select **MotBridge**.

Figure 29: Configuring LAN




The screenshot shows the 'Configuration' page with the 'REGION' set to 'United States of America'. Below is a table titled 'WI-FI INTERFACES' with columns: Enable, Status, Name, MAC Address, Antenna Bank, Mode, and LAN Segment.

Enable	Status	Name	MAC Address	Antenna Bank	Mode	LAN Segment
<input checked="" type="checkbox"/>	Configuring	Wi-Fi Client 2.4GHz	00:14:3e:70:0d:e6	B	Client	
<input checked="" type="checkbox"/>	XR90 2.4 GHz (wpa2): Broad...	Wi-Fi AP 2.4GHz	06:14:3e:70:0d:e6	A	Access Point	MotBridge
<input checked="" type="checkbox"/>	XR90-5G (wpa2): Broadcasti...	Wi-Fi A 5GHz	00:14:3e:70:0d:e5	A	Access Point	MotBridge
<input checked="" type="checkbox"/>	Disconnected	Wi-Fi B 5GHz	00:14:3e:70:0d:e4	B	Client	

6. Configure the Service Set Identifier (SSID), security mode, and password if required.

Leave the other fields in their default setting.

 **IMPORTANT:** You must perform step [step 2](#) to [step 6](#) to connect data modem tethered devices to the XR modem. Most APX radios can connect using the 2.4 GHz connection. APX NEXT radios and some of the newer APX radios can connect using the 5 GHz connection.

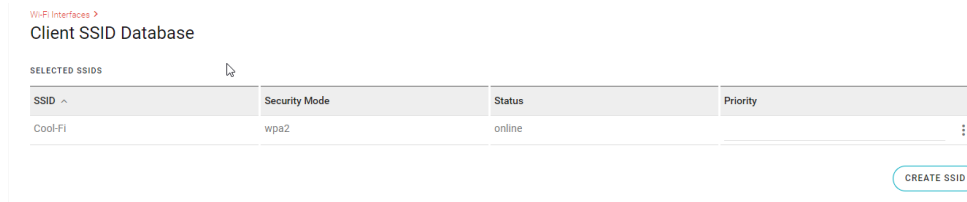
Wide Area Network (WAN) Configuration

7. Enable the 2.5 GHz and 5 GHz WAN interfaces.
8. At the **LAN Segment** field, leave the information as blank.

Client SSID Database Configuration

9. Select **Create SSID**.
10. Enter the access point information.
11. Select **Create** → **Save**.

Figure 30: Configuring SSID



2.3.1.4

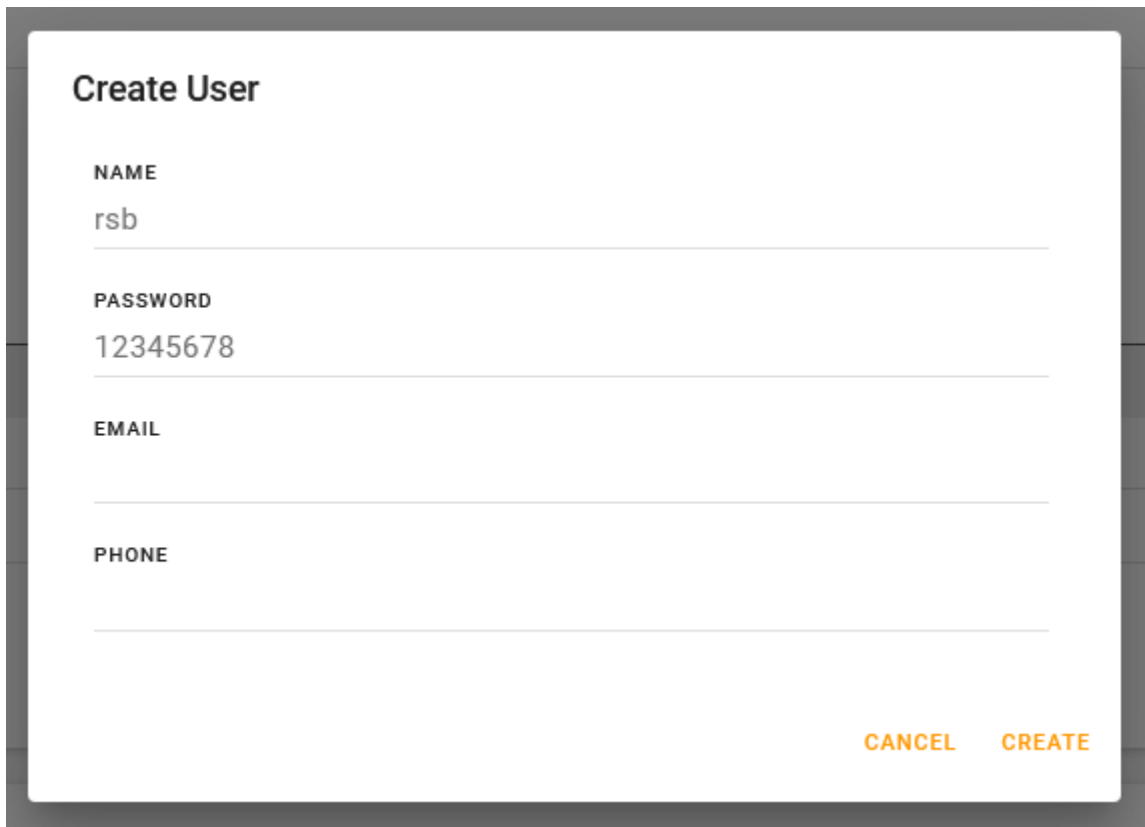
Adding New Users to the Container

The user defined in this section is used in the RSB application. The credentials must be included in the config file that is loaded into the modem.

Procedure:

1. Go to **System** → **User Accounts**.
2. Click **CREATE USER**.
3. At the **NAME** field, enter: `rsb`.
4. At the **PASSWORD** field, enter: `12345678`.
This password must match the password that is in the config file.
5. Click **Create** → **Save**.

Figure 31: Create User Configuration



The image shows a 'Create User' form with the following fields and values:

- NAME**: rsb
- PASSWORD**: 12345678
- EMAIL**: (empty)
- PHONE**: (empty)

At the bottom right of the form, there are two buttons: **CANCEL** and **CREATE**.

Figure 32: Users



USERS		
Name	Email	Phone
admin		
rsb		

Below the table is a **CREATE USER** button.

2.3.1.5

Enabling Container Usage

Procedure:

1. Go to **Apps** → **Container Application** → **General Status**.
2. Enable **Enabled**.
3. Click **Save**.

Figure 33: Container Usage



The image shows the 'General Status' for 'Container Applications (BETA)'. It includes a toggle switch for **ENABLE** which is currently set to **Enabled**, and a **STATUS** indicator which is **Ready**.

2.3.1.6

Adding New Registries

Procedure:

1. Go to **Apps** → **Registry Access**.
2. Click **CREATE REGISTRY ACCESS CONFIGURATION**.
3. At the **NAME** field, enter: `AWSSWIRegistry`.
4. At the **URL** field, enter: `http://public.ecr.aws`.
5. At the **AUTHENTICATION MODE** field, set as **None**.
6. Click **Create** → **Save**.

Figure 34: New Registry Configuration

NAME

AWSSWIRegistry

URL

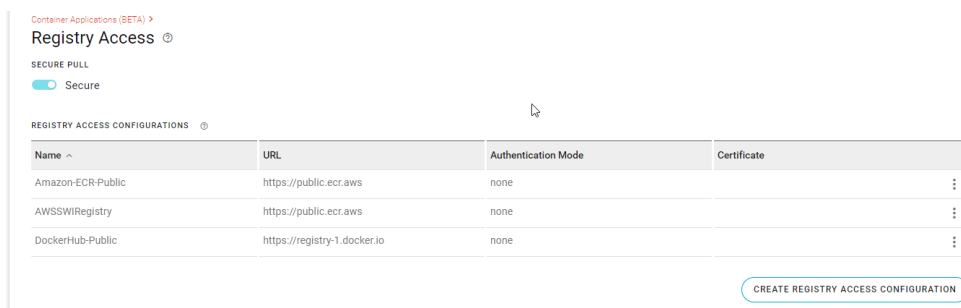
https://public.ecr.aws

AUTHENTICATION MODE

None

CERTIFICATE

Figure 35: Registry Access



Result: The application downloads to the modem.

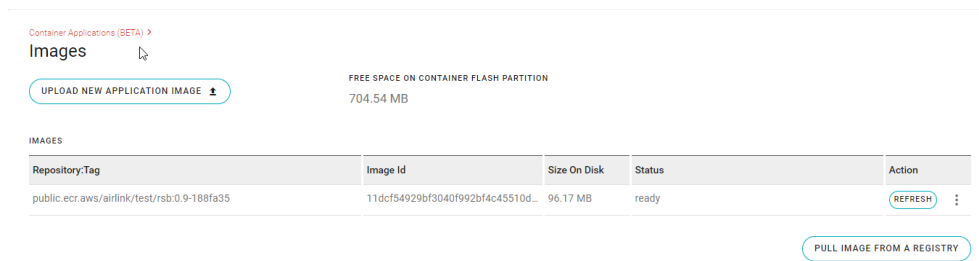
2.3.1.7

Creating Images from the Registry

Procedure:

1. Delete the existing rsb container, volume, and/or image if there are any.
2. Go to **Container Application** → **Images**.
3. Click **PULL IMAGE FROM A REGISTRY**.
4. At the **Image Reference** field, enter: `airlink/test/rsb:0.9-188fa35`.
5. To select registry configuration, click **X** and select **AWSSWIRegistry**.
6. Click **Create** → **Save**.

Figure 36: Images



Result: The modem will display updates in the status field as the image is downloading. When completed, you can create the volume from the config file.

2.3.1.8

Container Volume

The configuration file is uploaded into the container volume. The `config` file is contained in `config.tar`. You can modify the `config.json` file in the `tar` and include the user credentials before uploading the file.

The following items are information on the `config` file.

- The port must match the port that is listed in the Customer Programming Software (CPS) Data Wide section. The port configuration for MG90 is 21010. To keep the XR modem the same as the MG90, you must set the value to 21010.
- The RSB user password must match the password that is used to create the RSB user.
- The time interval sets the rate that the broadcasts are sent out. The recommended time interval is at 1 s or 1000 ms intervals.
- LanSegments are the segments that the broadcasts are sent out to. If required, you can include the default LAN in this segment. MotBridge is the primary LAN segment for these segments.
- You can set the firmware version number in this file. To keep the version in the right range for the radio firmware, you can set the firmware version to 4.4.0.7 or anything above this value. When the XR modem software is higher than this version, this field is no longer required.

This example depicts all the WAN-friendly names that are included in the JSON broadcast. The WAN names must match the names used in the codeplug, if any. This example also turns on the different JSON broadcasts. You can enable or disable the JSON broadcast as needed. True means enabled and false means disabled.

```
{
  "port": 21010,
```

```
"user": {
  "name": "rsb",
  "password": "12345678"
},
"timeIntervalMode": {
  "enabled": true,
  "timeIntervalMS": 1000
},
"wanStateChangeMode": {
  "enabled": true,
  "pollingIntervalMS": 500
},
"lanSegments": [
  "MotBridge"
],
"hardcodeVersion": "4.4.0.7",
"friendlyNameMap": {
  "Ethernet 3": "SAT",
  "XP1 Cellular": " VERIZON",
  "XP2 Cellular": " FirstNet",
  "Wi-Fi B 5GHz": "Wi-Fi-5G",
  "Wi-Fi AP 2.4GHz": "Wi-Fi-2G"
},
"broadcastData": {
  "appVersion": true,
  "osVersion": true,
  "vehicleID": true,
  "ignitionStatus": true,
  "mainBatteryVoltage": true,
  "wanNetworkType": true,
  "wanStatus": true,
  "wanActive": true,
  "wanActive6": true,
  "wanSignalStrength": true,
  "wanCellularRSSI": true,
  "wanCellularRSRP": true,
  "wanCellularRSRQ": true,
  "wanCellularSINR": true,
  "vpnStatus": true,
  "location": true,
  "gnssFix": true,
  "numberOfSatellites": true,
  "gnssAntennaConnected": true
}
}
```

2.3.1.9

Uploading the Container Volume

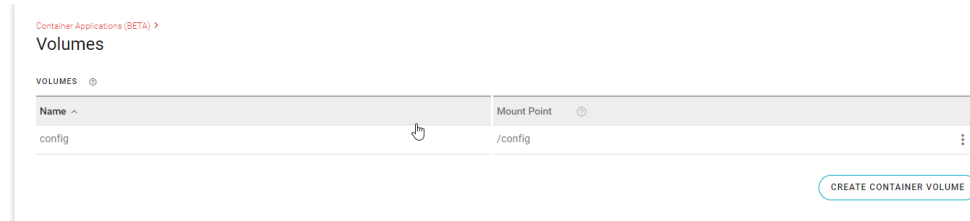
Procedure:

1. Go to **Apps** → **Container Applications** → **Volumes**.
2. Enter a name.
Step example: An example of a name is config.
3. At the **Mount Point** field, insert `/config`.

You can choose a preferred name but **Mount Point** must be `/config`.

4. Upload `config.tar`.
5. Click **Create** → **Save**.
6. Verify that the volume is listed.

Figure 37: Container Volume



2.3.1.10

Creating the Container Application

Procedure:

1. Go to **Apps** → **Container Applications** → **Container Status**.
2. Click **Create Container Application**.
3. Enter a name.
Step example: An example of a name is `rsb`.
4. Turn on **AUTOSTART**.
5. At the **IMAGE** field, select the uploaded container image.
6. At the **VOLUMES** field, select the created `config` option.
7. At the **COMMAND** field, enter: `./init.sh`
8. Turn on **IPV4 AUTO ASSIGNMENT** and **IPV6 AUTO ASSIGNMENT**.

Figure 38: Container Application Configuration

Create Container Application

NAME
rsb

AUTOSTART

IMAGE
public.ecr.aws/airlink/test/rsb:0.9-188fa35

VOLUMES
config

COMMAND
./init.sh

IPV4 AUTO ASSIGNMENT
 On

IPV6 AUTO ASSIGNMENT
 On

CANCEL CREATE

- 9. Click **Create**.
- 10. To apply the command, click **Save**.

Figure 39: Containers Status

Container Applications (BETA) >
Containers Status

CONTAINER LIST

Autostart	Name	Image	Volumes	Status	Logs	Action
<input checked="" type="checkbox"/>	rsb	public.ecr.aws/airlink/test/rsb:0.9-1...	config	running	LOGS ↓	STOP ⋮

CREATE CONTAINER APPLICATION

Result: The container starts running and stops after a short time.

2.3.2 Advanced Setup


These steps are required to access to Customer Enterprise Network (CEN) based applications such as Over the Air Programming (OTAP), Over the Air Rekeying (OTAR), and Intelligent MiddleWare (IMW) based location, text messaging, and applications.

A Virtual Private Network (VPN) is required for connecting the modem and the Customer network where the applications are located.

2.3.2.1

Setting Local Area Network (LAN)


Prerequisites: Ensure that your modem is connected using the provided IP address.

 **NOTE:** The default IP address is 192.168.1.1. while the default username and password is admin. Reset your modem to restore it to the factory default settings if needed.

Procedure:

1. Go to **Networking** → **Zones**.
2. At the **LAN Segments** field, select **Create**.
3. Enter a name.

Step example: An example of a name is MotBridge.

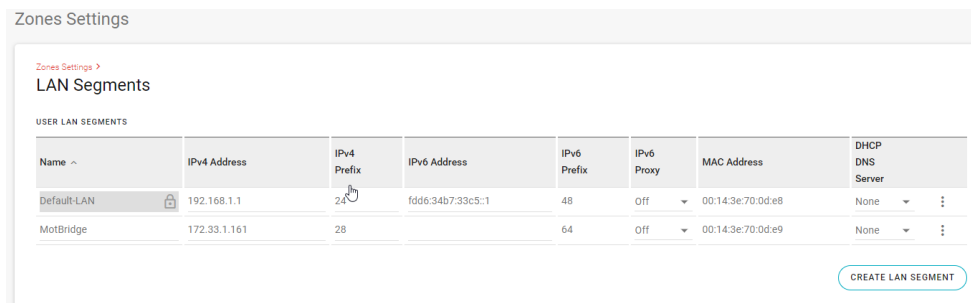
 **IMPORTANT:** You can choose a preferred name but must use the same name throughout the configuration process.

4. Enter the required IPv4 Address.
5. Enter the required IPv4 Prefix.
6. At the **DHCPV4 Server** field, select **On**.
7. Enter the required IPv4 pool starting address.
8. Enter the required IPv4 pool ending address.
9. Select **Create** → **Save**.

Leave the other fields in their default setting.

Result: If successful, the display shows MotBridge line item in the **User LAN Segments** section.

Figure 40: Setting LAN




The screenshot shows the 'ZONES SETTINGS' interface with a 'LAN SEGMENTS' section. Below the section title is a table of 'USER LAN SEGMENTS'. The table has columns for Name, IPv4 Address, IPv4 Prefix, IPv6 Address, IPv6 Prefix, IPv6 Proxy, MAC Address, and DHCP DNS Server. Two rows are visible: 'Default-LAN' and 'MotBridge'. The 'MotBridge' row shows an IPv4 Address of 172.33.1.161, an IPv4 Prefix of 28, an IPv6 Prefix of 64, and an IPv6 Proxy of Off. A 'CREATE LAN SEGMENT' button is located at the bottom right of the table.

Name ^	IPv4 Address	IPv4 Prefix	IPv6 Address	IPv6 Prefix	IPv6 Proxy	MAC Address	DHCP DNS Server
Default-LAN	192.168.1.1	24	fdde:34b7:33c5::1	48	Off	00:14:3e:70:0d:e8	None
MotBridge	172.33.1.161	28		64	Off	00:14:3e:70:0d:e9	None

2.3.2.2

Configuring the Modem to Use the Bridge

This process allows you to assign IP addresses to different LAN segments.

 **NOTE:** In the following example, Ethernet 1 is used for the computer to set up and monitor the modem. Meanwhile, Ethernet 2 is used for the mobile radio ethernet connection. Ethernet 3 is used for the satellite WAN connection.

Procedure:

1. Go to **Hardware Interfaces** → **Ethernet Interfaces** → **Configuration**.

2. To configure Ethernet 1 and Ethernet 2, perform the following actions:
 - a. At the **Enable** field, select **On**.
 - b. At the **WAN Auto Detect** field, select **Off**.
 - c. Set the **LAN Segment** field to **MotBridge**.
 - d. Select **Save**.


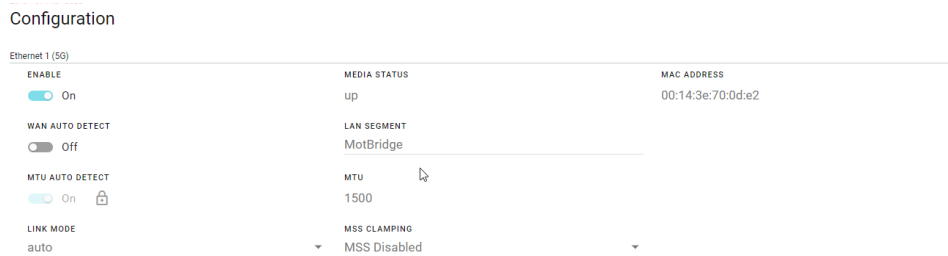
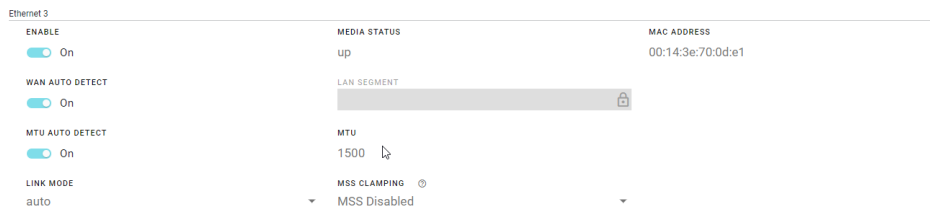
 **NOTE:** After you select **Save**, your computer connection will disconnect. The connection will reconnect with a new IP address from the MotBridge LAN IP address space. This connection process can take a few minutes. Removing and reinstalling the cable can help to speed up the process.

Figure 41: Configuring Ethernet 1 and Ethernet 2



3. To configure Ethernet 3, perform the following actions:
 - a. At the **Enable** field, select **On**.
 - b. At the **WAN Auto Detect** field, select **Off**.
 - c. At the **LAN Segment** field, leave the information as blank.
 - d. Select **Save**.

Figure 42: Configuring Ethernet 3



2.3.2.3

Setting Wi-Fi

The XR80 modem has one bank of Wi-Fi while the XR90 modem has two.

Procedure:

1. Go to **Hardware Interfaces** → **Wi-Fi Interfaces** → **Configuration**.
Local Area Network (LAN) Configuration
2. To edit the **Configuration** field, select the **Pen** icon.
3. Enable the 2.4 GHz and 5 GHz interfaces.
4. At the **Mode** field, select **Access Point**.
5. At the **LAN Segment** field, use one of the following options:

- To perform Simple Setup, select **Default-LAN**.
- To perform Advanced Setup, select **MotBridge**.

Figure 43: Configuring LAN

Enable	Status	Name	MAC Address	Antenna Bank	Mode	LAN Segment
<input type="checkbox"/> On	Configuring	Wi-Fi Client 2.4GHz	00:14:3e:70:0d:e6	B	Client	
<input type="checkbox"/> On	XR90 2.4 GHz (wpa2): Broad...	Wi-Fi AP 2.4GHz	06:14:3e:70:0d:e6	A	Access Point	MotBridge
<input type="checkbox"/> On	XR90-5G (wpa2): Broadcast...	Wi-Fi A 5GHz	00:14:3e:70:0d:e5	A	Access Point	MotBridge
<input type="checkbox"/> On	Disconnected	Wi-Fi B 5GHz	00:14:3e:70:0d:e4	B	Client	

6. Configure the Service Set Identifier (SSID), security mode, and password if required.

Leave the other fields in their default setting.



IMPORTANT: You must perform step [step 2](#) to [step 6](#) to connect data modem tethered devices to the XR modem. Most APX radios can connect using the 2.4 GHz connection. APX NEXT radios and some of the newer APX radios can connect using the 5 GHz connection.

Wide Area Network (WAN) Configuration

7. Enable the 2.5 GHz and 5 GHz WAN interfaces.
8. At the **LAN Segment** field, leave the information as blank.

Client SSID Database Configuration

9. Select **Create SSID**.
10. Enter the access point information.
11. Select **Create** → **Save**.

Figure 44: Configuring SSID

SSID	Security Mode	Status	Priority
Cool-Fi	wpa2	online	

[CREATE SSID](#)

2.3.2.4

Setting a Zone

This process allows your modem to select the correct Wide Area Network (WAN). You can set which connection for your modem to select first.

Procedure:

1. Go to **Networking** → **Zones**
2. At the **Zones** subsection, create a new zone by entering a name for *zone*.

Step example: An example of a name is Motozone.

3. To configure the new zone, arrange the interfaces in the following priority:
 - a. Ethernet 3
 - b. Wi-Fi 5 GHz

- c. Wi-Fi 2.4 GHz
- d. XP1 Cellular
- e. XP2 Cellular
- f. XP1 Ethernet
- g. XP2 Ethernet


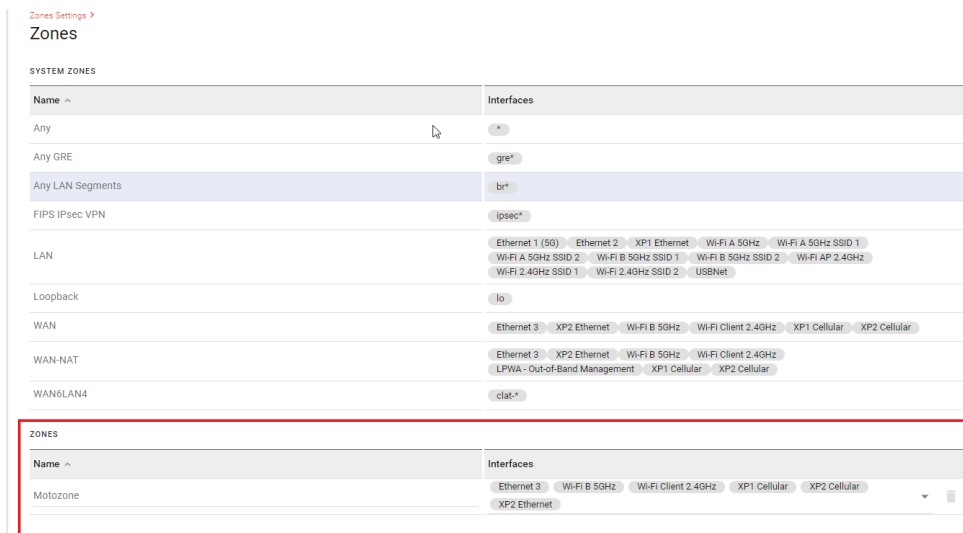
 **NOTE:** The Ethernet 3 is usually given the lowest priority. You can assign the Ethernet 3 with the highest priority to easily connect and disconnect the ethernet cable to allow your modem to switch WAN connection. You can also use the XP1 and XP2 Ethernet interfaces at the side of your modem as WAN or LAN connections.

Figure 45: Setting a Zone

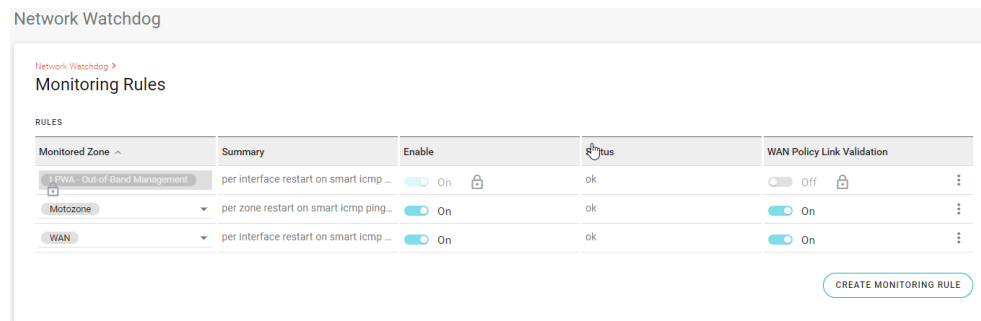


2.3.2.5 Setting Monitoring Rules

Procedure:

1. Go to **Networking** → **Network Watchdog**.
2. Click **CREATE MONITORING RULE**.
3. At the **Monitored Zone** field, select **Motozone**.
4. At the **Action** field, set to **per zone restart**.
5. At the **Method** field, set to **ICMP ping on idle traffic**.
6. At the **Idle threshold** field, enter: 100 kb.
7. At the **Interval** field, enter: 5 min.
8. At the **Max failure** field, enter: 3.
9. At the **Primary host** field, enter: `iana.org`.
10. At the **Secondary host** field, enter: `google.com`.
11. Enable **WAN Policy Link Validation**.
12. Click **Create** → **Save**.

Figure 46: Monitoring Rules



2.3.2.6

Configuring the VPN

Procedure:

1. Go to **Networking** → **VPN**.

2. Click **CREATE IPSEC TUNNEL**.

3. At the **Name** field, select **VPN**.

The name listed here is the friendly name in the JSON broadcasts. It must match the name that you have listed in the radios codeplug as the VPN-friendly name.

4. At the **Mode** field, enter: `Client`.

5. At the **LAN/Host mode** field, select **LAN**.

6. At the **IKE Version** field, select **IKEv2**.

The XR modem primarily supports IKEv2. This must match the VPN server configuration that is listed in the VPN spreadsheet.

7. Disable **Multiple SA's for IKEv2**.

8. Disable **MOBIKE**.

9. At the **Authentication Type** field, enter: `PSK`.

10. At the **PSK** field, enter `<Customer Specific Configuration>`.

11. At the **Peers** field, enter `<Customer Specific Configuration>`.

12. At the **Local Subnet** field, enter `<Customer Specific Configuration>`.

13. At the **Remote Subnet(s)** field, enter `<Customer Specific Configuration>`.

14. Leave the **Exempt Subnet(s)** and **Local Authentication ID** fields blank.

15. At the **Remote Authentication ID** field, enter `<Customer Specific Configuration>`.

16. At the **WAN Interface** field, select **Ethernet3, Wi-Fi b 5GHz, Wi-Fi Client 2.4GHz, XP1 Cellular, and XP2 Cellular**.

The selections must be in the same order as the WAN Interface selected in the Motozone.

17. Enable **Start**.

18. At the **Dead Peer Detection**, select **Restart**.

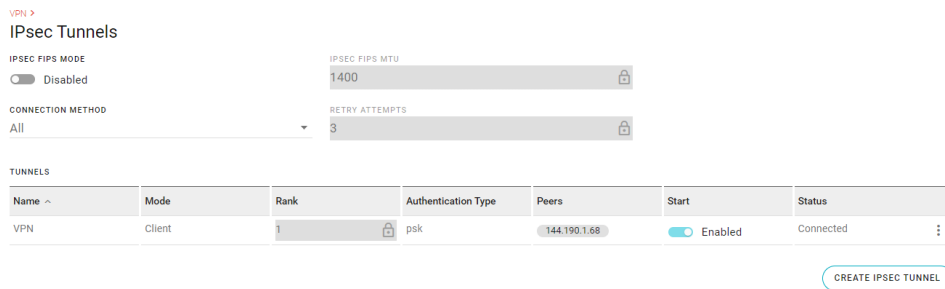
19. At the **DPD Interval** field, enter: `30 seconds`.

20. At the **IKE Rekey Time** field, enter: `7200 seconds`.

21. At the **IKE Encryption** field, enter: `aes256`.

22. At the **IKE Integrity** field, enter: sha256.
23. At the **IKE Diffie-Hellman Groups** field, enter: dh16 (Modp4096).
24. Enable **Perfect Forwarding Security**.
25. At the **ESP Rekey Time** field, enter: 7200 seconds.
26. At the **ESP Encryption** field, enter: aes256.
27. At the **ESP Integrity** field, enter: sha256.
28. At the **ESP Diffie-Hellman Groups** field, enter: dh16 (Modp4096).
29. Click **Create** → **Save**.

Figure 47: IPsec Tunnels



Result: VPN shows as connected.



NOTE: The VPN server for Uranus has been updated to support AES256-SHA256-DH16 encryption. If you are using other VPN server, you need to update it. The XR modem does not support the previous encryption type that was on the MG90 and GX440 based modem.

2.3.2.7

Configuring the Radio to Use the JSON Broadcasts

Procedure:

1. Perform the following procedures from the Simple Setup.
 - a. [Adding New Users to the Container on page 48](#)
 - b. [Enabling Container Usage on page 49](#)
 - c. [Adding New Registries on page 50](#)
 - d. [Creating Images from the Registry on page 51](#)
 - e. [Uploading the Container Volume on page 52](#)
 - f. [Creating the Container Application on page 53](#)
2. Proceed to [Setting the Container to Use MotBridge on page 60](#).

2.3.2.8

Setting the Container to Use MotBridge

Procedure:

1. Go to **Hardware Interfaces** → **Configuration**.
The interface shows a table with LAN Segments.

2. At the Container.rsb entry, set the **LAN Segment** for this container to **MotBridge**.

Figure 48: LAN Segment Configuration for the Container

Configuration

LAN SEGMENTS

Interface	Enable	LAN Segment
Ethernet 1 (5G)	<input checked="" type="checkbox"/> On	MotBridge
Ethernet 2	<input checked="" type="checkbox"/> On	MotBridge
Ethernet 3	<input checked="" type="checkbox"/> On	
LPWA - Out-of-Band Management	<input checked="" type="checkbox"/> On	
rsb	<input checked="" type="checkbox"/> On	MotBridge
USBNet	<input checked="" type="checkbox"/> On	Default-LAN
Wi-Fi 2.4GHz SSID 1	<input type="checkbox"/> Off	Default-LAN
Wi-Fi 2.4GHz SSID 2	<input type="checkbox"/> Off	Default-LAN
Wi-Fi A 5GHz	<input checked="" type="checkbox"/> On	MotBridge
Wi-Fi A 5GHz SSID 1	<input type="checkbox"/> Off	Default-LAN
Wi-Fi A 5GHz SSID 2	<input type="checkbox"/> Off	Default-LAN
Wi-Fi AP 2.4GHz	<input checked="" type="checkbox"/> On	MotBridge
Wi-Fi B 5GHz	<input type="checkbox"/> Off	

3. Restart the application.
4. Go to **Apps** → **Container Applications**.
5. At the **Containers Status** section, perform the following actions.
 - a. If the RSB application is running, stop this application.
 - b. Start the RSB application.
 - c. Verify that the **Status** of the container is *running*.

Figure 49: Containers Status

Container Applications (BETA) >

Containers Status

CONTAINER LIST

Autostart	Name	Image	Volumes	Status	Logs	Action
<input checked="" type="checkbox"/>	rsb	public.ecr.aws/airlink/test/rsb:0.9-1...	config	running	LOGS	STOP

CREATE CONTAINER APPLICATION

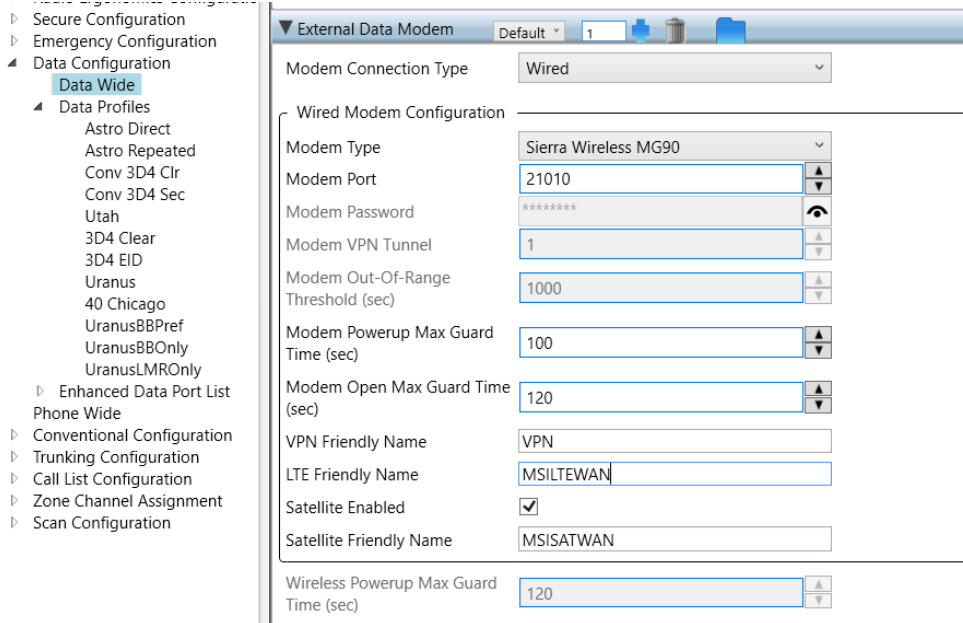
6. To view the application log file, click **LOGS**.
 The logs can take a few minutes to generate and contain broadcasts that are sent.

2.3.2.9

Radio Codeplug Configuration

The radio codeplug configuration for using the XR modem is the same as the configuration for using the MG90 modem.

Figure 50: Radio Codeplug Configuration for Using the Modem



2.3.2.10

Verifying JSON Broadcasts

Procedure:

1. Open a Telnet connection to the radio.
2. Enable the following logs.

```
dcmp:setname:SLIOCOMP:08  
dcmp:setname:UMAC:08  
dcmp:setname:Networking:08
```

Result: The log file lists the broadcasts.

Log File with Broadcast Listing

```
JSON broadcast part 1: {  "appVersion": "1.0",    "version": "4.4.0.7",  
"generalInformation": {    "mainBatteryVoltage": 24.112,    "ignitionOn":  
true  },    "wanState": [    {    "friendlyNa  
JSON broadcast part 2: me": "LPWA - Out-of-Band Management",  
"networkType": "cellular-4G",    "status": 1,    "active": false,  
"active6": false,    "signalStrength": -75,    "  
JSON broadcast part 3: RSSI": -75,    "RSRP": -101,    "RSRQ":  
-13,    "SINR": 2    },    {    "friendlyName": "FirstNet",  
"networkType": "cellular-4G",    "status": 1,    "  
JSON broadcast part 4: active": false,    "active6": false,  
"signalStrength": -74,    "RSSI": -74,    "RSRP": -111,    "RSRQ":
```

```

-18,      "SINR": -200.0    },      {      "friendly
JSON broadcast part 5: Name": "VERIZON",      "networkType":
"cellular-4G",      "status": 1,      "active": false,      "active6":
false,      "signalStrength": -65,      "RSSI": -65,      "R
JSON broadcast part 6: SRP": -97,      "RSRQ": -15,
"SINR": -1    },      {      "friendlyName": "SAT",      "networkType":
"ethernet",      "status": 1,      "active": true,      "active
JSON broadcast part 7: 6": true    },      {      "friendlyName":
"XP2 Ethernet",      "networkType": "ethernet",      "status": 0,
"active": false,      "active6": false    },      {
JSON broadcast part 8: "friendlyName": "XP1 Ethernet",      "networkType":
"ethernet",      "status": 0,      "active": false,      "active6":
false    },      {      "friendlyName": "Wi-Fi Cli
JSON broadcast part 9: ent 2.4GHz",      "networkType": "wifi",
"status": 1,      "active": false,      "active6": false,
"signalStrength": -61    },      {      "friendlyName": "Wi-F
broadcast part 10: i-5G",      "networkType": "wifi",      "status":
1,      "active": false,      "active6": false,      "signalStrength":
-60    }    ],      "vpnState": [      {      "frien
JSON broadcast part 11: dlyName": "VPN",      "status": 1    }    ],
"gnssStatus": {      "antennaConnected": true,      "numberSatellites": 6,
"fix": true    },      "location": {      "latitude": 2
JSON broadcast part 12: 6.65468,      "longitude": -80.20021    },
"vehicleID": "~",      "timestamp": {      "date": "01112023",      "time":
"2017"    }
  
```

2.4

Motorola Solutions VML750 Configuration

This section explains the configurations for the Motorola Solutions VML750 modem.

2.4.1

USB Configuration for VML750

Enable DHCP Server on the router, and ensure that the addresses in the DHCP pool do not conflict with any other subnets configured in the APX Mobile radio codeplug (Serial Link1, CAI, and so on). If the router uses a VPN in Site-to-Site mode to support multiple radios, each router must have a DHCP pool with a unique VPN Configuration.

- Clear Connection: 192.168.15.0/24 safe example DHCP pool for clear.
- VPN Connection (SHOWN): 172.16.1.0/24 example DHCP pool for VPN.

Figure 51: USB Configuration for VML750



Take note that there is a control layer for transferring router status information between the APX radio and the external router. The UDP port 49480 is used internally for this purpose.

2.4.2 Wi-Fi Configuration for VML750

The third-party router uses DHCP to assign IP addresses, so DHCP pools must be set up as described in [USB Configuration for VML750 on page 63](#).


 **NOTE:** The external router Wi-Fi is configured separately from the Wi-Fi field in the Customer Programming Software (CPS) R17.00.00 or later.

Figure 52: VML750 Wi-Fi Configuration (General)

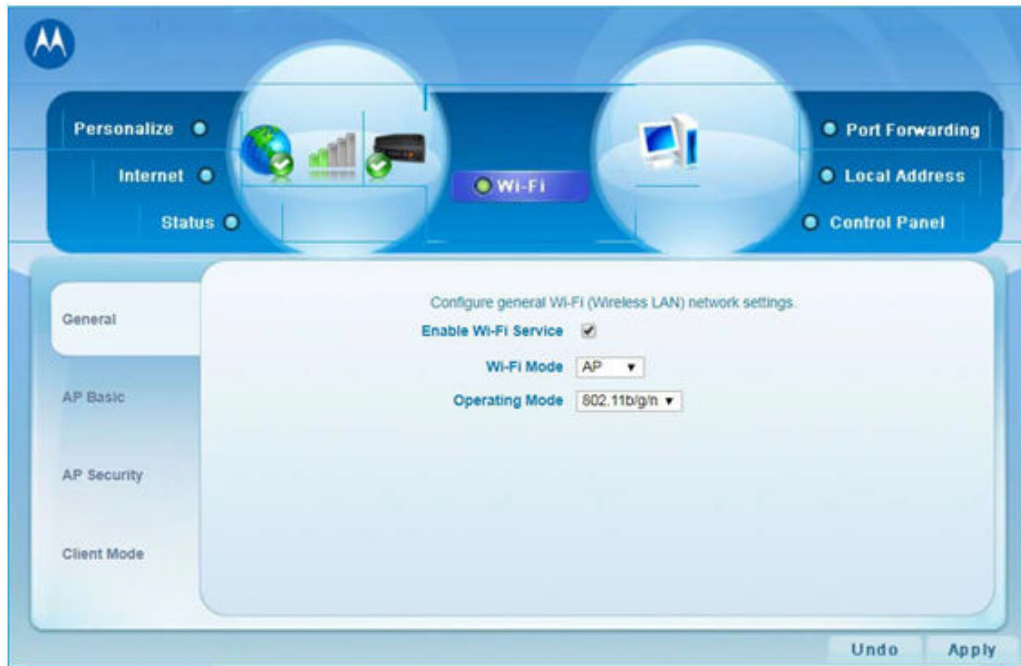


Figure 53: VML750 Wi-Fi Configuration (AP Basic)



Figure 54: VML750 Wi-Fi Configuration (AP Security)

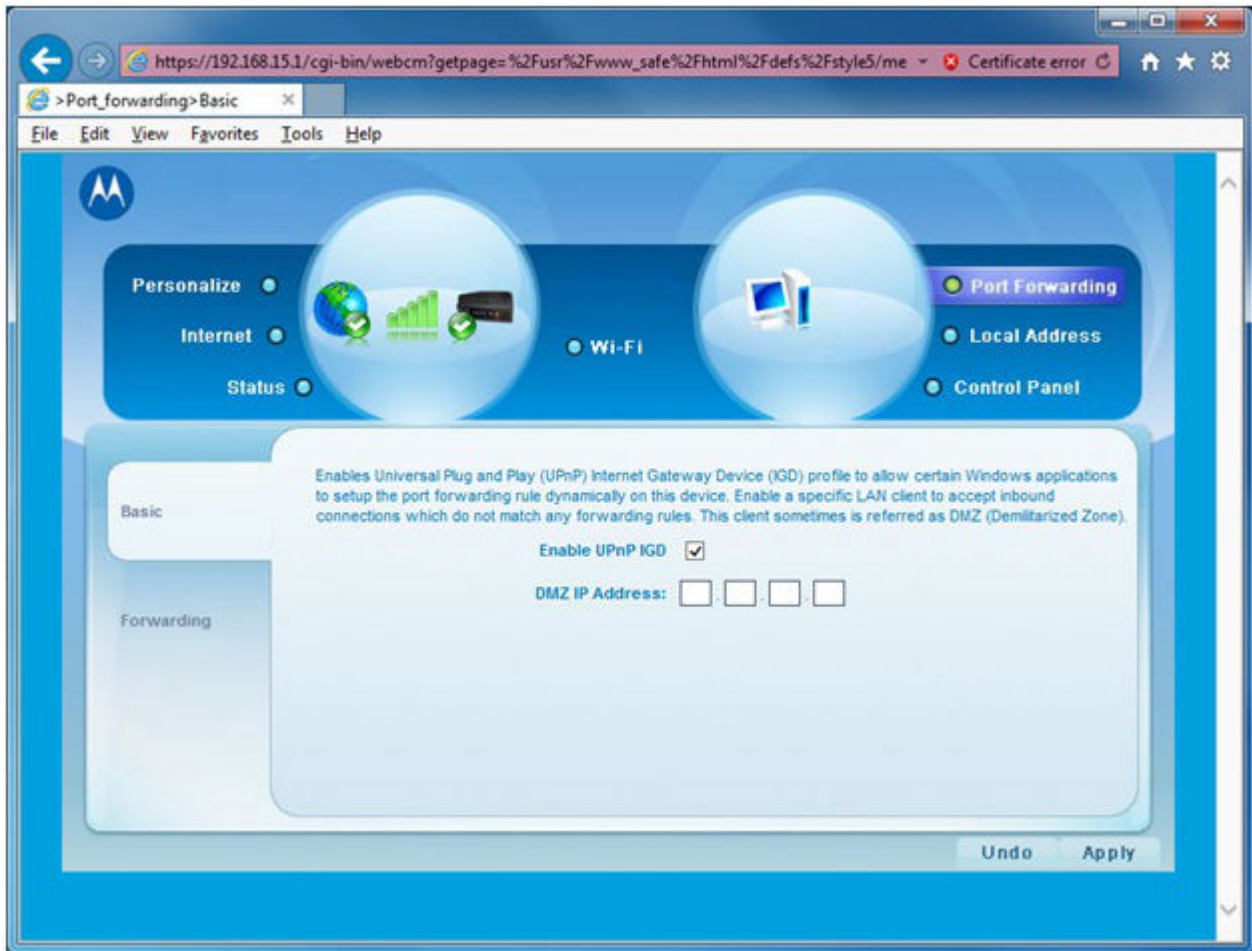


2.4.3

Port Forwarding Configuration for VML750

When the Data Modem tethering solution is configured to run in either a Clear or Remote Access VPN configuration, configure port forwarding must in the router for unsolicited data requests to arrive at the radio. All internal Apps and the Terminal Data apps listed in the radio NAT List are automatically configured in the router.

Figure 55: VML750 Port Forwarding Configuration



2.4.4

DMZ Usage

It is not advisable to use DMZ option on the third-party router when connecting to a radio. The DMZ option selects a local area network as the default route for unsolicited data requests from the infrastructure to the router.

The DMZ option implementation is manufacturer-specific and could invalidate the port forwarding entries added in the steps above. Only advanced users of the router should use the DMZ option with the APX radio.

2.4.5

VPN Configuration for VML750

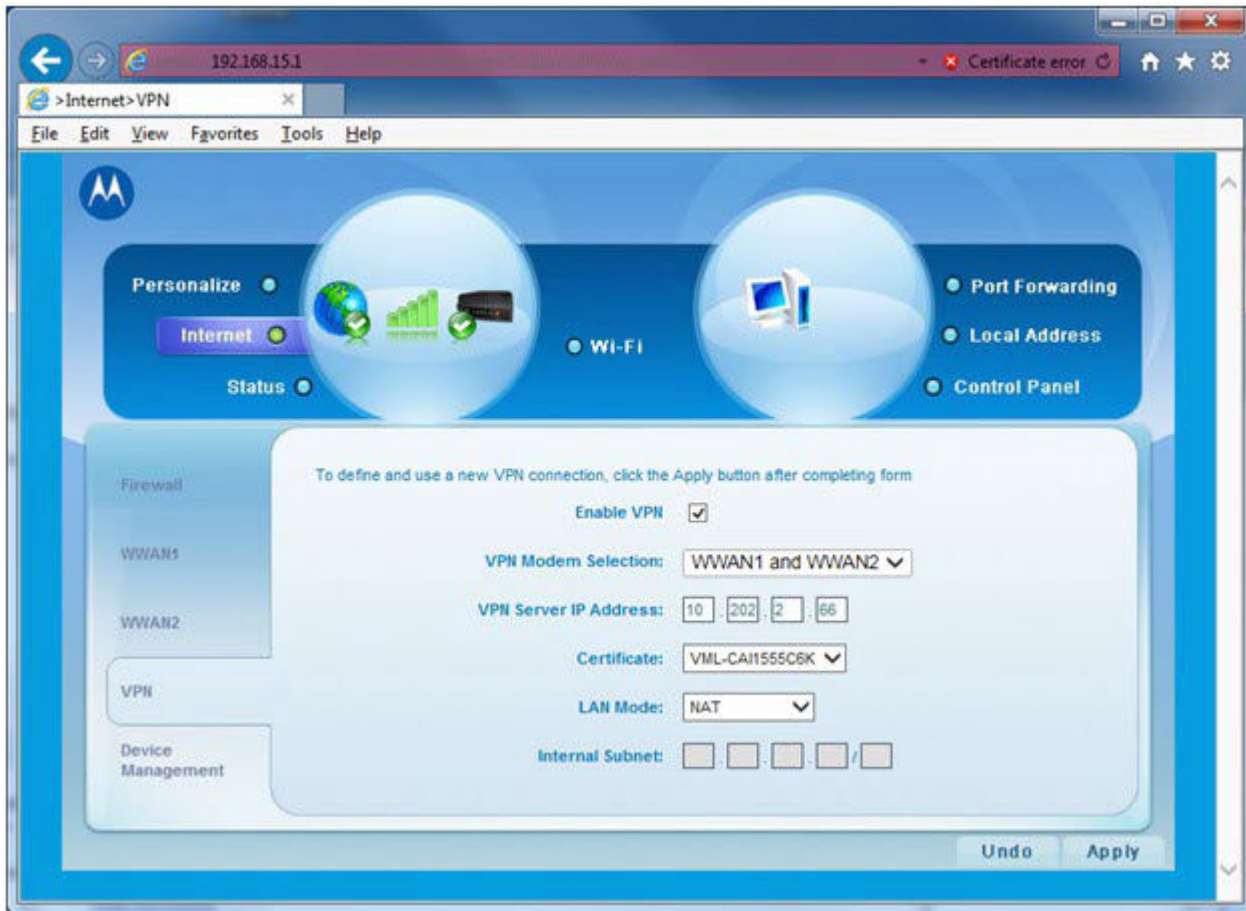
Remote Access VPN Tunnel Mode

A remote access VPN connection is made by a remote access client. A remote access client is a single computer user (VML750) who connects to a private network from a remote location. The VPN server provides access to the resources of the network to which the VPN server is connected. The packets sent across the VPN connection originate at the VPN client. In Remote Access VPN Tunnel Mode, only one radio may be connected to the VML750. To support multiple radios, it is necessary to use a Site-to-Site VPN Tunnel Mode.

The VPN client authenticates itself to the VPN server and, for mutual authentication, the VPN server authenticates itself to the VPN client. When a remote access connection is established, the VPN server assigns a dynamic IP to the VPN Client. Traffic originated from devices connected to the router private LAN is NATed to the obtained dynamic IP before any encryption.

- **Enable VPN** = Selected
- **VPN Modem Selection**⁵ = **None** or **WWAN1 and WWAN2**
- **VPN Server IP Address** = *<Customer Specific Configuration>*
- **Certificate** = *<Customer Specific Configuration>*
- **LAN Mode** = NAT

Figure 56: VML750 Remote Access VPN Tunnel Mode Configuration



Site-to-Site VPN Tunnel Mode

The VML750 also supports a Site-to-Site VPN Tunnel Mode. To use Site-to-Site Mode, the LAN Mode should be set to Mobile Router on the VPN tab of the configuration client. This mode is useful if multiple radios are simultaneously connected to the VML750. The addressing scheme used in Site-to-Site mode allows for servers in the CEN to communicate with each radio seamlessly through the VML750.

When deploying a Site-to-Site VPN, it is important that each VML750 in the customer fleet be assigned a DHCP address pool that is in a unique subnet, and a connection profile for each VML750's subnet must be

⁵ The VML allows settings **WWAN1 Only** or **WWAN2 Only**, but selecting these options cause data routing problems when the router switches between WWAN1 and WWAN2.

configured within the VPN server. This is necessary for the VPN Server to know which VML750 it should send data to in order to reach a particular radio.


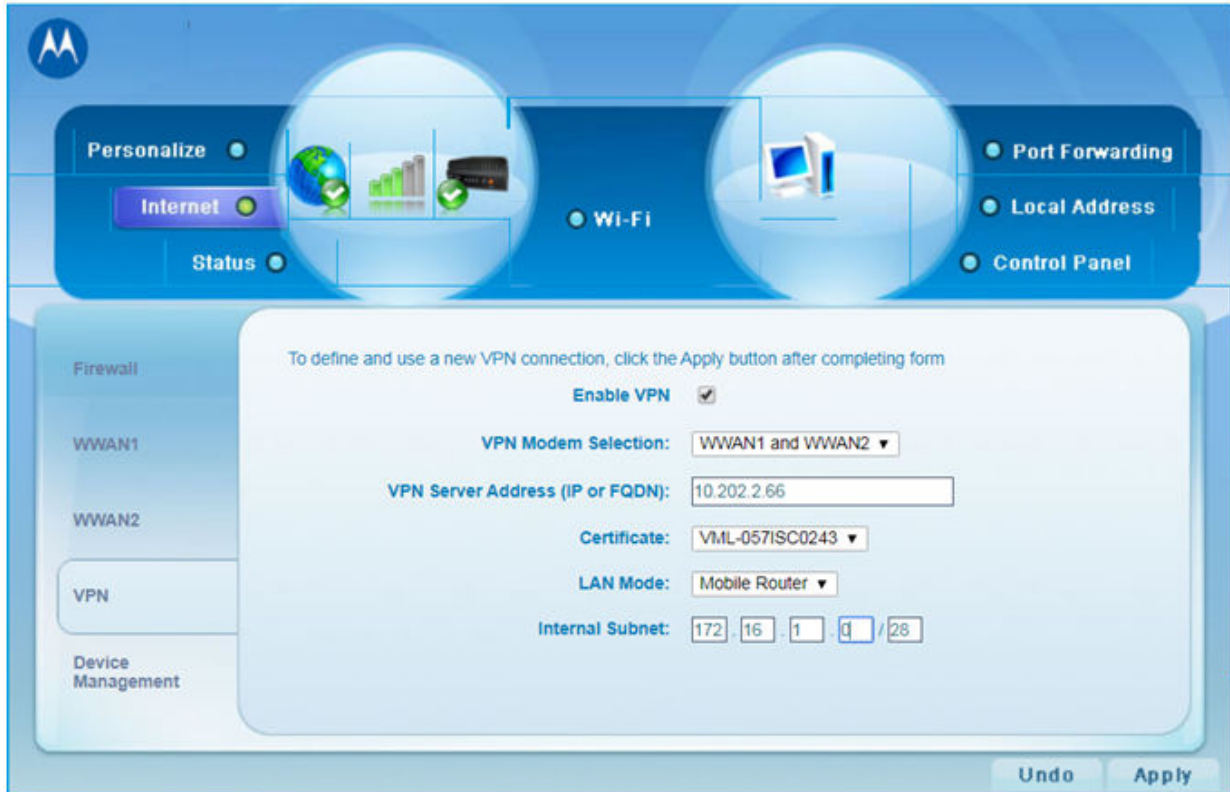
 **NOTE:** This setup example follows the configuration in the VPN Gateway for a 172.16.1.0/28 site.

Figure 57: VML750 Site-to-Site VPN Tunnel Mode Configuration



The screenshot displays the configuration interface for a VML750 device. The top navigation bar includes 'Personalize', 'Internet', 'Status', 'Wi-Fi', 'Port Forwarding', 'Local Address', and 'Control Panel'. The 'Internet' section is active, showing a sidebar with 'Firewall', 'WWAN1', 'WWAN2', 'VPN', and 'Device Management'. The 'VPN' section is expanded, displaying the following configuration options:

- Enable VPN:**
- VPN Modem Selection:** WWAN1 and WWAN2
- VPN Server Address (IP or FQDN):** 10.202.2.66
- Certificate:** VML-057ISC0243
- LAN Mode:** Mobile Router
- Internal Subnet:** 172.16.1.0 / 28

Buttons for 'Undo' and 'Apply' are located at the bottom right of the configuration area.

Chapter 3

APX Radio User Interface

3.1

Network Selection

Each radio may be programmed to operate with an attached external router. The access technology (LTE, 3G, etc.) and band class (BC14, BC13, etc.) for this router is irrelevant to the APX Radio.

Connectivity from this external router to the CEN (Customer Enterprise Network) must be configured, and a VPN link is recommended to secure this traffic. VPN is recommended when using a public connection.

Data service is configurable in the Customer Programming Software (CPS) for three radio modes: Broadband Only, Broadband Preferred, and Land Mobile Radio (LMR) Preferred.

Broadband Only

In this mode, all data is sent and received over the broadband network. ASTRO data service is not used. The Broadband Only mode is recommended for:

- LMR network that does not support LMR data services
- Conventional systems in which LTE and Satellite operation is required.
- ASTRO network with data services where expansion of the data services using ASTRO data channels is not desirable
- Broadband (Broadband i.e. LTE, 3G, etc.) *coverage seams* to avoid frequent switches between networks



NOTE: *Coverage seams* refer to gaps in Broadband coverage.

Broadband Preferred

All data is sent and received over the broadband network when it is available. ASTRO data service is used when broadband is not available. Broadband Preferred is available through the Customer Programming Software (CPS) with two options: Trunking & Broadband or Conventional & Broadband. Under certain conditions, a switch to either LMR or Broadband is triggered. The table illustrates network switch behavior.

Table 9: Network Selection between LMR and a Single Broadband WAN


Network Switch	Cause
Broadband to LMR	Loss of Broadband coverage Loss of Virtual Private Network (VPN) tunnel User presses MODM Off button
LMR to Broadband	Broadband coverage available Return to Broadband coverage User presses MODM On button where Broadband coverage is available

Broadband Preferred with Satellite

Under certain conditions, a switch to either LMR, LTE, or SAT is triggered. Cellular/LTE connection is preferred over Satellite when both are available. The table illustrates network switch behavior for MG90.

Table 10: Network Selection between LMR and a Modem with Cellular and Satellite WANs

Network Switch	Cause
Cellular to LMR	Loss of cellular coverage Loss of VPN tunnel User presses MODM off button
LMR to Cellular	Cellular coverage available User presses MODM on button whilst in cellular coverage
Cellular to SAT	MG90 modem indicates that Cellular service is not available but SAT service is available
SAT to Cellular	MG90 modem indicates that Cellular service is available

 **NOTE:** The radio will not switch to SAT if there is an LMR data connection available.


LMR Only

In the LMR Only mode, LMR data service is used. For LMR, two profile options are available with the Customer Programming Software (CPS): Trunking or Conventional. This mode is useful where LMR is preferred in areas of Broadband *coverage seams* to avoid frequent switches between networks. LMR Only may also be selected to minimize data costs. LMR Only mode may also be used when the network is not ready for Broadband. This situation can occur when the network expansion has not been completed.

3.2

Modem On/Off Button

The APX™ Radio MODM On/Off function may be used if the radio is programmed to operate in one of the broadband capable modes. This function is used to turn the APX Data Modem Tethering feature On/Off.

 **NOTE:** Some versions of the MG90 software utilize the MODM button for on/off control. Generic modem uses EMOD button for on/off control.

The MODM On/Off function is not remotely turning the attached external router On/Off. When the APX Radio is configured to connect to the external router using Wi-Fi, the act of turning the MODM function On will also activate Wi-Fi automatically if Wi-Fi is off.

The MODM On/Off function is accessible from the programmable buttons or from the radio menu selection. Five programmable buttons on the O3 control head, five bottom function programmable buttons on the O9 control head, and three programmable buttons on the Keypad Mic, are available for this feature as indicated in the diagram. The programmable buttons can be configured by a technician in your organization, using the Radio Management Customer Programming Software (CPS) available from Motorola Solutions. In CPS, go to **Radio Ergonomics Configuration** → **Controls (Mobile)** → **Control Head O2/O3/O5/O7/Keypad Mic and Accessories** → **Button Selections**. Your organization must inform radio users regarding the button assignments.

Figure 58: APX Mobile O2 Control Head Programmable Buttons



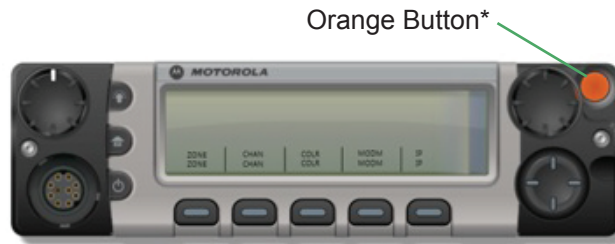
* These radio buttons are programmable

Figure 59: APX Mobile O3 Control Head Programmable Buttons



* These radio buttons are programmable

Figure 60: APX Mobile O5 Control Head Programmable Buttons



* These radio buttons are programmable

Figure 61: APX Mobile O7 Control Head Programmable Buttons



Orange Button*

* These radio buttons are programmable

Figure 62: APX Mobile O9 Control Head Programmable Buttons



Orange Button*

P1-P5 Button*

* These radio buttons are programmable

Figure 63: APX Mobile Keypad Mic Programmable Buttons



Side Top Button*

Side Middle Button*

Side Bottom Button*

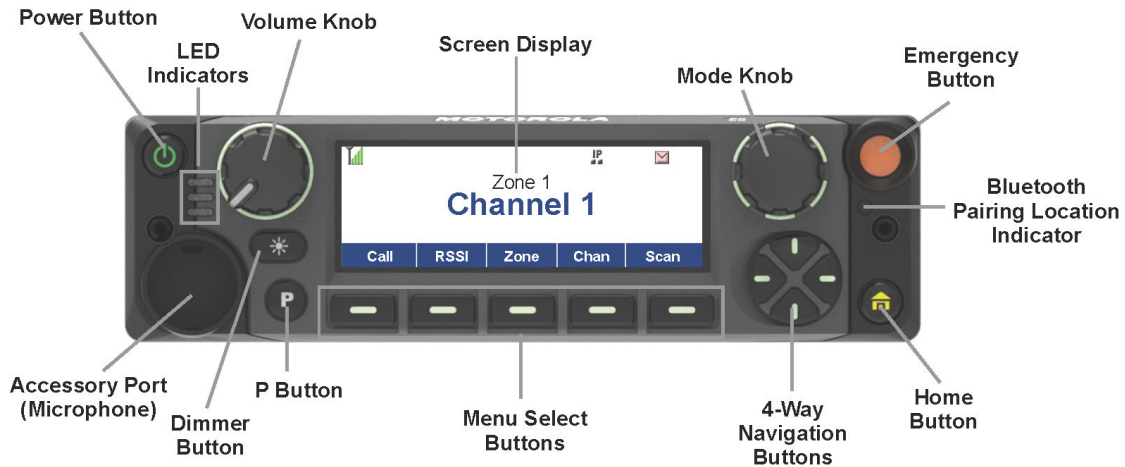
* These radio buttons are programmable

Figure 64: APX Portable Programmable Buttons



Figure 65: APX Mobile E5 Control Head Programmable Buttons

E5 Control Head



3.2.1

Turning On the Modem at the Modem Menu Screen

Procedure:

1. Perform one of the following actions:
 - Press the **MODM** button to enter the **MODM** screen.

- Press **Left** or **Right** to `Modem`. Press the **Menu Select** button directly below `Modem` to enter the **Modem** screen.

If external router is not ready or busy setting up, the display shows `Please wait`. Once the external router is ready, the display shows the **Modem** screen.

2. Perform one of the following actions:

- Press and hold the **Modem** button.
- Press the **Menu Select** button directly below `On` to enable router connection.

The screen prompts `Modem on` to indicate radio is initiating the external router connection. The **Status** shows `Connecting...` to indicate the radio is initiating connection to external router system.

Result: The display shows `Modem connected` once the radio is connected. The **Status** shows `Connected`. The external router icon appears at the display to indicate external router is connected. For MG90, the display shows `Modem active` once the modem is connected, selected a connection, and established VPN connection (if it has any). If there is an error where the router cannot establish a connection, the display shows `Modem error`.

If there is an error in which the external router cannot establish a connection with the carrier network due to misconfiguration (VPN or network access), lack of valid subscription, etc, the display shows `Modem service error` and the **Status** shows `Service error`.

If there are no external router networks available, the display shows `Modem no service` and the **Status** shows `No service` until successfully connected to external router or encounter service error.



NOTE: It is advisable to turn off the router if the radio prompts `Modem service error` or `Modem no service`. For the error no external router service available, turn on the router after you moved to another site to check the availability.

3.2.2

Turning On the Modem with Modem Button

Procedure:

Press and hold the preprogrammed **Modem** button.

The display shows `Modem on` to indicate radio is initiating the external router connection.

Result: The display shows `Modem connected` once the radio is connected and the **Status** shows `Connected`. The external router icon appears at the display to indicate router is connected. For MG90, the display shows `Modem active` once the modem is connected, selected a connection, and established VPN connection (if it has any). If there is an error where the router cannot establish a connection, the display shows `Modem error`.

If there is an error in which the external router cannot establish a connection with the carrier network due to misconfiguration (VPN or network access), lack of valid subscription, etc, the display shows `Modem service error`.

if there are no external router networks available, the display shows `Modem no service`.



NOTE: It is advisable to turn off the external router if the radio prompts `Modem service error` or `Modem no service`. For the error no external router service available, turn on the router after you moved to another site to check the availability.

3.2.3

Turning Off the Modem Connection

Procedure:

- Turning Off the Modem Connection via preprogrammed **Modem** button:
 - a. Press the preprogrammed **Modem** button to enter `Modem` screen.
 - b. Press and hold the preprogrammed **Modem** button.

The display shows `Modem Off` and the **Status** shows `Off` and the external router icon disappears to indicate the router connection is off.

- Turning Off the Modem Connection via `Modem` radio menu:
 - a. Press **Left** or **Right** to `Modem` and press the **Menu Select** button directly below `Modem` to access the `Modem` screen.
 - b. Press the **Menu Select** button directly below `Off` to disable router connection.

The display shows `Modem Off` and the **Status** shows `Off` and the external router icon disappears to indicate the router connection is off.

- c. Press the **Menu Select** button below `Exit` to return to Home screen.

3.3

Information at the Modem Screen

Here are the definitions of the statuses appeared below the `Status`, `Network` and `Signal Strength` shown on the `Modem` screen.

- The definitions of different statuses shown below the `Status` of `Modem` screen:

Connecting

The radio is trying to connect to an external router.

Connected

External router communication is currently on.

Disconnected

External router communication is currently disconnected.

Disabled

External router communication is currently disabled on the selected channel.

Off

External router communication of the radio is currently off.

No Service

No external router service detected at the current site.

Service Error⁶

There is an external router service error.

Modem Error⁶

Radio fails to communicate with the external router.

- The definitions of different statuses shown below the `Network` of `Modem` screen:

⁶ Bring the radio to the qualified technician to check the issue if the error persists.

<Network name>

The currently connected external router network name.

Unavailable

No external router network connected currently.

- The definitions of different statuses shown below the *Signal Strength of Modem* screen:

Please wait

The radio is trying to connect to an external router.

Unavailable

The radio does not have an external router connection currently.

Rating of the signal strength

You see one of the following rating when external router is connected:

Excellent > Good > Fair > Poor

VPN Status⁷

VPN established when the VPN has been established to the CEN and VPN not established when the VPN has not been established

3.4

Scenario of Changing from External Router-enabled Channel to External Router-disabled Channel

When entering a non-external router channel the status field in the Modem screen shows *Disabled*. Press or press and hold of the Modem button prompts short, low-pitched tone.

If the display is showing Modem screen when entering the external router-disabled channel, the display returns to Home screen immediately.

3.5

Scenario of Changing from External Router-Enabled Channel to Unprogrammed Channel

When entering an unprogrammed channel the display prompts *Unprogrammed* and the Modem menu disappears. Pressing the Modem button prompts short, low-pitched tone.

If the display is showing Modem screen when entering the unprogrammed channel, the display returns to Home screen immediately and you are unable to see nor access the Modem screen.

3.6

Scenario of Entering or Exiting Out-of-Range Site

When the radio moves beyond the external router network coverage, which means out-of-range, the radio prompts *Modem no service*. The modem screen is accessible. Refer to [Information at the Modem Screen on page 76](#) for the status shown at the Modem screen.


With the external router of the radio turned on, when the radio moves back to external router connected site, the radio prompts *Modem connected* and *Modem Active* for MG90.

⁷ For the MG90 modem only.

3.7

Status Icons

This section explains the icons related to the Data Modem Tethering feature that is displayed on the radio.

 **NOTE:** Some versions of the MG90 software do not indicate data activity arrows in the icons. When the radio has dynamic icons enabled and configured for MG90, the radio shows two icons, data icon and connection icon.












Icon/MG90 Data Icon	Description
BB	Broadband Network is Active Steady – Broadband Network is available and connected. Blinking – ARS user login failed while in Broadband Network.
↓ BB	Broadband Receiving The radio is receiving Broadband traffic.
↑ BB	Broadband Transmitting The radio is transmitting Broadband traffic.
↕ BB	Broadband Receiving and Transmitting The radio is receiving and transmitting Broadband traffic.
▪ BB	Broadband with ARS User Logged In Indicating ARS user logged in successfully with Broadband Network.
▪↓ BB	Broadband Receiving while ARS User Logged In Indicating ARS user logged in successfully with Broadband Network.
▪↑ BB	Broadband Transmitting while ARS User Logged In The radio is transmitting Broadband traffic with ARS user logged in.
▪↕ BB	Broadband Receiving and Transmitting while ARS User Logged In The radio is receiving and transmitting Broadband traffic with ARS user logged in.
	Ethernet is Active The radio is connected to an Ethernet device.
	Wi-Fi is Active The radio is connected to a Wi-Fi network. The number of bars displayed represents the signal strength of the Wi-Fi signal.

Table 11: MG90

Icons	Description
SAT	SAT Network is Active Steady – Satellite system is available and connected. Blinking – ARS user login failed while in Satellite system.

Icons	Description
	SAT Receiving The radio is receiving Satellite signal.
	SAT Transmitting The radio is transmitting Satellite signal.
	SAT Receiving and Transmitting The radio is receiving and transmitting Satellite signal.
	SAT with ARS User Logged In Indicating ARS user logged in successfully with Satellite system.
	SAT Receiving while ARS User Logged In Indicating ARS user logged in successfully with Satellite system.
	SAT Transmitting while ARS User Logged In The radio is transmitting Satellite signal with ARS user logged in.
	SAT Receiving and Transmitting while ARS User Logged In The radio is receiving and transmitting Satellite signal with ARS user logged in.
	VPN Network is Active Shown on the connection icon
	Ethernet is Active The radio is connected to an Ethernet device.

3.8

Types of Data Features Supported By the Radio

The following section provides overviews of the customer applications and scenarios supported by the radio using the external router tethering feature:

- Over-The-Air Programming (OTAP) using:
 - Customer Programming Software (CPS) R15.00.00 or later for wired configuration and R17.00.00 or later for Wi-Fi configuration.
 - Unified Network Services (UNS) 3.0 or later for basic Presence service.
- Firmware Update over Broadband using Unified Network Services (UNS) 5.1 or later for Enhanced Server Mode Presence service.
- Over-The-Air Re-keying (OTAR) using Key Management Facility (KMF) R7.14 or later.
- ASTRO® 25 Advance Messaging Solution (AMS) 2.0 or later, using UNS 3.0 or later for Presence Service.
- Location Service using UNS 3.0 or later.
- Presence Service using UNS 3.0 or later.
- Motorola Solutions Mobile Virtual Private Network (VPN) Gateway (Requirement of MG90, Optional but recommended for others.)
- SmartConnect

Table 12: Network Components Required for Broadband

Data Features or Components	UNS	KMF	CPS/Radio Management	AMS	Firewalls/ Switches
Codeplug Programming (OTAP)			Required		Required
Firmware Update over Broadband			Required		Required
OTAR		Required			Required
Messaging	Required			Required	Required
Location	Required				Required
Presence	Required				Required
Mobile VPN Gateway		Recommended			Required
SmartConnect					Required
Sensor Request Response Protocol (SRRP)	Required				Required

Codeplug and Firmware Programming Scenario for Radios with Data Modem Tethering

The radio can receive codeplug programming downloads over the broadband datapath provided by the attached external router. The codeplug is a configuration file that contains operation parameters and defines the radio *personality*. The firmware is the operational software that executes in the radio, firmware download enables OTA bug fixes and new features to be deployed remotely.

The following applications can be present on the radio for this scenario:

OTAP

Receives codeplug and/or firmware downloads from the Customer Programming Software (CPS) application.

Motorola Solutions Mobile VPN Gateway

Provides secure communication on the Broadband air interface with the external router.

Automatic Registration Service (ARS) for Presence Service

Uses the ARS Registration Interface to register with the Presence Serve in the UNS.

The advantages of using the broadband network compared to the Land Mobile Radio (LMR) for OTAP codeplug programming are:

- Subscriber units can receive and transmit LMR voice while simultaneously performing data operations over Broadband.
- Radios may be re-programmed over Broadband at any time without impacting the LMR network.
- Each subscriber unit moved to Broadband data reduces the demand on the LMR data network.

Firmware download is not supported on an LMR data channel, but is only supported over the Broadband channel utilized by the attached external router.

OTAR Scenario for Radios with Data Modem Tethering

OTAR is used for remotely managing encryption keys for voice and data. OTAR provides the ability to re-key portable and mobile radios remotely over an RF channel. Encryption keys for voice and data are initially

loaded into the device locally by a handheld portable device called the Key Variable Loader (KVL). New keys are sent in OTAR messages by the Key Management Facility (KMF). OTAR reduces the manpower and time in the field to rekey radio users manually. While OTAR is available in the LMR network, Broadband increases the performance for receiving new keys.

See the *ASTRO 25 Secure Communications - System Perspective* manual for more information on OTAR.

Messaging Scenario for Radios with Data Modem Tethering

The ASTRO® 25 Advanced Messaging Solution provides a mechanism to send text messages to radio users. Data Modem Tethering supports any version of the ASTRO® 25 Advanced Messaging Solution compatible with the ASTRO® 25 infrastructure release in which the solution is deployed. To enable ASTRO® 25 Advanced Messaging Solution for the radio, the UNS Presence Service is required.

The ASTRO 25 Advanced Text Messaging Solution consists of the PremierOne Server, the Smart Client, and the subscriber unit. Text messaging allows you to send information in a text format as a supplement to voice. Text messaging provides an alternative means of communication when voice communication is not practical or possible. Text messaging also provides a written record of information for later use, such as destination address for the next assignment or the status of a delivery. Be On the Lookout (BOLO) messages are high priority messages that might include missing/wanted persons or missing vehicles. BOLO messages are broadcast messages sent to user groups or talkgroups. Broadband data provides for faster delivery of text messages.

The following application must be present (as a client application on the radio, with a corresponding server in the Applications Network) for this scenario:

ASTRO Advanced Messaging Solutions application

Interfaces with the PremierOne server to receive text messages.

Automatic Registration Service (ARS)

Uses the ARS Registration Interface to register with the Presence Server in the UNS. Applications can subscribe to the presence of a subscriber unit, to be notified of the subscriber unit being active or not on the system, and the IP address currently allocated to the subscriber unit.

Location and SRRP Services Scenario for Radios with Data Modem Tethering

The UNS Location Service is a resource tracking solution that uses Global Positioning System (GPS) satellites to enable operators to locate and track outdoor personnel and vehicles. UNS Location Service enables third-party applications to monitor and archive the current location of GPS-based location reporting devices deployed in different types of radio access networks. For a radio with external Data Modem Tethering in Broadband Only or Broadband Preferred mode, the GPS location is sent over the Broadband network to a GPS application in an Applications Network.

The following applications must be present (as client applications on the radio, with a corresponding server in the Applications Network) for this scenario:

Location application

Periodically interfaces to the Location Server in the UNS to report its current location.

Automatic Registration Service (ARS) for Presence Service

Location Service relies on Presence Service and uses the ARS Registration Interface to register with the Presence Server in the UNS. Applications can subscribe to the presence of a subscriber unit, to be notified of the subscriber unit being active or not on the system, and the IP address currently allocated to the subscriber unit.

SmartConnect

When SmartConnect is active, the radio sends P25 voice and control packets to the SmartConnect gateway that is located in the Microsoft Azure cloud. The radio forms a TLS/TCP connection to the gateway for control signaling and a SRTP/UDP connection for voice packets. The MG90 modem must be configured to allow both the TCP connection and the UDP connection to the cloud.

SmartConnect should not use the VPN connection in the MG90 that is directed to the Motorola Solutions Customer Enterprise Network (CEN) where the other Motorola Solutions data services (such as the UNS and KMF) are located.

SmartConnect uses a DNS lookup to establish the TLS/TCP to the gateway so a fixed IP address is not available for the gateway control connection. The UDP IP address is supplied when the radio connects to the gateway and is also not a fixed IP address.

SmartConnect is a feature that is initiated at the radio, so dynamic NAT rules are automatically generated in the modems to handle proper routing of packets back to the radio.

For more information, see [Models of Data Routers Supported on page 17](#).

Chapter 4

Agency Applications Network

This chapter describes the agency architecture used for APX™ Data Modem Tethering solution.

4.1

Architecture That Supports APX Data Modem Tethering

The APX Data Modem Tethering solution is a converged ASTRO and Broadband system with the addition of the following components:

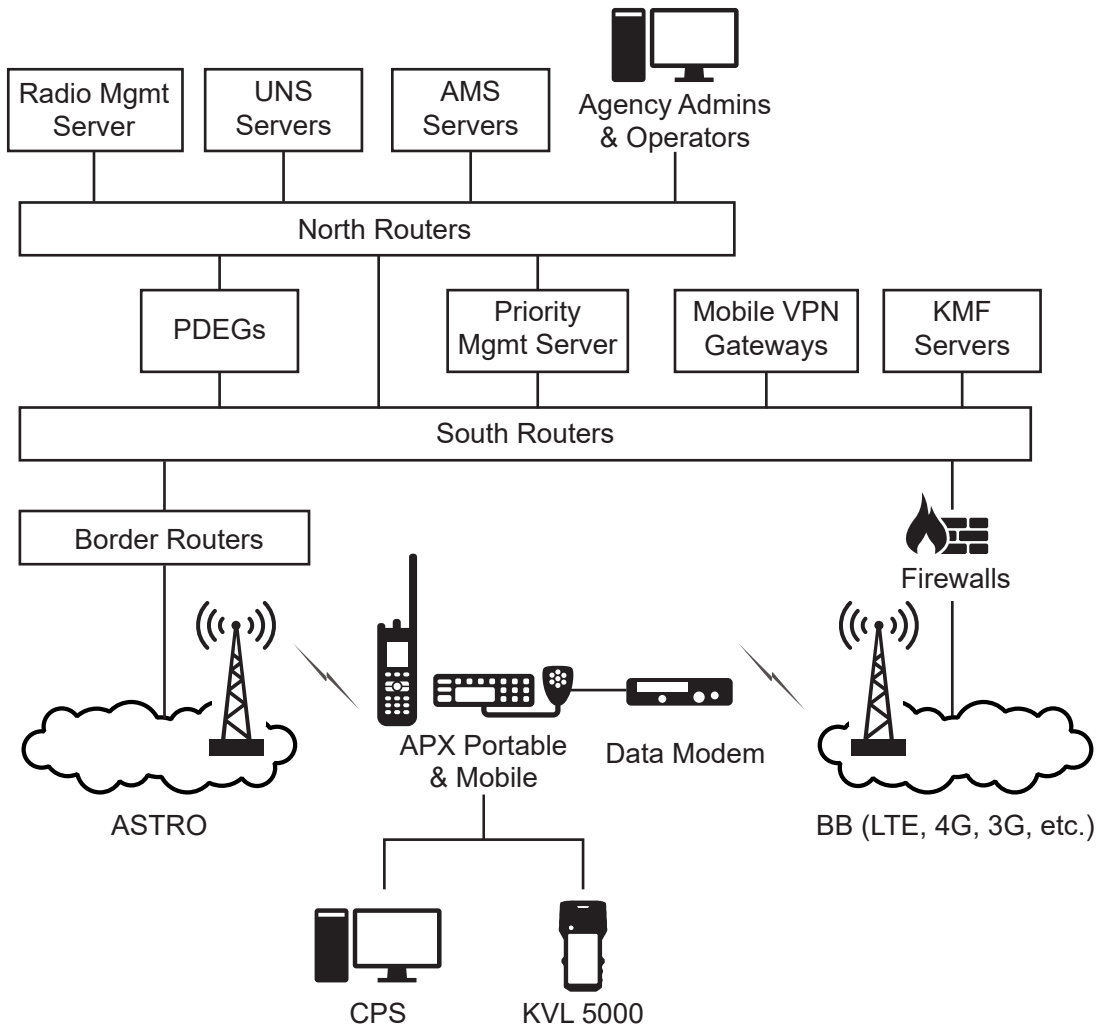
- Motorola Solutions Mobile Virtual Private Network (VPN) Gateway
- APX radio
- External Router (VML750 R3.1 or later, or Sierra Wireless routers)

This figure shows the reference architecture for the APX Data Modem Tethering solution. Redundancy is indicated with shadows behind the boxes. Details about each network component are described in the following sections.



NOTE: The north and south routers are Extreme X460 (Summit) Layer 2/Layer 3 switches that support both Open Systems Interconnect (OSI).

Figure 66: APX Data Modem Tethering Reference Architecture



Advanced Messaging Server

The ASTRO® 25 Advanced Messaging Server (AMS) supports messaging for APX Data Modem Tethering. See the *ASTRO 25 Advanced Messaging Solution Server Installation Guide* or the *ASTRO 25 Advanced Messaging Solution Server Provisioning Guide* for more information.

Agency Administrator and Operator Workstations

This workstation can include client software and browsers for managing the various servers in the Applications Network, such as the Unified Network Services (UNS), AMS, Key Management Facility (KMF), and Radio Management servers.

Application Servers and Workstations

Agency-level application servers and workstations communicate with ASTRO and LTE devices. These servers may be supplied by Motorola Solutions and/or by your organization. The AMS server is an example of an application server supplied by Motorola Solutions that supports APX Data Modem Tethering.

APX Radio

The APX radio is required to take advantage of this feature as it supports a USB interface to an external Motorola Solutions VML750 or a Sierra Wireless router. This could also be an APX 8500 Mobile or a Portable radio connected to the router using Wi-Fi.

VML 750

The Motorola Solutions VML750 is a broadband router that supports dual network operations, and operates on the bands/networks. See the *VML750 User Guide* for more information.

Sierra Wireless Routers

The Sierra Wireless router is a broadband router that supports single network operations, and operates on the bands/networks. See the *Sierra Wireless Data Modem User Guide* for more information.

Key Management Facility

The KMF provides management for the encryption keys used for APX Data Modem Tethering. The KMF is needed for Over-the-Air Re-Keying (OTAR). For more information see the *Key Management Facility* manual.

Key Variable Loader

Encryption keys for voice and data are initially loaded into the radio with the Key Variable Loader (KVL). See the *KVL 4000 Key Variable Loader ASTRO 25 User Guide* for more information.

Mobile VPN Gateway

The Motorola Solutions Mobile VPN Gateway is a high availability platform that provides a secure VPN tunnel into the agency network from the client in the Motorola Solutions VML750/Sierra Wireless routers. See the *Mobile VPN Gateway* manual for more information.

PDEG Encryption Unit

The PDEG Encryption Unit is used for data encryption for Land Mobile Radio (LMR) radios operating in a trunked system. For this solution, the PDEG is located between the north router and south router. See the *PDEG Encryption Unit* manual for more information.

Priority Management Server

The Priority Management Server supports Priority and Quality of Service (QoS) in the Broadband Network. It may be present on the same Proliant HP DL380 Gen9 platform as the UNS. See the *Priority Management Solution* manual for more information.

Radio Management Server

The Radio Management Server supports management of radios, codeplugs, and Over-The-Air Programming (OTAP). The Customer Programming Software (CPS) is the user interface to Radio Management.

Subsystem Transport Equipment

The Networking Subsystem interface is between the radio infrastructure and the application space and consists of Layer 2/Layer 3 switches called the north routers and south routers. The north routers connect to the network of application servers, and the south routers connect to the radio networks, LMR Radio Network Infrastructure (RNI), and Broadband Radio Access Network (RAN). The Broadband data path enters this subsystem through the agency firewall prior to connecting to the south routers. The LMR data path enters this subsystem through the Border Router.

Unified Network Services

The UNS server is needed for Presence and Location Services. Based on CPS configuration, the UNS exchanges Automatic Registration Services (ARS) and GPS Location information with the radio. See the *UNS Configuration Manager User Guide* or the *Unified Network Services Software Installation and Administration Guide* for more information.

4.2

Data Routing That Supports APX Data Modem Tethering

The APX Data Modem Tethering feature supports data services over Land Mobile Radio (LMR) or Broadband. The same application servers in the agency are supported regardless of whether the radio is using LMR or Broadband for data services. This section describes differences in data routing from the radio to the application servers.

APX Radio Data over LMR

For data traffic sent from the radio, the data leaves the LMR network and is routed to the Border Routers. Encrypted traffic gets routed to the PDEG Encryption Unit where it is decrypted and then sent to the north routers. Un-encrypted traffic is routed directly from the south routers to the north routers. From the north routers, the traffic is routed to the application servers.

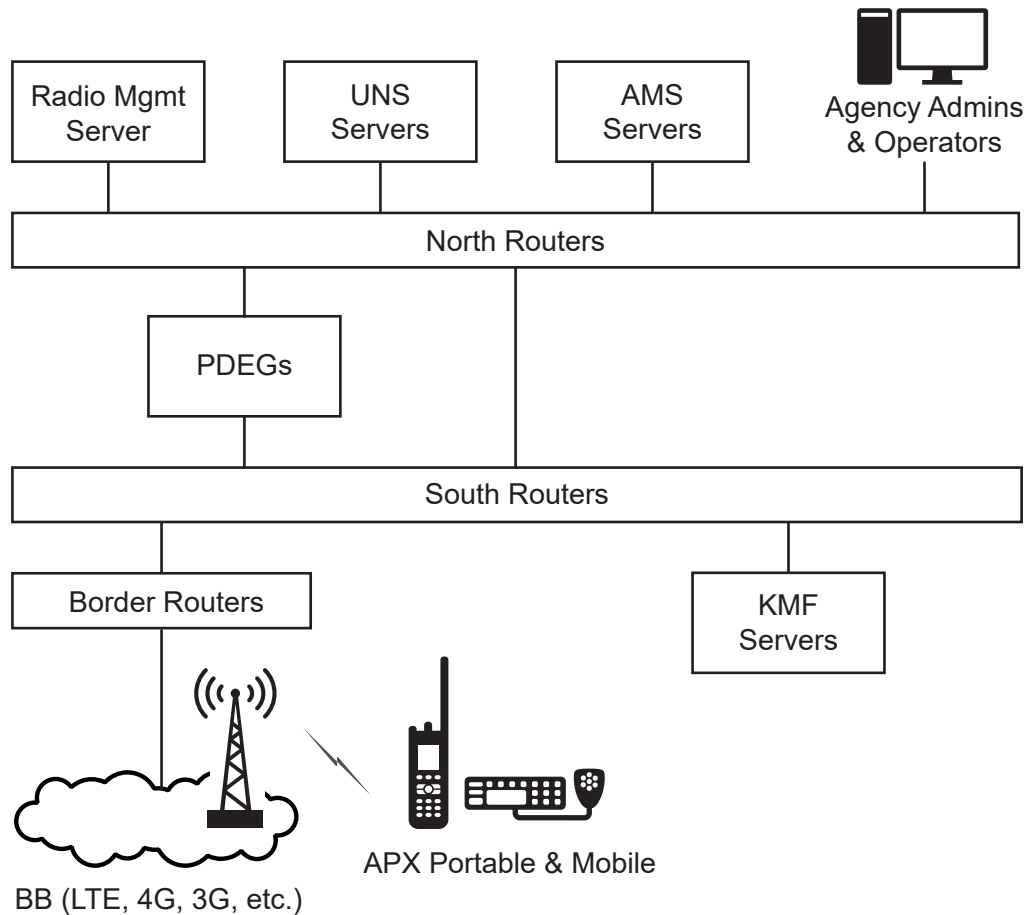
For data traffic sent to the radio, if a PDEG Encryption Unit is present, the data from the application servers is sent from the north routers to the PDEG Encryption Unit and then from the PDEG Encryption Unit to the south routers. If a PDEG Encryption Unit is not present, the traffic goes from the north routers to the south routers. From the south routers, the traffic is routed to the Border Routers and then to the LMR network.

Over-The-Air Rekeying (OTAR) traffic is sent between the radio and Key Management Facility (KMF). The KMF is directly connected to the south routers and has its own encryption.



NOTE: The north and south routers are Extreme X460 (Summit) Layer 2/Layer 3 switches that support both Open Systems Interconnect (OSI).

Figure 67: APX Radio LMR Data Path



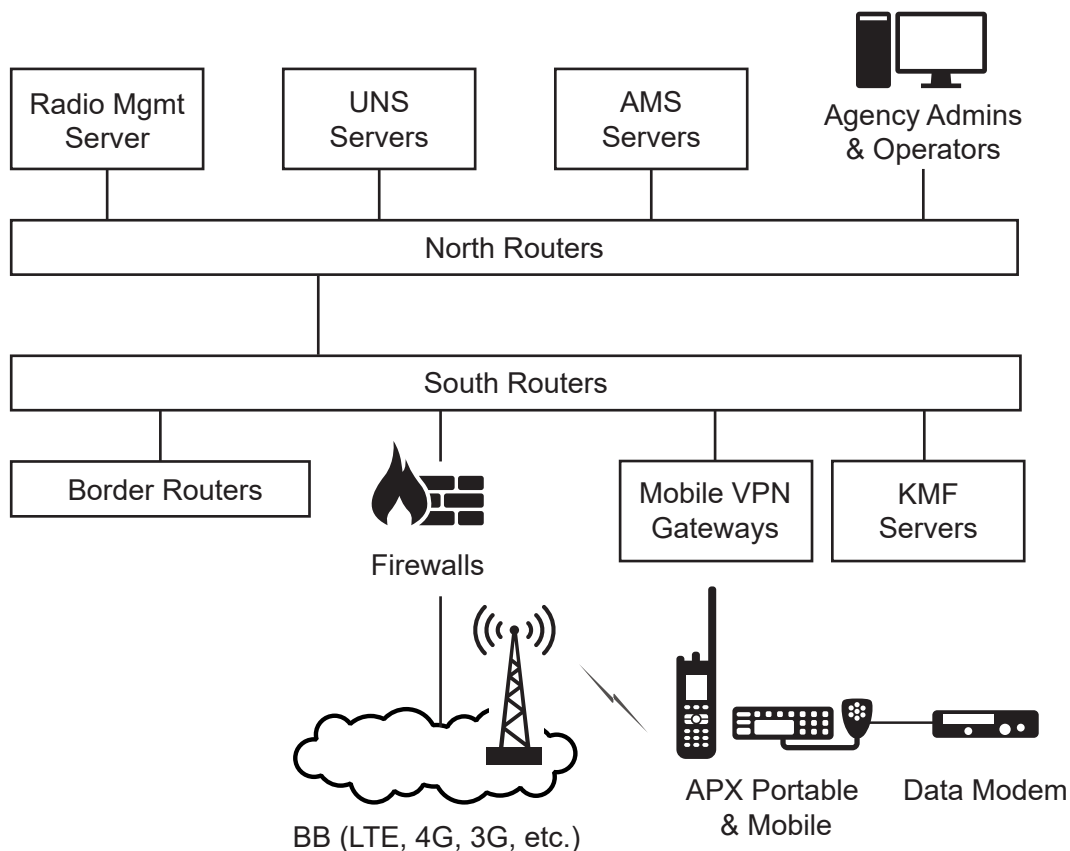
APX Radio Data over Broadband

For data traffic sent from the radio via the tethered router, the data arrives from the Broadband network at the agency firewall and is routed to the south routers. Encrypted traffic is routed to the Mobile Virtual Private Network (VPN) Gateway where it is decrypted and sent back to the south routers. Traffic that was not encrypted, or has just been decrypted by the Mobile VPN Gateway, is routed directly from the south routers to the north routers. From the north routers, the traffic is routed to the application servers.

For data traffic sent to the radio, the traffic arrives from the application servers at the north routers and is sent to the south routers. Secure radios have their traffic routed to the Mobile VPN Gateway where it is encrypted and then sent back to the south routers. Traffic from radios not configured to be secure, or traffic from radios that are secure and has just been encrypted by the Mobile VPN Gateway is then routed to the agency firewall and then to the Broadband network.

OTAR traffic is sent between the radio and KMF. The KMF is directly connected to the south routers and has its own encryption. Due to the inability to create bypass rules in the external routers, if the VPN is enabled, it will transport all data from the router. This effectively will double encrypt the OTAR traffic.

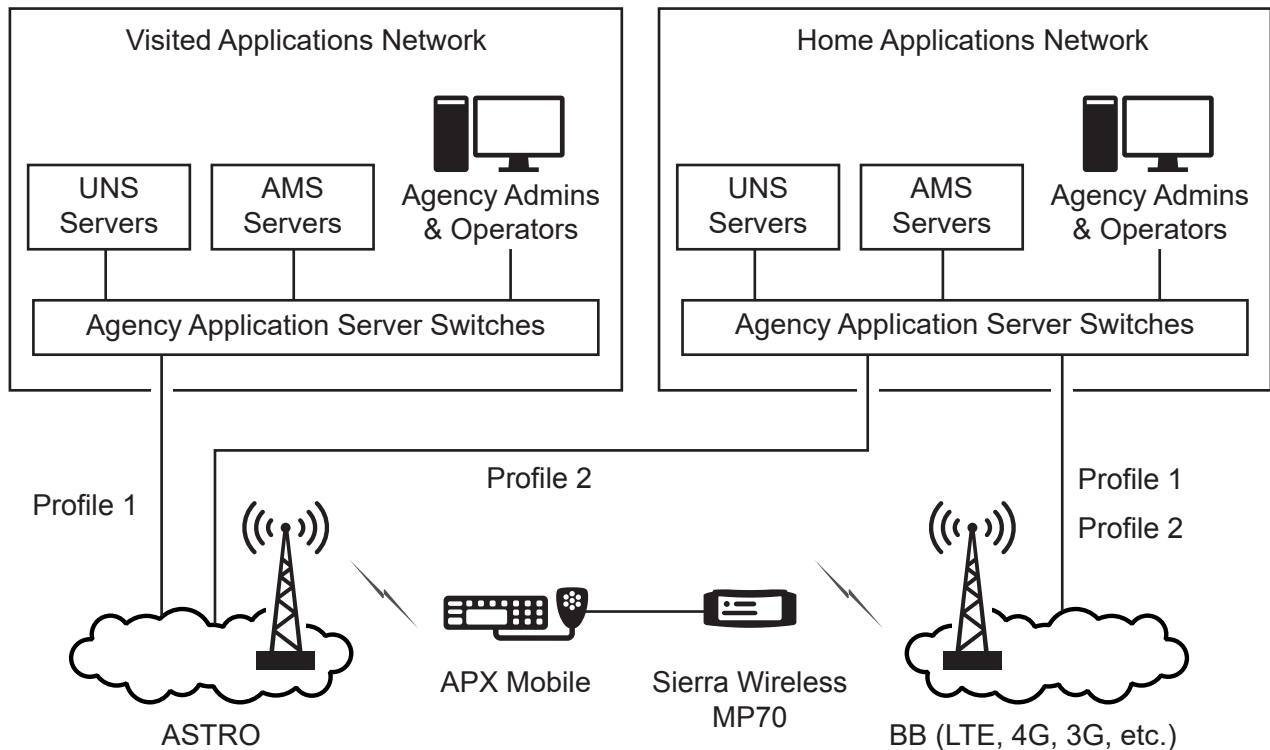
Figure 68: APX Radio Broadband Data Path



APN Selection in the Radio Profile

The Access Point Name (APN) is the name of a logical access point associated with a public or private packet data network. The term APN is used in the ASTRO[®] 25 and Broadband systems but have some differences in the two networks. While the radio allows multiple data profiles, called *personalities*, each may be associated with a different network, and thus contains an implied APN. It should be noted that the APN is not actually exposed as a configurable parameter for LMR systems, as it is implied with the system configuration. The Motorola Solutions VML750 supports a dual network configuration in-which 2 separate SIM cards are installed, and thus 2 separate APNs can be supported. The Sierra Wireless routers (except MG90) support a single SIM card, and thus a single APN is supported.

Figure 69: Single APN for Sierra Wireless Router



4.3

Network Security That Supports APX Data Modem Tethering

The APX® Data Modem Tethering solution supports data encryption across both the Land Mobile Radio (LMR) and Broadband networks.

LMR Data Encryption

LMR data encryption is supported with the PDEG Encryption Unit for trunked systems and CAI Data Encryption Module (CDEM) for conventional systems. The CDEM is located in the Radio Network Infrastructure (RNI) and functions the same for the radio as for other models of conventional radios. For radios operating in a trunked system, data encryption using the PDEG is supported. The PDEG is located between the north and south routers for this solution. When the PDEG is deployed for encryption of data over trunked systems, the Motorola Solutions Mobile Virtual Private Network (VPN) Gateway must be deployed for encryption of data traffic over Broadband access networks. However, the PDEG is optional if Mobile VPN Gateway is used for Broadband data encryption. Any version of the PDEG compatible with the deployed ASTRO® 25 infrastructure system release is supported. Additional information can be found in the ASTRO® 25 *Information Assurance Features Overview*.

Broadband Data Encryption

The Broadband traffic enters the agency network through a Fortinet firewall, prior to connecting to the south routers. The Motorola Solutions Mobile VPN Gateway provides data encryption for radios operating in the Broadband system. The Mobile VPN Gateway is an IPsec-based encryption solution with a high availability server residing between the north and south routers in the agency and a client on the APX external data

modems (VML750 or Sierra Wireless data modems). The IPsec client provides encryption of data traffic on the Broadband air interface to the Mobile VPN Gateway. The Sierra Wireless router uses Pre-Shared Keys (PSK) or Certificates for mutual authentication between the client and server prior to negotiating security credentials for the connection. The Motorola Solutions VML750 uses Certificates for mutual authentication between the client and server prior to negotiation security credentials for the connection.



NOTE: The north and south routers are Extreme X460 (Summit) Layer 2/Layer 3 switches that support both Open Systems Interconnect (OSI).

If the Mobile VPN Gateway fails, whether in a redundant configuration or not, and the APX external router is configured to use secure data, **Broadband Preferred** subscribers switch to ASTRO.

Border Router

Access control lists on the ASTRO® 25 Border Routers keep the Broadband network traffic from entering the private radio network infrastructure.

Chapter 5

Implementation of APX Data Modem Tethering

This chapter includes the processes and procedures required to implement APX® Data Modem Tethering.

5.1

APX Radio Data over Broadband Implementation Pre-Planning

Before beginning [Expanding a System to Add Broadband for Existing ASTRO 25 Data Services on page 91](#), ensure that the following questions have been answered.

- Is Over-The-Air Rekeying (OTAR)/Key Management Facility (KMF) used?
- Is the data service operating on an ASTRO® 25 trunked system?
- Is the data service operating on an ASTRO® 25 conventional system?
- Is Encryption used?
 - Trunked?
 - Conventional?
 - Broadband?
- Are any data services required?
 - Presence/Location?
 - Text Messaging / Presence?
- Will any pieces of equipment be redundant?
 - Unified Network Services (UNS)?
 - KMF?
 - PDEG Encryption Unit?
 - Mobile Virtual Private Network (VPN) Gateway?
 - If any of the above are redundant, then the north routers and the south routers must be redundant.
- Is the Advanced Messaging Solution Server to be co-hab with UNS Presence?
- Contact your Motorola Solutions representative for information about obtaining Verizon service.

5.2

Expanding a System to Add Broadband for Existing ASTRO 25 Data Services

Perform this procedure to expand a system to add APX radio Data over Broadband for existing ASTRO® 25 data services.

Locate the following manuals referenced in this process for equipment included in your system:

- *APX™ Radio User Guides*
- *ASTRO® 25 Advanced Messaging Solution Server Installation Guide*
- *ASTRO® 25 Advanced Messaging Solution Server Provisioning Guide*
- *Enterprise OS Software Reference Guide*
- *Enterprise OS Software User Guide*
- *Key Management Facility (KMF)*
- *KVL 4000 Key Variable Loader ASTRO® 25 User Guide*
- *Mobile VPN Gateway*
- *Motorola Network Router (MNR) S6000 Hardware User Guide*
- *Secure Communications – System Perspective*
- *Unified Network Services Software Implementation Guide*
- *Unified Network Services Software Installation and Administration Guide*
- *Unified Network Services Configuration Manager User Guide*

Verify that the ASTRO® 25 network is installed with one of the following releases or a higher release:

- A7.11
- A7.13
- System release higher than A7.13

Verify that the ASTRO network is running one of the following system configurations before beginning this expansion.

- M1
- M2
- M3

If this system includes the Public Safety LTE network from Motorola Solutions, verify that system release R6.0 or higher is installed. For this purpose, Motorola Solutions personnel can create a version of the Public Safety LTE *End-To-End Acceptance Test Plan* customized for the options implemented in your system.

Verify that all hardware required for this expansion has been received on site. In addition to the ASTRO and Broadband networks, the following are required:

- APX radios
- Motorola Solutions VML750 or Sierra Wireless routers
- Motorola Solutions Mobile VPN Gateway (if LTE encryption is used)
- ASTRO border routers
- Extreme x460 switches

Verify that the following is available if the Mobile VPN Gateway is required:

- Network Time Protocol (NTP) server
- Domain Controller with Active Directory if authentication of VPN clients will use Active Directory account credentials
- HP DL380 Gen9 server (one for non-redundant Mobile VPN Gateway configuration, two for redundant Mobile VPN Gateway configuration)
- Detailed information and technical specifications on the HP DL380p Gen9 server, see <http://www.hp.com/go/docs>
- Mobile Virtual Private Network Server Application DVD

- ESXi 5 1u1 Installation Media
- VMware vSphere Configuration Media

Verify that the following is available for the subsystem defined for this solution:

- CD containing the XOS binary image and Secure Shell (SSH) module image
- Extreme Networks Core License Voucher (paper form)
- Laptop with TFTP server installed, SSH and telnet clients (example putty or TeraTerm), an Ethernet port and serial console port (or USB port and USB to serial port external adaptor)
- Agency IP configuration for the switch OOBM ports (the port assigned IP address and network mask)
- Pre-customized `.xsf` configuration file for the switch based on the agency IP parameters

Verify that all devices are running the required version of the operating system.

Verify that Customer Programming Software (CPS) for wired (R15.00.00 or later) or Wi-Fi (R17.00.00 or later) configuration is installed on a computer in the Applications Network.

Verify that Core Security Management Server (CSMS) is in the Radio Network Infrastructure (RNI) if the Mobile VPN Gateway is used.

Verify that applications are running a supported version before beginning the expansion. The supported versions are:

- ASTRO® 25 Advanced Messaging Service Release 2.0 or later
- Unified Network Services (UNS) Release 3.0 or later

Verify that there is sufficient AC power supply, racking space, and required environmental conditions.

If using a commercial Broadband network (e.g. Verizon), establish accounts with that carrier.

Determine IP address range for the commercial Broadband network.

Activate the commercial Broadband (e.g. Verizon) subscription.

Determine firewall rules for applications used by the radio.

Ensure that the Agency Internet Firewall supports commercial Broadband carrier Mobile Private Network interface.

If using the Mobile VPN Gateway, determine and configure the VPN parameters on the external router per the [VPN Configuration for VML750 on page 67](#).

If using the Mobile VPN Gateway, determine and configure the VPN parameters on the VPN Gateway per the “Device Connection Profiles Configuration” section in the *Mobile VPN Gateway* manual.


Determine and configure the data-wide settings for radio data communications transitions between the Broadband data network and the Land Mobile Radio (LMR) data network:


- Modem Type
- Modem Port (Sierra Wireless Airlink Only)
- Modem Password (Sierra Wireless Airlink Only)
- Modem VPN Tunnel (Sierra Wireless Airlink Only)
- MG90 modem (if used) is running Firmware version 4.3 or later.
- Calculate radio timers
 - APCO Avalanche time
 - Broadband Checkback Time
 - Modem Out-Of-Range Threshold time
 - Modem Powerup Max Guard Time


- Modem Open Max Guard Time

Procedure:


1. Install and configure the north and south routers. See [Installing and Configuring X460 Switches on page 106](#) in this manual.
2. Connect cables between the switch routers according to your unique system IP Plan.
3. If using Over-The-Air Re-keying (OTAR) then:
 - a. If the KMF is not installed, install the KMF. See “KMF Installation” in the *Key Management Facility* manual.
 - b. Configure the KMF for this feature. See “KMF Configuration” in the *Key Management Facility* manual.


 **NOTE:** Create records for the radios.
 - c. Connect the KMFs to the south switch routers.
4. If using encryption on the LMR air interface and the ASTRO system is a trunked system:
 - a. Install the PDEG Encryption Unit if not installed. See “PDEG Encryption Unit Installation” in the *PDEG Encryption Unit* manual.
 - b. Configure the PDEG. See “PDEG Encryption Unit Configuration” in the *PDEG Encryption Unit* manual.
 - c. Configure a PDEG record on the KMF. See “PDEG Encryption Unit Configuration” in the *Key Management Facility* manual.
 - d. Connect the PDEG to the north router and south router.
5. If the Location Service or Presence Service are required, perform expansion for the Unified Network Services (UNS).
 - If the UNS server is present and needs to support Public Safety LTE Priority Management, verify that UNS 3.0 or higher is installed on a Proliant HP DL380 Gen9 that is sized to support Priority Management.

 **NOTE:** For configuring Priority service on the UNS (which is not related to the APX Data Modem Tethering feature) see the Quality of Service (QoS) and Priority Management topics in the *UNS Configuration Manager User Guide*.
 - If the UNS Server is present, and does not need to support public Safety LTE Priority Management, verify that UNS 3.0 or higher is installed. It can be installed on the hardware used for previous releases of the UNS in the ASTRO system.
 - If the UNS Server is not present, install the UNS Server. See “UNS Installation” in the *Unified Network Services Software Installation and Administration Guide*.
 - If Presence Service is required, configure Presence on the UNS. See “Configuring UNS Presence Service” in the *UNS Configuration Manager User Guide*.
 - If Location Service is required, configure Location on the UNS. See “Configuring Location Service” in the *UNS Configuration Manager User Guide*.

 **IMPORTANT:** Add the radios to the device list in the UNS
6. If text messaging is needed, perform expansion for the ASTRO® 25 Advanced Messaging Solution (AMS) server.

- a. If necessary, install the R2.0 AMS server software. See the *ASTRO 25 Advanced Messaging Solution Server Installation Guide*.


 **IMPORTANT:** Add the radios to the AMS Server.

- 7. Configure the Border Router. See [Configuring the Border Router on page 98](#).
- 8.  **NOTE:** The inclusion and changes to the Access Control List (ACL) file for the Border Routers are optional. Only a template ACL file is included as a part of the TNCT generation.
 If your system requires Access Control Lists (ACL), configure the ACL. See [Updating the ACL File on page 102](#).
- 9. Connect the Border Router to the south router.
- 10. Using Customer Programming Software (CPS), configure a sample set of radios with the *Conventional* or *Trunking* Data Profile Type. See the *Customer Programming Software Online Help*.
- 11. Download the codeplug to the radios.
- 12. If encryption is used, load encryption keys into the radios:

If...	Then...
KVL is not used	perform the following actions: <ul style="list-style-type: none"> a. Load the keys in the KMF. See “Creating a Key Using the Keyboard” in the “KMF Configuration” chapter in the <i>Key Management Facility</i> manual. b. Perform a Keypset Changeover to initiate OTAR. See “Keypset Changeover” in the <i>Key Management Facility</i> manual. c. Record the keys for possible use in step 17.
KVL is used	perform the following actions: <ul style="list-style-type: none"> a. Load the keys in the KMF. See “Creating a Key Using the Keyboard” in the “KMF Configuration” chapter of the <i>Key Management Facility</i> manual. b. Connect the KVL to the radio. See “Connecting the KVL to Target Devices” in the <i>KVL 4000 Key Variable Loader ASTRO 25 User Guide</i>. c. Enter encryption keys into the KVL See “KVL 4000 Managing Encryption Keys” and KVL 4000 - Loading Encryption Keys” in the <i>KVL 4000 Key Variable Loader ASTRO 25 User Guide</i>. d. Load encryption keys into the radio. See “Loading Encryption Keys into Target Devices” in the <i>KVL 4000 Key Variable Loader ASTRO 25 User Guide</i>. e. Record the keys for use in step 17.

- 13. Verify access to data services using the LMR data path.

If...	Then...
OTAR is configured	perform the following actions: <ul style="list-style-type: none"> a. Perform a Keypset Changeover to initiate OTAR. See “Keypset Changeover” in the <i>Key Management Facility</i> manual. b. Verify that the OTAR message was sent by viewing the KMF Event Log. c. Record the new keys for use in step 17

If...	Then...
Advanced Message Service is configured	Send a text message to or from the radio. See the <i>APX Radio User Guides</i> .
Location and Presence are configured	perform the following actions: <ol style="list-style-type: none"> a. Enable location with a pre-programmed button on the radio. See the <i>APX Radio User Guides</i>. b. Trigger a location update. c. Display the most recent device location update at the UNS Server. See “Viewing Current UNS Location Service Location Reports” in the <i>Unified Network Services Software Installation and Administration Guide</i>. d. Verify that a location update was sent to the UNS. <p> NOTE: Location requires Presence to also be installed.</p>
OTAP is required	perform the following actions: <ol style="list-style-type: none"> a. Disable Location Service in the radio profile with CPS and download the codeplug. b. Trigger a location update. c. Verify that Location Service is disabled by displaying the most recent device location at the UNS Server. See “Viewing Current UNS Location Service Location Reports” in the <i>Unified Network Services Software Installation and Administration Guide</i>. d. Verify that a location update was not sent to the UNS. e. Enable Location Service in the radio profile and download the codeplug.

APX radio data service over the LMR air interface is now verified. You are ready to perform the Broadband expansion.

14. Install the Agency Firewall.
15. Apply the Firewall configuration files that support the data services being implemented over broadband. See the unique IP plan for your system.
16. Connect the Firewall to the south router.
17. If encryption is required for Broadband data, perform the Motorola Solutions Mobile VPN Gateway expansion.
 - a. Install the Mobile VPN Gateway server. See “Mobile VPN Gateway Installation” in the *Mobile VPN Gateway* manual.
 - b. Configure the Mobile VPN Gateway for use with the Motorola Solutions VML750 router. See “Mobile VPN Gateway Configuration” in the *Mobile VPN Gateway* manual.

- i. Select the Certificate authentication method. See *Generating the Certificate Signing Request and Importing the Certificate Chain*.
 - ii. Add the Certificate configured in the Motorola Solutions VML750 router. See *VML750 User Guide*.
 - iii. Choose the ASTRO Subscriber profile. See *Creating Connection Profile for the Mobile VPN Gateway*.
 - c. Configure the Mobile VPN Gateway for use with the Sierra Wireless routers. See “Mobile VPN Gateway Configuration” in the *Mobile VPN Gateway* manual.
 - i. For operating with the Sierra Wireless routers. Select the Pre-Shared Key authentication method. See *Adding Pre-Shared Keys for ASTRO Site-To-Site*.
 - ii. Add the Pre-Shared Keys configured in the Sierra Wireless router. See [VPN Configuration for VML750 on page 67](#).
 - iii. Choose the ASTRO Subscriber profile. See *Creating Connection Profile for the Mobile VPN Gateway*.
 - d. Connect cables between the south router and the Motorola Solutions Mobile VPN Gateway.
18. Using CPS, configure the following:
 - a. Data Profile Type *Broadband-Only*. See *Customer Programming Software Online Help*.
 - b. Configuration parameters for the external router (e.g. Sierra Wireless vs. Motorola Solutions VML, timer values for modem characteristics, etc.)
19. Download the codeplug.
20. Using specific modem configuration GUI, configure the respective modems to operate with an attached subscriber
 - a. Configure the Motorola Solutions VML750 router
 - i. General configuration can be found in the [Sierra Wireless \(ALEOS\) Configuration on page 27](#) section of this document.
 - ii. If a VPN is used, Certificate installations procedures can be found in the *VML750 User Guide*.
 - b. Configure the Sierra Wireless router
 - i. General configuration can be found in the [Sierra Wireless \(ALEOS\) Configuration on page 27](#).
 - ii. If a VPN is used, ensure that the Pre-shared key configured in [step 17](#) is also provisioned in the Sierra Wireless router.
21. Verify data services by repeating [step 13](#).
22. Verify network selection operation.
 - a. Configure a radio Data Profile Type to *Conventional & Broadband* or *Trunking & Broadband*. See *Customer Programming Software Online Help*.
 - b. Turn off external router mode on the radio. See [Turning Off the Modem Connection on page 76](#).
 - c. Verify that MODM mode is off.

The 4G icon disappears.
23. Verify data services by repeating [step 13](#)
24. Configure all the remaining radios.

5.3

Configuring the Border Router

After an upgrade, perform this procedure after Motorola Solutions generates the new configuration for the Border Routers and the configuration files are loaded on the Border Routers.

Prerequisites:

- Locate the following manuals required for this procedure:
 - *Motorola Network Router (MNR) S60000 Hardware User Guide*
 - *Enterprise OS Software Reference Guide*
 - *Enterprise OS Software User Guide*
- Hardware needed:
 - Border Router
 - South router
 - Computer with serial port capability
 - Serial connector for connection between the computer and routers
- Passwords and account information needed:
 - Terminal server `user name` and `password`
- Documents needed
 - IP Plan and architecture for the Public Safety LTE sub-system
- TNCT - generated files needed:
 - For non-redundant setup: configuration file Border Router 1
 - For redundant setup: configuration files for Border Router 1 and Border Router 2



NOTE: While editing the `<filename>.cfg` configuration files, ensure that there is only one command per line and there are no extra characters at the end of the line.

Procedure:

1. Launch the TFTP server software and select the destination TFTP file directory where the files are to reside on the computer.
2. Connect the computer to the Border Router.
3. Launch a terminal emulation program and open a console session into the Border Router using the following parameters:
 - Baud rate: 9600
 - Bits: 8
 - Parity: N
 - Stop Bit: 1
 - Flow control: NO
4. At the **NetLogin:** prompt, enter the `user name`. Press ENTER.
5. At the **password:** prompt, enter the `password`. Press ENTER.
6. Ping the computer where the TFTP server is located to ensure connectivity.
7. At the prompt, type `cd` to navigate to the directory where the current configuration files reside. Press ENTER.

8. At the prompt, type the following commands, and press ENTER.

- `copy boot.cfg <IP address of the TFTP server>:<cfg filename>`

Where `<.cfg filename>` is the name of the router configuration file specific to the router you are backing up. For example, the boot configuration file for a Border Router could be `br1_boot.cfg`.

The configuration files are transferred to the TFTP server and the prompt reappears.

9. Open the downloaded configuration file copied from the Border Router in a text editor.
10. In the configuration file, locate the following section heading: `# IP Address Setup :`
11. Insert the following text below the `# IP Address Setup` section heading:

```
ADD !v1 -Port VirtualPort 1 Vlan <VLAN ID>
```

The VLAN to be configured for the virtual port is the VLAN assigned to the Border Router in the ASTRO Border Router ICD and LTE architecture document.

12. Locate the following statement in the `IP Address Setup` section:

```
SETDefault !1 -IP NET addr = <IP address><netmask>
```

13. Change the port 1 to virtual port v1. The IP address of the virtual port on the Border Router is configured as outlined in the IP plan.

```
SETDefault !v1 -IP NET addr = <Border Router IP Address><Border Router Netmask>
```



NOTE: The Border Router IP address and Border Router Netmask for the virtual port are in the IP plan.

14. Locate the statements below in the Open Shortest Path First (OSPF) configuration section of the configuration file:

```
# OSPF Setup :
SETDefault !1 -OSPF HelloTime = 1
SETDefault !1 -OSPF RouterDeadTime = 4
...
SETDefault !1 -OSPF CONTROL = Enable
```

```
# OSPF Setup :
```

15. Change the OSPF configurations for the port 1 to be enabled on virtual port 1 instead. Ensure that the OSPF HelloTime and the OSPF RouterDeadTime are configured as below:

- Hello time = 1 sec
- Router dead time = 4 sec

```
#OSPF Setup :
SETDefault !v1 -OSPF HelloTime = 1
SETDefault !v1 -OSPF RouterDeadTime = 4
...
SETDefault !v1 -OSPF CONTROL = Enable
```

16. Locate the following statements in the OSPF Setup section:

```
# OSPF Setup :
...
SETDefault -OSPF SPFDelay = 100
SETDefault !v1 -OSPF CONTROL = Enable
SETDefault -OSPF QuickNotify = Vrrp
```

17. Configure the OSPF AreaId to `<LTE AreaId>` from the IP Plan. The OSPF area ID is configured just preceding the OSPF configuration to enable OSPF.

```
# OSPF Setup :
...
```

```
SETDefault -OSPF SPFDelay = 100
SETDefault !v1 -OSPF AreaId = <LTE AreaId>
SETDefault !v1 -OSPF CONTrol = Enable
SETDefault -OSPF QuickNotify = Vrrp
```

18. If the LTE south routers, enable the OSPF authentication.

a. Locate the statements below:

```
#OSPF Setup :
SETDefault !v1 -OSPF HelloTime = 1
...
SETDefault -OSPF QuickNotify = Vrrp
```

b. Add the authentication statements after the QuickNotify statements as shown below:

```
#OSPF Setup :
SETDefault !v1 -OSPF HelloTime = 1
...
SETDefault -OSPF QuickNotify = Vrrp
Add !v1 -OSPF SecretKey 1 <key1><key2>
SETDefault !v1 -OSPF ActiveKey 1
SETDefault !v1 -OSPF AuthCont = MD5Secure
```



NOTE: The OSPF secret key ID, key, and authentication control parameters can be obtained from the IP plan. The parameters shown above are examples.

19. Locate the Virtual Router Redundancy Protocol (VRRP) configuration section in the configuration file.

```
# VRRP Setup :
ADD !1 -VRRP Backup Aowner 1 100.98.2.254
SETDefault !1 -VRRP AdvertiseInt = 300 1
SETDefault !1 -VRRP HoldTime = 900 1
SETDefault !1 -VRRP Priority = 254 1
SETDefault !1 -VRRP Control = (Enable, PreEmpt) 1
```

20. Change the VRRP configurations for the port 1 to be enabled on virtual port 2. Do not change the configurations for the VRRP.

```
# VRRP Setup :
ADD !v1 -VRRP Backup Aowner 1 100.98.2.254
SETDefault !v1 -VRRP AdvertiseInt = 300 1
SETDefault !v1 -VRRP HoldTime = 900 1
SETDefault !v1 -VRRP Priority = 254 1
SETDefault !v1 -VRRP Control = (Enable, PreEmpt) 1
```

21. Locate the Direct Notify configuration section in the configuration file.

```
# Direct Notify Setup :
SETDefault !1 -POrt DirectNotify = Enable
```

22. Change the Direct Notify configurations for the port 1 to be enabled on virtual port 1. Do not change the configurations.

```
# Direct Notify Setup :
SETDefault !v1 -POrt DirectNotify = Enable
```

23. Save changes to the configuration file and close.

24. Use this edited `boot.cfg` file to load on the Border Router.

25. Launch the TFTP server software and select the destination TFTP file directory where the files reside on the computer. Connect this computer to the Applications Network. Configure the computer by assigning the computer with an available IP address on the Application network.

26. Launch a terminal emulation program and open a console session into the Border Router using the following parameters:

- Baud rate: 9600

- Bits: 8
- Parity: N
- Stop Bit: 1
- Flow control: NO

27. At the **NetLogin:** prompt, enter the login ID. Press ENTER.

28. At the **password:** prompt, enter the login ID. Press ENTER.

29. Ping the computer where the TFTP server is located to ensure connectivity.

30. At the prompt, type `cd` to go to the directory that holds the current configuration files. Press ENTER.

31. At the prompt, type the following commands, and press ENTER.

```
copy <TFTP Server IP Address>:<.cfg filename> a:\primary\boot.cfg
```

Where *<.cfg filename>* is the name of the router configuration file specific to the router you are loading/pushing files. For example, the boot configuration file for a border router could be `br1_boot.cfg`.

The configuration file is transferred to the router from the TFTP server, and the prompt reappears.

32. At the prompt, type `reboot`. Press ENTER.

The Border Router reboots.

33. At the **NetLogin:** prompt, enter the login ID and press ENTER.

34. At the **password:** prompt, enter the login ID. Press ENTER.

35. To verify that the configuration file was successfully loaded without error, enter the following at the command prompt: `SF 9`

The log which appears on the console screen shows any error that may have been caused during the configuration file load.

36. Verify that there are no errors in the log file while loading the `boot.cfg` file.

Contact Motorola Solutions Support Center (SSC) if you find errors in the log file.

37. To verify that the virtual port was created and configured successfully, enter the following at the command prompt:

- `show !v1 -Port virtualport`
- `show !v1 -IP netaddr`

The virtual port properties appear on the console screen. Verify that the configuration matches the configuration set above.

38. To verify that the OSPF configuration on the virtual port was configured successfully, enter the following at the command prompt: `show !v1 -OSPF configuration`

The virtual port OSPF properties appear on the console screen. Verify that the configuration matches the configuration set above.

39. Repeat [step 1](#) through [step 38](#) for a redundant Border Router.

5.4

Updating the ACL File

Perform this procedure to optionally configure Access Control Lists (ACL). Update the ACL file based on your system needs and requirements using the Enterprise OS Software Reference Guide. This procedure is provided as a reference.

Prerequisites:

- Locate the following manuals required for this procedure:
 - *Motorola Network Router (MNR) S60000 Hardware User Guide*
 - *Enterprise OS Software Reference Guide*
 - *Enterprise OS Software User Guide*
- Hardware needed:
 - Border Router
 - South router
 - Computer with serial port capability
 - Serial connector for connection between the computer and routers
- Passwords and Account Information needed:
 - Terminal server `user name` and `password`
- Documents needed:
 - IP plan and architecture for the Public Safety LTE subsystem
- TNCT - generated files:
 - For non-redundant systems: ACL configuration file for Border Router 1
 - For redundant systems, ACL configuration files for Border Router 1 and Border Router 2



NOTE: While editing the `<filename>_acl.cfg` configuration files, ensure that there is only one command per line and there are no extra characters at the end of the line.

Procedure:

1. Launch the TFTP server software and select the destination TFTP file directory where the files are to reside on the computer.
2. Connect the computer to the Border Router.
3. Launch a terminal emulation program and open a console session into the Border Router using the following parameters:
 - Baud rate: 9600
 - Bits: 8
 - Parity: N
 - Stop Bit: 1
 - Flow control: NO
4. At the **NetLogin:** prompt, enter the `user name`. Press ENTER.
5. At the **password:** prompt, enter the `password`. Press ENTER.
6. Ping the computer where the TFTP server is located to ensure connectivity.
7. At the prompt, type `cd` to navigate to the directory where the current configuration files reside. Press ENTER.

8. At the prompt, type the following commands, and press ENTER:

- `copy boot.cfg <IP address of the TFTP server>:<cfg filename>`

Where `<.cfg filename>` is the name of the router configuration file specific to the router you are backing up. For example, the boot configuration file for a border router could be `br1_boot.cfg`.

The configuration files are transferred to the TFTP server and the prompt reappears.

9. Navigate to the folder where the TNCT generated files are located for the system. Open the ACL configuration file generated by the TNCT for the Customer Enterprise Network (CEN) Border Router in the system in a text editor.



NOTE: `<cfg ACL filename>` is the name of the CEN ACL configuration file specific to the router.

10. Locate the Firewall Address lists section of the configuration file.

```
# Firewall Address Lists :
...
ADD -FireWall AddressList CEN 224.0.0.0/24
```

11. Add new statements to create a new address list for the subscribers. Insert these new lines at the end of the Firewall Address Lists section of the configuration file.

```
# Firewall Address Lists :
ADD -FireWall AddressList SUBSR 98.33.0.0/24
ADD -FireWall AddressList SUBSR 98.34.0.0/24
```



NOTE: The IP address of the subscriber subnets can be obtained from your system IP Plan. Use Network Address Translation (NAT) IPs whenever a NAT address is used in the Applications Network or otherwise. See your IP plan for the correct NAT IP addresses.

12. Locate the Filter Creation section of the ACL configuration file as shown below:

```
# Filter Creation:
...
Add -FireWall filter LAN_filt(
Permit from Data
Permit to Data
Permit from CEN
Permit to CEN
Permit from ZNM
Permit to ZNM
Permit from NMD
Permit to NMD
)
```

13. Add the newly created subscriber address lists to the LAN filter. Ensure that the traffic to and from the subscriber subnets are set to permit. Subscriber subnet filter properties are:

- Permit to Subscriber subnet
- Permit from Subscriber subnet

```
# Filter Creation:
...
Add -FireWall filter LAN_filt(
Permit from Data
Permit to Data
Permit from CEN
Permit to CEN
Permit from ZNM
Permit to ZNM
Permit from NMD
Permit to NMD
Permit from SUBSR
```

```
Permit to SUBSR
)
```

14. Locate the `Apply Filter and Configure Firewall Settings for Ethernet LAN Ports` section of the ACL configuration file as shown below:


```
# Apply Filter and Configure Firewall Settings for Ethernet LAN Ports :
# Set default action of the firewall
```

15. Change the LAN filter configurations for port 1. Ensure that the configurations for the Virtual Router Redundancy Protocol (VRRP) are not changed.

```
# Apply Filter and Configure Firewall Settings for Ethernet LAN Ports :
# Set default action of the firewall
SetD !1 -FireWall InFilter = LAN_filt
SetD !1 -FireWall DefActionIn = (Deny, Log)
SetD !1 -FireWall DefActionOut = (Deny, Log)
```

16. Repeat [step 10](#) through [step 15](#) with appropriate IP address and IP subnet to allow additional traffic through the Border Router.

17. Save the changes to the configuration file as a new file named `cen001br1_lte_acl.cfg` and close.

18.  **NOTE:** Perform this step only if the changes to the ACL file were made, and the ACL file has to be included as part of the setup.

In a text editor, open the `boot.cfg` file downloaded from the switch router.

19. Locate the `NAT Setup` section of the configuration file as shown below.

```
# NAT Setup :
SETDefault !v3 -NAT CONTROL = Enable
...
ADD !v3 -NAT AddressMap 100.98.3.2 10.3.249.83 bidirectional
```

20. Add a statement to include the new ACL file. Including the following statements right after the NAT address configuration setup:

```
# NAT Setup :
SETDefault !v3 -NAT CONTROL = Enable
...
ADD !v3 -NAT AddressMap 100.98.3.2 10.3.249.83 bidirectional

# Router ACL Setup :
include cen001br1_lte_acl.cfg
```

21. Save the changes to the text file and close.

22. Use this edited `boot.cfg` file and the edited `cen001br1_lte_acl.cfg` file to load on the Border Router.

23. Launch the TFTP server software and select the destination TFTP file directory where the files will reside on the computer. Connect this computer to the Applications Network. Configure the computer by assigning the computer with an available IP address on the Application network.

24. Launch a terminal emulation program and open a console session into the Border Router using the following parameters:

- Baud rate: 9600
- Bits: 8
- Parity: N
- Stop Bit: 1
- Flow control: NO

25. At the **NetLogin:** prompt, enter the login ID. Press **ENTER**.

26. At the **password:** prompt, enter the login ID. Press ENTER.
27. Ping the computer where the TFTP server is located to ensure connectivity.
28. At the prompt, type `cd` to go to the directory that holds the current configuration files. Press ENTER.
29. At the prompt, type the following commands, and press ENTER.

```
copy <TFTP Server IP Address>:<.cfg filename> a:\primary\boot.cfg  
copy <TFTP Server IP Address>:<.cfg ACL filename>  
a:\primary\boot_acl.cfg
```

Where **<.cfg filename>** is the name of the router configuration file specific to the router you are loading/pushing files. For example, the boot configuration file for a border router could be `br1_boot.cfg`.

Where **<.cfg ACL filename>** is the name of the router ACL configuration file specific to the router you are loading/pushing files. For example, the boot configuration file for a border router could be `cen001br1_acl.cfg`.

The configuration files are transferred to the router from the TFTP server, and the prompt reappears.

30. At the prompt, type `reboot`. Press ENTER.

The Border Router reboots.

31. At the **NetLogin:** prompt, enter the login ID. Press ENTER.
32. At the **password:** prompt, enter the login ID. Press ENTER.
33. To verify that the configuration file was successfully loaded without error, enter the following at the command prompt: `SF 9`

The log which appears on the console screen shows any error that may have been caused during the configuration file load.

34. Verify that there are no errors in the log file while loading the `boot.cfg` file.



NOTE: Contact Motorola Solutions Support Center (SSC) if you find errors in the log file.

35. To verify that the virtual port was created and configured successfully, enter the following at the command prompt:

- `show !v1 -Port virtualport`
- `show !v1 -IP netaddr`

The virtual port properties appear on the console screen. Verify that the configuration matches the configuration set above.

36. To verify that the Open Shortest Path First (OSPF) configuration on the virtual port was configured successfully, enter the following at the command prompt: `show !v1 -OSPF configuration`

The virtual port OSPF properties appear on the console screen. Verify that the configuration matches the configuration set above.

37. Repeat [step 1](#) through [step 36](#) for a redundant Border Router.

Chapter 6

Agency Application Network Switches

This chapter provides information and procedures for installing the Extreme Networks Summit X460 switches.

Extreme Networks X460 Description

The X460 switch provides copper RJ-45 10/100/1000BASE-T LAN ports, a separate Out-Of-Band-Management (OOBM) port and a serial port for local access. Each switch is deployed with dual hot-swappable power supplies for redundancy as well as dual fans. An upgrade to the Core license is included by default and must be enabled. This upgrade is a one-time procedure done during the initial installation of the switch.

6.1

Installing and Configuring X460 Switches

When and where to use: Use this general sequence for X460 Switch installation and configuration.

Procedure:

1. See [Switch Hardware Installation on page 106](#).
2. See your unique system IP Plan for cabling connection information.
3. See [Switch Software: Preparation for Installation/Upgrade on page 106](#).
4. See [Installing XOS and SSH Modules and .XSF on X460 Switch on page 111](#).
See [Switch Install Log Files on page 121](#) for an example of an install on the 24t model of the X460.
5. See [Switch Configuration Backup and Restore on page 116](#).

6.2

Switch Hardware Installation

Hardware Installation

For detailed information on-site requirements, general cabling techniques, and switch hardware installation, see *Summit Family Switches Hardware Installation Guide*.

6.3

Switch Software: Preparation for Installation/Upgrade

Extreme Networks Summit X460-G2 switch require an operating system install as part of installation. A functioning operating system is installed on the hardware, but this operating system must be upgraded prior to use in the system. The recommended procedure is for the operating system upgrade to be performed before configuration of the switch. The installation procedure is covered in section [Installing XOS and SSH Modules and .XSF on X460 Switch on page 111](#).

Prerequisites

Ensure that you have the following:

- Laptop with TFTP server installed, Secure SHell (SSH) and Telnet clients (for example, PuTTY or TeraTerm), an Ethernet port and serial port (or USB port and USB to serial port external adaptor). Install the recommended TFTP server on the laptop. 3CD (from 3Com) TFTP server is recommended. Other TFTP servers may not be able to transfer the entire file.
- Extreme Networks Core License Voucher (paper form).
- The Extreme XOS (summitX-xx.x.x.x.xos) and SSH module (summitX-xx.x.x.x-ssh.xmod) software copied to the laptop

Connect the switch management port to the laptop. Configure both sides with an IP address on the same subnet.

Switch File Types

On the switch, all files are in one place / directory. Only one single directory is visible to the user and contains all files but the software image files. The software images `.xos` or `.mod` are downloaded for installation and are not visible in the file list. Only one file can be downloaded and installed at a time. Their location is hidden from the user.



NOTE: The pre-defined extensions of the files do matter to Extreme software and should not be changed.

- `.xos`: an OS binary image file
 Example: `summitX-15.3.2.11.xos`
- `.xmod`: a loadable binary software module
 Example: `summitX-15.3.2.11-ssh.xmod`
- `.xsf`: a text script config file used as a reference configuration file
 Example: `diesel10-PNR-R6v001_rel.xsf`
- `.cfg`: xml format config file used to store configuration on the switch
 Example: `diesel10-RSR-R6v001_orig.cfg`
- `.pol`: a policy file (text)

Table 13: X460 Switch Configuration File Types

Parameter	<code>.cfg</code>	<code>.xsf</code>
Type/Relative Size	XML: large	ASCII Text: small
Contents	Switch-internal config representation	CLI commands (a script) Human readable with comments
Editable	No, should not be edited manually	Yes (using text editor)
Transferable between switches	No; specific to the switch it was saved on	Yes; can be copied from one switch and loaded on another
Usage	Switch internal format, backup and restore	Installing configuration, replicating configuration, backup and restore

Parameter	.cfg	.xsf
Effect on running config	Swapping configuration: when selected, it has no immediate effect. On the next reboot, it <i>completely replaces</i> the running config and persists until changed again.	When loaded, it has immediate <i>incremental</i> effect on the running config (equivalent to copy pasting its contents to CLI) but the changes do not survive after reboot unless the running .cfg was saved before reboot.

6.4

General Commands for Working with the Switch


The switch can be logged on to and managed through its serial console port, Out-Of-Band-Management (OOBM) Ethernet port or any of its 48 in-band ports. In the latter two cases, the connection uses an IP protocol like Telnet, TFTP, Secure Shell (SSH), Site Control Path (SCP), SFTP, or SNMP. When logged on to the switch and executing commands to connect to external devices or transfer files, some commands (for example, Telnet or SSH connections and various file transfer commands) default to using the OOBM port while other commands (for example, ping, traceroute) default to using in-band ports. This preference can be explicitly overridden. The selection of the OOBM port is done by specifying the Virtual Router (VR) it is contained in. This name of this VR is “VR-Mgmt” while the VR associated with the 48 in-band ports is by default named “VR-Default.”

The following table includes a set of the basic commands and information needed during initial install, upgrade, backup, and restore activities.

Table 14: Basic Commands for Switch Install, Upgrade, and Backup and Restore

Function	Description / Example
CLI History	The command history prints the list commands executed in a session (similar to Linux).
Command options: The question mark: ?	Prints all options available to choose from for any specific started command. By itself, prints all available commands on the switch.
Command options: The TAB key	Automatically completes a partially typed command, part of a command (similar to Linux shell), or prints a list of options at any level in a command (same as ? mark).
Switch prompt	<ul style="list-style-type: none"> Set to reflect the system name and current PM config version (and also the current VR if different than VR-Default) At the end of the prompt, a counter (29 in the following example) is displayed indicating the number of shell commands already executed in the current session. Example: (vr VR-Mgmt) diesel10-PNR-R6v001.29 # A star (*) in the prompt indicates that configuration changes have been made and have not been saved yet.
Reboot	Example: reboot , reboot time 11 11 2011 03 58 29 , reboot cancel
Enabling and disabling ports (selected ports or all ports)	[enable disable] port [<port_list> <all>] Examples: enable ports 1 , enable ports 5-11 , disable ports all
Port mirroring (for sniffing)	Enabling ports: enable ports 24 , enable mirroring to port 24

Function	Description / Example
	<p>Selecting ports: <code>configure mirroring add port 1-10</code></p> <p>Selecting all ports in a VLAN: <code>configure mirroring add vlanv502_PNR_AFG</code></p> <p>Selecting ports in VLAN: <code>conf mirror add vlan v502_PNR_AFG port 7</code></p> <p><code>show mirroring</code> to display the current settings.</p>
Switching between VRs	<p>Examples: <code>virtual-router <VR-Default></code>, <code>virtual-router VR-Mgmt <VR-Mgmt></code></p>
SSH and telnet from the switch	<p><code>ssh2 vr<VR-Default>root@192.168.5.199ssh2 vr<VR-Default>platforms@192.168.5.146telnet vr<VR-Default>192.168.5.146</code></p>
Ping from VR Mgmt or VR Default (can optionally specify source IP)	<p><code>ping vr<VR-Mgmt>10.6.150.1</code></p> <p><code>ping vr<VR-Default>192.168.5.146</code></p> <p><code>ping192.168.5.146</code></p> <p><code>ping192.168.5.146 from 192.168.5.145</code></p> <p><code>ping vr<VR-Default>192.168.5.146 from 192.168.5.209</code></p>
Traceroute	<p><code>traceroute192.168.5.146</code></p> <p><code>traceroute192.168.5.146 from 192.168.5.209</code></p> <p>This command is not recommended in Priority Management (PM) Server due to the inherit limitations in asymmetric routing environment.</p>
CPU utilization	<p><code>top</code></p>
Copy, Rename, Delete, and list files	<p>By default, the following commands operate on files in the internal storage called internal-memory. A memory card modifier before a file name refers to a file in the USB drive.</p> <p><code>cp<from_file>to <to_file>, mv <old_file><new_file>, rm<file></code></p> <p>Examples: <code>cp test.xsf test2.txt</code>, <code>cp test.xsf memorycard test2.txt</code>, <code>mv test1.xsf test101.xsf</code>, <code>rm test2.txt</code></p>
List	<p><code>ls</code> lists internal storage</p> <p><code>ls<memorycard></code> lists USB stick contents (if plugged in)</p> <p>No directories, no change directory possible.</p>
SCP2 copy	<p><code>scp2 vr<vr_name><user>@<ipaddress><:remote_file>< local_file ></code></p> <p><code>scp2 vr <vr_name><local_file><user>@ <ipaddress><:remote_file></code></p> <p>Example: <code>scp2 vr "VR-Mgmt" test101.xsf myuser@173.61.0.65:test101.xsf</code></p> <p>Example: <code>scp2 vr "VR-Default" test101.xsf platforms@192.168.5.146:test101.xsf</code></p>
TFTP	<p><code>tftp 10.44.35.91 -p -l psig.cfg -r PM.cfg</code></p>

Function	Description / Example
	<pre>tftp 10.44.35.91 -g -r grep.xsf -l xgrep.xsf</pre> <p> NOTE: The first command transfers the <code>psig.cfg</code> file from the switch to the TFTP server and names it there as <code>PM.cfg</code>; the second command transfers <code>grep.xsf</code> from the TFTP server and saves it as <code>xgrep.xsf</code> on the switch local storage.</p>
SFTP	There is no SFTP client on the switch. SFTP can only be used from an external host.
Download	For binary images (<code>.xos</code> and <code>.xmod</code>) and bootrom only.
Upload	<p>Logs: <code>upload log 10.44.35.91 vr <VR-Mgmt>mylog.txt</code></p> <p>Config: <code>upload configuration 10.44.35.91 myconfig.xsf</code></p> <p>Debug: <code>show tech all log to file</code> then <code>upload debug 10.44.35.91</code></p> <p>There is no upload for software images.</p>
Saving config as a script	<code>save configuration as-script my_conf</code>
Saving config	<p><code>save configuration my_conf</code></p> <p>A star (*) in the prompt indicates that configuration changes have been made and have not been saved yet.</p>
Swapping running file	<p><code>use configuration my_conf</code></p> <p>Requires switch reboot to activate.</p>
Determining the running config	<code>show switch</code>
Uploading configuration to TFTP server	<code>upload configuration 10.44.35.91 myconfig.xsf</code>
Loading a script file	<p><code>load script my_script</code></p> <p><code>load script psig 192.168.5</code></p>
Unsaved configuration	Any configuration change results in showing a star (*) in the prompt until the changes are saved to a <code>.cfg</code> file.
sh config	Displays the configuration explicitly set by the admin.
sh config <func_area> detail	Displays the detailed configuration for the specific functional area including any defaults that were not explicitly set by the admin.
sh config detail	Displays the detailed configuration for all functional areas including any defaults that were not explicitly set by the admin.

6.5

Installing XOS and SSH Modules and .XSF on X460 Switch

Perform this procedure for first-time installation, or in the case of a recovery of the Extreme X460 switch.

Prerequisites:

The following are required to perform this procedure:

- CD containing the XOS binary image and Secure Shell (SSH) module image.
- Extreme Networks Core License Voucher (paper form)
- Laptop with TFTP server installed, SSH, and Telnet clients (for example, PuTTY or TeraTerm), an Ethernet port, and serial console port (or USB port and USB to serial port external adaptor).
 - Install the recommended 3CD (from 3Com) TFTP server. Other TFTP servers may not be able to transfer the entire file.
 - Ensure that the laptop security settings do not block the usage of a TFTP server.
 - Start/enable the TFTP server and test if it is working by using an external TFTP client (for example, another laptop) to transfer a file from the TFTP server running on the laptop to the client.
 - Copy the XOS and SSH module binary files from the `Network\Extreme_Switches\Software_Images\` directory on the CD to the laptop.
 - Ensure the TFTP server default local path is set to the directory where the software has been copied on the laptop Hard Drive.
- Ensure that the X460 Out-Of-Band-Management (OOBM) port is connected to the laptop with a Point-to-Point regular Ethernet cable.
 - A crossover cable is NOT required but would work.
- A serial connection is established from the laptop to the Extreme switch console.
 - Use a USB-to-serial port adaptor if the laptop has no serial port connector.
- Agency IP configuration for switch OOBM ports (the port assigned IP address and network mask).
- Pre-prepared `.xsf` configuration file for the switch based on the agency IP parameters.



NOTE:

This procedure assumes some example values for agency IP parameters. Replace those parameters with the actual agency IP parameters when executing the procedures.

The example admin and user names for the agency are `agency_admin` and `agency_user`.

When and where to use: This procedure is used for a first-time installation or in the case of a recovery.



NOTE: This procedure assumes some example values for agency IP parameters. Replace those parameters with the actual agency IP parameters when executing the procedures.

- The example admin and user names for the agency are `agency_admin` and `agency_user`.
- The XOS binary image file/version is `summitX-15.3.2.11.xos` and the SSH module binary file/version is `summitX-15.3.2.11-ssh.xmod`.
- The configuration files prepared for the switch.

Procedure:

1. Boot the configuration.
 - a. Power and boot up the switch.
 - b. Using the serial console port connection:

- Connect to the switch using a PuTTY or TeraTerm (or other) client that supports serial connection.
- Login using the default credentials: `admin` as user name and blank password.



NOTE: A (pending-AAA) login: prompt appears first. Press ENTER to get to the normal login prompt where the admin and empty password are used.

- Answer all initial security-related first-time boot-up questions.

See the example installation logs in [Switch Install Log Files on page 121](#) for the list of questions and default answers.

2. Configure the OOBM Ethernet port by entering the following commands in the CLI:

- a. `configure vlan "Mgmt" ipaddress<xx.x.xxx.xxx>`
- b. `configure iproute add default<xx.x.xxx.xxx> vr "VR-Mgmt"`
- c. To validate that this configuration has been applied correctly, inspect the output of the following commands:

```
show vlan "Mgmt"
virtual-router "VR-Mgmt"
show iproute
ping 10.6.150.1
```

The ping command checks connectivity to the TFTP server.

- d. Run the following command afterwards and note the change in the prompt back to what it was before running the second of the four commands: `virtual-router "VR-Default"`.

3. This OS image upgrade and SSH module install steps are performed twice, once on the primary partition and once on the secondary partition of the switch. The switch is rebooted after each partition is upgraded.

- a. Run the following command to determine the current software version on the primary and the secondary partitions:

```
show switch
```

This command indicates the current active partition. A fragment of example output:

```
Image Booted:
Primary ver:   12.5.4
Secondary ver: 5
```

The provided output indicates that the same 12.5.4.5 software version is present on the primary and the secondary partitions, and that the switch has been booted from the secondary partition.

- b. Download and install the XOS binary image using the following command:

```
download image <xx.x.xxx.xxx><summitX-15.3.2.11.xos>
download image <xx.x.xxx.xxx><summitX-15.3.2.11-ssh.xmod>
```

- c. Enter Yes to the question Do you want to install image after downloading?.

The images are installed by default to the currently inactive partition. The example shows the switch was booted from the secondary partition.

- d. Run the `show switch` command again and note the **Image Selected** and **Image Booted** fields.

The following lines from the output of the command reflect this example:

```
Image Selected: primary
Image Booted:   secondary
```



```
Primary ver:      15.3.2.11
Secondary ver:    12.5.4.5
```

- e. Enter `save configuration` to save the current configuration.
- f. Accept the default file name proposed to save the config.
- g. Reboot the switch using the `reboot` command.
- h. After the switch boots back up, log on again through the serial connection using the same credentials.
- i. Run the `show switch` command to confirm the updated/installed image version number.
- j. Run the `show management` command and examine the output for the field **SSH access** to confirm that the SSH module has been installed successfully.

If the module was installed correctly and given SSH has not been enabled yet, the SSH access field looks like in the provided example:

```
SSH access: Disabled (Key invalid, tcp port 22 vr all)
```

- k. When the switch is being enabled for the first time, upgrade the image on the other partition of the switch (the secondary one in the example) from the factory default version (12.5.4.5 in the example) to the recommended version (15.3.2.11).

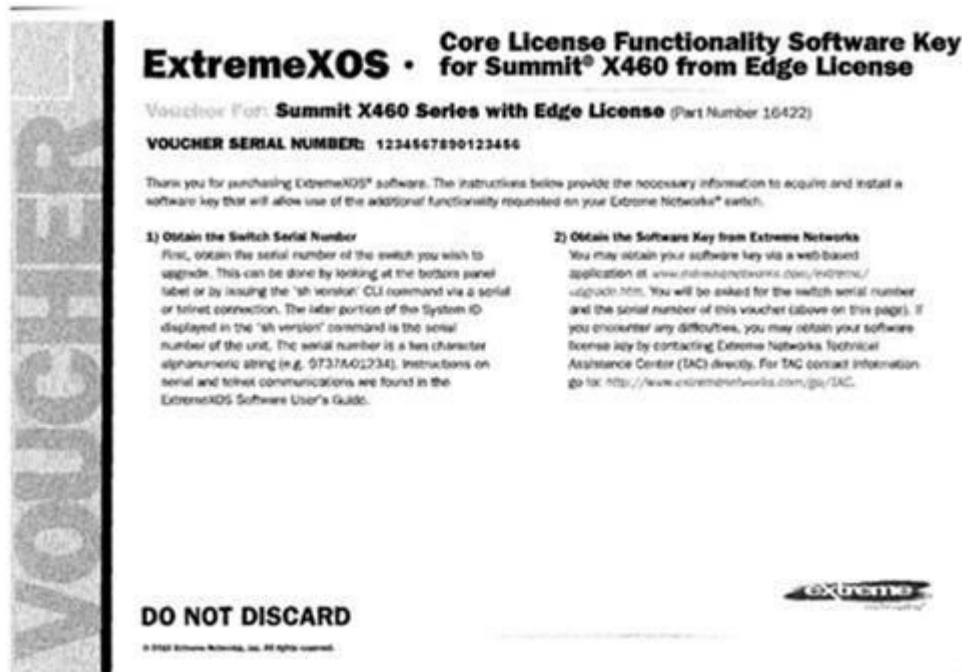
Run the same download commands again (and show commands to confirm success).

This time, the software images are downloaded and installed on the secondary partition as it is the currently inactive one after the recent reboot. Reboot the switch again similar to what was done after the first set of download command.

- l. After the switch boots back up, log on again through the serial connection using the same credentials. Run the `show switch` command to confirm that both partitions now have the recommended software version
4. Install the Extreme Networks Core License.

The paper voucher appears as follows:

Figure 70: Extreme Switch Voucher



The paper voucher does NOT include the Core License Key ultimately sought. Follow the voucher instructions to obtain the key from Extreme Networks web-based application or by contacting Extreme Networks technical support.

The serial number printed on the voucher and the switch serial number are required. Use the `show version` command on the switch to obtain its serial number. In the example fragment of output below, the switch serial number is emphasized:

```
Switch      : 800321-00-03 <1052G-04810> Rev 3.0 BootROM:
IMG: 12.5.4.5
PSU-1      : EDPS-300AB A-S6 800386-00-03 1052E-44810 Rev 0.0 PSU-2      :
NONE NONE NONE Rev 0.0
```

Use the following command to apply the Core license key after obtaining it from Extreme Networks:

```
enable license<xxxx-xxxx-xxxx-xxxx-xxxx>
```

where `<xxxx-xxxx-xxxx-xxxx-xxxx>` is the serial number obtained from Extreme Networks.

5. Enable SSH and generate the SSH key.

The `enable ssh2` command enables SSH. This command enables SSH access to the switch through the OOBM port and any of the 48 in-band ports. However, for security reasons, Motorola Solutions recommends enabling access only through the OOBM port using the `enable ssh2 vr "VR-Mgmt` command.

When SSH is being enabled on the switch for the first time, an SSH key is generated. It may take up to 10 minutes and may timeout (failure). Repeat the command in case it times out. The SSH server is listening on port 22 (default). This command also enables an SFTP server and the usage of secure copy (SCP).

To validate that SSH is configured correctly, run the `show management` command and examine the **SSH access** field which should look like following example:

```
SSH access: Enabled (Key valid, tcp port 22 vr all)
```

The provided output is a result of the `enable ssh2` command. In case SSH was enabled on the OOBM port only, the **SSH access** field appears as follows:

SSH access: Enabled (Key valid, tcp port 22 vr VR-Mgmt)

Motorola Solutions highly recommends that you do not rely solely on the outputs provided in the examples as confirmation of success and attempt an SSH connection from the laptop to `<admin>@<10.6.150.155>` over port 22. A successful login using SSH provides full confirmation that the SSH configuration was successful.



NOTE: In the rare case that the output of `show management` is as expected, but the SSH attempt fails, double check the setting of the SSH client on the laptop and attempt to reconfigure SSH by running:

```
disable ssh2  
  
configure ssh2 key
```

Use one of the `enable` commands as desired. This command explicitly configures a new SSH key. This command can take up to 10 minutes and must be repeated if a timeout occurs. If desired for security reasons, telnet can now be disabled (assuming SSH has been verified working) using the command `disable telnet`.

6. Create agency local user and admin accounts as needed; delete default 'user' and 'admin' accounts (security recommendation):

Use the `show accounts` command to display the current default user account on the switch.

- To configure the accounts mentioned in the assumption section, choose strong passwords and use the following two commands:

```
create account user agency_user <password1>  
create account admin agency_admin <password2>
```

- To delete the default accounts use the commands:

```
delete account <user>  
delete account <admin>
```

- Use the `show accounts` command again to confirm the configuration changes were successful.



NOTE: An asterisk (*) appears in the prompt because of the configuration changes applied and because the modifications have not been saved yet.

7. Configure failsafe account if needed.

The failsafe account can be optionally configured at this stage, if it was not done during the initial boot-up sequence (initial security questions). The failsafe account is a last resort user account used to log on to the switch in the case of a failure to log on using existing normal accounts. The failsafe accounts are never locked out, no matter how many consecutive failed logon attempts. Access using the failsafe account can be restricted to log on through the serial console port, OOBM port, and/or the 24 in-band ports. In the latter two cases, access can be restricted to SSH and/or Telnet protocol.

- a. To configure a failsafe account run the following command:

```
configure failsafe-account
```

- b. When prompted, enter the username and password, and repeat/confirm the password.

- c. To control the access mean using the failsafe account, first run the following command to deny all access means:

```
configure failsafe-account deny all
```

- d. To selectively permit failsafe account access:

- Only through the serial console port, use the following command:

```
configure failsafe-account permit serial
```

- Only using SSH via the OOBM port, use the command:

```
configure failsafe-account permit ssh vr Mgmt
```
 - Through all available ports and protocols use the following command:

```
configure failsafe-account permit all
```
- e. Use the `show failsafe-account` command to check and confirm the setting.
8. Save the initial configuration changes.
Use the `save configuration` command and confirm/accept the suggested file name.

**NOTE:**

When the configuration is saved, the (*) symbol in the prompt does not appear.

9. Load the `.xsf` file to configure switch.

The reference `.xsf` file (`diesel110-PNR-R6v001_rel.xsf` in this example) and the two other auxiliary (optional) configuration files (`default.xsf` and `PM.xsf`) must be first transferred to the switch using TFTP. Nothing is required for the two auxiliary files beyond transferring them to the switch. The main configuration file must be activated using the following command:

```
load script diesel110-PNR-R6v001_rel
```



NOTE: Note the lack of the `.xsf` extension in this command.

After loading, the configuration file adds the initial commands that were entered manually. It then saves the resulting new configuration and reboots the switch to activate it. The script is designed to halt its operation in case of an unexpected error (some errors are expected and are ignored as this script is also used for upgrades, and not initial configuration). If an unexpected error is encountered, the reboot to activate the configuration is NOT performed.

6.6

Switch Configuration Backup and Restore

The Summit X460 switch can locally store many configuration files. The files can also be transferred to an external backup location over the network using TFTP, SFTP, or Site Control Path (SCP), or via regular copy to external USB drive. A `.cfg` file saved from a particular switch can later be reloaded to that same switch to restore the saved configuration. See “Managing the Configuration File” in the *ExtremeXOS Concepts Guide*.

Chapter 7

APX Data Modem Tethering Troubleshooting

This chapter provides troubleshooting information about the expansion feature that adds the Broadband network capability for APX Data Modem Tethering features.

7.1

Overview of Troubleshooting of APX Data Modem Tethering

This chapter provides various problem-solving scenarios and resources to help you diagnose and troubleshoot the APX™ Data Modem Tethering feature.

If troubleshooting instructions do not help you resolve your issue, contact Motorola Solutions. Ensure that you collect logs and data. See [APX Data Modem Tethering Event Logging on page 118](#).

Table 15: Troubleshooting Instructions for APX Data Modem Tethering

Symptom / Issue	Instructions
Over-The-Air Programming (OTAP) fails	<ul style="list-style-type: none"> • Ensure network availability. • Ensure availability of Radio Management system. • Ensure connectivity to network. • Verify network routing.
Over-The-Air Re-keying (OTAR) fails	<ul style="list-style-type: none"> • See <i>OTAR Failures</i> in the <i>Key Management Facility</i> manual.
Text Messaging fails	<ul style="list-style-type: none"> • Verify Presence Service is working. • See <i>Troubleshooting in ASTRO Advanced Messaging Solution Server Installation Guide</i>.
Location Service fails	<ul style="list-style-type: none"> • Ensure that Location Service is enabled on the radio. • Ensure that the UNS is operational. • See <i>Viewing Logs</i> in the <i>UNS Configuration Manager User Guide</i>.
Presence Service fails	<ul style="list-style-type: none"> • Ensure that the UNS is operational. • See <i>Viewing Logs</i> in the <i>UNS Configuration Manager User Guide</i>.

7.1.1

Radio Troubleshooting

The radio has a number of Broadband status icons. Examples of status information available and how it may be used is listed. See [Status Icons on page 78](#).

- Status of Broadband Network
 - Broadband network is active icon (4G, 3G, 2G)
- Broadband Data service activity
 - Broadband Receiving icon
 - Broadband Transmitting icon
 - Broadband Receiving and Transmitting icon
- Location or Messaging Service activity
 - Broadband Receiving while Automatic Registration Service (ARS) user logged in
 - Broadband Transmitting while ARS user logged in
 - Broadband Receiving and Transmitting while ARS user logged in
 - Broadband icon is Blinking (ARS login failed)

The MODM menu screen in [Figure 59: APX Mobile O3 Control Head Programmable Buttons on page 72](#) can be accessed by pressing the pre-programmed MODM button on the radio. See [Figure 58: APX Mobile O2 Control Head Programmable Buttons on page 72](#) for information about the MODM buttons.

7.1.2

APX Data Modem Tethering Event Logging

Centralized logging can be configured on several of the network elements in the APX™ Mobile Data Modem Tethering Reference Architecture.

Logging should be turned on before problems occur. See [Table 16: Resources for APX Data Modem Tethering Centralized Logging Configuration on page 118](#) for network elements with logging capability.

Table 16: Resources for APX Data Modem Tethering Centralized Logging Configuration

Network element	Manual Name	Procedure or Manual Section
Advanced Messaging Solution	<i>ASTRO® 25 Advanced Messaging Solution Server Installation Guide</i>	<i>Logging</i>
Key Management Facility (KMF)	<i>Key Management Facility</i>	<i>Collecting KMF Client Logs</i> <i>Collecting KMF Server Logs and Data</i>
Mobile VPN Gateway	<i>Mobile VPN Gateway</i>	<i>Managing Centralized Syslog Client Configuration</i>
Unified Network Services	<i>Unified Network Services Server Platform Guide</i>	<i>Configuring Virtual Management Server Syslog Settings</i>
Unified Network Services (for server sized to accommodate Priority Management)	<i>Unified Network Services Server Platform Guide</i>	<i>Configuring Virtual Management Server Syslog Settings</i>

7.1.3

Functional Constraints in the Current Release

- ASTRO data features not supported for APX Data Modem Tethering:
 - Applications that use ASTRO broadcast data services are not compatible with Broadband data service. An example is Transit.
 - Analog conventional data is not supported.
- Data Capacity:
 - Unencrypted data (refer to ASTRO 25 system data capacity)
 - Encrypted Broadband data
 - 10,000 active users per Mobile VPN Gateway
 - 20,000 active users per Broadband APN
 - 33,000 total users per Broadband APN

Chapter 8

Recovery of APX Data Modem Tethering

This chapter includes information about the recovery of network elements used for the APX™ Data Modem Tethering feature.

The following manuals may be useful for Disaster Recovery.

Table 17: Resources for Recovery of APX Data Modem Tethering

Manual Name	Chapter or Section
<i>Key Management Facility</i>	KMF Disaster Recovery
<i>Mobile VPN Gateway</i>	Mobile Virtual Private Network (VPN) Gateway Server Disaster Recovery
<i>Unified Network Services Server Platform Guide</i>	<i>UNS Server Platform Disaster Recovery</i>
<i>Unified Network Services Server Platform Guide (for server sized to accommodate Priority Management)</i>	<i>UNS Server Platform Disaster Recovery</i>

Chapter 9

Switch Install Log Files

Introduction

The logs in this appendix are from a 24t (24-port) model of the Extreme Networks X460 and X460-G2 switches and are based on an Agency Applications Network that includes Priority Management.

Switch Boot-Up

Copyright 2014 Extreme Networks, Inc.

Starting CRC of Default image
Using Default image ...

Copyrights 2014 Extreme Networks, Inc.

Press and hold the <spacebar> to enter the bootrom: 0
Loading Secondary OS Image

Starting ExtremeXOS 15.6.1b4
Copyright (C) 1996-2014 Extreme Networks. All rights reserved.
Protected by US Patent Nos: 6,678,248; 6,104,700; 6,766,482; 6,618,388;
6,034,957; 6,859,438; 6,912,592; 6,954,436; 6,977,891; 6,980,550;
6,981,174; 7,003,705; 7,017,082; 7,046,665; 7,126,923; 7,142,509;
7,149,217; 7,152,124; 7,154,861; 7,245,619; 7,245,629; 7,269,135; 7,448,045;
7,447,777; 7,453,874; 7,463,628; 7,483,370; 7,499,679; 7,502,374; 7,539,750;
7,522,516; 7,546,480; 7,552,275; 7,554,978; 7,558,273; 7,568,107; 7,577,996;
7,581,024; 7,580,409; 7,580,350; 7,584,262; 7,599,292; 7,602,721; 7,606,249;
7,606,240; 7,606,263; 7,613,209; 7,619,971; 7,646,773; 7,646,770; 7,649,879;
7,657,619; 7,657,635; 7,660,259; 7,660,894; 7,668,969; 7,672,228; 7,675,915;
7,689,678; 7,693,158; 7,710,993; 7,719,968; 7,724,734; 7,724,669; 7,733,899;
7,752,338; 7,773,507; 7,783,733; 7,792,058; 7,813,348; 7,814,204; 7,817,549;
7,817,633; 7,822,038; 7,822,032; 7,821,931; 7,823,199; 7,822,033; 7,835,348;
7,843,927; 7,856,019; 7,860,006; 7,889,750; 7,889,658; 7,894,451; 7,903,666;
7,908,431; 7,912,091; 7,936,764; 7,936,687; 7,944,942; 7,983,192; 7,990,850;
8,000,344; 8,055,800; 8,059,658; 8,072,887; 8,085,779; 8,107,383; 8,117,336;
8,117,657; 8,135,007; 8,139,583; 8,159,936; 8,160,074; 8,161,270; 8,174,980;
8,204,070; 8,208,418; 8,233,474; 8,255,996; 8,274,974; 8,279,874; 8,295,188;
8,331,373; 8,369,344; 8,412,838; 8,437,359; 8,442,030; 8,464,093; 8,464,312;
8,499,093; 8,520,507; 8,560,693; 8,583,833; 8,605,726; 8,605,732; 8,659,993;
8,660,118; 8,705,532; 8,707,432; 8,724,638; 8,730,963; 8,751,647; 8,751,649.

(pending-AAA) login:
Authentication Service (AAA) on the master node is now available for login.
login: admin
password:



NOTE: Login with admin account and empty password.

ExtremeXOS
Copyright (C) 1996-2014 Extreme Networks. All rights reserved.
Protected by US Patent Nos: 6,678,248; 6,104,700; 6,766,482; 6,618,388;
6,034,957;
6,859,438; 6,912,592; 6,954,436; 6,977,891; 6,980,550; 6,981,174; 7,003,705;
7,017,082;
7,046,665; 7,126,923; 7,142,509; 7,149,217; 7,152,124; 7,154,861; 7,245,619;

```

7,245,629; 7,269,135; 7,448,045; 7,447,777; 7,453,874; 7,463,628; 7,483,370;
7,499,679;
7,502,374; 7,539,750; 7,522,516; 7,546,480; 7,552,275; 7,554,978; 7,558,273;
7,568,107;
7,577,996; 7,581,024; 7,580,409; 7,580,350; 7,584,262; 7,599,292; 7,602,721;
7,606,249;
7,606,240; 7,606,263; 7,613,209; 7,619,971; 7,646,773; 7,646,770; 7,649,879;
7,657,619;
7,657,635; 7,660,259; 7,660,894; 7,668,969; 7,672,228; 7,675,915; 7,689,678;
7,693,158;
7,710,993; 7,719,968; 7,724,734; 7,724,669; 7,733,899; 7,752,338; 7,773,507;
7,783,733;
7,792,058; 7,813,348; 7,814,204; 7,817,549; 7,817,633; 7,822,038; 7,822,032;
7,821,931;
7,823,199; 7,822,033; 7,835,348; 7,843,927; 7,856,019; 7,860,006; 7,889,750;
7,889,658;
7,894,451; 7,903,666; 7,908,431; 7,912,091; 7,936,764; 7,936,687; 7,944,942;
7,983,192;
7,990,850; 8,000,344; 8,055,800; 8,059,658; 8,072,887; 8,085,779; 8,107,383;
8,117,336;
8,117,657; 8,135,007; 8,139,583; 8,159,936; 8,160,074; 8,161,270; 8,174,980;
8,204,070;
8,208,418; 8,233,474; 8,255,996; 8,274,974; 8,279,874; 8,295,188; 8,331,373;
8,369,344;
8,412,838; 8,437,359; 8,442,030; 8,464,093; 8,464,312; 8,499,093; 8,520,507;
8,560,693;
8,583,833; 8,605,726; 8,605,732; 8,659,993; 8,660,118; 8,705,532; 8,707,432;
8,724,638;
8,730,963; 8,751,647; 8,751,649.

```

```
=====
Press the <tab> or '?' key at any time for completions.
```

```
Remember to save your configuration changes.
```

```
The switch currently has all management methods enabled for convenience reasons.
Please answer these questions about the security settings you would like to use.
```

```
Telnet is enabled by default. Telnet is unencrypted and has been the target of
security exploits in the past.
```

```
Would you like to disable Telnet? [y/N]: No
```

```
SNMP access is enabled by default. SNMP uses no encryption, SNMPv3 can be
configured to eliminate this problem.
```

```
Would you like to disable SNMP? [y/N]: No
```

```
All ports are enabled by default. In some secure applications, it maybe more
desirable for the ports to be turned off.
```

```
Would you like unconfigured ports to be turned off by default? [y/N]: Yes
```

```
Disabling all ports ... done
```

```
Changing the default failsafe account username and password is highly
recommended. If you choose to do so, please remember the username and
password as this information cannot be recovered.
```

```
Would you like to change the failsafe account username and password
now? [y/N]: No
```

```
Would you like to permit failsafe account access via the management port?
```

```
[y/N]: Yes
```

Enabling failsafe account access via the management port ... telnet ssh

The switch can proactively attempt to send basic configuration and operational switch information for the purpose of assisting technical support to resolve customer-reported issues. Uploaded data is encrypted if the ssh.xmod is installed. Otherwise, a reduced switch data set is sent in clear text that contains no customer-specific information.

Would you like to disable the automatic switch reporting service?

[Y/n]: No

Enabling the automatic reporting service ... done Since you have chosen less secure management methods, please remember to increase the security of your network by taking the following actions:

- * **change your admin password**
 - * **change your failsafe account username and password**
 - * **change your SNMP public and private strings**
 - * **consider using SNMPv3 to secure network management traffic**
 - * **install the ssh.xmod**

Configuring User Accounts and Deleting Default Account

```
* X460G2-24t-10G4.1 # delete account "user"
* X460G2-24t-10G4.2 # create account user agency_user
password:
Reenter password:
* X460G2-24t-10G4.3 # create account admin agency_admin
password:
Reenter password:
```



NOTE: This example is for deleting “user” account and creating “agency_user” as a user account, and “agency_admin” as an admin account. To keep password empty, press ENTER twice.

Configuring the Management OOBM Port

```
* X460G2-24t-10G4.7 # configure "Mgmt" ipaddress 1.1.1.1/24
IP interface for VLAN Mgmt has been created.
* X460G2-24t-10G4.8 # configure iproute add default 1.1.1.2 vr "VR-Mgmt"
* X460G2-24t-10G4.9 # show vlan "Mgmt"
```

```
VLAN Interface with name Mgmt created by user
  Admin State:      Enabled      Tagging:    802.1Q Tag 4095
  Description:      Management VLAN
  Virtual router:   VR-Mgmt
  IPv4 Forwarding:  Disabled
  IPv4 MC Forwarding: Disabled
  Primary IP:       1.1.1.1/24
  IPv6 Forwarding:  Disabled
  IPv6 MC Forwarding: Disabled
  IPv6:             None
  STPD:             None
  Protocol:         Match all unfiltered protocols
  Loopback:         Disabled
  NetLogin:         Disabled
  OpenFlow:         Disabled
  TRILL:            Disabled
  QosProfile:       None configured
  Flood Rate Limit QosProfile: None configured
  Ports: 1.         (Number of active ports=1)
  Untag: Mgmt-port on Mgmt is active
```

• Switching to the VR Mgmt virtual router

```
* X460G2-24t-10G4.10 # virtual-router "VR-Mgmt"

* (vr VR-Mgmt) X460G2-24t-10G4.11 # show iproute
Ori Destination Gateway Mtr Flags VLAN
Duration
#s Default Route 1.1.1.2 1 UG---S-um--f- Mgmt
0d:0h:0m:37s
#d 1.1.1.0/24 1.1.1.1 1 U-----um--f- Mgmt
0d:0h:1m:4s

Origin(Ori): (b) BlackHole, (be) EBGp, (bg) BGP, (bi) IBGP, (bo) BOOTP,
(ct) CBT, (d) Direct, (df) DownIF, (dv) DVMRP, (e1) ISISL1Ext,
(e2) ISISL2Ext, (h) Hardcoded, (i) ICMP, (i1) ISISL1 (i2) ISISL2,
(is) ISIS, (mb) MBGP, (mbe) MBGPEExt, (mbi) MBGPInter, (mp) MPLS Lsp,
(mo) MOSPF (o) OSPF, (o1) OSPFExt1, (o2) OSPFExt2,
(oa) OSPFIntra, (oe) OSPFAsExt, (or) OSPFInter, (pd) PIM-DM, (ps) PIM-SM,
(r) RIP, (ra) RtAdvrt, (s) Static, (sv) SLB_VIP, (un) UnKnown,
(*) Preferred unicast route (@) Preferred multicast route,
(#) Preferred unicast and multicast route.

Flags: (b) BFD protection requested, (B) BlackHole, (c) Compressed, (D) Dynamic,
(f) Provided to FIB, (G) Gateway, (H) Host Route, (l) Calculated LDP LSP,
(L) Matching LDP LSP, (m) Multicast, (p) BFD protection active, (P) LPM-r
outing,
(R) Modified, (s) Static LSP, (S) Static, (t) Calculated RSVP-TE LSP,
(T) Matching RSVP-TE LSP, (u) Unicast, (U) Up, (3) L3VPN Route.

MPLS Label: (S) Bottom of Label Stack
Mask distribution:
  1 default routes 1 routes at length 24

Route Origin distribution:
  1 routes from Direct 1 routes from Static

Total number of routes = 2
Total number of compressed routes = 0
```

Verifying connectivity to the laptop (TFTP server) * (vr VR-Mgmt) X460G2-10G4.12

```
* (vr VR-Mgmt) X460G2-24t-10G4.12 # ping 1.1.1.2
Ping(ICMP) 1.1.1.2: 4 packets, 8 data bytes, interval 1 second(s).
16 bytes from 1.1.1.2: icmp_seq=0 ttl=128 time=8.066 ms
16 bytes from 1.1.1.2: icmp_seq=1 ttl=128 time=0.565 ms
16 bytes from 1.1.1.2: icmp_seq=2 ttl=128 time=0.458 ms
16 bytes from 1.1.1.2: icmp_seq=3 ttl=128 time=0.466 ms

--- 1.1.1.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% loss
round-trip min/avg/max = 0/2/8 ms
```

Switching back to the default VR

```
* (vr VR-Mgmt) X460G2-24t-10G4.13 # virtual-router "VR-Default"
```

Upgrading the Software Images

```
* X460G2-24t-10G4.14 # show switch

SysName: X460G2-24t-10G4
SysLocation:
SysContact: support@extremenetworks.com, +1 888 257 3000
System MAC: 00:04:96:98:FB:7E
```

```
System Type: X460G2-24t-10G4

SysHealth check: Enabled (Normal)
Recovery Mode: All
System Watchdog: Enabled

Current Time: Tue Apr 7 20:25:30 2015
Timezone: [Auto DST Disabled] GMT Offset: 0 minutes, name is UTC.
Boot Time: Tue Apr 7 20:19:47 2015
Boot Count: 7
Next Reboot: None scheduled
System UpTime: 5 minutes 42 seconds

Current State: OPERATIONAL
Image Selected: secondary
Image Booted: secondary
Primary ver: 15.5.1.6
Secondary ver: 15.5.1.6

Config Selected: NONE
Config Booted: Factory Default
* X460G2-24t-10G4.15 # download image 1.1.1.2 summitX-15.6.1.4.xos
Note: The inactive partition (primary) will be used for installation.Do you
want to install image after downloading? (y - yes, n - no, <cr> - cancel)
Yes

Downloading to Switch.....
.....
Installing to primary partition!

Installing to Switch.....
.....
Image installed successfully
This image will be used only after rebooting the switch!

* X460G2-24t-10G4.16 # show switch

SysName: X460G2-24t-10G4
SysLocation:
SysContact: support@extremenetworks.com, +1 888 257 3000
System MAC: 00:04:96:98:FB:7E
System Type: X460G2-24t-10G4

SysHealth check: Enabled (Normal)
Recovery Mode: All
System Watchdog: Enabled

Current Time: Tue Apr 7 20:28:14 2015
Timezone: [Auto DST Disabled] GMT Offset: 0 minutes, name is UTC.
Boot Time: Tue Apr 7 20:19:47 2015
Boot Count: 7
Next Reboot: None scheduled
System UpTime: 8 minutes 27 seconds

Current State: OPERATIONAL
Image Selected: primary
Image Booted: secondary
Primary ver: 15.6.1.4
Secondary ver: 15.5.1.6
```

```
Config Selected:  NONE
Config Booted:   Factory Default
```

Loading SSH module:

```
X460G2-24t-10G4.2 # show management
CLI idle timeout           : Enabled (20 minutes)
CLI max number of login attempts : 3
CLI max number of sessions  : 8
CLI paging                 : Enabled (this session only)
CLI space-completion       : Disabled (this session only)
CLI configuration logging   : Disabled
CLI scripting              : Disabled (this session only)
CLI scripting error mode    : Ignore-Error (this session only)
CLI persistent mode        : Persistent (this session only)
CLI prompting              : Enabled (this session only)
Telnet access              : Enabled (tcp port 23 vr all)
                           : Access Profile : not set
SSH Access                 : ssh module not loaded.
Web access                 : Enabled (tcp port 80)
                           : Access Profile : not set
Total Read Only Communities : 1
Total Read Write Communities : 1
RMON                       : Disabled
SNMP access                : Enabled
                           : Access Profile : not set
SNMP Compatibility Options :
  GETBULK Reply Too Big Action : Too Big Error
  IP Fragmentation            : Disallow
SNMP Notifications        : Enabled
SNMP Notification Receivers : None
SNMP stats:               InPkts 0      OutPkts 0      Errors 0      AuthErrors 0
                           Gets   0      GetNexts 0     Sets   0      Drops   0
SNMP traps:               Sent   0      AuthTraps Enabled
SNMP inform:              Sent   0      Retries 0      Failed 0
X460G2-24t-10G4.3 #
(vr VR-Mgmt) X460G2-24t-10G4.19 # download image 1.1.1.2 summitX-15.6.1.4-
ssh.xmod

Do you want to install image after downloading? (y - yes, n - no, <cr> - cancel)
Yes

Downloading to Switch
Installing to primary partition!

Installing to SwitchError: Failed to install image - version mismatch between XOS
and xmod

* X460G2-24t-10G4.20 # download image 1.1.1.2 summitX-15.6.1.4-ssh.xmod
Do you want to install image after downloading? (y - yes, n - no, <cr> - cancel)
Yes

Downloading to Switch...
Installing to primary partition!

Installing to Switch.....
SSL will be usable after restart of thttpd process. Restart snmpMaster process t
o use AES/3DES users for SNMPv3.

Image installed successfully
* X460G2-24t-10G4.18 # save configuration install
```

No default configuration database has been selected to boot up the system.
Save configuration will set the new configuration as the default database.

Do you want to save configuration to install.cfg? (y/N) Yes

Saving configuration on master done!

Configuration saved to install.cfg successfully.

The selected configuration will take effect after the next switch reboot.

X460G2-24t-10G4.19 # **reboot**Are you sure you want to reboot the switch? (y/N) Yes

The system is going down NOW!

Sending SIGKILL to all processes

Requesting system reboot

Copyright 2014 Extreme Networks, Inc.

Starting CRC of Default image

Using Default image ...

Copyright 2014 Extreme Networks, Inc.

Press and hold the <spacebar> to enter the bootrom: 0

Loading Primary OS Image

Starting ExtremeXOS 15.7.1b4

Copyright (C) 1996-2015 Extreme Networks. All rights reserved.

This product is protected by one or more US patents listed at <http://www.extreme-networks.com/patents> along with their foreign counterparts.

(pending-AAA) login:

Authentication Service (AAA) on the master node is now available for login.

login: admin

password:

ExtremeXOS

Copyright (C) 1996-2015 Extreme Networks. All rights reserved.

This product is protected by one or more US patents listed at <http://www.extreme-networks.com/patents> along with their foreign counterparts.

Press the <tab> or '?' key at any time for completions.

Remember to save your configuration changes.

X460G2-24t-10G4.1 # **show switch**

SysName: X460G2-24t-10G4
SysLocation:
SysContact: support@extremenetworks.com, +1 888 257 3000
System MAC: 00:04:96:98:FB:7E
System Type: X460G2-24t-10G4

SysHealth check: Enabled (Normal)
Recovery Mode: All
System Watchdog: Enabled

Current Time: Tue Apr 7 20:31:43 2015
Timezone: [Auto DST Disabled] GMT Offset: 0 minutes, name is UTC.
Boot Time: Tue Apr 7 20:30:28 2015

```

Boot Count:      8
Next Reboot:    None scheduled
System UpTime:  1 minute 15 seconds

Current State:  OPERATIONAL
Image Selected: primary
Image Booted:  primary
Primary ver:    15.6.1.4
Secondary ver:  15.5.1.6

Config Selected: install.cfg

Config Booted:  install.cfg

install.cfg      Created by ExtremeXOS version 15.6.1.4
                  173498 bytes saved on Tue Apr  7 20:29:50 2015

```

X460G2-24t-10G4.1 # show management

```

CLI idle timeout           : Enabled (20 minutes)
CLI max number of login attempts : 3
CLI max number of sessions  : 8
CLI paging                 : Enabled (this session only)
CLI space-completion       : Disabled (this session only)
CLI configuration logging   : Disabled
CLI scripting              : Disabled (this session only)
CLI scripting error mode    : Ignore-Error (this session only)
CLI persistent mode        : Persistent (this session only)
CLI prompting              : Enabled (this session only)
Telnet access              : Enabled (tcp port 23 vr all)
                           : Access Profile : not set
SSH access                 : Disabled (Key invalid, tcp port 22 vr all)
                           : Access Profile : not set
Web access                 : Enabled (tcp port 80)
                           : Access Profile : not set
Total Read Only Communities : 1
Total Read Write Communities : 1
RMON                      : Disabled
SNMP access               : Enabled
                           : Access Profile : not set
SNMP Compatibility Options :
  GETBULK Reply Too Big Action : Too Big Error
  IP Fragmentation             : Disallow
SNMP Notifications        : Enabled
SNMP Notification Receivers : None
SNMP stats:
  InPkts 0      OutPkts 0      Errors 0      AuthErrors 0
  Gets 0       GetNexts 0      Sets 0       Drops 0
SNMP traps:
  Sent 0      AuthTraps Enabled
SNMP inform:
  Sent 0      Retries 0      Failed 0

```

Upgrading image on the secondary partition

```

X460G2-24t-10G4.3 # download image 1.1.1.2 summitX-15.7.1.4.xos
Note: The inactive partition (secondary) will be used for installation.
Do you want to install image after downloading? (y - yes, n - no, <cr> -
cancel)
Yes

```

```

Downloading to Switch.....
.....

```


Installing to **secondary partition!**

Installing to Switch.....
.....

Image installed successfully
This image will be used only after rebooting the switch!
X460G2-24t-10G4.4 # **show switch**

SysName: X460G2-24t-10G4
SysLocation:
SysContact: support@extremenetworks.com, +1 888 257 3000
System MAC: 00:04:96:98:FB:7E
System Type: X460G2-24t-10G4

SysHealth check: Enabled (Normal)
Recovery Mode: All
System Watchdog: Enabled

Current Time: Tue Apr 7 21:03:27 2015
Timezone: [Auto DST Disabled] GMT Offset: 0 minutes, name is UTC.
Boot Time: Tue Apr 7 20:58:13 2015
Boot Count: 9
Next Reboot: None scheduled
System UpTime: 5 minutes 14 seconds

Current State: OPERATIONAL
Image Selected: **secondary**
Image Booted: primary
Primary ver: 15.6.1.4
Secondary ver: **15.7.1.4**

Config Selected: install.cfg
Config Booted: install.cfg

install.cfg Created by ExtremeXOS version 15.6.1.4
173498 bytes saved on Tue Apr 7 20:29:50 2015

Loading SSH module to the secondary partition

X460G2-24t-10G4.6 # **download image 1.1.1.2 summitX-15.7.1.4-ssh.xmod**
Do you want to install image after downloading? (y - yes, n - no, <cr> - cancel)
Yes

Downloading to Switch...
Installing to **secondary partition!**

Installing to Switch.....
SSL will be usable after restart of thttpd process. Restart snmpMaster process t
o use AES/3DES users for SNMPv3.

Image installed successfully
X460G2-24t-10G4.7 # **rebootAre you sure you want to reboot the switch? (y/N) Yes**
Sending SIGKILL to all processes
Requesting system reboot

Copyright 2014 Extreme Networks, Inc.

Starting CRC of Default image
Using Default image ...

Copyright 2014 Extreme Networks, Inc.

Press and hold the <spacebar> to enter the bootrom: 0
Loading Secondary OS Image

Starting ExtremeXOS 15.7.1b4

Copyright (C) 1996-2015 Extreme Networks. All rights reserved.

This product is protected by one or more US patents listed at <http://www.extremenetworks.com/patents> along with their foreign counterparts.

(pending-AAA) login: admin

(pending-AAA) password:

Failed to connect to authentication service (Master node unknown)!

Login incorrect

(pending-AAA) login:

Authentication Service (AAA) on the master node is now available for login.

login: admin1

password:

ExtremeXOS

Copyright (C) 1996-2015 Extreme Networks. All rights reserved.

This product is protected by one or more US patents listed at <http://www.extremenetworks.com/patents> along with their foreign counterparts.

=====
Press the <tab> or '?' key at any time for completions.

Remember to save your configuration changes.

X460G2-24t-10G4.1 # show switch

SysName: X460G2-24t-10G4

SysLocation:

SysContact: support@extremenetworks.com, +1 888 257 3000

System MAC: 00:04:96:98:FB:7E

System Type: X460G2-24t-10G4

SysHealth check: Enabled (Normal)

Recovery Mode: All

System Watchdog: Enabled

Current Time: Tue Apr 7 21:07:28 2015

Timezone: [Auto DST Disabled] GMT Offset: 0 minutes, name is UTC.

Boot Time: Tue Apr 7 21:06:38 2015

Boot Count: 10

Next Reboot: None scheduled

System UpTime: 50 seconds

Current State: OPERATIONAL

Image Selected: **secondary**

Image Booted: **secondary**

Primary ver: **15.6.1.4**

Secondary ver: **15.7.1.4**

Config Selected: install.cfg

Config Booted: install.cfg

```

install.cfg          Created by ExtremeXOS version 15.6.1.4
                    173498 bytes saved on Tue Apr  7 20:29:50 2015
X460G2-24t-10G4.2 # show management
CLI idle timeout    : Enabled (20 minutes)
CLI max number of login attempts : 3
CLI max number of sessions : 8
CLI paging          : Enabled (this session only)
CLI space-completion : Disabled (this session only)
CLI configuration logging : Disabled
CLI scripting       : Disabled (this session only)
CLI scripting error mode : Ignore-Error (this session only)
CLI persistent mode : Persistent (this session only)
CLI prompting       : Enabled (this session only)
Telnet access       : Enabled (tcp port 23 vr all)
                    : Access Profile : not set
SSH access          : Disabled (Key invalid, tcp port 22 vr all)
                    : Access Profile : not set
Web access          : Enabled (tcp port 80)
                    : Access Profile : not set
Total Read Only Communities : 1
Total Read Write Communities : 1
RMON                : Disabled
SNMP access         : Enabled
                    : Access Profile : not set
SNMP Compatibility Options :
  GETBULK Reply Too Big Action : Too Big Error
  IP Fragmentation            : Disallow
SNMP Notifications      : Enabled
SNMP Notification Receivers : None
SNMP stats:             InPkts 0      OutPkts 0      Errors 0      AuthErrors 0
                       Gets   0      GetNexts 0      Sets   0      Drops      0
SNMP traps:             Sent    0      AuthTraps Enabled
SNMP inform:            Sent    0      Retries  0      Failed 0

```

Enabling SSH

```

X460G2-24t-10G4.3 # enable ssh2
WARNING: Generating new server host key
This could take approximately 15 minutes and cannot be canceled. Continue? (y/N)
) Yes
.....Key Generated
* X460G2-24t-10G4.4 # show management
CLI idle timeout    : Enabled (20 minutes)
CLI max number of login attempts : 3
CLI max number of sessions : 8
CLI paging          : Enabled (this session only)
CLI space-completion : Disabled (this session only)
CLI configuration logging : Disabled
CLI scripting       : Disabled (this session only)
CLI scripting error mode : Ignore-Error (this session only)
CLI persistent mode : Persistent (this session only)
CLI prompting       : Enabled (this session only)
Telnet access       : Enabled (tcp port 23 vr all)
                    : Access Profile : not set
SSH access        : Enabled (Key valid, tcp port 22 vr all)
                    : Access Profile : not set
Web access          : Enabled (tcp port 80)
                    : Access Profile : not set
Total Read Only Communities : 1

```

```

Total Read Write Communities      : 1
RMON                               : Disabled
SNMP access                        : Enabled
                                   : Access Profile : not set
SNMP Compatibility Options        :
  GETBULK Reply Too Big Action    : Too Big Error
  IP Fragmentation                : Disallow
SNMP Notifications                 : Enabled
SNMP Notification Receivers       : None
SNMP stats:      InPkts 0      OutPkts 0      Errors 0      AuthErrors 0
                  Gets  0      GetNexts 0      Sets  0      Drops  0

SNMP traps:      Sent  0      AuthTraps Enabled
SNMP inform:     Sent  0      Retries  0      Failed 0
* X460G2-24t-10G4.5 #
* X460G2-24t-10G4.5 # show ssh2 private-key

```

Output of the following command displays the private key:

```

*X460G2-24t-10G4.6 # save configurationThe configuration file install.cfg
already exists.
Do you want to save configuration to install.cfg and overwrite it? (y/N) Yes
Saving configuration on master .... done!
Configuration saved to install.cfg successfully.

```

Upgrading the Switch License

```

*X460G2-24t-10G4.10 # enable license <license key>
Enabled license successfully.

```

Loading the Switch Software Configuration

```

X460G2-24t-10G4.7 # tftp get 1.1.1.2 PNR.xsf
Downloading PNR.xsf to switch... done!
X460G2-24t-10G4.8 # load script PNR.xsf

```



NOTE: The following script configures the switch:

```

* geocen1-PNR.9 # reboot
Do you want to save configuration changes to currently selected configuration
file (install.cfg) and reboot?
(y - save and reboot, n - reboot without save, <cr> - cancel command) Yes

Sending SIGKILL to all processes
Requesting system reboot

```