AirLink MG90

Software Configuration Guide

SIERRA WIRELESS®

4118700
Rev 6

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the Sierra Wireless modem are used in a normal manner with a well-constructed network, the Sierra Wireless modem should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Sierra Wireless accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the Sierra Wireless modem, or for failure of the Sierra Wireless modem to transmit or receive such data.

Safety and Hazards

Do not operate the Sierra Wireless modem in areas where blasting is in progress, where explosive atmospheres may be present, near medical equipment, near life support equipment, or any equipment which may be susceptible to any form of radio interference. In such areas, the Sierra Wireless modem **MUST BE POWERED OFF**. The Sierra Wireless modem can transmit signals that could interfere with this equipment.

Do not operate the Sierra Wireless modem in any aircraft, whether the aircraft is on the ground or in flight. In aircraft, the Sierra Wireless modem **MUST BE POWERED OFF**. When operating, the Sierra Wireless modem can transmit signals that could interfere with various onboard systems.

Note: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. Sierra Wireless modems may be used at this time.

The driver or operator of any vehicle should not operate the Sierra Wireless modem while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some states and provinces, operating such communications devices while in control of a vehicle is an offence.

Limitation of Liability

The information in this manual is subject to change without notice and does not represent a commitment on the part of Sierra Wireless. SIERRA WIRELESS AND ITS AFFILIATES SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE OR ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE ANY SIERRA WIRELESS PRODUCT, EVEN IF SIERRA WIRELESS AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THEY ARE FORESEEABLE OR FOR CLAIMS BY ANY THIRD PARTY.

Notwithstanding the foregoing, in no event shall Sierra Wireless and/or its affiliates aggregate liability arising under or in connection with the Sierra Wireless product, regardless of the number of events, occurrences, or claims giving rise to liability, be in excess of the price paid by the purchaser for the Sierra Wireless product.

Patents

This product may contain technology developed by or for Sierra Wireless Inc. This product includes technology licensed from QUALCOMM®. This product is manufactured or sold by Sierra Wireless Inc. or its affiliates under one or more patents licensed from MMP Portfolio Licensing.

Copyright

Trademarks

Sierra Wireless®, AirPrime®, AirLink®, AirVantage® and the Sierra Wireless logo are registered trademarks of Sierra Wireless, Inc.

Windows® and Windows Vista® are registered trademarks of Microsoft Corporation.

QUALCOMM® is a registered trademark of QUALCOMM Incorporated. Used under license.

Other trademarks are the property of their respective owners.

Contact Information

Sales information and technical support, including warranty and returns	Web: sierrawireless.com/company/contact-us/ Global toll-free number: 1-877-687-7795 6:00 am to 5:00 pm PST
Corporate and product information	Web: sierrawireless.com

Revision History

Revision number	Release date	Changes
1	October 2016	Document created
2	January 2017	MC74xx used to identify radio module series, replacing MC7455 Clarified AMM statement in Configuring an MG90 Router Added GPS fields to new section NMEA Messaging 'Additional Options' Added fields to Table 13-2, Cellular Info section (MEID, Band Number, Bandwidth, RSRP, RSRQ, SINR, Hardware Version, Roaming Indicator, Service, Provision Status) Added Advanced modem Initialization example for private network link in Cellular WAN Link Configuration and Table 17-3 Updated Configuring VPN Profiles (reboot requirement for VPN updates)
3	July 2017	Added new radio modules—MC7354, Bandrich M535
4	November 2017	Noted Bluetooth adapter default configuration in Devices > Bluetooth. Added LED chase sequence for firmware updates in Table 23-1.

Revision number	Release date	Changes
5	June 2018	Added Advanced Configuration Login Added GPS Forwarding Threshold options Added PPPoE WAN support for USB-to-Ethernet adapter Added note indicating IKEv2 VPNs only, when MOBIKE is used Added note concerning module firmware update when device has two different Sierra Wireless modules Support for multiple Host-to-LAN simultaneous VPN servers Added LCI options for private DNS zones Added GPIO and GPIO Status applications Added EM75xx module support Added Status Broadcast option Updated Cellular WAN Link Configuration MTU Size fields Added Enable/disable option to LAN Access Points configuration Added IGMP Snooping enable/disable to LAN Segment Configuration Added GPS Dead Reckoning configuration and updated GNSS LED behavior Removed option to enable/disable automatic purging of unused firmware images Added FirstNet SIM support for use with EM7565 modules Added DSCP option to QoS Priority Rules Added option to switch MG90 from non-FIPS to FIPS (one way only) Updated Management Tunnel Configuration (added UDP ports, replaced selectable monitors with Tunnel Automatic Monitor)
6	August 2018	Added Purge on Next Boot field for purging firmware images Noted Split Access security consideration Added ‘Automatic’ option for Gateway Virtual IP assignment

Contents

1: Introduction

Overview

The MG90 Local Configuration Interface (LCI) is the MG90 router's browser-based configuration utility.

You can use the LCI to:

- Log in and configure device parameters
- Adjust network settings
- Change security settings
- Update events reporting and control outputs

Note: This document refers to the AirLink Mobility Manager (AMM), Sierra Wireless' cloud-based application. AMM is a re-branding of oMM—this document applies to oMM 2.15.1 and higher, and AMM.

About This Document

This document describes how to configure various MG90 features, provides a full listing of interface parameters, and provides additional information for troubleshooting the MG90.

- Configuration tasks
  - Router Access and Configuration on page 13
  - Performance Tuning on page 60
  - Configuring Startup/Shutdown Behavior on page 17
  - Preparing the Network Interfaces on page 19
  - Administration on page 23
  - Setting Up The WAN on page 31
  - Setting up the LAN on page 52
  - How to configure a VPN on page 63
  - Setting up GPS connectivity on page 70
  - Applications on page 74
  - Updating the System on page 75
- LCI—Tab parameters
  - Status Tab on page 83
  - Devices Tab on page 93
  - Security Tab on page 100
  - LAN Tab on page 102
  - WAN Tab on page 131
  - GPS Tab on page 188
  - General Tab on page 196
  - Logs Tab on page 207
  - Applications Tab on page 209
  - Logout Tab on page 215
- Additional information
  - LEDs on page 216

FIPS vs. Non-FIPS

This document describes features and options for non-FIPS-enabled and FIPS-enabled MG90 routers.

Important: *MG90 routers cannot be 'cross-graded' (FIPS to non-FIPS, non-FIPS to FIPS) through the software interface. To convert an MG90, contact Sierra Wireless Support.*

Tools and Reference Documents

For MG90-related tools and documentation, go to http://source.sierrawireless.com.

Table 1-1: Related Documents

Document	Description
MG90 Hardware User Guide	This document describes how to: • Install the MG90 router hardware • Connect the antennas • Connect a notebook computer and other input/output (I/O) devices • Interpret the router's LEDs

2: Router Access and Configuration

Configuring an MG90 Router

To configure an MG90 router, use either of the following methods:

- Use the browser-based LCI to directly configure the router (as described in this guide).
- If you have more than one MG90 router, use the AirLink Mobility Manager (AMM) application to copy (deploy) the configuration from one of your other routers to this router (refer to your AMM documentation for instructions).

  Log in to the AMM to monitor and manage your MG90 routers as described in the AirLink Mobility Manager Operation and Configuration Guide. If the MG90 does not appear in your AMM account dashboard, refer to your AMM documentation or contact Sierra Wireless Technical Support (see Contact Information on page 3).

Accessing the Local Configuration Interface (LCI)

Note: The LCI supports Internet Explorer 11 running on a Windows PC. Other browsers and devices may work but have not been certified by Sierra Wireless.

To access the LCI:

1. Insert the SIM card(s), if applicable. Refer to the AirLink MG90 Hardware User Guide (available from https://source.sierrawireless.com) for details.
2. Power on the MG90 router. The router should fully power up within two minutes.
3. Launch your browser and enter the router's IP address: http://172.22.0.1/MG-LCI.

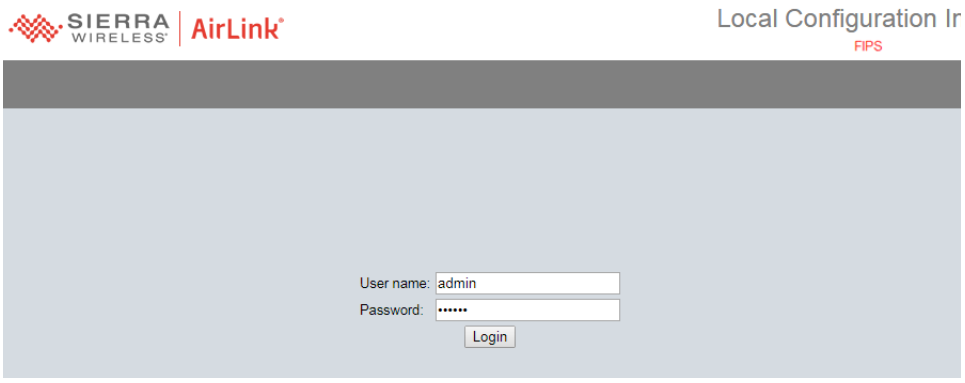

Figure 2-1: LCI Login Screen

Note: The red 'FIPS' indicator in the top-right portion of the screen appears only if the MG90 uses a FIPS-compliant encryption module.

4. Log in using the default admin user credentials:
   - User Name: admin
   - Password: admin (This is the default password)

Note: Make sure to change the admin password to prevent unauthorized access to the device. Otherwise, a warning dialog will appear, indicating that the user name and password must be different. See Configuring User Access on page 26 for instructions on Updating Users.

The MG90 has two account types (see Configuring User Access on page 26 for details):
- admin—Used to directly access the LCI and update the MG90's configuration.
- user—Used to access the LCI to show the current status.

Advanced Configuration Login

After logging in to the LCI as an admin user, most screens are readily accessible. However, some screens will display an Advanced Configuration Login screen to re-enter the admin user credentials (username, password) for additional security. After entering the credentials, all of the following pages can be accessed:
- Status > Broadcast
- GPS
- General > Auto Software Update
- Application configuration pages

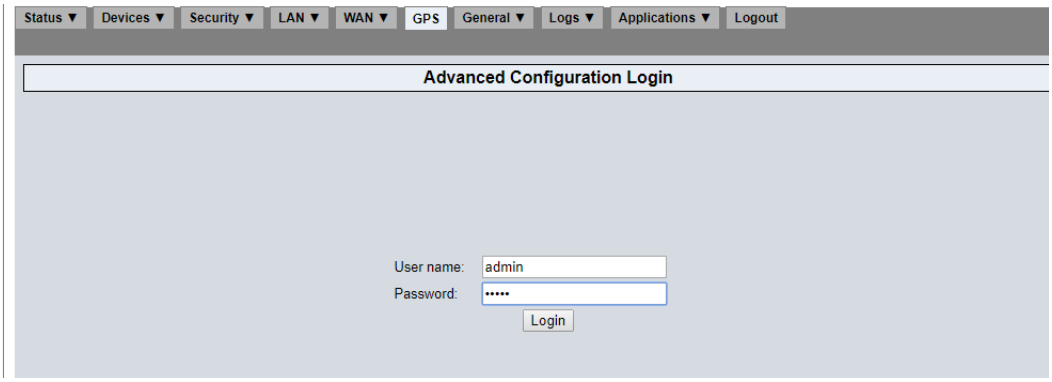

Figure 2-2: Advanced Configuration Login Screen

Navigating the LCI Tabs and Screens

The following are some basic tips for navigating in the LCI and updating the MG90's configuration:
- Most configuration changes take effect as soon as they are saved. If a change requires a router reboot (such as a change to the serial port), a message will appear.
  - Screens with a Save or Submit button—Click the button to save any changes made on the current screen.
  - You cannot 'undo' a change that has been saved.
  - Changes that have not been saved are automatically canceled if you:
    - Click the Cancel button (if available)
    - Change to a different tab

- Use the browser options to go forward or backward
- Refresh browser window to return to the WAN Status screen.

- Browser options:
  - Forward/Back icons (and keyboard shortcuts)—Regular browser functionality. Use these to move forward and backward through your history. Note that this cancels any changes in progress.
  - Refresh icon (and keyboard shortcut—for example, F5 for IE and Chrome)—Cancels any changes in progress and returns to the WAN Status screen.
- Log out—To log out of the LCI, click the Logout tab.

Figure 2-3: Log out of the LCI

Viewing Only Configuration Settings (Easy Access)

The MG90 includes a read-only Easy Access page, which allows users on all devices connected to the unit to view the unit's operational status without logging in to the LCI.

To view the Easy Access page from a device (e.g. laptop) connected to the unit, use your browser to navigate to http://172.22.0.1/MG-LCI/easyaccess.html.

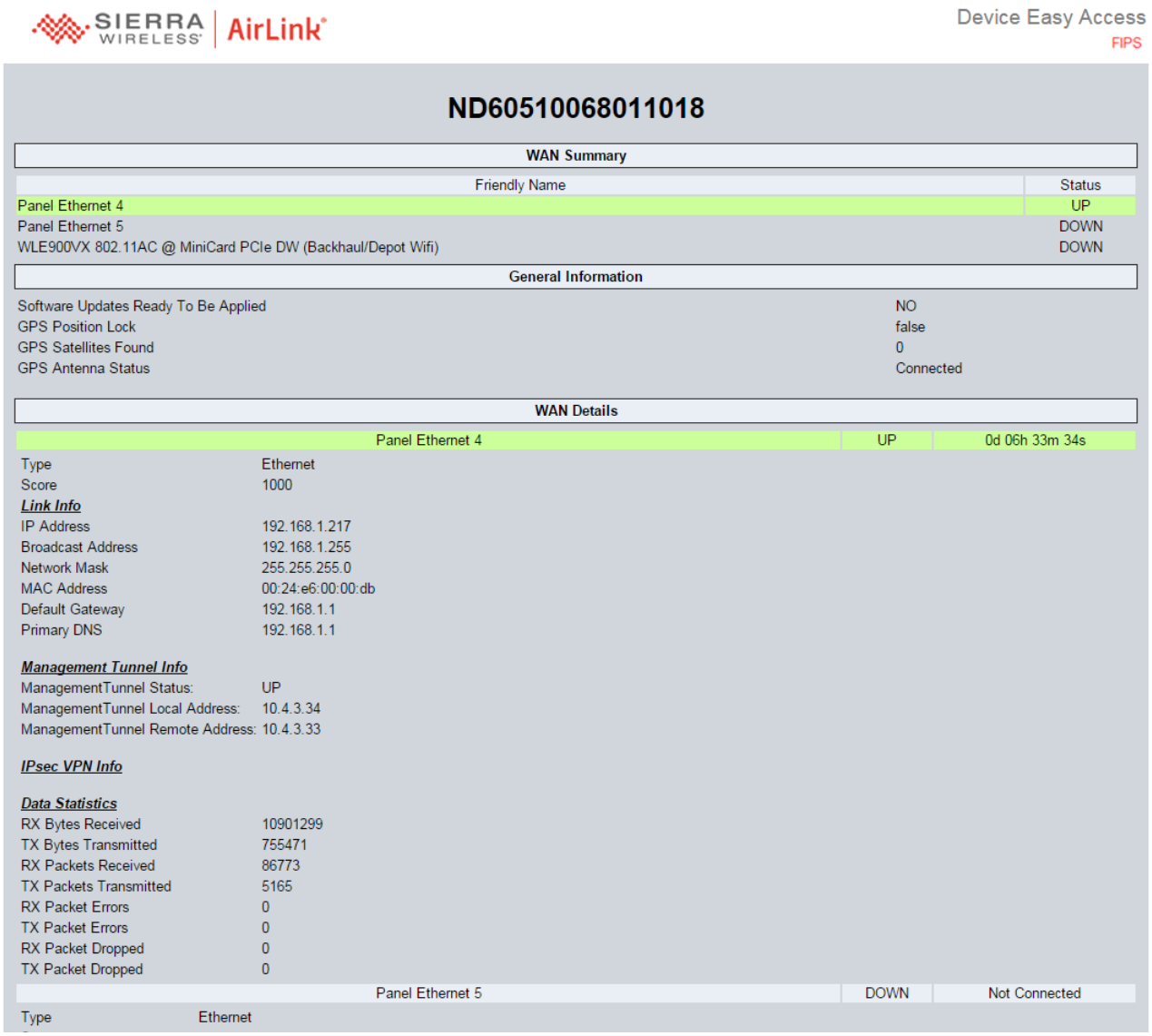

Figure 2-4: Easy Access Page

Note: The red 'FIPS' indicator in the top-right portion of the screen appears only if the MG90 uses a FIPS-compliant encryption module.

3: Configuring Startup/Shutdown Behavior

The MG90 startup behavior (automatic or manual) and shutdown behavior (automatic or manual) can be customized options on the LCI's General tab.

Startup Behavior

The MG90's default configuration is to boot (turn on) automatically (if AutoPower is selected) when ignition is detected. To modify the startup behavior:

1. Go to General > Startup.

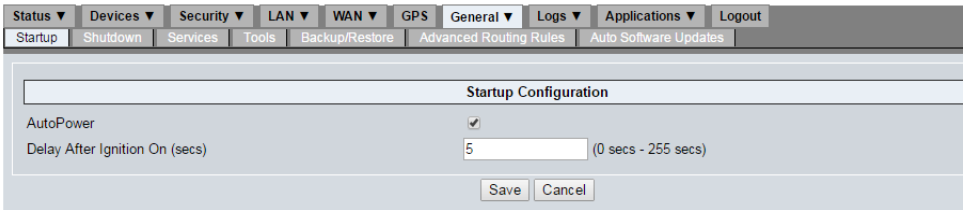

Figure 3-1: Startup Behavior Configuration (LCI: General > Startup)

2. Select/deselect AutoPower as appropriate:
   - Selected—MG90 turns on automatically when ignition is detected.
   - Deselected—MG90 does not turn on automatically. After the vehicle ignition is turned on, the Reset button on the front panel must be pressed to turn the device on.
3. In the Delay After Ignition On field (if AutoPower is selected), enter the delay (in seconds) to wait after turning on the ignition before the MG90 will turn on.
4. Click Save.

For detailed field information, see General > Startup on page 196.

Shutdown Behavior

The MG90 automatically shuts down when excessive or insufficient power is detected, or when extreme temperature conditions are encountered (using the unit's built-in temperature sensor).

To modify the shutdown behavior (temperature and voltage thresholds):

1. Go to General > Shutdown.

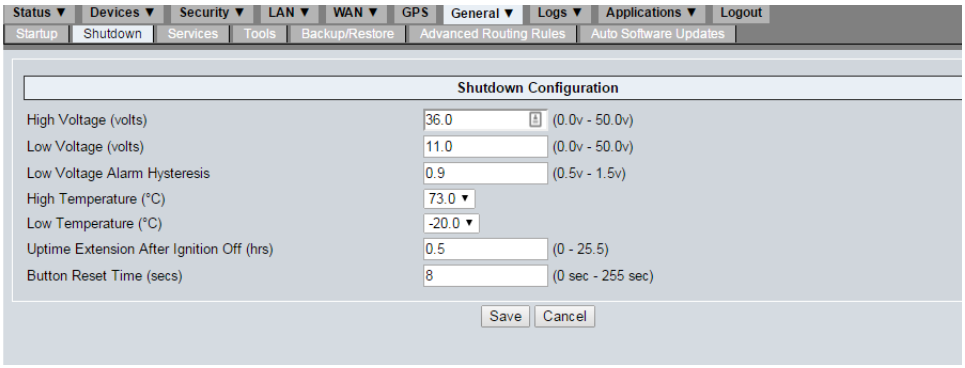

Figure 3-2: Shutdown Configuration (LCI: General > Shutdown)

2. Configure the voltage and temperature fields as appropriate.
   For example, adjust the Low Voltage value if you want the MG90 to shutdown when operating off the vehicle battery and the battery charge is getting too low.
   For detailed field information, see General > Shutdown on page 196.

Note: Voltage readings are subject to cable length and will always be slightly lower than the voltage measured at the source.

3. Click Save.

When the MG90 shuts down due to a high/low voltage or high/low temperature condition, the unit's Power LED turns solid red, and stays red until the condition is resolved. For more information on the MG90's LED patterns, see LEDs on page 216.

4: Preparing the Network Interfaces

The MG90 is pre-configured with devices that provide LAN and/or WAN connectivity, including LTE radios, Wi-Fi modules, and Ethernet ports.

Before using the MG90, verify the settings for each device to ensure they are properly configured for LAN or WAN data communications. Device types include:

- Cellular devices (e.g. pre-installed MC7354, MC74XX, EM75XX modules)—See Configuring Cellular Devices on page 19.
- Ethernet ports (pre-installed ports on rear panel)—See Configuring Ethernet Ports on page 20.
- Wi-Fi devices (e.g. pre-installed Wi-Fi modules)—See Configuring Wi-Fi Devices on page 20.
- Serial modem (e.g. Harris Land Mobile Radio)—See Configuring a Serial Modem Device on page 21.
- Serial port (Device connected to serial port on rear panel) —See Configuring the Serial Port on page 21.
- Internal Bluetooth device—See Configuring the Bluetooth Device on page 22.

Configuring Cellular Devices

To verify and configure cellular device settings:

1. Go to Devices > Cellular:

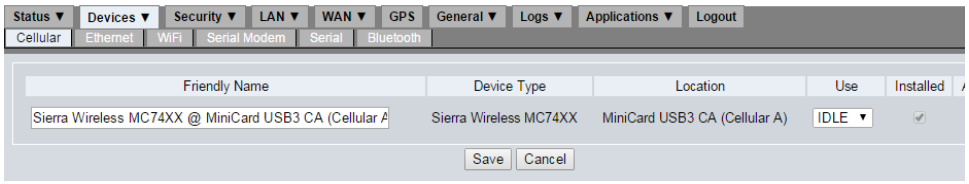

Figure 4-1: LCI: Devices > Cellular

Note: Your MG90 will have one or two cellular devices installed:

   a. If desired, enter descriptive names for each device in the Friendly Name fields.(The Friendly Name is used to identify the device in other LCI screens.)

   b. If the Installed field is not marked (checked) for a device that you know is physically installed (has not been temporarily removed), contact Sierra Wireless Technical Support for assistance (see Contact Information on page 3).

   c. In the Use drop-downs for each device, select the current usage state:
      - WAN—Use the device to connect the MG90 to a mobile network.
      - IDLE—Do not use the device for WAN connections at this time.

Important: *Ensure at least one device is set to WAN so the unit can connect to a network when away from Wi-Fi access points (for example, outside of a depot, away from the depot's access point.*

   d. If you made any changes, click Save.

Configuring Ethernet Ports

To verify and configure Ethernet port settings:

1. Go to Devices > Ethernet:

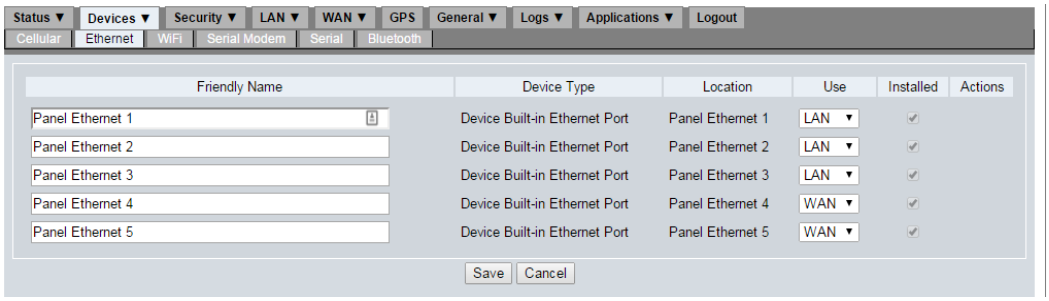

Figure 4-2: LCI: Devices > Ethernet

   a. In the Use drop-downs for each port, select the current usage state:
      - LAN—Use the port to connect a device to the MG90's LAN.
      - WAN—Use the port to connect the MG90 to a WAN.
      - IDLE—Do not use the port to connect devices at this time.
   b. If the Installed field is not marked (checked) for any of the ports, contact Sierra Wireless Technical Support for assistance (see Contact Information on page 3).
   c. If you made any changes, click Save.

Configuring Wi-Fi Devices

To verify and configure Wi-Fi device settings:

1. Go to Devices > Wi-Fi:

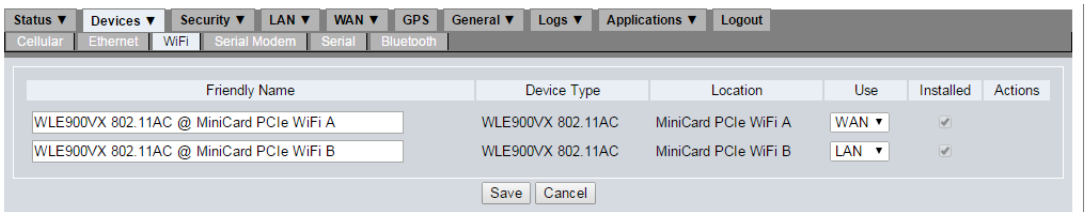

Figure 4-3: LCI: Devices > Wi-Fi

   a. In the Use drop-downs for each device, select the current usage state:
      - LAN—Use the module as an access point ('Vehicle Wi-Fi') for wireless devices to connect to the router. (Wi-Fi B is set to LAN by default.)
      - WAN—Use the module for 'Depot Wi-Fi', which is used when the MG90 returns to a depot that has a wireless AP available. (Wi-Fi A is set to WAN by default.)
      - IDLE—Do not use the Wi-Fi module at this time.
   b. If the Installed field is not marked (checked) for a device that you know is physically installed (has not been temporarily removed), contact Sierra Wireless Technical Support for assistance (see Contact Information on page 3).
   c. If you made any changes, click Save.

Configuring a Serial Modem Device

To verify and configure serial modem device settings:

1. If you have a serial modem (Harris Land Mobile Radio) attached to the RS-232 serial port, go to Devices > Serial Modem:

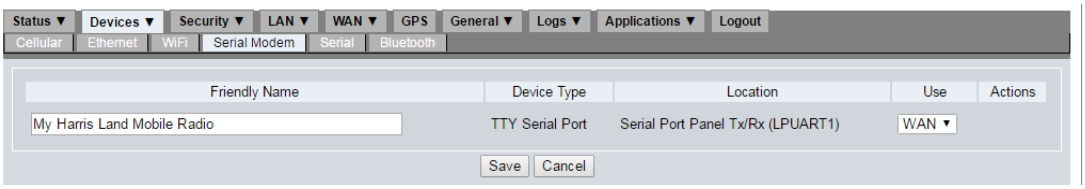

Figure 4-4: LCI: Devices > Serial Port

   a. In the Use drop-down, select one of the following:
      - WAN—Enable the serial modem.
      - IDLE—Do not use the serial modem at this time.
   b. If you made any changes, click Save.

Configuring the Serial Port

To verify and configure the RS-232 DB9 serial port settings:

1. Go to Devices > Serial:

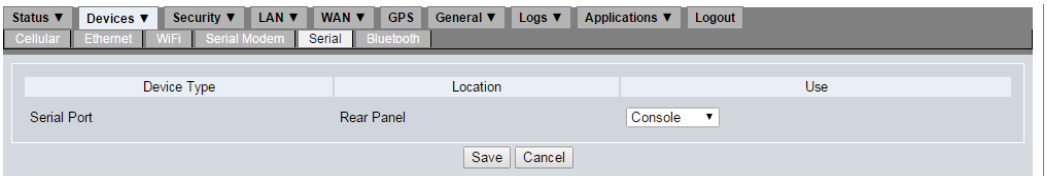

Figure 4-5: LCI: Devices > Serial

   a. In the Use drop-down, select the port's current usage state:
      - Console—This option should only be selected under the direction of Sierra Wireless Technical Support.
      - Application—Connect the serial port to a device that uses a serial connection (for example, a serial modem (see Configuring a Serial Modem Device on page 21) or an external GPS device (see Setting up GPS connectivity on page 70).
   b. If you changed the Use value, click Save.

Configuring the Bluetooth Device

To verify and configure the internal Bluetooth device's settings:

1. Go to Devices > Bluetooth:

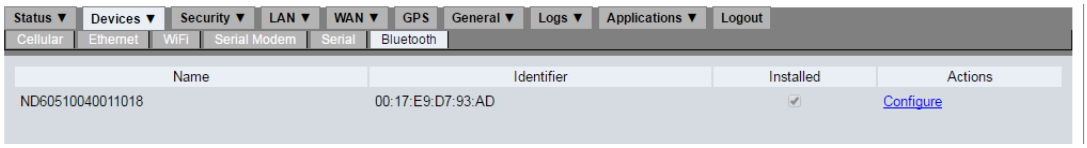

Figure 4-6: LCI: Devices > Bluetooth

   a. Click Configure in the Actions column.
   b. Configure the fields as appropriate. For detailed field information, see Bluetooth Adapter Configuration (Devices > Bluetooth > Configure) on page 98.
   c. Click Save.

5: Administration

Some typical MG90 administration tasks that you can perform in the LCI include:

- Display MG90 device and WAN status details:
  - See Displaying General Information on page 23.
  - See Obtaining WAN Status Details on page 24.
- Configure access to the MG90 access:
  - See Configuring User Access on page 26.
  - See Changing the Root Password on page 27.
- Backup/restore the MG90. See Backing up and Restoring Configuration Settings on page 28.
- Use advanced tools to manage and troubleshoot the MG90:
  - See Configuring Services on page 29.
  - See Using the Diagnostic Tools on page 29.
  - See Running Custom Scripts on page 30.

Displaying General Information

To display general MG90 details (such as serial number, hardware and software version numbers, voltage, temperature, and basic GPS data):

1. Go to Status > General.

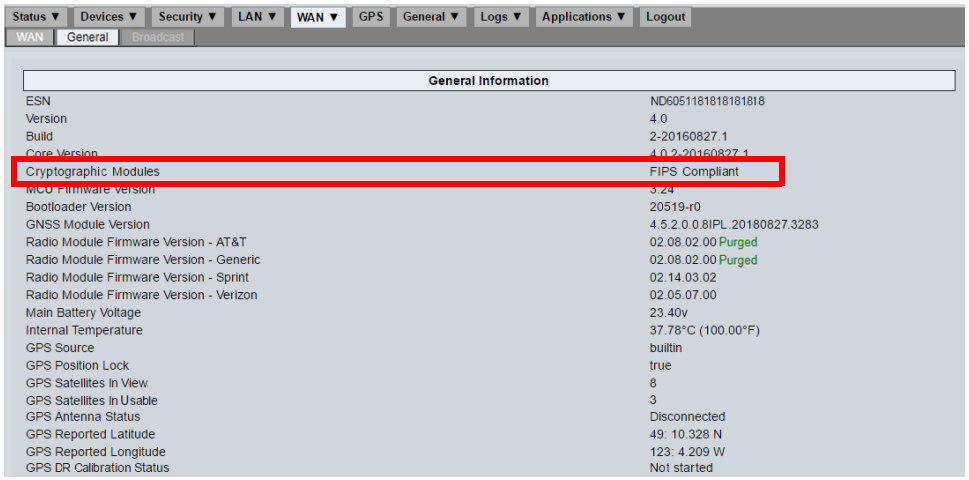

Figure 5-1: LCI: Status > General

Note: The 'Cryptographic modules' entry (shown above) appears only if the MG90 uses a FIPS-compliant encryption module.

For detailed field information, see General Information on page 89.

Obtaining WAN Status Details

To display detailed WAN status information, including the MG90's IP address, data transmission statistics, etc.):

1. Go to Status > WAN.
2. Select Show Extended Status.

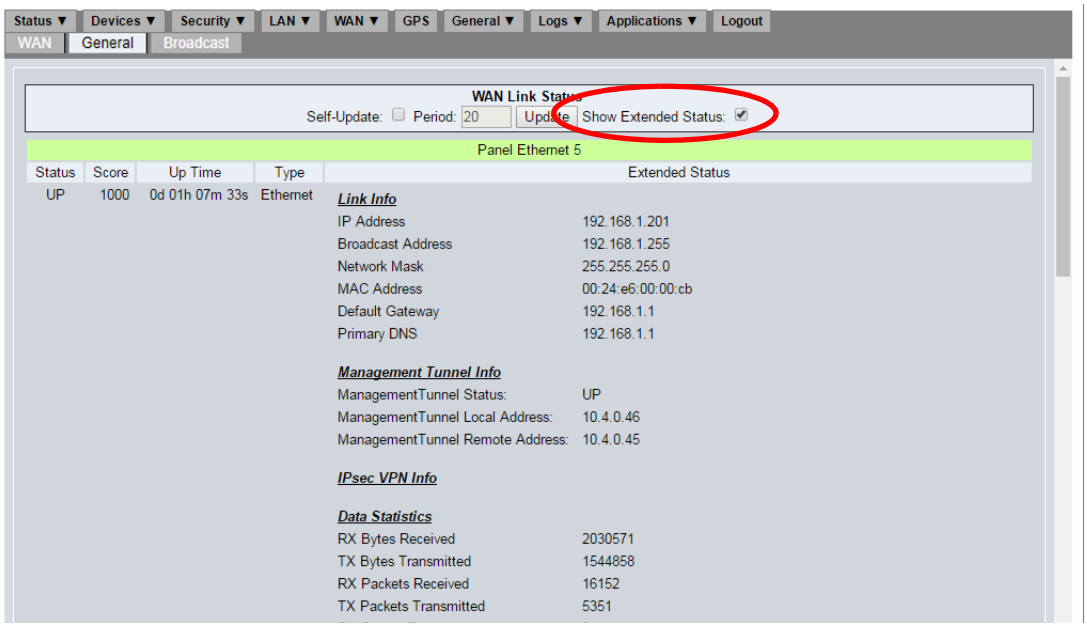

Figure 5-2: LCI: Status > WAN > Extended Status

For detailed field information, see Extended status screen on page 84.

Broadcast Router Status

The MG90 can be configured to broadcast device status information (including GPIO, WAN, GNSS, VPN, and general status details) at regular intervals, when GPIO states change, or both. Selected data items are broadcast (in JSON format) on a specific UDP port on one or more LAN segments, and users on those LAN segments can use a network analyzer (e.g. tcpdump) to listen for data packets on the UDP port.

To configure status broadcasting:

1. Go to Status > Broadcast.

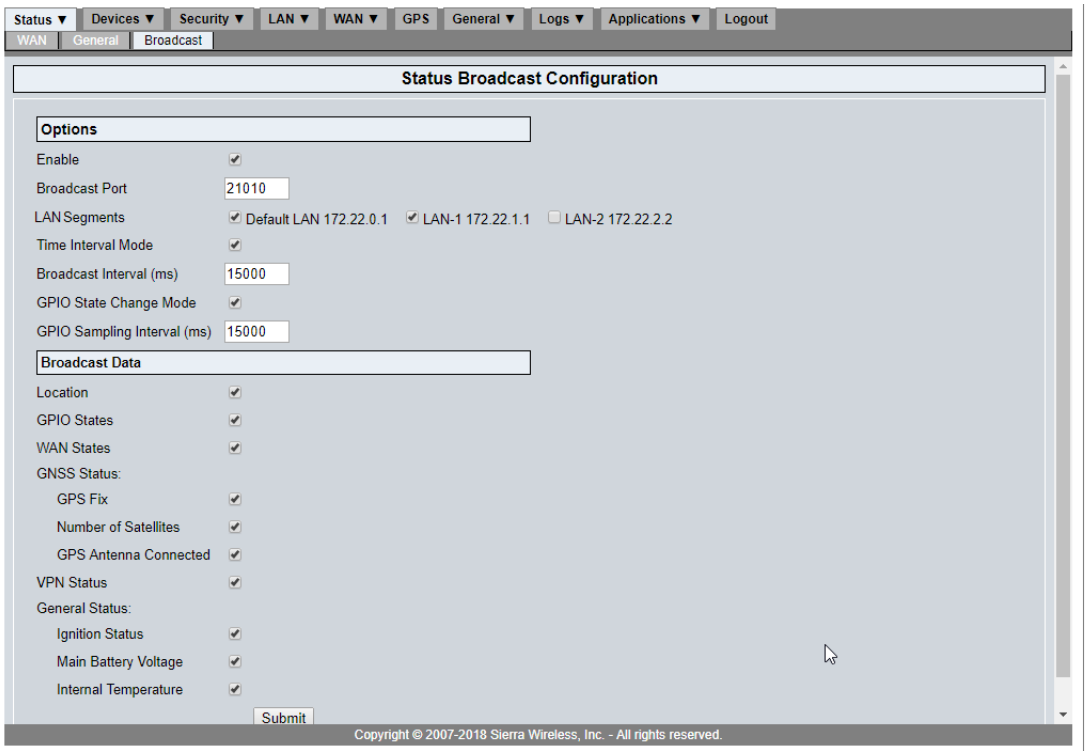

Figure 5-3: LCI: Status > Broadcast

2. Select Enable to activate the broadcast feature.
3. Set the broadcast scheduling options:
   a. In the Broadcast Port field, enter the UDP port to use for broadcasting.
   b. In LAN Segments, select one or more LAN Segments to use for broadcasting.
   c. To broadcast status details on a regular schedule, select Time Interval Mode and enter the Broadcast Interval (in milliseconds).
   d. To broadcast status details when the state of any GPIO changes, select GPIO State Change Mode and enter the GPIO Sampling Interval (in milliseconds) at which GPIO states are checked.

Note: Broadcast Interval, GPIO Sampling Interval, or both must be selected for broadcasting to be enabled. If neither option is selected, the Enable option is cleared when Submit is clicked.

4. Select the status details to be included in broadcasts:
   - Location—Latitude and longitude
   - GPIO States—GPIO input/output states (all five GPIOs)
   - WAN States—State of each individual WAN link (includes Friendly Name, Status (0 or 1), Active (true or false), Signal Strength in dBm)
   - GPS Fix—Fix available (true or false)
   - Number of Satellites—Number of usable satellites
   - GPS Antenna Connected—True or false
   - VPN Status—0 or 1
   - Ignition Status—True or false
   - Main Battery Voltage—Voltage, in volts

- Internal Temperature—Temperature, in °C

5. Click Submit. The selected Broadcast Data details are compiled into a JSON-formatted file and broadcast over UDP based on the selected Options. (For the JSON schema and an example, see JSON Data on page 218.)

For detailed field information, see Broadcast on page 91.

Configuring User Access

By default, the LCI includes one Administrator-type user account ('admin'). Additional accounts (user names) can be created with the following user types:

- Administrator—Administrator users can access and update all screens in the LCI.
- User—Regular Users can view the basic status information (WAN > Status), but not make any changes in the LCI.

Note: User names are case-sensitive.

Important: *Sierra Wireless recommends that you create strong, unique passwords for each Administrator-type account on each MG90 to prevent unauthorized access to the device. Make sure the username and password are different, otherwise a warning dialog to remind you will appear at each login until the password is changed.*

Adding Users

To add a new user account:

1. Go to Security > Users.

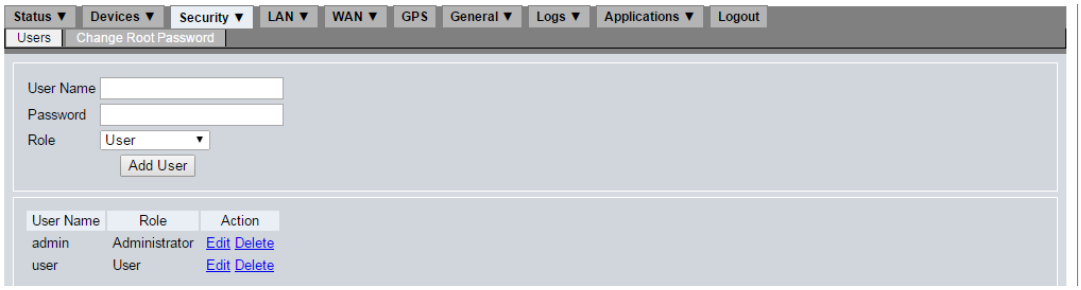

Figure 5-4: LCI: Security > Users

2. Enter the User Name that will be used to log in to the LCI.
3. Enter a Password for the account.
4. In the Role drop-down, select the account type:
   - Administrator—Select if the user needs full access to the LCI.
   - User—Select if the user needs only to view MG90 status details.
5. Click Add User.

Important: *Make sure there is always at least one user with the 'Administrator' role before logging out or disconnecting. If there are no administrators remaining, the LCI will not be accessible and the MG90 will require a factory reset to regain access.*

Updating Users

To modify an existing user account's password:

1. Go to Security > Users.
2. Click Edit in the Action column for the account to modify.
3. Modify the Password field.
4. Click Edit User.

Deleting Users

To delete a user account:

1. Go to Security > Users.
2. Click Delete in the Action column for the account.
3. Click OK when prompted to confirm the deletion.

For detailed field information, see Security > Users on page 100.

Important: *Make sure there is always at least one user with the 'Administrator' role before logging out or disconnecting. If there are no administrators remaining, the LCI will not be accessible and the MG90 will require a factory reset to regain access.*

Changing the Root Password

The MG90 can be remotely accessed for advanced diagnostics by your IT department or Sierra Wireless Technical Support by using a root password, which is defaulted to the MG90's serial number.

Important: *Sierra Wireless recommends that you create strong, unique root passwords for each MG90 to prevent unauthorized users from changing router settings. You will need to provide the password to authorized users who need to access the MG90.*

Important: *If you forget the root password, it cannot be recovered. You must perform a factory reset to restore it to the default value (the MG90's serial number). To perform the factory reset, press and hold the Reset button on the MG90's front panel until all the LEDs turn solid white. Release the button, and the LEDs remain white while the factory reset is in progress. When the reset finishes, the MG90 powers off and, if AutoPower is enabled, reboots.*

To change the root password:

1. Go to Security > Change Root Password.

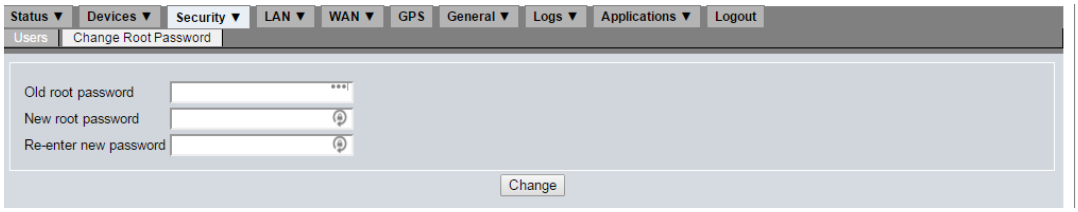

Figure 5-5: LCI: Security > Change Root Password

2. Enter the Old root password (by default, this is the MG90's serial number).
3. Enter the New root password. (Note—The password must be 8+ characters.)
4. Re-enter the new password to confirm.
5. Click Change.

For detailed field information, see Security > Change Root Password on page 101.

Backing up and Restoring Configuration Settings

The MG90's current configuration can be manually backed up if required, and can be restored from stored backup files. (You can save multiple backup versions.)

If you have an AMM (AirLink Mobility Manager) account through Sierra Wireless (or operate your own AMM server), the current configuration is also saved automatically each time the MG90 connects to the AMM account. This copy of the configuration file can be deployed through the AMM to any other MG90 routers registered to your AMM account. Refer to your AMM documentation for instructions.

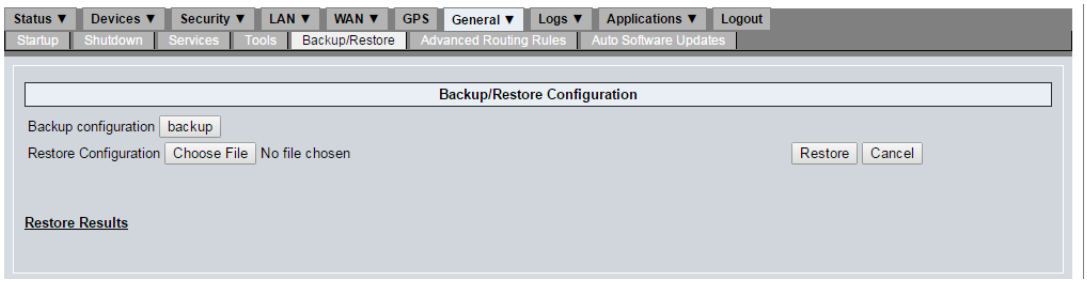

Figure 5-6: LCI: General > Backup/Restore

Important: *Before you restore a configuration to the MG90, ensure the device's software version number matches the version number of the unit used to create the original configuration file—if they don't match, the MG90 may not function properly. See Displaying General Information on page 23 to view an MG90's version information.*

Backing up the current configuration

To back up the MG90's configuration:

1. Go to General > Backup/Restore.
2. Click backup. The configuration file saves automatically to your default downloads folder.
3. In Windows Explorer, move the configuration file from the downloads folder to a folder where you want to save your backup files.

Restoring an earlier configuration

To restore a configuration from a previous backup:

1. Go to General > Backup/Restore.
2. Click Choose File/Browse. (The button label depends on the browser being used. Typically, the label is Choose File or Browse.)
3. Navigate to the folder containing your backup files.

4. Select the appropriate backup file and click OK.
   The fully qualified filename appears in the Restore Configuration field.

Note: If you decide not to restore the selected backup file, click Cancel.

5. Click Restore. When the restoration is complete, comprehensive details appear in the Restore Results section.

For detailed field information, see General > Backup/Restore on page 201.

Configuring Services

Events generated on the MG90 are reported to the AMM. By default, the address of the AMM is provided to the MG90 by DNS servers managed by Sierra Wireless.

To view and configure event reporting settings:

1. Go to General > Services.
2. If necessary, modify appropriate settings.

Note: These settings should only be modified as directed by Sierra Wireless.

For detailed field information, see General > Services on page 198.

Using the Diagnostic Tools

The MG90 includes several command line diagnostic tools to help with upgrading, provisioning, and troubleshooting.

To use a diagnostic tool:

1. Go to General > Tools.
2. Select the tool to use in the Command drop-down. For descriptions of available tools, see General > Tools on page 199.
3. Enter any command line arguments to use with the tool in the Arguments field (see Figure 5-7 for a 'ping' example).
4. Click Execute. If the tool produces an output it appears under Results.

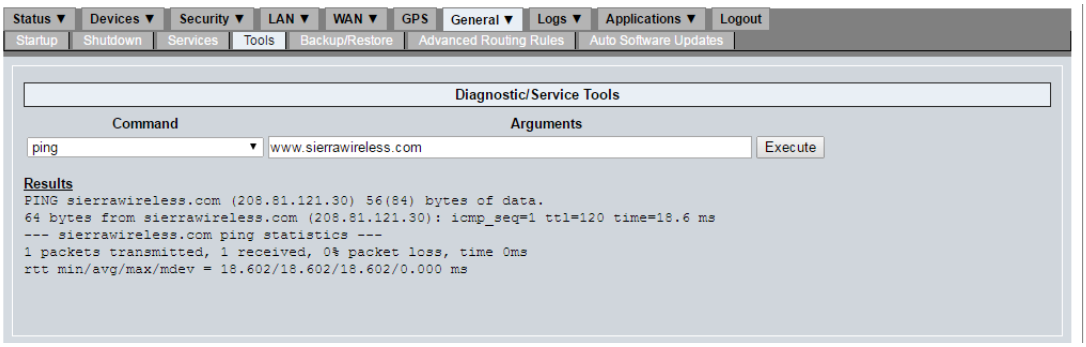

Figure 5-7: Tool example—ping

Running Custom Scripts

Administrators (e.g. your IT department or Sierra Wireless Technical Support) can run custom scripts on the MG90 to perform advanced functionality and device customization. These scripts are run from the General > Advanced Routing Rules tab.

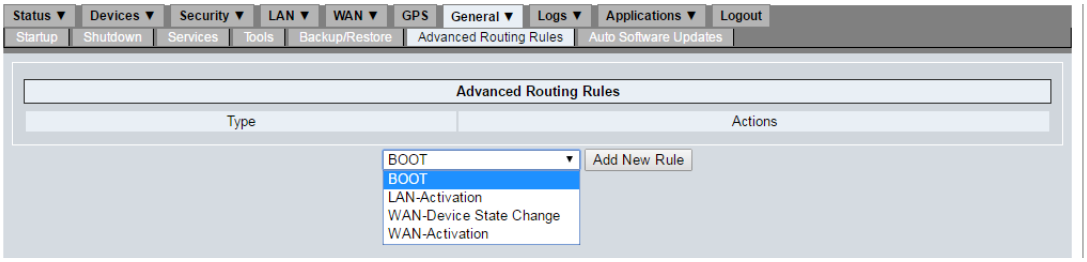

Figure 5-8: Advanced Routing Rules Screen

This should only be attempted by individuals who are proficient with Linux shell scripting and when a result cannot be achieved using the standard configuration measures available from the LCI.

Important: *Since incorrect use of this feature may disable the unit, Sierra Wireless recommends that such configuration be done in consultation with Sierra Wireless Technical Support.*

For detailed option information, see General > Advanced Routing Rules on page 201.

6: Setting Up The WAN

The MG90 can connect to the WAN using three device types:

- Cellular—Typically used when the vehicle is traveling outside the area around its depot.
- Wi-Fi—Typically used when the vehicle returns to a depot that has an AP available for the MG90 to connect to as a client.
- Ethernet—By default, Port 5 is configured for WAN access, and Ports 1–4 are configured for LAN access.

Multiple devices can be active (configured for WAN) at the same time to provide redundant WAN access should one or more connections go down.

Note: The MG90 does not support USB-to-Ethernet adapters for WAN operation.

Basic WAN Link Configuration

Each device that is currently configured for WAN connectivity is listed as a WAN link on the WAN > Links tab. (See Preparing the Network Interfaces on page 19 to configure devices for WAN use.)

Note: If a device (such as an LTE radio) was removed from the MG90 while it was configured for WAN usage, it appears in this list with the 'Enabled' flag not selected and will have a Delete option in the Actions column.

To configure the settings for a WAN link:

1. Go to WAN > Links.

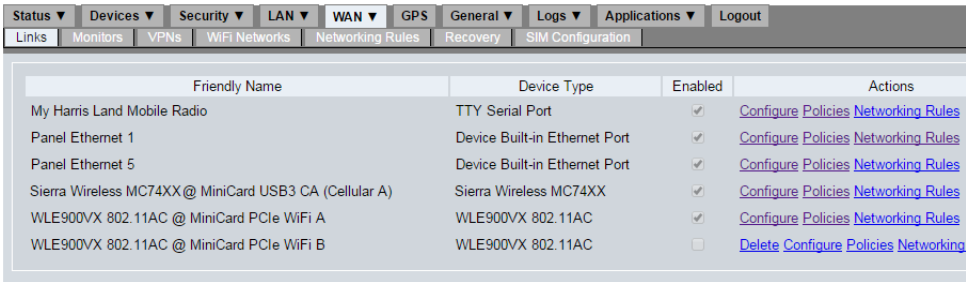

Figure 6-1: WAN > Links Tab

2. Click Configure in the Actions column for the link.
3. Configure the link using the appropriate procedure:
   - Cellular link—See Cellular WAN Link Configuration on page 32.
   - Wi-Fi link—See Wi-Fi WAN Link Configuration on page 33.
   - Ethernet link—See Ethernet WAN Link Configuration on page 34.
   - Serial link—See Serial WAN Link Configuration on page 36.

Cellular WAN Link Configuration

Cellular WAN links provide connectivity wherever cellular reception is available. The Cellular WAN Link Configuration screen allows you to view and modify connection settings for an installed radio module with an activated SIM installed.

In the Cellular WAN Link Configuration screen (see Figure 6-2 below):

1. Configure the fields for the selected cellular device. For detailed field information, see Cellular WAN Link Configuration on page 138.

Tip: *If the WAN link is a private network that requires a user name and password for access, enter the following command in the Advanced Modem Initialization String field: AT$QCPDPP=1\,1\,<password>\,<username>*
For example:

AT$QCPDPP=1\,1\,3AD29482\,6045551234@static.carrier.ca

2. Click Save.

For information on specific settings for your card, contact your carrier or visit http://source.sierrawireless.com.

Note: The fields displayed vary depending on radio module type and LCI settings.

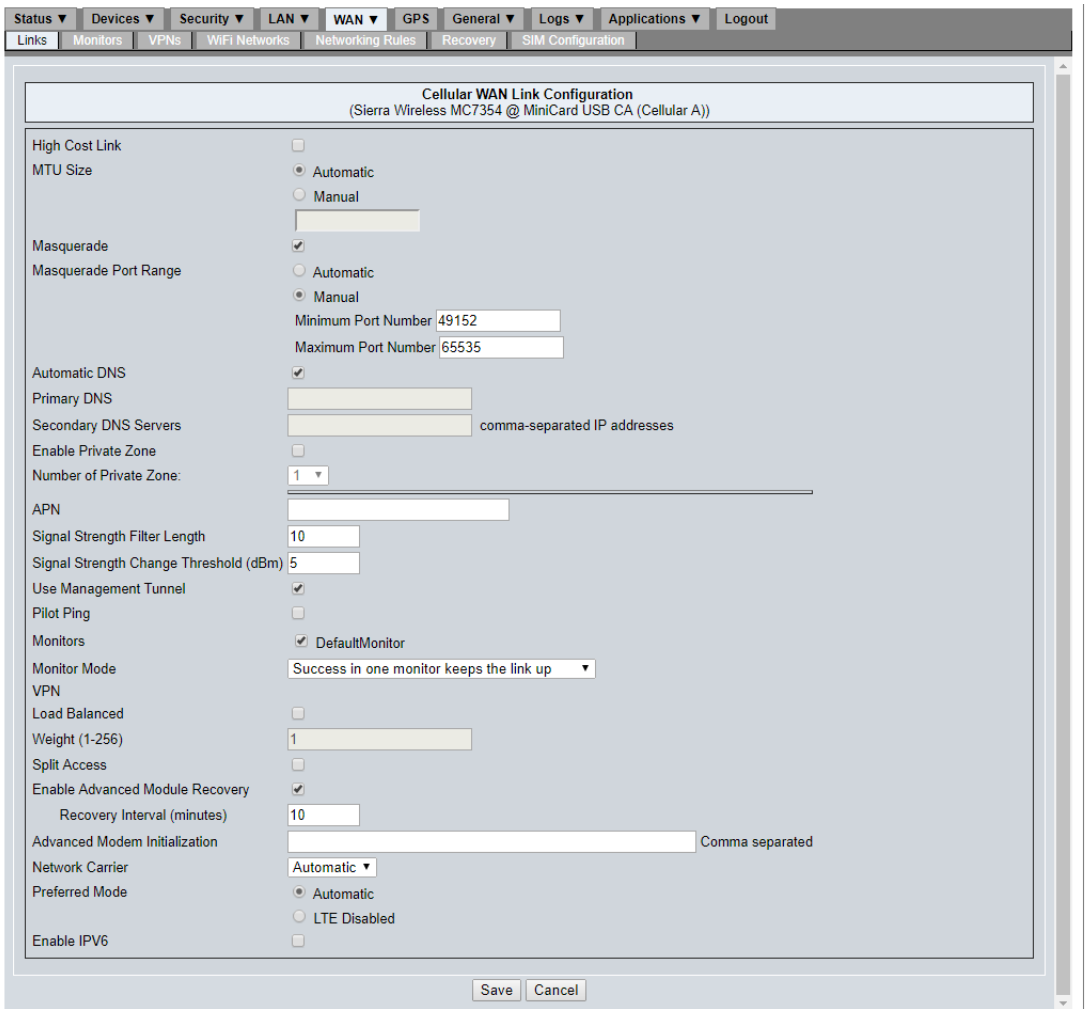

Figure 6-2: Cellular WAN Link Configuration (LCI: WAN > Links > Configure)

Wi-Fi WAN Link Configuration

Wi-Fi WAN links provide WAN access via Wi-Fi access points (AP), which are often available in locations such as vehicle depots. These links are usually configured as the primary WAN access method, since it is usually preferable to utilize an AP when available. The Wi-Fi WAN Link Configuration screen allows you to view and modify connection settings for the MG90's Wi-Fi modules.

In the Wi-Fi WAN Link Configuration screen (see Figure 6-3 below):

1. Configure the fields for the selected Wi-Fi device. For detailed field information, see Wi-Fi WAN Link Configuration on page 143.
2. After configuring a Wi-Fi WAN link, select the AP profile(s) that this Wi-Fi WAN link will connect to. (The AP profiles store credentials and other information required to communicate with an AP. See Defining an Access Point Profile for Wi-Fi Links on page 37 for details.)
3. Click Save.

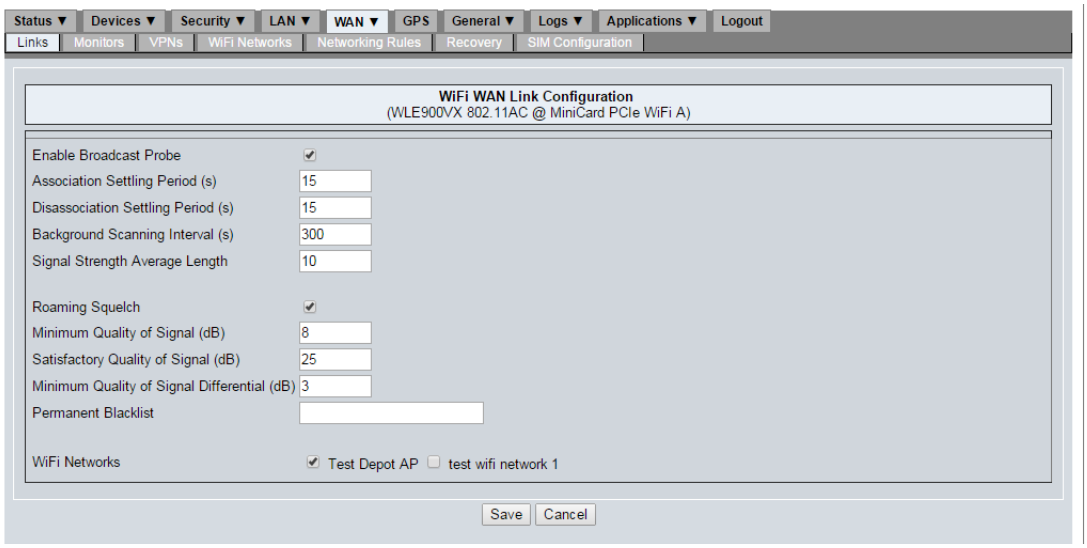

Figure 6-3: Wi-Fi WAN Link Configuration (LCI: WAN > Links > Configure)

Ethernet WAN Link Configuration

An Ethernet (wired) connection can also be used to provide WAN access to the MG90, though this is less common since the main purpose of the MG90 is to provide mobile WAN access using wireless methods.

In the Ethernet WAN Link Configuration screen (see Figure 6-4 below):

1. Configure the fields for the selected Ethernet device. For detailed field information, see Ethernet WAN Link Configuration on page 133.
2. Click Save.

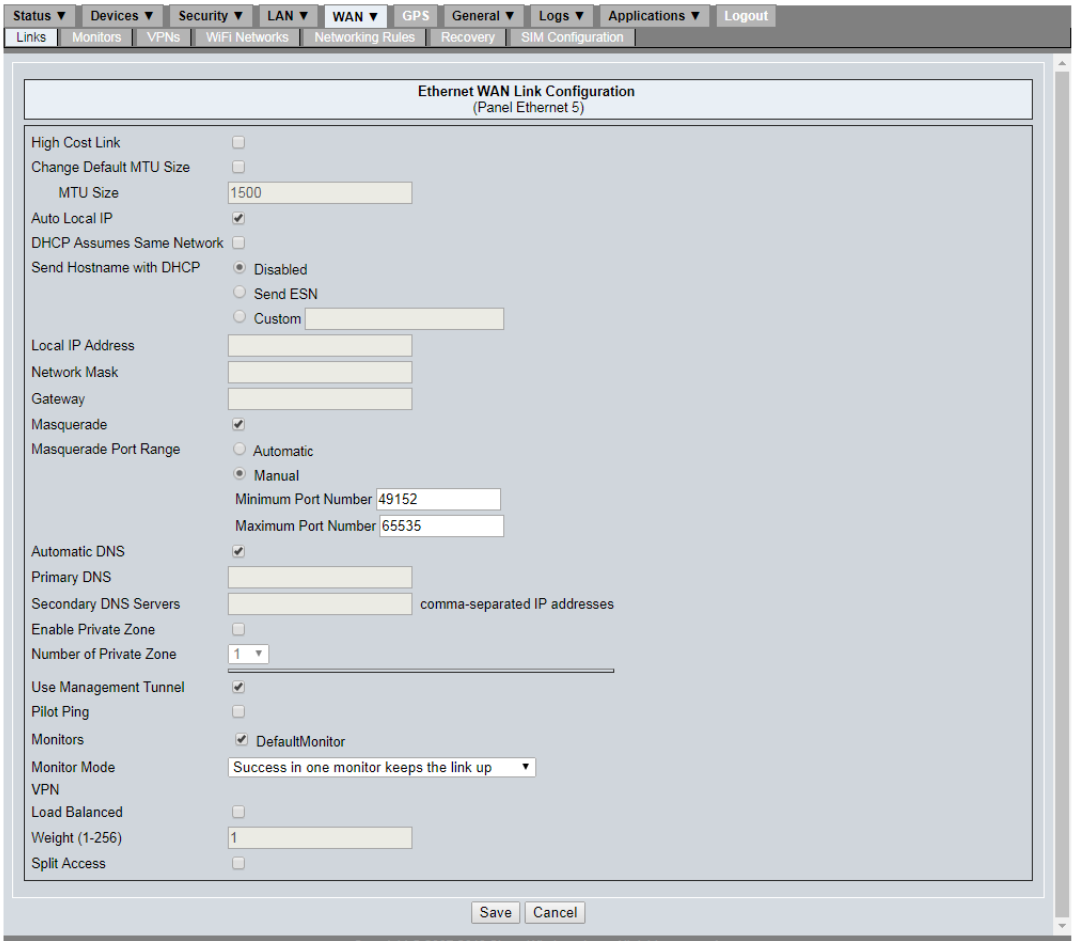

Figure 6-4: Ethernet WAN Link Configuration (LCI: WAN > Links > Configure)

Setting up PPPoE WAN

A StarTech USB2100 USB-Ethernet adapter can be connected to an available USB slot on the back panel of the MG90 to support a PPPoE WAN link to a connected LMR (Land Mobile Radio) such as a Motorola HPD radio.

Note: Only one adapter can be used.

To set up the MG90:

1. Power off the MG90.
2. Attach the StarTech USB2100 USB-Ethernet adapter to an available USB slot on the back panel.
3. Connect the Ethernet end of the adapter to the PPPoE server device (e.g. the Motorola HPD radio).
4. Power on the MG90.

The connected device will appear on the WAN Link Status screen (Status > WAN) with Status=UP and Type=Ethernet.

Serial WAN Link Configuration

The MG90's serial port can be used to connect a serial modem (Harris Land Mobile Radio) WAN device that has been set up as described in Configuring the Serial Port on page 21 and Configuring a Serial Modem Device on page 21.

The Serial WAN Link Configuration screen allows you to view and modify connection settings for the serial modem.

In the Serial WAN Link Configuration screen (see Figure 6-5 on page 36):

1. Configure the fields for the serial modem. See Serial (modem) WAN Link Configuration on page 146 for details.
2. Click Save.

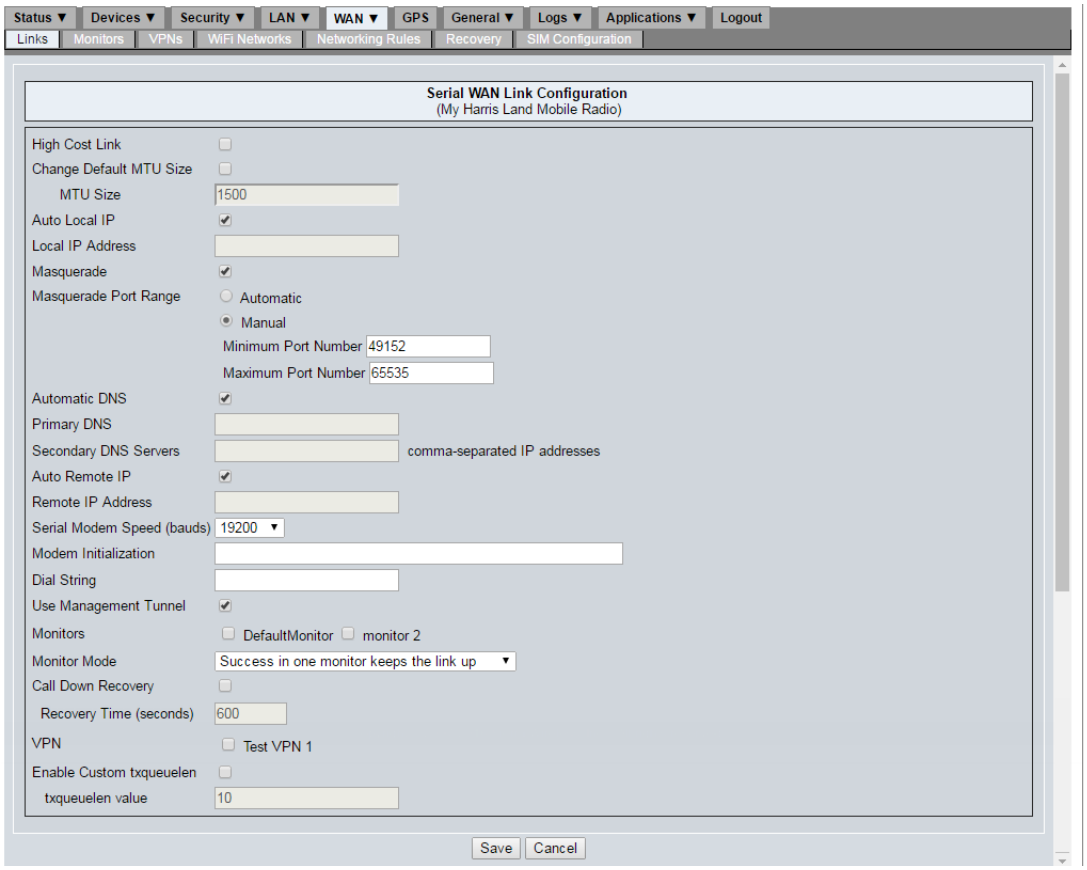

Figure 6-5: Serial WAN Link Configuration (LCI: WAN > Links > Configure)

Defining an Access Point Profile for Wi-Fi Links

Access Point (AP) profiles must be created for each Wi-Fi AP that the MG90 will use to access the WAN (for example, an AP at a depot). An AP profile contains the settings and credentials required for the MG90 to connect to the AP (for example, access, security, network settings, etc.). These settings must match the settings defined at the actual Wi-Fi AP.

To define and use an AP profile:

1. Define the AP profile:
   a. Go to WAN > Wi-Fi Networks.
   b. Click Add New Wi-Fi Network. The Wi-Fi Network Configuration screen appears.

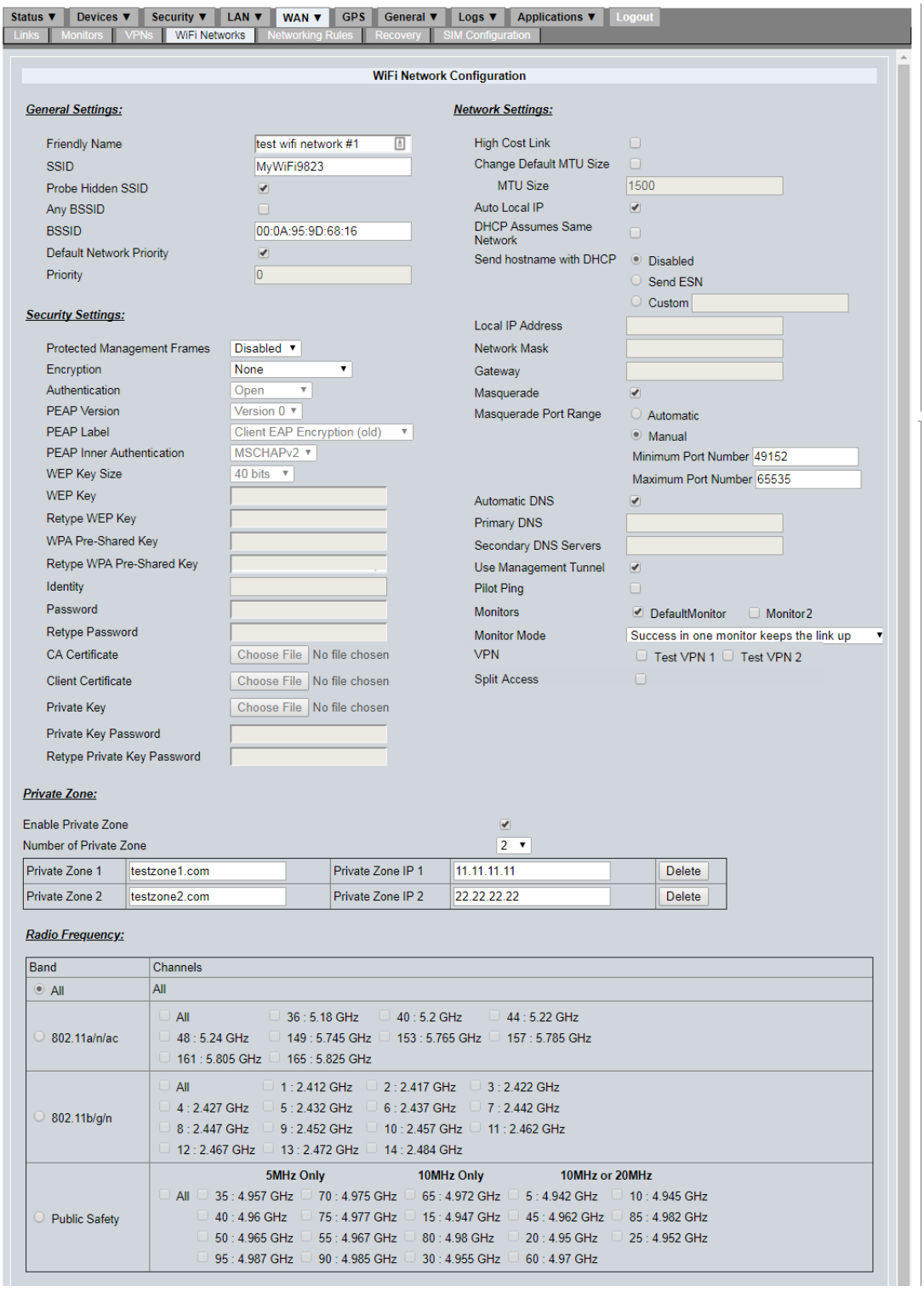

Figure 6-6: Wi-Fi Network (Access Point) Configuration

c. Configure the AP profile settings based on how they are configured in the actual AP itself. For detailed field information, see WAN > Wi-Fi Networks > Add New Wi-Fi Network/Configure Network on page 169.

d. Click Save.

2. Configure Wi-Fi links to use the AP profile:
   a. Go to WAN > Links.
   b. For each Wi-Fi link that will be able to connect to the AP:
      i. Click Configure in the Actions column for the link.
      ii. In the list beside the Wi-Fi Networks field, select the AP profile. (Note that a Wi-Fi link can have more than one AP profile selected.)

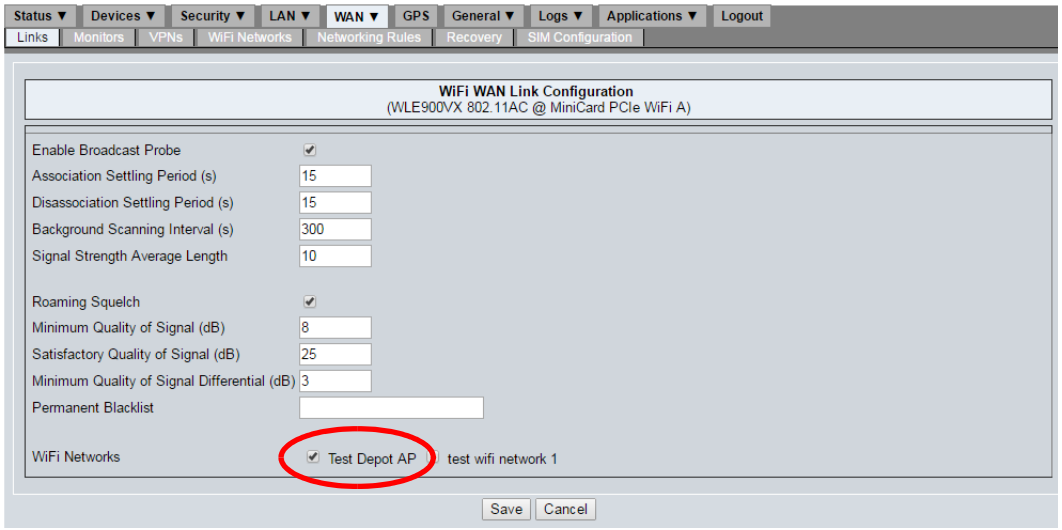

Figure 6-7: Selecting a Wi-Fi AP profile for a WI-Fi WAN Link

   iii. Click Save.

Note: If multiple Wi-Fi access points are defined, each access point is listed and available for selection in the Wi-Fi link's configuration settings.

Using Pilot Ping to Pre-test WAN Links

The MG90 can use a 'pilot ping' to determine if a WAN link (Cellular, Ethernet, or Wi-Fi) can pass traffic before the link is identified as established. If pilot ping is enabled and the link cannot pass traffic, it will not be identified as established.

Note: The pilot ping feature for each WAN link is disabled by default, and each link is configured separately.

To enable/disable the pilot ping feature for a Cellular or Ethernet WAN link:

1. Go to WAN > Links.
2. Click Configure in the Actions column for the link.
3. Select Pilot Ping to enable, or deselect to disable the feature. For detailed field information, see WAN Link Configuration (WAN > Links > Configure) on page 132.
4. Click Save.

To enable/disable the pilot ping feature for a Wi-Fi WAN link:

1. Go to WAN > Wi-Fi Networks.
2. Click Configure in the Actions column for the Wi-Fi network that the Wi-Fi WAN link uses.
3. Select Pilot Ping to enable, or deselect to disable the feature. For detailed field information, see WAN > Wi-Fi Networks > Add New Wi-Fi Network/Configure Network on page 169.
4. Click Save.

Using WAN Monitors to Detect Lost Connections

The MG90 can use 'monitors' to detect and try to recover from high-level communication failures occurring on a healthy connection between a WAN link and the carrier network. For example, when the MG90 is out of range of the carrier network but the connection is not dropped, the link cannot pass traffic.

A monitor accomplishes failure detection and recovery by periodically checking against its pre-configured parameters for conditions such as a minimum number of connection failures, timeouts, etc.

Tip: *Sierra Wireless strongly recommends that one or more monitors be created and configured for cellular devices.*

Note: Currently, the only supported monitoring method is ICMP ping monitoring.

Creating or modifying monitors

To create or modify a monitor:

1. Go to WAN > Monitors.
2. Click Add New WAN Monitor to create a new monitor, or click Configure in the Actions column to modify an existing monitor.
3. Modify the monitor settings as required to detect a connection that can no longer pass traffic, and ensure the correct Source Address is selected (Monitored Link IP for link monitoring, or the source LAN segment address for VPN monitoring).

   For detailed field information, see WAN > Monitors > Configure on page 157.
4. Click Save.

Enabling monitors on WAN links

To use monitors on a Cellular or Ethernet link, enable them in the link details:

1. Go to WAN > Links.
2. Click Configure in the Actions column for the link.
3. Select the desired monitor(s) in the Monitors list. (Note—More than one monitor can be selected.)
4. Click Save.

To use monitors on a Wi-Fi link, enable them in the Wi-Fi networks (AP profiles) selected in the link:

1. Check which Wi-Fi networks can be used by the Wi-Fi link:
   a. Go to WAN > Links.
   b. Click Configure in the Actions column for the link.

c. Make note of the Wi-Fi networks that are selected.

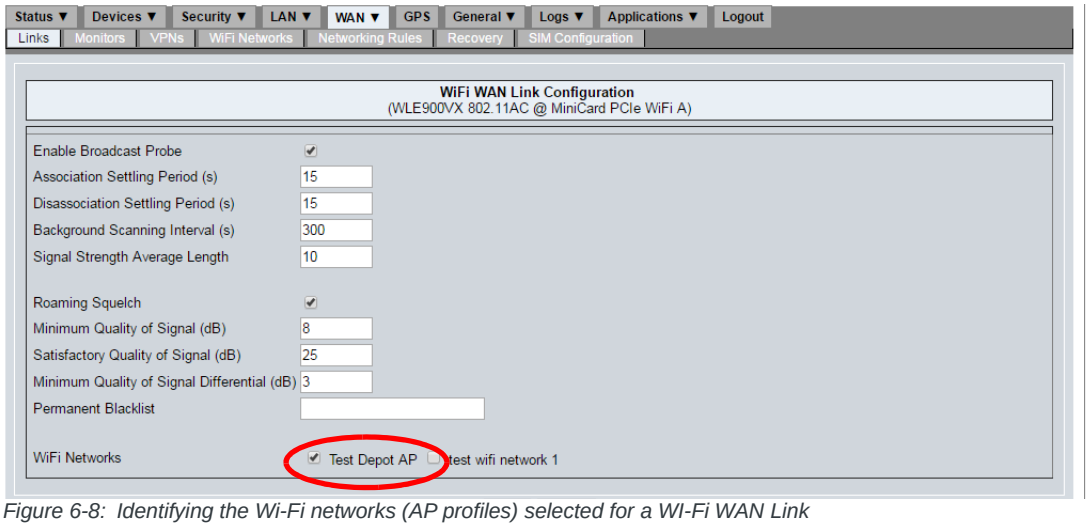

Figure 6-8: Identifying the Wi-Fi networks (AP profiles) selected for a WI-Fi WAN Link

2. Go to WAN > Wi-Fi Networks.

3. For each Wi-Fi network that will have monitors added:

a. Click Configure in the Actions column for the desired network.

b. In the Network Settings area, select the desired monitor(s) in the Monitors list. (Note—You can select more than one monitor.)

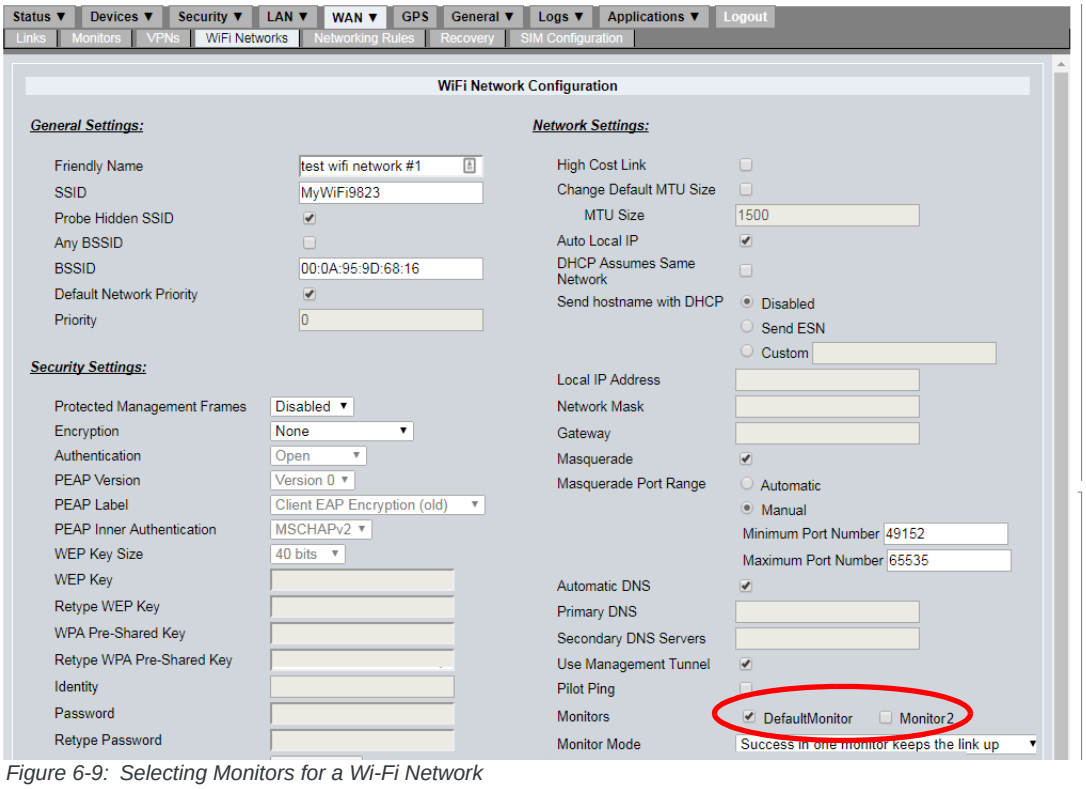

Figure 6-9: Selecting Monitors for a Wi-Fi Network

c. Click Save.

Deleting monitors

To delete a monitor:

1. Go to WAN > Monitors.
2. Click Delete in the Actions column for the monitor to delete.
3. Click OK when prompted to confirm the deletion.

Setting up WAN Link Policies

WAN Link policies are configurable rules that enable the MG90 to choose which WAN links to use at any given time to maintain optimal, cost-effective connectivity across a range of external conditions.

If you have more than one WAN link defined, you may want to define policies to determine which WAN link to use.

Policies determine which link should be used based on a scoring system where:

- Each link starts with a base score of 1000.
- Each link can be individually adjusted by using the Priority Score in the Dynamic Priority Policy screen.
- The link's score may be decreased by defined Penalty values when the link is down, the vehicle's velocity is too high, or the signal strength is too low.
- The link's score may adjusted by defined amounts when the MG90 is in a certain geographical area, or during specific time periods.
- Each link is evaluated based on its score and the link with the highest score is set to the active link.

Reasons for using link policies include:

- Reducing or eliminating loss of connectivity and associated downtime
- Reducing or eliminating issues associated losing and re-establishing connections, such as having to rebuild a VPN connection
- Maintaining a stable connection
- Maintaining the fastest throughput available
- Reducing cellular usage costs
- Using low-cost links, such as Wi-Fi

The MG90 supports the following link policy types, which you can combine and tune for optimal connectivity and performance:

- Dynamic priority policy—Provides managed switching between WAN links when a link in use goes down. For details, see Dynamic Priority Policy Overview on page 43.
- Geographic region policy—Defines coverage areas for a WAN link where the link would be the preferred connection device (areas where the device has a strong connection). For details, see Geographical Regions Policy Overview on page 46.
- Time period policy—Defines times of day when a WAN link should be used (for example, when bandwidth costs are lower, or when network congestion is typically light). For details, see Time Period Policy Overview on page 47.
- Velocity policy—Defines a maximum vehicle speed for a WAN link to be used (for example, to use a Wi-Fi WAN link only when at its depot, traveling in the yard at low speed). For details, see Velocity Policy Overview on page 47.
- Signal strength policy—Defines the minimum preferred signal strength for a WAN link (for example, to use a Wi-Fi link only when it has a strong enough signal). For details, see Signal Strength Policy Overview on page 48.

Defining WAN link policies

To define policies for a WAN link:

1. Go to WAN > Links.
2. Click Policies in the Actions column for the link.
3. Click Configure in the Actions column for a desired policy type.
4. Select Enable this policy.
5. Configure the policy settings. For detailed field information for each policy type, see WAN Link Policy Configuration (WAN> Links > Policies) on page 150.
6. Click Save.

   When the WAN Link Policy Configuration screen redisplays, you will see the policy's Enabled checkbox is selected.
7. Repeat for any additional policies that should be configured.

Note: Policy configurations are unique for each link, and must configured on a per link basis as required. For example, if you have Velocity policies on two Wi-Fi WAN links, they are configured separately, even if they are set up with identical details.

Special Considerations for Wi-Fi Links

When planning how policies will be used to select/deselect Wi-Fi links, remember to consider the Association Settling Period and Disassociation Settling Period values for each Wi-Fi link (see Wi-Fi WAN Link Configuration on page 143 for a description of these settings).

These settings prevent accidental selection and deselection of a Wi-Fi link which could occur when brief Wi-Fi connectivity is available (e.g. when driving past a depot's Wi-Fi hotspot).

Note: These settings are not available on cellular devices.

By default, these values default to 15 seconds, and will prevent a Wi-Fi link's status from changing from "DOWN" to "UP" (Association Settling Period) or "UP" to "DOWN" (Disassociation Settling Period). This makes the link unavailable for selection by a policy during the settling period time frame.

As a result, penalties and recovery periods of policies on Wi-Fi links can generally be set to 0, since the two settling periods already handle most situations where brief Wi-Fi connectivity is to be ignored.

Dynamic Priority Policy Overview

The Dynamic Priority Policy is intended for use when an MG90 has multiple WAN devices that can provide backup connections when the active link in use goes down.

The policy provides a managed switch between WAN links, where the next-best link is used until the link that went down reconnects and maintains a stable connection for a defined recovery period (long enough to prove that it is 'trustworthy'). This prevents the active link from switching back and forth to an unstable link (a link that quickly and repeatedly goes up and down).

The Dynamic Priority Policy Configuration screen includes two groups of settings:

- Priority score—When enabled, the Priority Score adjustment is added to the link's base score of 1000. Use this to indicate the relative priority of each WAN link. (Note that you can assign the same priority to more than one link if they are equally preferable.)

Important: *Although this setting appears on the configuration screen of the Dynamic Priority Policy, it is not specific to that policy and can be set and used with any policy.*

- Dynamic priority policy—If enabled, a link's score automatically decreases by the Link Down Penalty value when the link goes down (e.g. when it loses its connection). When the link comes back up, it 'proves' its stability over the Recovery Period during which the penalty is gradually reduced. By tuning the Penalty and Recovery Period values, you can ensure a link is only used when it has a stable connection.

  For example, if a link has a score of 1200 when it goes down and has a Link Down Penalty of 120:
  - The link's score immediately drops to 1080 (1200 - 120).
  - If the Recovery Period is:
    - 0 seconds—The link's score immediately returns to 1200 when the link comes back up.
    - 60 seconds—The link's score increases by 2 points per second when the link comes back up (120 point penalty / 60 seconds).

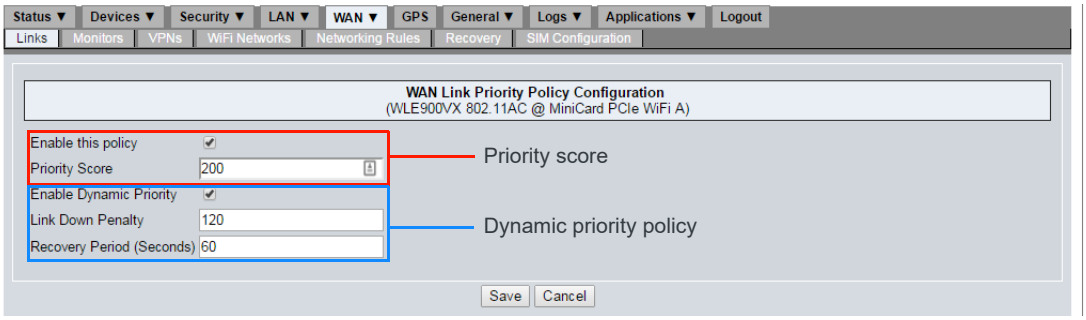

Figure 6-10: Dynamic Priority Policy—Example

Dynamic Priority Policy Example

In this example, a vehicle carries an MG90 that has three WAN links—two LTE radios (C1 and C2) and a Wi-Fi radio. The Wi-Fi radio is the most preferred device, followed by C1 and then C2. To model this in the Dynamic Priority policy the following settings were used:

Table 6-1: Example of Dynamic Priority Settings

	Wi-Fi	C1	C2
Base Score	1000	1000	1000
Priority Score	300	200	100
Link Down Penalty	Not Enabled	300	300
Recovery Period	Not Enabled	120	120

Figure 6-11 is a simple time line showing the dynamic priority policy affecting the WAN link scores:

- T_1— Vehicle is not near a depot; C1 (score=1200) is the current WAN link.
- T_2—C1 connection is lost. C1's score is re-calculated (1200 - Penalty(300) = 900). C2 has a higher score (1100), so C2 becomes the current WAN link.
- T_3—C1 re-establishes connection and begins its 120 second recover period, increasing its score by 300/120 points per second. C2 is still the current WAN link.
- T_4—C1 score has increased and is now higher than C2's score. C1 is restored as the current WAN link (and continues to increase its score while it is still in the recovery period).
- T_5—C1 score is now back to normal (1200).
- T_6—Vehicle enters the Wi-Fi zone of a depot. Wi-Fi has a higher score (1300), so Wi-Fi becomes the active link.

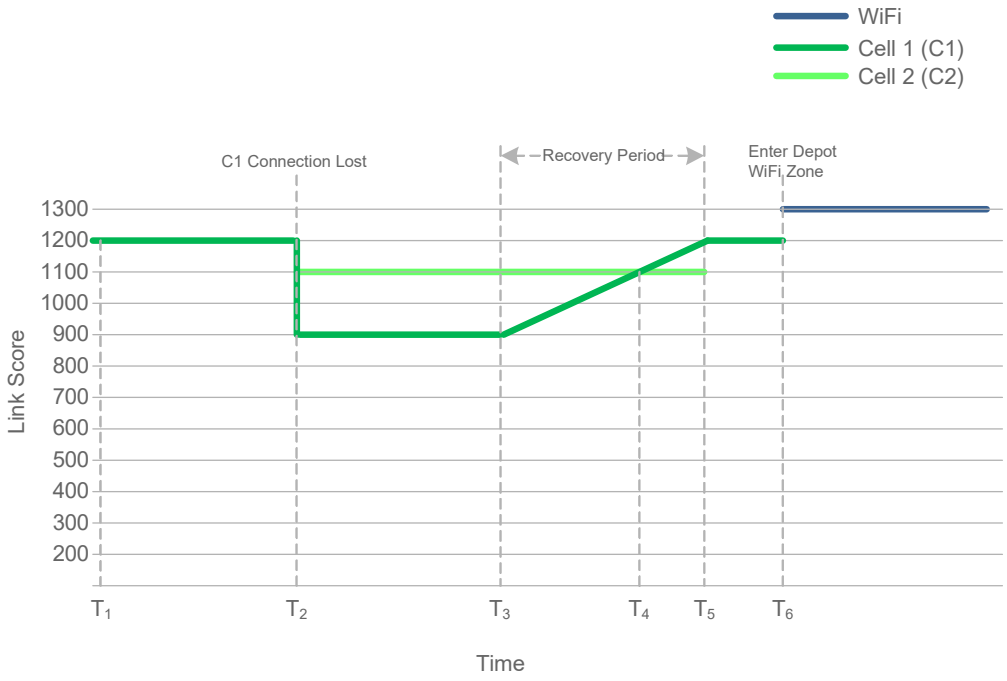

Figure 6-11: Dynamic Priority Timeline—Example

Note: Figure 6-11 provides a basic introduction to how policies use scoring to switch between links. In practice, other factors (such as a Wi-Fi device's Association Settling Period) mean that switches won't happen instantaneously.

Tip: *A priority score of 100 with a penalty of 300 and a 120 second recovery time, make for good, "granular" numbers to use because they make it easy to monitor switchovers (e.g. via logging) when using the Dynamic Priority policy. In particular, a 120 second recovery time allows for a ping monitor to occur every 30 seconds so that three pings occur during the recovery period.*

For detailed field information, see Table 17-7, WAN > Links > Policies > Configure (Dynamic) screen fields, on page 152.

Geographical Regions Policy Overview

The Geographical Regions Policy is used to increase a WAN link's score in up to three geographic areas (rectangular) to make it the preferred link in those areas.

This policy is often used when the quality and/or cost of coverage for particular areas is known and not likely to change.

For example:

- If the cellular coverage for different carriers is known to be good in certain areas, then regions for those areas can be defined on the respective WAN links and scores applied accordingly.
- If a Wi-Fi connection is available (e.g. in and around a depot), then a region for the depot could be defined for the Wi-Fi WAN link with a very high score to ensure the Wi-Fi WAN link is used when the vehicle is in or near the yard.

Geographical Regions Policy Example

In this example, a vehicle carries an MG90 with two cellular WAN links (LTE radios—C1 and C2) and operates in an area (Figure 6-12 on page 47) where:

- C1 has the best coverage in one region (Region 1)
- C2 has the best coverage in another region (Region 2)
- The coverage areas for C1 and C2 overlap. In the overlap area, C1 is preferred over C2.

To provide the best coverage and prevent unnecessary switchovers throughout the vehicle's journey, the following policy settings were used:

Table 6-2: Example of Geographical Regions Policy Settings

Cellular WAN Link	Dynamic Priority Policy	Geographic Region Policy
C1	Priority (Base) Score: 1200	Region 1 Score: 300 Region 2 Score: 0
C2	Priority (Base) Score: 1100	Region 1 Score: 100 Region 2 Score: 300

The overall score for a cellular link is then calculated as follows:

- Single region: Overall score = Priority Score + Score for current region
- Overlapping regions: Overall score = Priority Score + Score for first overlapped region + Score for second overlapped region + ...

For example, when the vehicle is in:

- Region 1:
  - C1 score = 1200 + 300 = 1500
  - C2 score = 1100 + 100 = 1200
  - C1 will be used (if available) when the vehicle is fully in Region 1.
- Region 2:
  - C1 score = 1200 + 0 = 1200
  - C2 score = 1100 + 300 = 1400
  - C2 will be used (if available) when the vehicle is fully in Region 2.

- Overlap (Region 1 and Region 2):
  - C1 score = 1200 + 300 + 0 = 1500
  - C2 score = 1100 + 100 + 300 = 1500
  - C1 and C2 are equally preferable. As shown in Figure 6-12, when the vehicle moves from one region into the overlapping zone, a switch between cellular links will not occur.

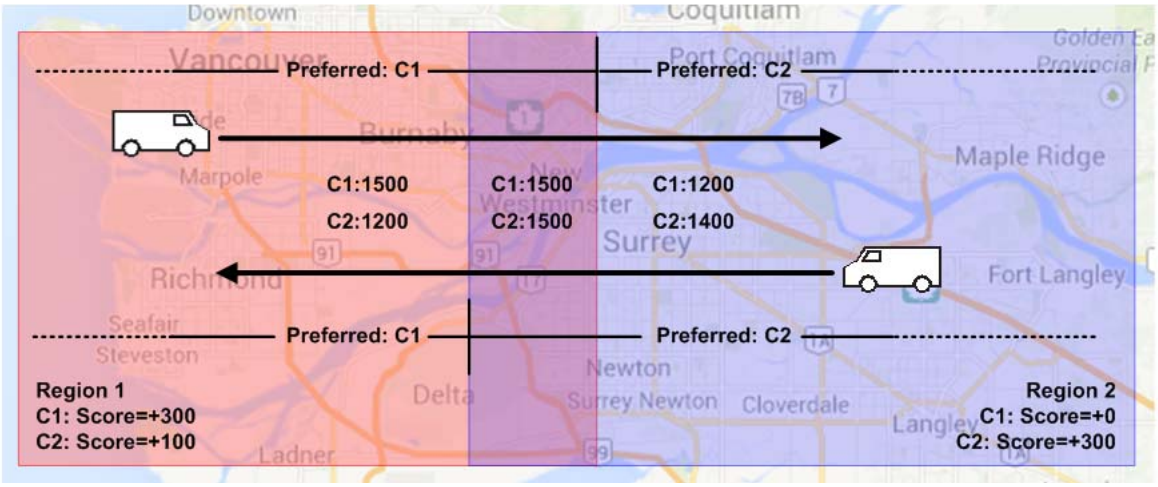

Figure 6-12: Geographical Regions Example with Overlapping Regions

Note: Region boundaries are defined using latitude and longitude coordinates. You must determine and manually enter these coordinates—the MG90's LCI does not provide a mapping interface to visually define zones.

For detailed field information, see Table 17-8, WAN > Links > Policies > Configure (Geographical) screen fields, on page 153.

Time Period Policy Overview

The Time Period Policy is used to increase a WAN link's score during defined time periods (up to three periods per link) to make it the preferred link during those periods.

This policy is typically used to take advantage of reduced data costs or to compensate for bandwidth saturation periods. For example:

- If a normally preferred WAN link's throughput is known to drop during a particular time of day (e.g. due to network congestion), define a time period policy with a high score on a different WAN link to temporarily use that link and maintain acceptable throughput.
- If a carrier provides cheaper cellular coverage during evenings, define a time period policy for that WAN link.

For detailed field information, see Table 17-9, WAN > Links > Policies > Configure (Time Period) screen fields, on page 154.

Velocity Policy Overview

The Velocity Policy is used to decrease a WAN link's score when the vehicle exceeds a maximum velocity.

This policy is typically used when a Wi-Fi WAN link is used at a depot that has Wi-Fi coverage in the depot area and in a small zone outside of the depot. When the vehicle travels inside the depot, it travels at low speed (for example, a maximum of 20 mph). When it leaves the depot and begins to pass out of the coverage zone, it increases its speed.

If a velocity policy is defined with an appropriate speed threshold, the current WAN link will switch seamlessly from the Wi-Fi link to (for example) a cellular WAN link without a drop in connection, preventing issues such as having to rebuild a VPN connection which would occur if the Wi-Fi link dropped without switching to the cellular link.

For example (as shown in Figure 6-13), a velocity policy could be set with a 20 mph threshold. When the vehicle leaves the depot and begins accelerating, it switches over to a cellular WAN link before it reaches the edge of the Wi-Fi coverage area.

If the vehicle re-enters the Wi-Fi coverage area at a speed lower than the maximum, the Wi-Fi WAN link 'proves' its stability over the Recovery Period during which the penalty is gradually reduced. By tuning the Penalty and Recovery Period values, you can ensure a link is only used when the vehicle appears to be staying in the coverage area (rather than simply passing through).

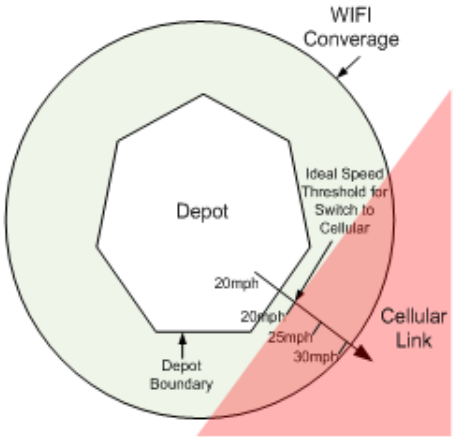

Figure 6-13: Setting a Speed Threshold to Switch to Cellular before Wi-Fi Coverage is lost

Note: GPS "jitter" can occur when the vehicle is parked or the GPS signal is weak (such as when indoors or in a covered area), which can cause the speed threshold(s) defined in the Velocity Policy to be satisfied, resulting in an inadvertent switch in links. Sierra Wireless recommends that a GPS repeater be installed near the depot to reduce GPS jitter.

For detailed field information, see Table 17-10, WAN > Links > Policies > Configure (Velocity) screen fields, on page 155.

Signal Strength Policy Overview

The Signal Strength Policy is used to decrease a cellular or Wi-Fi WAN link's score when the connection's signal strength falls below a minimum threshold, which makes other WAN links with stronger signals more preferable.

When the signal strength rises back above the threshold, it 'proves' its stability over the Recovery Period during which the penalty is gradually reduced. By tuning the Penalty and Recovery Period values, you can ensure the link has a strong and stable signal before switching back to it.

When setting the signal strength thresholds for the WAN links:

- If a specific WAN link is generally preferred (e.g. due to lower data plan costs), then the Signal Strength Policy for that link should indicate a lower threshold (lower quality) than the policies on the other links. This will help ensure that the preferred link is utilized the most as signal strengths between devices fluctuate.
- If multiple WAN links are equally preferable, the thresholds in the Signal Strength Policies for each link should be set the same. This will prevent unnecessary switchovers from occurring since both devices are designated as equally capable.

Important: *The default threshold of -85 dBm is typically sufficient to drop bad connections that may not cause ping monitor failures.*

For detailed field information, see Table 17-11, WAN > Links > Policies > Configure (Signal Strength) screen fields, on page 156.

Use Cases

Dynamic Priority Policy and Velocity Policy Combination

The following example shows how to combine the Dynamic Priority Policy with the Velocity Policy to choose between links.

In this example, an MG90 has two WAN links enabled—a Wi-Fi link and a cellular link. The user wants to use the Wi-Fi link whenever possible since the Wi-Fi link has superior performance, connection quality, and lower usage costs than the cellular link.

Table 6-3: Example Dynamic and Velocity Policy parameters

Policy	Field	Wi-Fi		Description
None (Basic score)		1000		Base score assigned to all links.
Priority Score		200		Wi-Fi is the preferred link, so a priority score is added to the base score.
Dynamic	Penalty	600		If the Wi-Fi link is lost, the link's score will drop below the Cellular link's score.
	Recovery Period	780 s		When the Wi-Fi link comes back up, it takes 780 seconds (13 minutes) for the penalty to be completely removed.
Velocity	Speed	25 mph		The depot has a 25 mph speed limit.
	Penalty	400		When the vehicle leaves the depot and increases its speed to the local speed limit (say, 30 mph), the Wi-Fi link score drops below the Cellular score and the Cellular link becomes active.
	Recover Period	240s		When the vehicle re-enters the depot area (and slows below 25 mph), it takes 240 seconds (4 minutes) for the penalty to be completely removed.

Figure 6-14 is a simple timeline showing how the MG90 uses this configuration to choose between its WAN links (Wi-Fi and cellular).

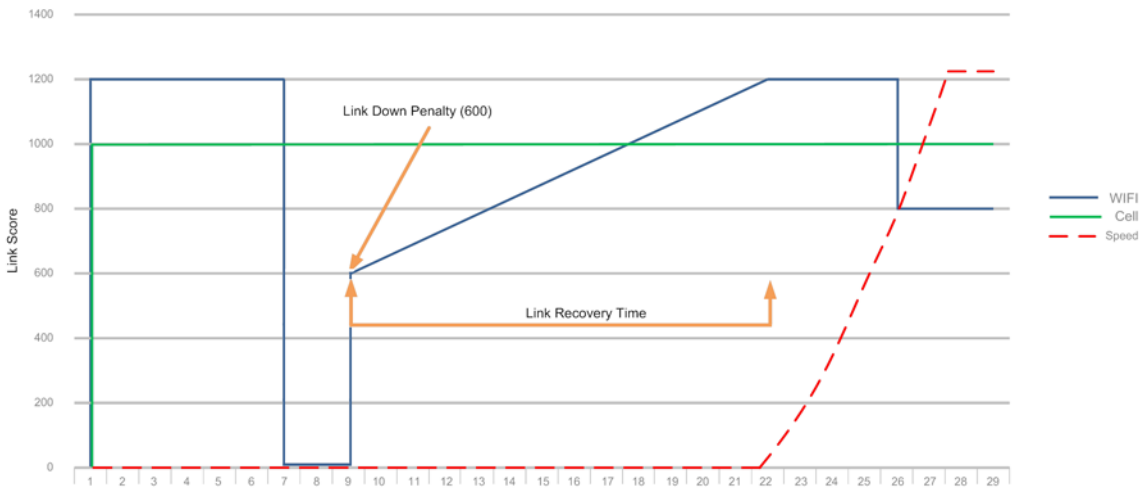

Figure 6-14: Dynamic Priority and Velocity Policy Combination

The following can be observed on this timeline:

- Wi-Fi starts with a higher score of 1200; cellular with 1000. The vehicle is stationary (speed is 0 mph).
- At 7 minutes, the Wi-Fi connection is lost and the cellular connection takes over.
- At 9 minutes, the Wi-Fi link recovers and the Dynamic Priority Policy sets its score to 600 (1200 - 600 penalty), which is lower than the cellular link's score (1000). The Wi-Fi link's score increases over its link recovery period at a rate of 0.77 points per second (600 point penalty recovered over 13 minutes).
- At 18 minutes:
  - The Wi-Fi link's score has recovered enough to exceed the cellular link's score, and the Wi-Fi link becomes the active link again.
  - At around the same time the vehicle starts to accelerate.
- At 26 minutes, the vehicle's speed exceeds the speed threshold defined in the Velocity Policy on the Wi-Fi link. The Wi-Fi link's score drops by 400 points (velocity penalty) causing the cellular link to take over.

Setting up the WAN Firewall

Configuring WAN Networking Rule Firewall Settings

WAN firewall settings are configured by creating WAN networking rules.

The MG90's WAN firewall can deny/allow access to incoming and outgoing traffic based on a source/destination IP address combination, using TCP, UDP, or both protocols. The firewall also supports port forwarding so services within the MG90's LAN may be accessible over the WAN.

Note: There are three 'levels' of networking rules—LAN segment, WAN link, and Global (LAN). If there is a conflict between any of these rules, LAN segment rules override WAN link and global rules, and WAN link rules override global rules.

Defining WAN Firewall Rules

To define WAN firewall rules:

1. Go to WAN > Networking Rules.
2. Select the rule type in the drop-down (Access Blocking, Access Granting, or Port Forwarding).
3. Click Add New Networking Rule.
4. Enter a descriptive name for the rule in the Rule Name field.
5. Select the traffic Direction affected by the rule.
6. Configure the remaining fields. For detailed field information for each rule type, see WAN > Networking Rules on page 179.
7. Click Save.

Note: You can combine Access Blocking and Access Granting rules to implement very specific access policies. Multiple rules of each type may also be created.

Deleting WAN Firewall Rules

To delete a WAN firewall rule:

1. Go to WAN > Networking Rules.
2. Click Delete in the Actions column for the desired rule.
3. Click OK when prompted to confirm the deletion.

WAN Link Recovery

The MG90 can be configured to reboot after WAN connectivity has been down for a specified amount of time.

To enable WAN recovery:

1. Go to WAN > Recovery.
2. Select WAN Link Recovery.
3. Configure each recovery setting as required. For detailed field information, see WAN > Recovery on page 185.
   - WAN Link Recovery—If enabled, forces the MG90 to reboot (after specified time) if WAN connectivity is lost.
   - Remote Configuration WAN Recovery—If enabled, restores the previous configuration (after specified time) when changes that were made remotely on an AMM caused a loss of WAN connectivity.
4. Click Save.

In addition to using the WAN recovery feature, the Pilot Ping option for Cellular, Ethernet, and Wi-Fi WAN link options can be used to determine if a WAN link can pass traffic before the link is identified as established, and ping Monitors can attempt to restart a failed WAN link. See field listings in WAN Link Configuration (WAN > Links > Configure) on page 132. (for Pilot Ping and Monitors), and Using WAN Monitors to Detect Lost Connections on page 40.

7: Setting up the LAN

The MG90 provides LAN access using two methods:

- Wired—Access via Ethernet ports 1–5. By default, ports 1–4 are configured for LAN, and port 5 is configured for WAN. To assign Ethernet ports for LAN use, see Configuring Ethernet Ports on page 20.
- Wireless—Access via Wi-Fi Access Points (AP). (Each Wi-Fi radio can be used as a unique access point.) To assign Wi-Fi devices for LAN use, see Configuring Wi-Fi Devices on page 20.

Note: The MG90 does not support USB-to-Ethernet adapters for LAN operation.

Before deploying the MG90, make sure to configure the LAN links with appropriate security and settings. The following topics describe typical setup requirements:

Ethernet LAN Link Configuration

Note: LAN configuration of each Ethernet port can be set regardless of its current use (WAN, LAN, IDLE).

To configure Ethernet ports for LAN access:

1. Go to LAN > Ethernet Links.

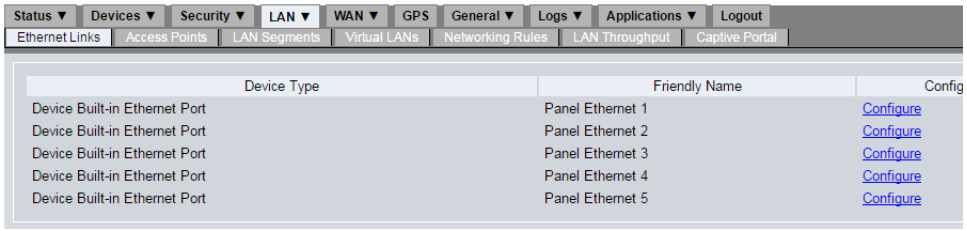

Figure 7-1: LCI: LAN > Ethernet Links

2. Enable (or disable) 802.1x network access control for a specific Ethernet port. (Note: If you disable network access control, any device that connects to the port can access the network.):
   a. Click Configure for the desired Ethernet port.
   b. Select Enable wired 802.1x network access control to display the configuration fields (or deselect the checkbox to disable network access control).
   c. Configure the 802.1x settings. For detailed field information, see LAN Ethernet Configuration (LAN > Ethernet Links > Configure) on page 103.

d. Click Save.

LAN Access Point Configuration

Note: LAN configuration of each Wi-Fi device can be set regardless of its current use (WAN, LAN, IDLE).

To configure LAN access points (maximum one AP for each Wi-Fi radio in the MG90):

1. Go to LAN > Access Points.
2. Click Configure in the Actions column for the desired device.
3. Configure the access point settings. For detailed field information, see Access Point Configuration (LAN > Access Points > Configure) on page 106.

Note: Each access point can be enabled/disabled as required. Disabling a configured access point does not affect the configuration options, it only prevents the access point from being used.

4. Click Save.

Configuring LAN Segments

LAN segmentation, and the process of adding LAN segments, is used for advanced networking scenarios when LAN traffic from different devices must be partitioned.

For example, LAN segmentation can be used when public Internet access is made available for Wi-Fi users while private onboard equipment connected to the MG90's Ethernet ports must not be accessible by Wi-Fi users. Multiple LAN segments are useful for specifying different network policies or routing rules on each segment.

By default, the MG90 is pre-configured with one LAN segment (“Default LAN”) on which all factory-enabled LAN links operate:

- Ethernet links—Can be assigned to one segment only
- Wi-Fi links—Can be assigned to multiple segments when configured with up to three additional BSSIDs. For example, a Wi-Fi link with one additional BSSID can be assigned to two segments.

Before deploying an MG90, it's important to review how the LAN segment(s) are configured on the unit to ensure that network traffic visibility remains as secure as possible.

Add/Configure LAN Segments

By default, the MG90 includes one LAN Segment—Default LAN, and all LAN-capable devices are assigned to that segment.

To add or configure LAN segments:

1. Go to LAN > LAN Segments.

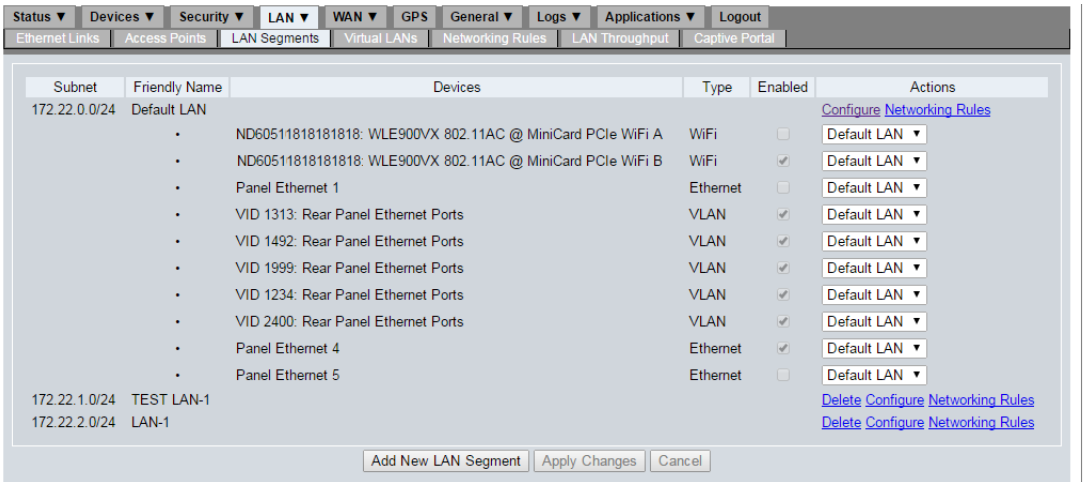

Figure 7-2: Configuring or adding a LAN segment

2. If you want to:
   - Add a new LAN segment—Click Add New LAN Segment.
   - Modify an existing LAN segment—Click Configure in the Actions column for the desired segment.
3. Configure the segment's settings. For detailed field information, see LAN Segment Configuration (LAN > LAN Segments > Configure) on page 116.

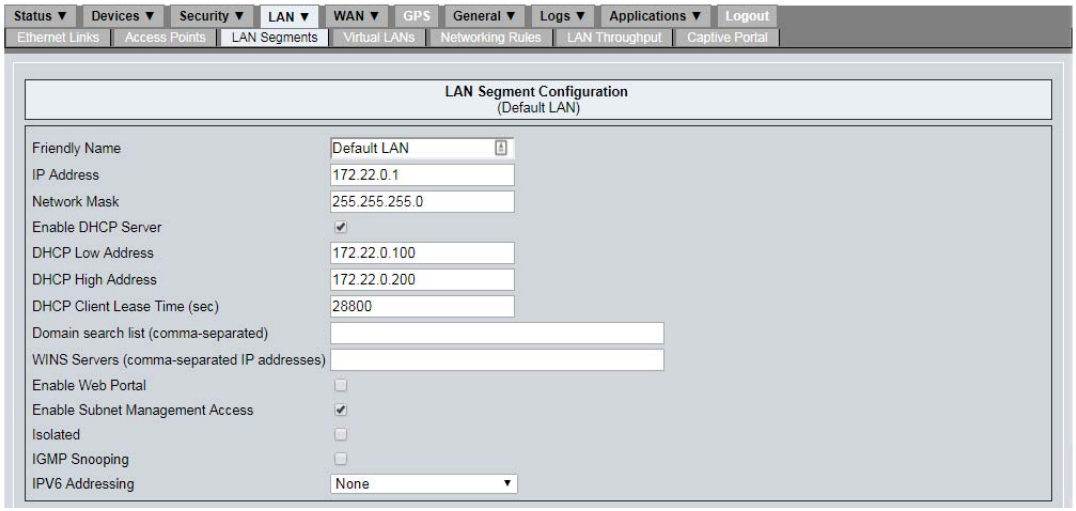

Figure 7-3: LAN segment configuration screen

4. Click Save.

Note: Each LAN segment must have a different scope (i.e. IP address range or network mask) from the other segments. A warning appears if an attempt is made to cross segment scopes, as shown in Figure 7-4:

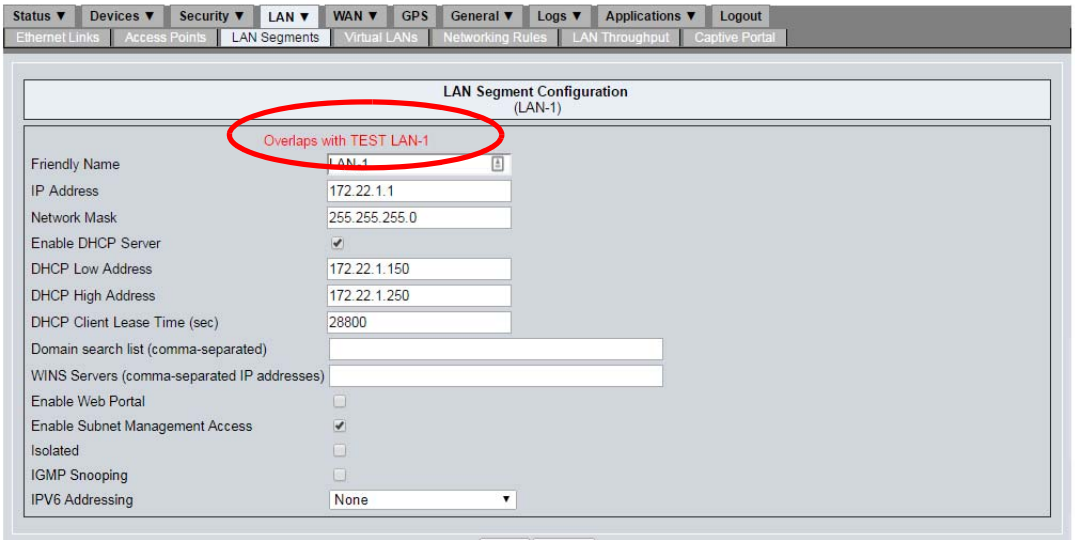

Figure 7-4: Warning for a segment configuration address range which overlaps another

Assign a Device to a Different LAN Segment

To assign a device to a different LAN segment:

1. Go to LAN > LAN Segments.
2. Locate the device you want to reassign, then select the desired LAN segment from the drop-down in the device's Actions.
3. Click Apply Changes. The screen will refresh and the device listing now appears in the LAN Segment you selected.

Delete a LAN Segment

If required, you can delete any of the LAN segments that you created (the Default LAN cannot be deleted). This can only be done if there are no devices on the segment (the Delete option will not appear on a segment that is in use).

To delete a LAN segment:

1. Go to LAN > LAN Segments.
2. Click Delete in the Actions column for the segment.
3. Click OK when prompted to confirm the deletion.

When a segment is deleted, the interface(s) that were assigned to it are reassigned to the Default LAN segment.

Configuring DHCP and Static IP Addresses

Each LAN segment can be configured to assign IP addresses to LAN devices using DHCP, or can utilize statically assigned IP addresses.

LAN segment default settings:

- Default LAN segment:
  - DHCP address range: 172.22.0.100–172.22.0.200
  - Router address: 172.22.0.1
- Default additional LAN segments:
  - DHCP address range: 172.22.*x*.100–172.22.*x*.200
  - Router address: 172.22.*x*.1
    The ‘x’ value increments from the previous segment. For example, the first additional segment would use ‘1’, the second would use ‘2’, etc.

Note: The settings noted above are default settings. These can be modified as necessary.

To configure the IP addresses for a LAN segment:

1. Go to LAN > LAN Segments.
2. Click Configure in the Actions column for the segment.
3. Set the desired address assignment method (DHCP or Static IP) as follows (for detailed field information, see LAN Segment Configuration (LAN > LAN Segments > Configure) on page 116):
   - To use DHCP:
     i. Select Enable DHCP Server.
     ii. Assign the DHCP address range and lease time in the DHCP Low Address, DHCP High Address, and DHCP Client Lease Time fields.
   - To use static IP addresses:
     i. De-select Enable DHCP Server.
     ii. Ensure each device on the segment has been configured with a unique static IP address (using the configuration tools available on each device).
4. Click Save.

Setting up the LAN Firewall

Configuring LAN Networking Rule Firewall Settings

LAN firewall settings are configured by creating LAN networking rules.

The MG90's LAN firewall can deny/allow access to incoming and outgoing traffic based on a source/destination IP address combination, using TCP, UDP, or both protocols.

Note: There are three ‘levels’ of networking rules—LAN segment, WAN link, and Global (LAN). If there is a conflict between any of these rules, LAN segment rules override WAN link and global rules, and WAN link rules override global rules.

Defining LAN Firewall Rules

To define LAN firewall rules on the MG90:

1. Go to LAN > Networking Rules.
2. Select the rule type in the drop-down (Access Blocking or Access Granting).
3. Click Add New Networking Rule.
4. Enter a descriptive name for the rule in the Rule Name field.
5. Select the traffic Direction affected by the rule.
6. Configure the remaining fields. For detailed field information for each rule type, see LAN > Networking Rules, and LAN > LAN Segments > Networking Rules on page 119.
7. Click Save.

Note: You can combine Access Blocking and Access Granting rules to implement very specific access policies. Multiple rules of each type may also be created.

Deleting LAN Firewall Rules

To delete a LAN firewall rule:

1. Go to LAN > Networking Rules.
2. Click Delete in the Actions column for the desired rule.
3. Click OK when prompted to confirm the deletion.

Setting up Virtual LANs

Virtual LANs (VLAN) can be used when devices inside the vehicle require VLAN tagging for their operation, or when the vehicle LAN has a switch with VLAN tagging enabled. If a vehicle has VLANs configured, or requires additional Ethernet ports, they can be added by using a switch and VLAN tagging.

For information on VLAN configuration settings, see VLAN Configuration (LAN > Virtual LANs) on page 118.

Setting up Captive Portals

The MG90 supports the use of Captive Portals to control access to specific Wi-Fi networks.

When a user connects to a captive portal to access a Wi-Fi network, they may have to identify themselves, agree to an acceptable use policy, and arrange payment for fee-based services if available (for example, paying for premium services (higher speeds, access to certain websites or content, etc.).

Captive portals can be managed either by external portal servers (providing the full range of captive portal functionality), or by the MG90 via its built-in ‘miniportal’ that provides a more limited range of features. Some features that captive portals can provide include:

- General access to free Wi-Fi without requiring user authorization
- Limiting access to authorized users (sign-in required)

- Per user directed marketing
- Per user quota management
- Traffic shaping/bandwidth throttling
- Fee based services
- Content filtering to block inappropriate content

Figure 7-5 on page 59 shows a basic overview of how the captive portal feature works, with references to settings in LAN > Captive Portal > Configure on page 127.

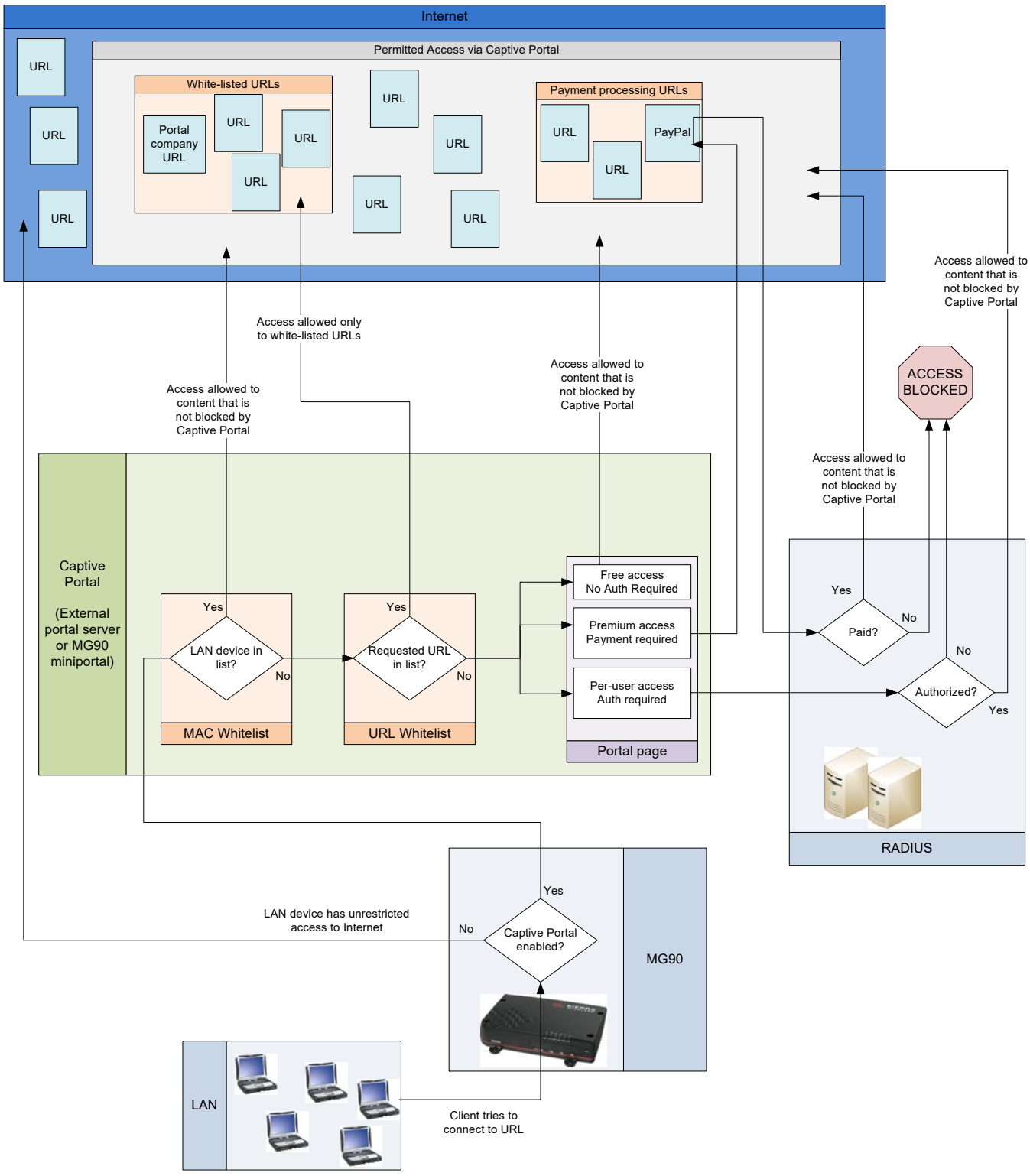

Figure 7-5: Captive Portal Overview

8: Performance Tuning

The MG90 includes features that can be used to customize ('tune') its performance characteristics. These features includes:

- Load balancing—Optimize traffic carried over multiple WAN links. See Configuring Load Balancing, below.
- Quality of Service—Define transmission performance requirements for traffic sent to the WAN and/or LAN. See Setting Quality of Service (QoS) on page 61.
- LAN throughput reporting—Track data usage via the AMM. See Configuring LAN Throughput Reporting Frequency on page 62.

Configuring Load Balancing

The MG90 includes a load balancing feature that controls the amount of traffic carried over multiple active WAN links.

To use load balancing to take advantage of higher bandwidth links, lower cost links, etc., enable the feature on at least two WAN links:

1. Go to WAN > Links.
2. For each link to be used for load balancing:
   a. Click Configure in the Actions column for the desired link.
   b. Select Load Balanced.
   c. Specify the Weight for the link. (See the Load balancing example below for details.)
   d. Click Save.

Note: When traffic is being carried on load-balanced links, any links that are UP, not active, and not load-balanced will not carry any traffic.

Load balancing example

When load balancing is used, the MG90 uses each link's weight to calculate the load (percentage of total traffic) it will carry.

For example, if two links (LinkA and LinkB) are configured for load balancing:

Assume: LinkA_weight = 50; LinkB_weight = 100

LinkA_load = LinkA_weight / (LinkA_weight + LinkB_weight) = 50 / 150 = 33%

LinkB_load = LinkB_weight / (LinkA_weight + LinkB_weight) = 100 / 150 = 67%

Therefore: LinkB will be used to handle twice as much traffic as LinkA.

Note: Load balancing is accomplished by randomly assigning TCP sessions or UDP packet streams to connected WAN links participating in the load balanced group. Therefore, load balancing is NOT link bonding (i.e. datagrams from a single session sent over multiple WAN connections).

Setting Quality of Service (QoS)

The MG90 supports Quality of Service policies (networking rules) for router traffic, to ensure minimum or maximum performance for specific applications or services. QoS policies can be created for:

- The entire WAN or individual WAN links, including VPN traffic (since QOS policies are applied to traffic queued for the WAN link before the traffic is encrypted)
- The entire LAN or individual LAN segments

QoS policies can be applied to traffic between the MG90 router and specified WAN or LAN entities. Depending on the connection type (WAN or LAN) and the source and destination addresses used, policies apply to incoming traffic (ingress), outgoing traffic (egress), or both directions.

Important: *If you create multiple QoS policies, ensure the settings in different policies don't conflict with each other.*

Defining QoS Policies

Defining WAN QoS policies

To define a WAN QoS policy:

1. Go to WAN > Networking Rules.
2. Select QoS Prioritizing in the drop-down and click Add New Networking Rule.
3. Enter a descriptive name in the Rule Name field.
4. Configure the fields. For detailed field information, see WAN > Networking Rules on page 179.
5. Click Save.

Defining WAN link QoS policies

To define a WAN Link QoS policy:

1. Go to WAN > Links.
2. Click Networking Rules in the Actions column for the link.
3. Select QoS Prioritizing in the drop-down and click Add New Networking Rule.
4. Enter a descriptive name in the Rule Name field.
5. Configure the fields. For detailed field information, see WAN > Networking Rules on page 179.
6. Click Save.

Defining LAN QoS policies

To define a LAN QoS policy:

1. Go to LAN > Networking Rules.
2. Select QoS Prioritizing in the drop-down and click Add New Networking Rule.
3. Enter a descriptive name in the Rule Name field.
4. Configure the fields. For detailed field information, see WAN > Networking Rules on page 179.
5. Click Save.

Defining LAN segment QoS policies

To define a LAN Segment QoS policy:

1. Go to LAN > LAN Segments.
2. Click Networking Rules in the Actions column for the segment.
3. Select QoS Prioritizing in the drop-down and click Add New Networking Rule.
4. Enter a descriptive name in the Rule Name field.
5. Configure the fields. For detailed field information, see WAN > Networking Rules on page 179.
6. Click Save.

Configuring LAN Throughput Reporting Frequency

If you have an AMM account through Sierra Wireless, or operate your own AMM server, the MG90 can automatically send LAN Throughput data (LAN traffic statistics) to the AMM for data usage reporting and device management.

The reporting frequency is based on LAN Throughput Configuration options:

- Threshold—Automatically send a report when this much data has been collected, as long as the Minimum Report Interval has elapsed.
- Minimum Report Interval—Wait at least this long between sending reports. even if the Threshold amount of data has been collected.
- Maximum Report Interval—Wait no longer than this between sending reports. Automatically send a report even if the Threshold amount of data has not been collected.

Note: Sierra Wireless recommends that you use the MG90's default interval and threshold values to maintain the optimum frequency for sending the LAN Throughput report.

To configure the reporting frequency:

1. Go to LAN > LAN Throughput.

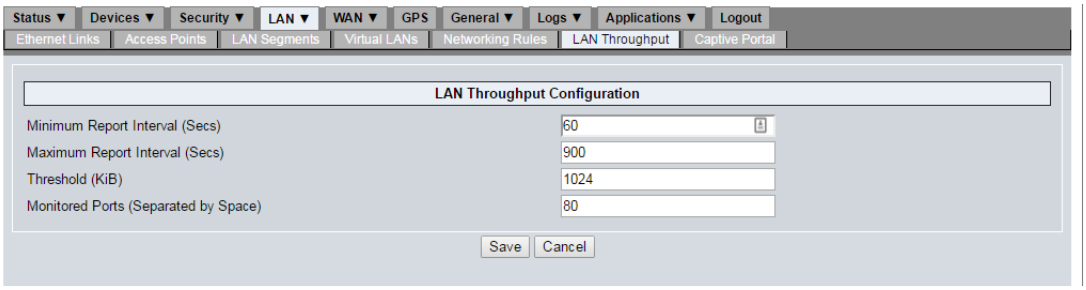

Figure 8-1: LAN Throughput Configuration

2. Configure the fields. For detailed field information, see LAN > LAN Throughput on page 125.
3. Click Save.

9: How to configure a VPN

The MG90 can be configured to provide access to one or more Virtual Private Networks (VPNs). A VPN allows LAN devices connected to the MG90 to access an enterprise network and vice-versa.

The MG90 supports the following VPNs and VPN related technologies:

- IPsec VPNs—LAN to LAN (most common) and Host to LAN.
  See source.sierrawireless.com for documentation on configuring IPsec VPNs for the MG90.
- Certificates and pre-shared keys

Note: A management tunnel VPN is provided for communication between the MG90 and AMM. This VPN can be configured as required, but cannot be deleted.

Details Required to Configure VPNs

A VPN is configured on the MG90 by creating a VPN profile with settings that match those of a VPN server.

Before you can configure a VPN, you need the following information:

- MG90
  - LAN IP Subnetwork
  - LAN Mask
  - LAN IP Address
  - Security components such as pre-shared key, certificates etc.

Note: Using pre-shared keys (PSK) for authentication on some VPN servers will require the MG90 to have a static IP on the WAN interface used for VPN.

- VPN Server
  - Server IP Address
  - Destination Network IP Address
  - Destination Network Mask
  - Security components such as pre-shared key, server certificates etc.

Configuring VPN Profiles

To configure a new VPN Profile:

1. Ensure one or more WAN links have been properly configured as described in Basic WAN Link Configuration on page 31.
2. Ensure one or more LAN segments have been configured as described in Configuring LAN Segments on page 53.

3. Go to WAN > VPNs.

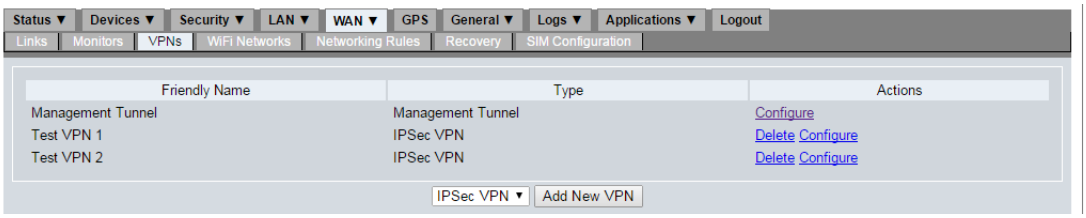

Figure 9-1: VPN Listing Screen

4. Click Add New VPN. (Note—The drop-down beside the button indicates IPsec VPN—This is the only option.)
5. Configure the VPN fields with the settings of the VPN server being used. For detailed field information, see IPSec VPN Configuration (WAN > VPNs > Add New VPN, and WAN > VPNs > (IPSec VPN) > Configure) on page 161.
6. Click Save.

Tip: *When first testing a VPN, Sierra Wireless recommends that monitors be temporarily disabled to test that all other configuration parameters are working properly.*

To update an existing VPN Profile:

1. Go to WAN > VPNs.

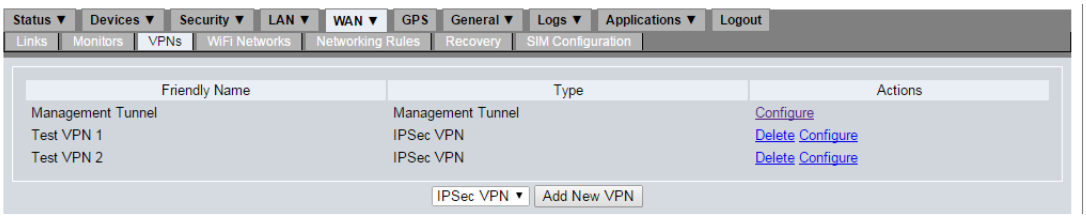

Figure 9-2: VPN Listing Screen

2. Click Configure in the Action column for the VPN profile to modify.
3. Configure the VPN fields with the settings of the VPN server being used. For detailed field information, see IPSec VPN Configuration (WAN > VPNs > Add New VPN, and WAN > VPNs > (IPSec VPN) > Configure) on page 161.
4. Click Save.
5. Reboot the MG90.

Important: *The MG90 must be rebooted after making changes to an existing VPN profile for the changes to take effect.*

Tip: *When first testing a VPN, Sierra Wireless recommends that monitors be temporarily disabled to test that all other configuration parameters are working properly.*

Setting Up Dead Peer Detection (DPD)

An MG90 VPN profile can be configured to send packets to a VPN server in an effort to detect dead connections. Doing so helps speed up reconnection to a VPN server.

To detect dead connections:

1. If the VPN uses:
   - IKEv1—Enable Dead Peer Detection (DPD) on the VPN configuration screen to detect when a VPN service is down.
   - IKEv2—If multiple WAN links are available, Sierra Wireless recommends:
     - Enable MOBIKE, which will automatically switch links when one goes down.

       and
     - Disable DPD because it can interfere with the fast switching provided by MOBIKE.

       MOBIKE has been tested by Sierra Wireless against Sierra Wireless' ACM VPN server. For more information on compatibility with VPN servers contact Sierra Wireless Technical Support for assistance (see Contact Information on page 3).
2. Sierra Wireless recommends that a monitor be configured to detect a dead connection to the VPN server and to attempt to reconnect to it. For information on creating a monitor, see Using WAN Monitors to Detect Lost Connections on page 40.
   a. Create the monitor with the following settings:
      - Host—Set to a host that can be reached only through the VPN
      - Source Address—Set to a LAN segment assigned to the VPN.
   b. In the VPN Configuration screen, assign the monitor to the VPN profile by selecting it in the Monitors field.

Multi-VPN Support

The MG90 supports the creation of multiple VPN tunnels per WAN link.

With this feature, you can apply one or more VPN policies. Select the desired policies in the VPN field, as shown in Figure 9-3. For:

- Cellular WAN links—Go to WAN>Links>Configure
- Ethernet WAN links—Go to WAN>Links>Configure
- Wi-Fi networks—Go to WAN>WiFi Networks>Configure

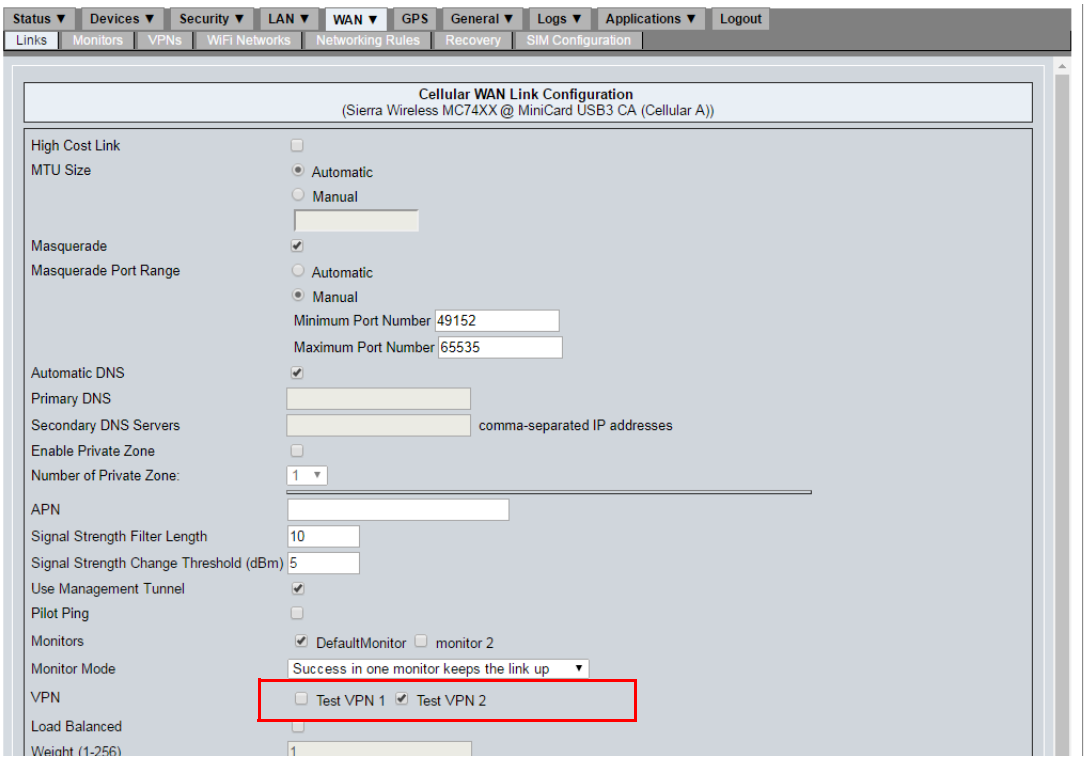

Figure 9-3: Selecting Multiple WAN Links

The multi-VPN feature has the following attributes and restrictions:

- Each WAN link/Wi-Fi network can have up to 10 VPNs.
- If a WAN link/Wi-Fi network has multiple VPNs:
  - All of the VPNs must be in HOST-to-LAN mode, or all must be in LAN-to-LAN mode.
  - All of the VPNs must use IKEv2. Do not use IKEv1 for any VPNs.
  - None of the VPNs can have both a local and remote subnet overlapping at the same time.
- Each VPN tunnel can have distinct ping monitors.
- The LCI validates the address spaces to ensure there is no collision between VPNs applied to the same WAN link.
- The MG90 controls bandwidth to ensure a single VPN does not consume all available bandwidth on a WAN link.

To view the VPNs that are assigned to a WAN link:

1. Go to Status > WAN.
2. Select Show Extended Status.

3. The VPN details appear in the link's IPsec VPN Info section:

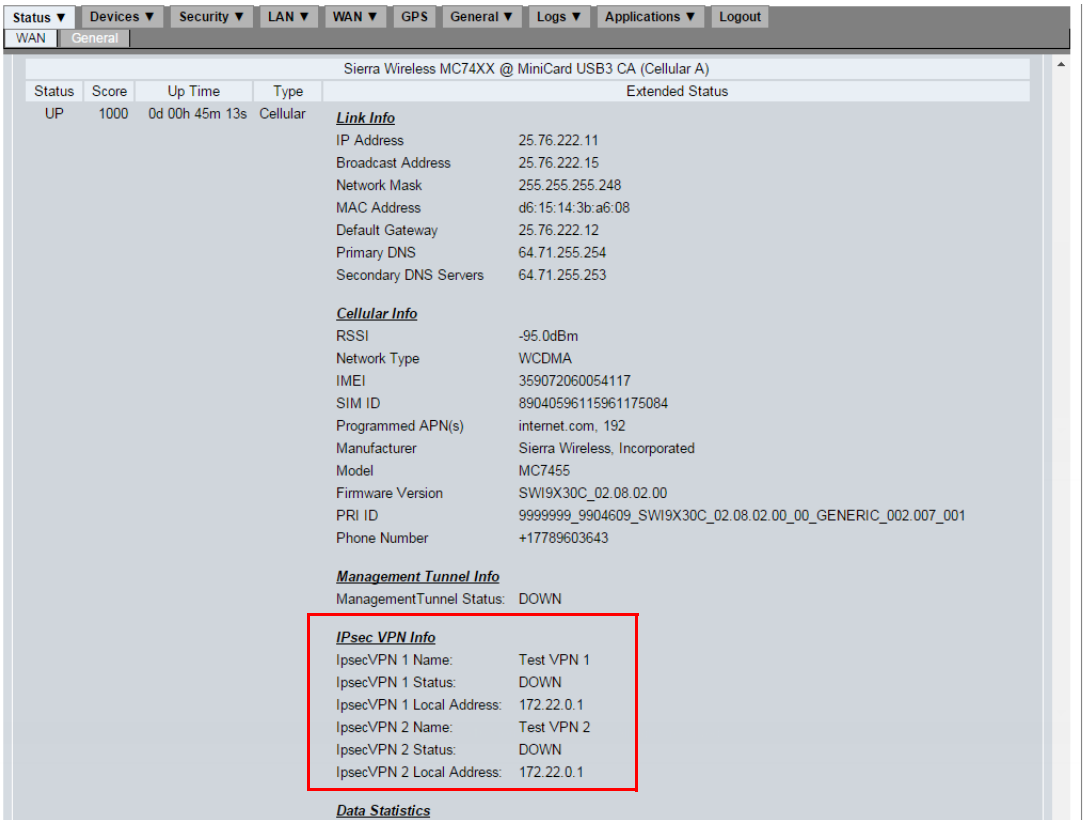

Figure 9-4: Viewing the VPNs assigned to a WAN Link

Configuring DNS Zones for Private DNS Server Use

In deployments that make use of VPNs with internal DNS servers (to resolve specific internal domains) and public DNS servers, the MG90 must be configured to use DNS zones.

Important: *The preferred method for configuring private DNS zones (LCI WAN Link Private Zone Configuration) is via WAN interface configuration in the LCI for Ethernet, Cellular, and Wi-Fi networks. The legacy method (Manual Private Zone Configuration) should not be used to configure new private DNS zones.*

Note: Private zones created in the Link Configuration screens are independent of the zones defined by the legacy method.

LCI WAN Link Private Zone Configuration

In the Ethernet or Cellular WAN Link Configuration screens, use the Private Zone fields to define up to 10 private zones.

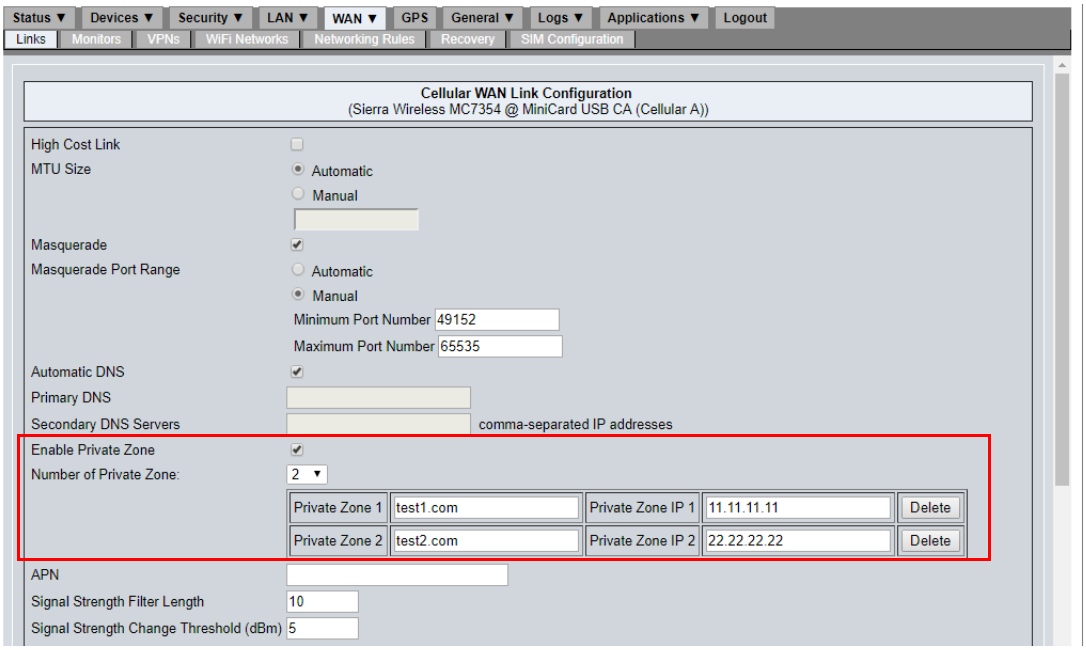

Figure 9-5: Private Zone Configuration

To configure up to ten private DNS zones for an Ethernet or Cellular WAN Link, or Wi-Fi Network:

1. In the LCI, go to WAN > Links or WAN > WiFi Networks and click Configure for the Ethernet link, Cellular link, or Wi-Fi network that will have private zones configured.
2. Select Enable Private Zone.
3. Select the Number of Private Zones to configure. A table of private zone fields will appear.
4. For each private zone being configured:
   - In Private Zone <#>, enter the domain name to be resolved by the internal DNS server.
   - In Private Zone IP <#>, enter the address of the internal DNS server.
5. Click Save.

To stop using private zones for a link or Wi-Fi network:

1. Deselect Enable Private Zone. The list of private zones is not deleted, and will re-appear if private zones are re-enabled.
2. Click Save.

To delete private zones:

1. Click Delete beside each zone to delete. The entry clears on-screen.
2. Click Save.

Manual Private Zone Configuration

The private zone configuration method described in this section is being replaced by the LCI WAN Link Private Zone Configuration. Installations that have not used this method must use the LCI.

Note: Installations that have already used this method can continue to use it, as well as the preferred LCI method above.

To configure one or more MG90s for DNS zones:

1. In the LCI, set the Primary DNS and Secondary DNS Servers fields to the addresses of the public DNS servers to be used. (Applies to the WAN > Links configuration screens (Ethernet, Cellular) and WAN > Wi-Fi Networks configuration screen.)
2. Using a plain-text editor, create a DNS zones file named “private-zone.conf”. In this file, indicate the domains to be resolved by the indicated internal DNS servers.

   For example (filename: private-zone.conf):

   ```
   zone “customer.local” IN {
                type forward;
                forward only
                forwarders { 10.5.1.1; 10.6.1.1; };
   };
   zone “customer.internal” IN {
                type forward;
                forward only;
                forwarders { 10.5.1.1; 10.6.1.1; };
   ];
   ```

   In this example, the domains “customer.local” and “customer.internal” are both to be resolved by the internal DNS servers “10.5.1.1” or “10.6.1.1”. Any other domains will be resolved by the public DNS servers specified in the WAN Link’s Primary DNS and Secondary DNS Servers fields.
3. Use AMM to store the file on the MG90(s):
   a. In AMM, select Config > Deploy F> Upload to copy the file to the AMM.
   b. Select Config > Deploy > Deploy to store the file on selected MG90s.

Note: Refer to the AMM Operation and Configuration Guide for details or contact Sierra Wireless Technical Support for assistance (see Contact Information on page 3).

10: Setting up GPS connectivity

The MG90 provides GPS connectivity via the following devices types:

- Internal GPS receiver—Pre-equipped. This is the default GPS device.
- External GPS device—Optional device connected via a serial or USB connection, or through Ethernet (using the UDP protocol).

The GPS location data can be:

- Reported to an AMM and the customer‘s mapping system.
- Forwarded over the WAN to additional servers with a static IP address or host name.
- Forwarded over the LAN to a local host.
- Forwarded to a device connected to the MG90‘s serial port.

Note: If an external GPS source is used, only the TAIP LN message can be forwarded. If the internal GPS is used, any TAIP or NMEA message can be forwarded either locally or remotely.

The MG90 also supports Dead Reckoning, which is a feature that uses the MG90's built-in inertial sensors to provide location reporting. Dead Reckoning operates alongside satellite (GNSS) navigation, and maintains location tracking capability when a GNSS signal is impaired or temporarily unavailable.

The MG90 uses its last known GNSS position along with sensor input to calculate vehicle position. For example, when the vehicle enters a tunnel, parking garage, or urban canyon, Dead Reckoning data augments data from the weakened GNSS signal and helps maintain accurate location reporting.

Dead Reckoning can operate just using the MG90's integrated sensors, or with speed input (if available) from an OBD-II or HDOBD connection.

GPS Configuration Set Up

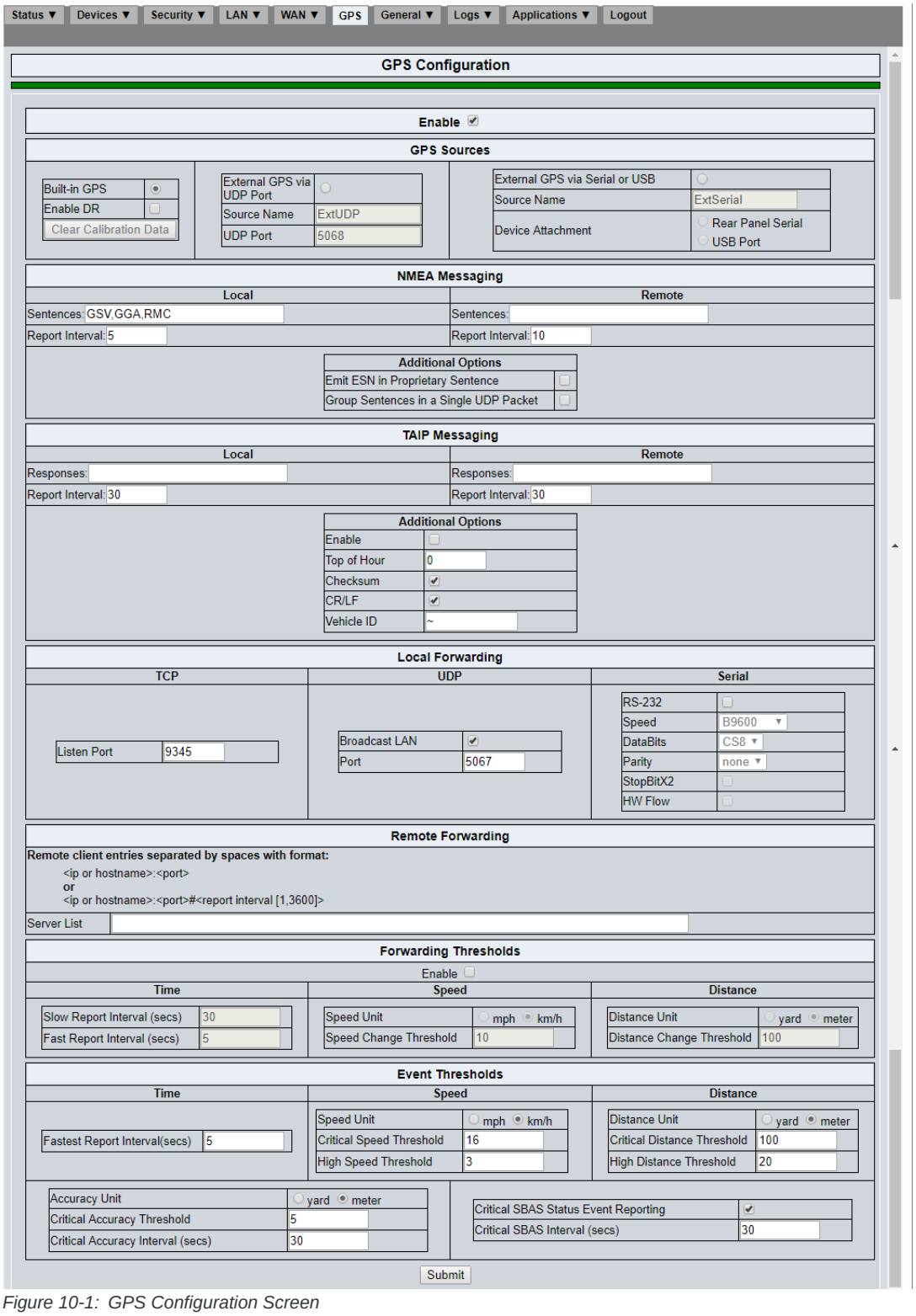

Figure 10-1: GPS Configuration Screen

For detailed field information, see Table 18-1, GPS screen fields, on page 189.

To configure the GPS settings:

1. Go to the GPS tab.
2. Select Enable.
3. In the GPS Sources section, select the GPS source:
   - Built-in GPS
   - External GPS via UDP port (through WAN)
   - External GPS via Serial or USB
4. Optionally, if Built-in GPS is selected, Dead Reckoning can be enabled. To use the Dead Reckoning feature, follow Configuring Dead Reckoning on page 73.
5. Configure the NMEA Messaging and TAIP Messaging if required.

   If using TAIP Messaging, ensure the Enable checkbox under Additional Options is selected.
6. Configure the Local Forwarding options as required:
   - TCP/UDP—Allows data to be sent to the LAN using the respective protocol.
   - Serial—Allows data to be sent to a device connected to the MG90's serial port. (The MG90's serial port settings must match those of the receiving system.)
     Note that Serial forwarding requires that the Serial port "Use" value be set to Application in the Devices > Serial tab.
7. Configure the Remote Forwarding options if required—Enter a space-separated list of IP addresses or host names to send the GPS data to.
8. Configure the Forwarding Thresholds options if NMEA/TAIP messages should be forwarded at variable intervals dependent on vehicle speed, distance traveled, and time elapsed.
   - To use variable interval reporting:
     - Select Enable. (The Report Interval fields in NMEA Messaging and TAIP Messaging will turn gray and not be considered.)
     - Set the maximum (Slow Report Interval) and minimum (Fast Report Interval) times between reports, regardless of speed and distance thresholds.
     - Set the speed threshold (change in speed since last report) that causes report to be forwarded.

       For example:
       - If Fast Report Interval is 5 and the last report was sent >= 5 seconds ago, and
       - If Speed Change Threshold is 10.50 mph and the speed at the last report was 40.0 mph,
       - Then a report is immediately forwarded if the vehicle's speed drops to 29.50 mph or rises to 50.50 mph.
     - Set the distance threshold (change in position since last report) that causes report to be forwarded.

       For example:
       - If Fast Report Interval is 5 and the last report was sent >= 5 seconds ago, and
       - If Distance Change Threshold is 100.25 meters,
       - Then a report is immediately forwarded if the vehicle's location changes (since the last report) in any direction by 100.25 meters.
   - To use fixed interval reporting, deselect Enable, and use the Report Interval values in the TAIP Messaging Local and Remote sections.
9. Configure the Event Thresholds, which control how frequently GPS information will be broadcast to the AMM.
10. Click Submit.

Configuring Dead Reckoning

To configure the MG90 to use Dead Reckoning (DR):

1. In the GPS Configuration screen, select Enable DR.
2. Click Submit.
   The Clear Calibration Data button becomes available.
3. Move the vehicle into an area with open sky to get a clear GPS fix.
4. Click Clear Calibration Data to clear old calibration information (if previously calibrated) and begin recalibrating.

Note: When Dead Reckoning is enabled, the initial calibration process begins automatically as soon as the vehicle is in motion with a GNSS antenna attached.

5. The calibration process can take anywhere from 5 to 30 minutes once the vehicle is in motion, depending on driving conditions. The Status > General screen will show the GPS DR Calibration Status as “In progress” once the calibration begins.

   To shorten the calibration time, ‘exercise’ the sensors by performing multiple stops, starts, turns, and acceleration/deceleration on straight stretches.

   For optimal calibration:
   - Drive the vehicle in open sky conditions
   - Undergo several turns
   - Stop and start the vehicle several times in a straight line (braking for, and accelerating away from stop signs, for example)
6. When calibration is finished, the GPS DR Calibration Status on the Status > General page changes to “Complete”, and the MG90’s GNSS LED will reflect the current DR state.

Table 10-1: GNSS LED DR State Indication

Color	State
Solid Green	Satellite fix is available, and Dead Reckoning is inactive (disabled, or not calibrated)
Solid Blue	Satellite fix available, and Dead Reckoning is active
Flashing Blue	No satellite fix is available, and Dead Reckoning is active
Flashing Amber	No satellite fix is available, and Dead Reckoning is inactive (disabled, or not calibrated)
Off	GNSS is off or antenna is not attached.

11: Applications

Several value added applications are available for the MG90 that enhance and extend the MG90's capabilities.

See Applications Tab on page 209.

12: Updating the System

The MG90 can be updated by downloading software and firmware updates over the WAN either automatically or by having Sierra Wireless manually "push" the update to the unit.

Configuring Auto Software Updates

The MG90 can be configured to check for and download updates over a WAN link, including:

- Software updates for the MG90—See Installing Software Updates on page 76.
- Firmware updates for cellular modules—See Module Firmware Images on page 77.

To configure automatic software update download and installation:

1. Go to General > Auto Software Updates.

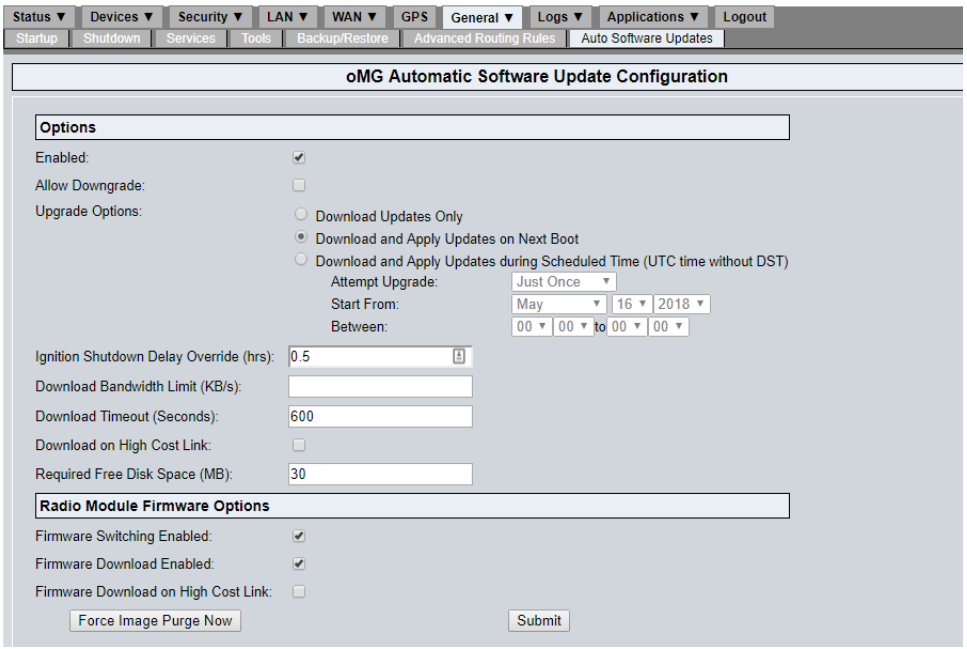

Figure 12-1: Accessing configuration options for Automatic Software Updates

2. In the Options section:
   a. Select Enabled to enable automatic updates, or deselect to disable.
   b. Configure the remaining fields (see Table 19-8 on page 204 for detailed information):
      - Set the appropriate Upgrade Options to schedule update installations. See Installing Software Updates on page 76 for details.
      - Set the remaining Options to control download behavior.

Note: By default, Download on High Cost Link is not selected, so software downloads occur on low cost links only. If you select this option, firmware downloads can also occur over high cost links.

3. Click Submit.

Installing Software Updates

Software updates are released periodically by Sierra Wireless to an on-line repository, for download and installation by MG90 devices.

If Auto Software Updates are:

- Enabled—The MG90 checks the repository for available downloads each time it boots or when settings are changed in the General > Auto Software Updates tab.
- Disabled—Updates can be manually downloaded by using the “download-new-software-updates” tool (see Over the Air Updates on page 81 for details).

After updates have been downloaded to the MG90, they are installed based on the selected Upgrade Options:

- Download Updates Only—Updates are not automatically installed. To install any stored updates, select one of the other Upgrade Options. The updates will be installed as described for those options.
- Download and Apply Updates on Next Boot—(Default option) Updates install automatically when the MG90 boots.
- Download and Apply Updates during Scheduled Time—Updates install automatically during a scheduled time slot (‘Between’), based on the selected Attempt Upgrade option:
  - Just Once—Installation attempt occurs only during the scheduled date and time slot (‘Between’).
  - Every Day—Installation attempts can occur every day, beginning on the Start From date.
  - Every Week—Installation attempts can occur once per week, beginning on the Start From date.
  - Every Month—Installation attempts can occur once per month, beginning on the Start From date. If the Start From date is the last day of the month (e.g. 30 June), then attempts occur on the last day of each month (e.g. 31 January, 28 February, 31 March, 30 April, etc.)

Important: *For MG90s that contain two different Sierra Wireless radio modules (e.g. MC7354+MC7455, MC7455+EM7511, etc.), make sure a SIM card is installed for at least one of the radio modules prior to an OTA firmware update. Otherwise, if firmware is downloaded OTA, the MG90 will not install the downloaded firmware, and will continue running its current version. In this case, to complete the upgrade:*

• Install new firmware using a USB stick,

or

• Insert a SIM for one or both modules, select and run General > Tools > “clean-local-software-update-cache”, and then reboot.

Note: In cases where the MG90 is never shut off (i.e. when a vehicle is in operation 24 hours per day, 7 days per week), use the ‘Scheduled Time’ upgrade option to install updates.

While an update is installing, the MG90’s LEDs display an amber ‘chase’ pattern (LEDs blink in sequence from left to right). For more information on LED patterns, see LEDs on page 216.

Important: *Do not remove the MG90's power while the LED chase is occurring.*

Note: Boot time increases by 5–6 minutes while installation is in progress.

Module Firmware Images

The MG90 ships with the following firmware images for its MC7354/MC74XX/EM75XX cellular module(s):

- Mobile network provider-specific—Images for certain mobile network providers (for example, in the U.S., AT&T, Verizon, and Sprint)
- Generic—Generic image for other mobile network providers (e.g. T-Mobile, US Cellular, Bell, Telus, Rogers, etc.). The modules are factory-configured with this image.

Updated image files are released by Sierra Wireless to an on-line repository. If enabled, the MG90 checks this repository periodically to see if a newer version of the current firmware is available and downloads it for automatic installation the next time the MG90 boots. See Automatic Firmware Downloads on page 77 for details.

When the MG90 boots, it checks whether the correct firmware is being used for the installed SIMs (Cellular A uses SIM slots A1 (default) and A2, and Cellular B uses SIM slots B1 (default) and B2). If a SIM requires a different firmware than the current image, the MG90 will, if enabled, install the correct image. See Firmware Image Switching on page 78 for details. While the new firmware image is installing on the modem, the MG90's LEDs display a green 'chase' pattern (each LED will blink in sequence from left to right).

Note: The boot time will increase by 5–6 minutes while the installation is in progress.

Important: *Do not remove the MG90's power while the LED chase is occurring.*

Important: *Do not replace SIMs while the MG90 is powered on. Power off the MG90, replace the SIM(s), then power on.*

Automatic Firmware Downloads

When the MG90 is running, it can periodically check the on-line repository for newer versions of the current firmware on the installed cellular module(s). If a newer version is available, it downloads automatically and will be installed the next time the MG90 boots.

To enable automatic firmware downloads:

1. Go to General > Auto Software Updates.
2. Select Firmware Download Enabled.
3. By default, Firmware Download on High Cost Link is not selected, so firmware downloads occur on low cost links only. If you select this option, firmware downloads can also occur over high cost links.
4. Click Submit.

Firmware Image Switching

When the MG90 boots, the current firmware images on the installed cellular modules are compared with the associated SIMs' mobile network providers. If different images are required (e.g. an AT&T SIM is inserted in SIM slot A1 and the current image is Verizon), the MG90 can, if enabled, 'switch' the image (install the correct firmware on the module) to the correct version.

To enable firmware switching:

1. Go to General > Auto Software Updates.
2. Select Firmware Switching Enabled.
3. Click Submit.

If an image switch is required and the correct image is not stored on the MG90, it is automatically downloaded from the on-line repository (see Automatic Firmware Downloads on page 77 for details.), if enabled.

The image switching process, and the options that may affect its success, are shown in Figure 12-2, below.

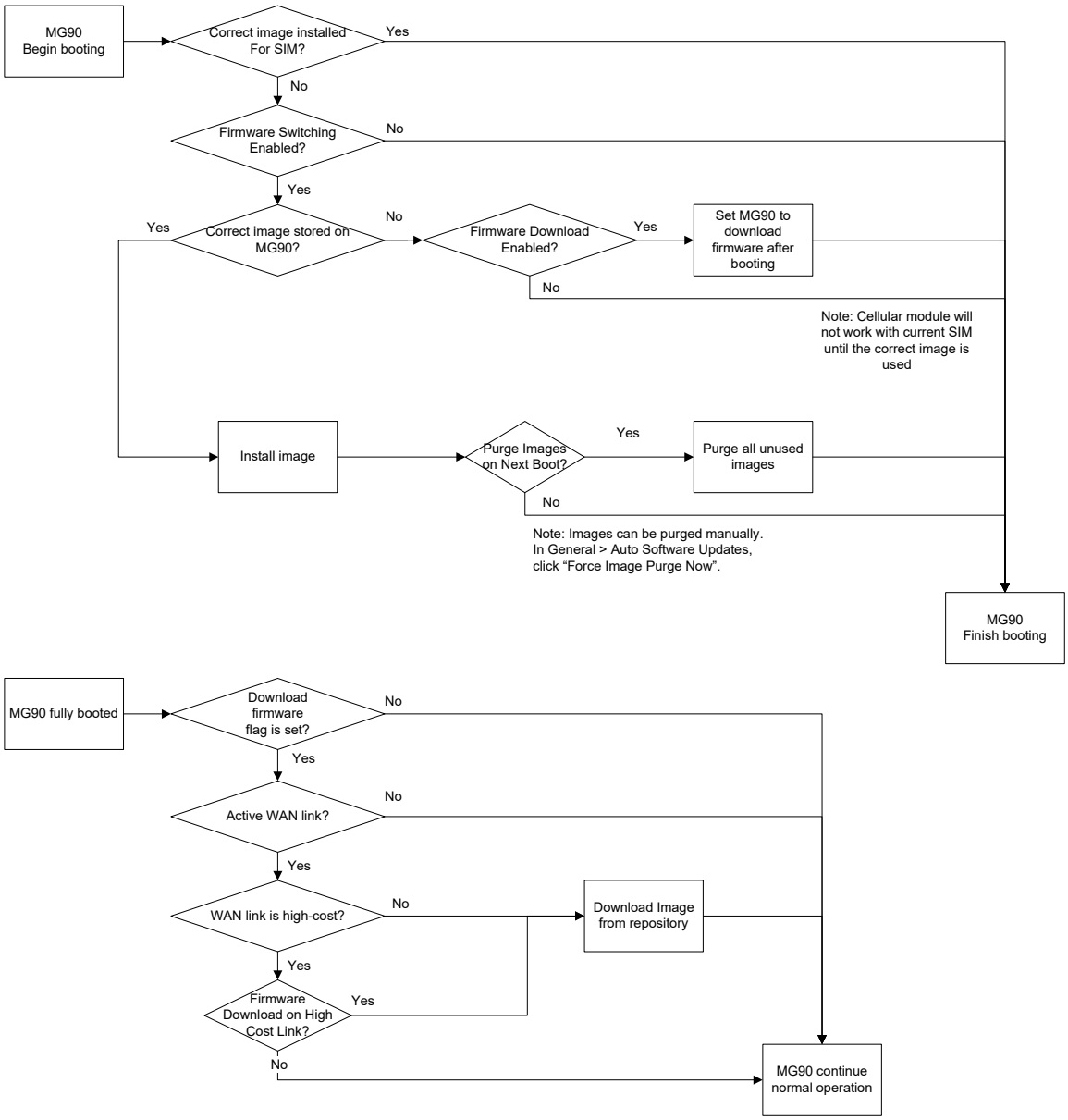

Figure 12-2: Firmware Switching Process

While the new firmware image is installing on the modem, the MG90's LEDs display a green ‘chase’ pattern (each LED will blink in sequence from left to right). When the installation finishes, the LEDs return to their normal behavior. (See LEDs on page 216 for details).

Purging Firmware Images

To save space on the MG90, the Purge Images on Next Boot option can be selected to automatically purge (on the next boot) all firmware images on the router after all of the MG90’s radio modules have connected and been loaded with the correct images.

For example:

a. When the MG90 is shipped, it includes the generic and carrier images.

b. SIMs are inserted for all radio modules, but one module is set to IDLE.

c. The MG90 boots and installs appropriate images for the active modules.

d. At some later time, the remaining IDLE module is set to WAN.

e. The MG90 boots and installs the image for the module.

f. The next time the MG90 boots, if Purge Images on Next Boot is enabled, all firmware image files are removed (purged) automatically.

g. If a SIM for a different carrier is then inserted for a module, the MG90 will attempt to download the appropriate firmware.

For detailed information, see General > Auto Software Updates on page 203.

To enable/disable automatic image file purging:

1. Go to General > Auto Software Updates.
2. Select Purge Images on Next Boot to enable image file purging, or deselect to disable.
3. Click Submit.

Note: The images on the MG90 can be manually purged to save space, even if all modules have not been loaded appropriate firmware (for example, if a module cannot connect, is kept IDLE, does not have a SIM, etc.). To do this, use the Force Image Purge Now button in General > Auto Software Updates.

Listing Firmware Images

To list the firmware images currently stored on the MG90 (but not necessarily installed on the radio modules), navigate to Status > General:

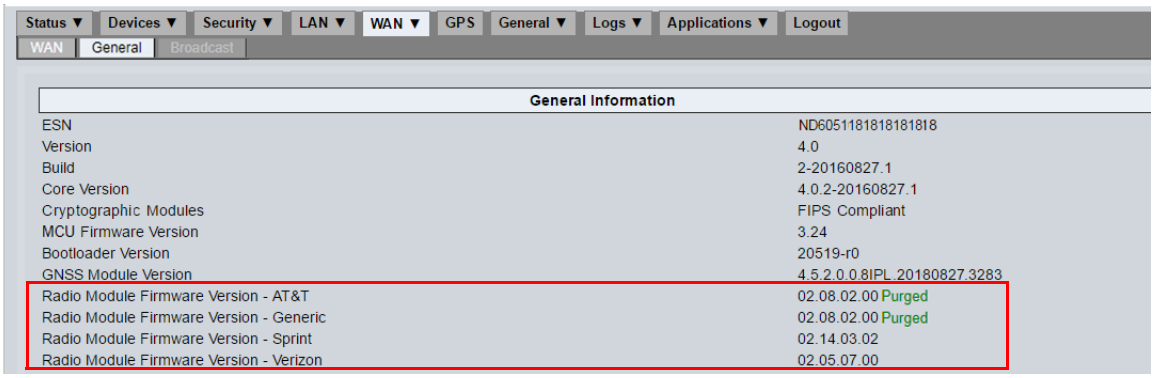

Figure 12-3: Viewing the Available Module Firmware Image Packages

To confirm which images are loaded on the radio modules, check the Extended Status page (Status > WAN > Show Extended Status. These may be different from the listings in General Information if:

- Firmware switching is disabled
- Firmware switching for a module has not yet happened
- Module has newer firmware than the firmware for the current MGOS release

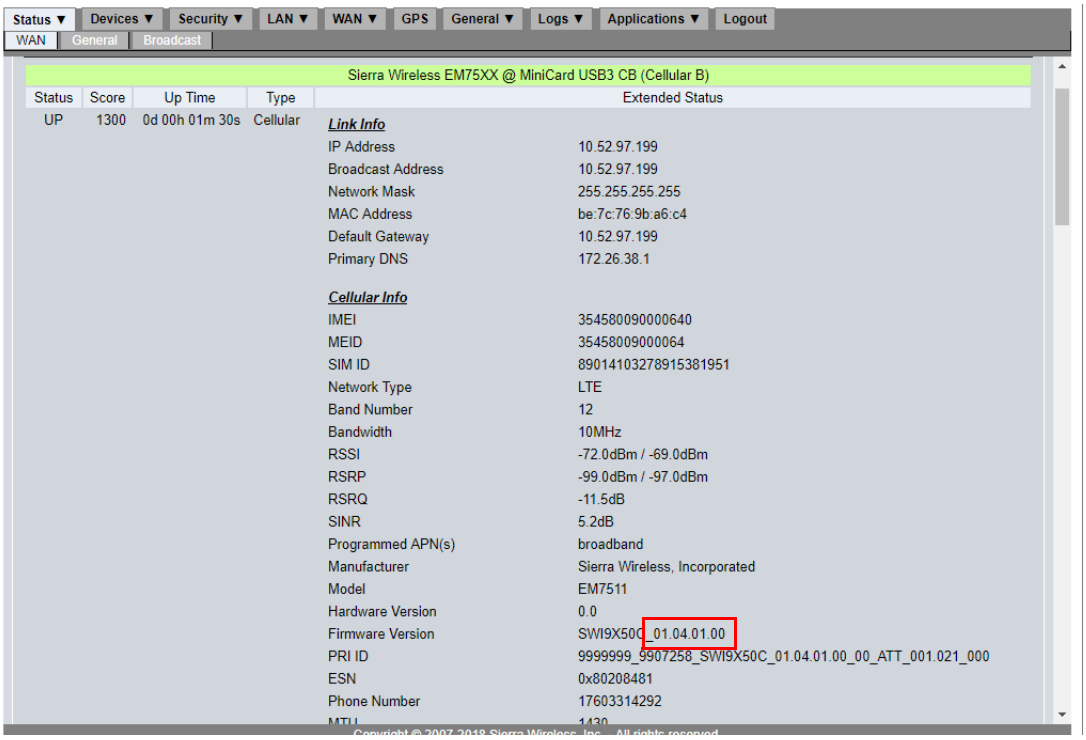

Figure 12-4: Viewing Installed Module Firmware

Over the Air Updates

AirLink Support can publish upgrades "over the air" based on the terms of a service contract agreement.

If an MG90 has been configured to automatically check for updates, the software will be downloaded when the unit comes online. When the software is successfully downloaded to an MG90, it will be installed and will take effect after the router is rebooted. See Installing Software Updates on page 76 for details.

Alternatively, the unit can be forced to download and install the software using the Diagnostic/Service Tools page of the LCI.

Important: *For MG90s that contain two different Sierra Wireless radio modules (e.g. MC7354+MC7455, MC7455+EM7511, etc.), make sure a SIM card is installed for at least one of the radio modules prior to an OTA firmware update. Otherwise, if firmware is downloaded OTA, the MG90 will not install the downloaded firmware, and will continue running its current version. In this case, to complete the upgrade:*

- *Install new firmware using a USB stick,*

or

- *Insert a SIM for one or both modules, select and run General > Tools > "clean-local-software-update-cache", and then reboot.*

To manually download software updates with this tool:

1. Go to General > Tools:

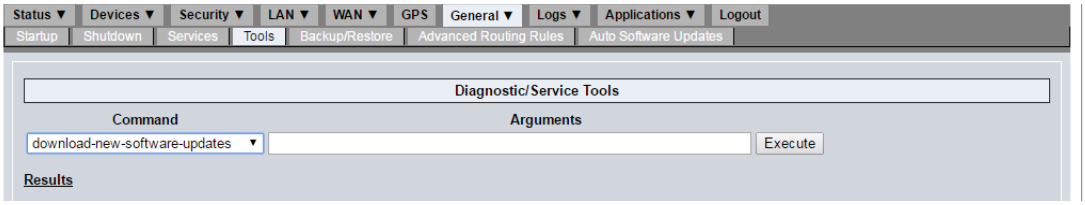

Figure 12-5: Accessing the Diagnostic/Service Tools page

2. In the Command pull-down, select download-new-software-updates.
3. Click Execute. A series of messages will be displayed.
4. When prompted to reboot, press and release the Reset button to reboot the MG90.

13: Status Tab

This chapter describes the Status tab, which displays information about connected WAN devices, and details of the MG90's current hardware and software status.

The Status tab includes the following sub-tabs:

- WAN— Status of all links (devices) that are currently configured for WAN access. See WAN Link Status Tab on page 83.

Note: WAN Link Status is the first screen that appears when you log in to the LCI.

- General—MG90 hardware and software details. See General Information on page 89.
- Broadcast—Status Broadcast options. See Broadcast on page 91.

WAN Link Status Tab

The WAN Link Status tab (Status > WAN) displays summary information when the screen appears, and extended (detailed) information when Show Extended Status is selected.

Summary status screen

The summary WAN Link Status screen lists all devices (links) that are currently configured for WAN access, and their connection status. The currently active link is highlighted in green as shown in Figure 13-1.

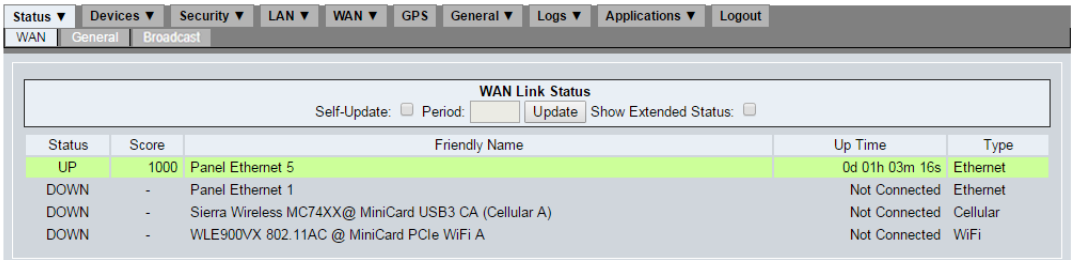

Figure 13-1: WAN Link Status summary screen (Status > WAN)

Table 13-1: WAN Link Status (Summary) screen fields/buttons

Field/Button	Description
Self-Update	Select to make the screen automatically refresh every <Period> seconds.
Period	Number of seconds between automatic screen refreshes (when Self-Update is selected). • Valid range: 5–99. (Note—If you enter 0–4, the value rounds up to 5 automatically.) • Other values—Ignored
Update (button)	Click to refresh the screen.

Table 13-1: WAN Link Status (Summary) screen fields / buttons (Continued)

Field / Button	Description
Show Extended Status	Select to display detailed information about the WAN links. See Extended status screen on page 84.
Status	Current state of the WAN link • UP—Link is connected • DOWN—Link is not connected *Note: More than one link can be UP at the same time. The active link is highlighted in green.* If you want to stop the currently active link from carrying traffic, either temporarily set its status to IDLE (e.g. in Devices > Cellular), or fine-tune its policies to adjust its score (see Setting up WAN Link Policies on page 42.)
Score	Priority score used to dynamically determine which WAN link will be used The MG90 tries to use the link with the highest score as the active link. For details on configuring links to dynamically change based on connection status, geographic location, time of day, etc., see Setting up WAN Link Policies on page 42.
Friendly Name	Descriptive name for the WAN link To change the description, see the Devices Tab on page 93.
Up Time	Connection duration • UP link—Amount of time the link has been connected for current session. • DOWN link—“Not Connected”
Type	WAN link type • Cellular—An LTE radio installed in the MG90. • Ethernet—One of the Ethernet ports on the MG90’s back panel. • Wi-Fi—A Wi-Fi radio installed in the MG90. • Serial modem—An optional Harris Land Mobile Radio connected to the MG90’s serial port.

Extended status screen

The extended WAN Link Status screen lists all devices (links) that are currently configured for WAN access, and configuration details and traffic data for each link. The currently active link is highlighted in green as shown in Figure 13-2.

Note: This screen is read-only, none of the information displayed can be updated from this screen.

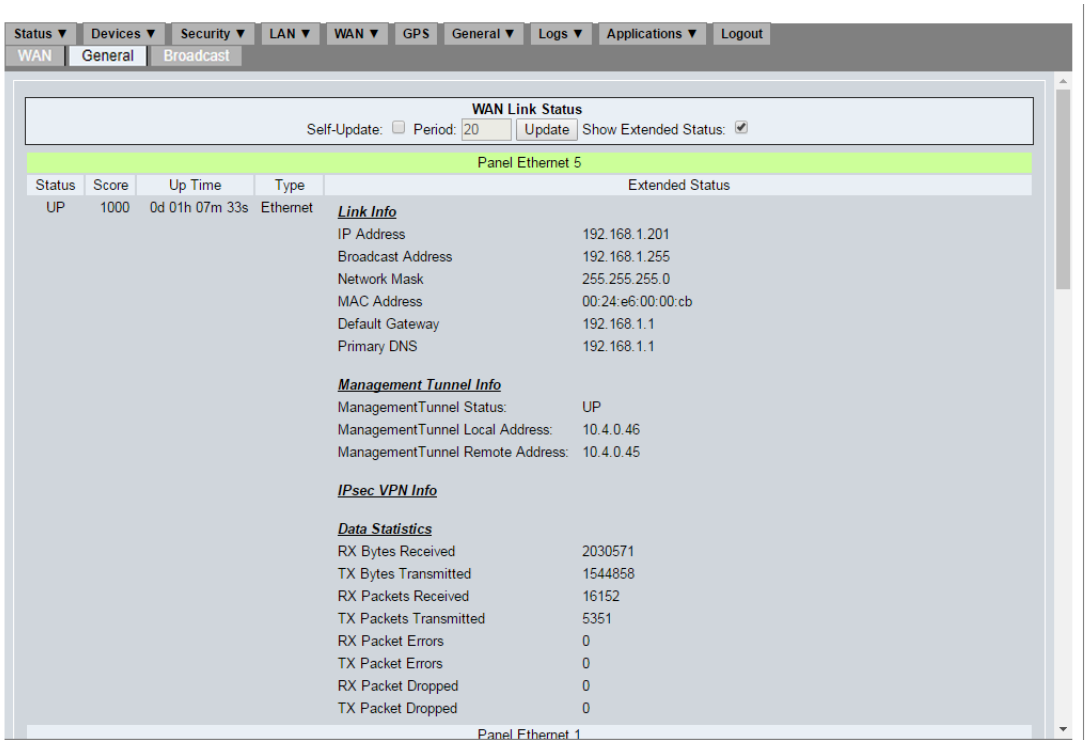

Figure 13-2: WAN Link Status extended screen (Status > WAN > Extended Status)

Table 13-2: WAN Link Status (Extended) screen fields

Field	Description
Status	Current state of the WAN link • UP—Link is connected • DOWN—Link is not connected *Note: More than one link can be UP at the same time. The active link is highlighted in green.* If you want to stop a link from carrying traffic link, either: • Set the link's status to IDLE (e.g. in Devices > Cellular), or • Fine-tune the link's policies so its scores will adjust appropriately. (See Setting up WAN Link Policies on page 42.)
Score	Priority score used to dynamically determine which WAN link will be used The MG90 tries to use the link with the highest score as the active link. To configure links to dynamically adjust their scores based on connection status, geographic location, time of day, etc., see Setting up WAN Link Policies on page 42.
Up Time	Connection duration • UP link—Amount of time the link has been connected for current session. • DOWN link—"Not Connected"

Table 13-2: WAN Link Status (Extended) screen fields (Continued)

Field	Description
Type	WAN link type: • Cellular—LTE radio installed in the MG90. • Ethernet—One of the Ethernet ports on the MG90's back panel. • Wi-Fi—Wi-Fi radio installed in the MG90. • Serial modem—Optional Harris Land Mobile Radio connected to the MG90's serial port.
Extended Status	Detailed information about the WAN link, including configuration, link, and performance data. The information displayed depends on the type of WAN Link (Cellular, Ethernet, or Wi-Fi).
Link Info (appears only for Cellular or Ethernet WAN devices)	
IP Address	IPv4 address assigned to the link Example: 192.168.1.201
Broadcast Address	IPv4 address of the subnet that the link is part of
Network Mask	Network mask assigned to the link
MAC Address	MAC address of the link
Default Gateway	IPv4 address of the gateway that assigned the link's IP Address
Primary DNS	Mobile Network Operator's DNS IP Address
Secondary DNS Servers	IPv4 addresses of the mobile network operator's secondary DNS servers
Cellular Info (appears only for Cellular WAN devices)	
IMEI	Cellular device's unique International Mobile Equipment Identity code
MEID	Cellular device's unique Mobile Equipment Identifier
SIM ID	Identification number for the SIM card in use
SIM Type	FirstNet—Indicates a FirstNet SIM is installed. *Note: Field appears only if a FirstNet SIM is installed.*
Network Type	Type of network the gateway is connected to • CDMA • EVDO • GSM • HDR • HSPA • LTE • WCDMA • 1XRTT
Band Number	LTE band number that device is connected to

Table 13-2: WAN Link Status (Extended) screen fields (Continued)

Field	Description
Bandwidth	LTE bandwidth
RSSI	Received Signal Strength Indicator • Good: ≥ -60 dB • Fair: ≥ -80 dB • Poor: ≥ -90 dB • Inadequate: ≤ -100 dB
RSRP	LTE Reference Signal Received Power (signal power)
RSRQ	LTE Reference Signal Received Quality
SINR	LTE Signal-to-interference-plus-noise ratio (SINR level)
Programmed APN(s)	APN(s) that are pre-programmed in the radio module
Manufacturer	Name of the cellular device's manufacturer
Model	Cellular device's model number
Hardware Version	Cellular device's hardware version number
Firmware Version	Firmware version running on the cellular device
PRI ID	Configuration identification code ("Product Release Instructions ID number")
Phone Number	Phone number associated with the SIM card in use
Roaming Indicator	Roaming state • "Home"—Not roaming • Name of carrier—Roaming
Service	Service type (e.g. "LTE", "UMTS")
Provision Status	(Sprint only) "Provisioned" or "Not Provisioned"
Wi-Fi Info (appears only for Wi-Fi WAN devices)	
WPA State	Wi-Fi connection state: • COMPLETED • DISCONNECTED
Band	802.11 network access control protocol version
SSID	Basic Service Set Identifier The identifier that appears to a device when it scans for access points.
Mode	802.11 operation mode • adhoc—This option is used only when the AP that the link is connected to is using WEP. • Managed—Default
Frequency	Wi-Fi frequency
Access Point	Wi-Fi device's MAC address

Table 13-2: WAN Link Status (Extended) screen fields (Continued)

Field	Description
Link Quality	Wi-Fi signal quality Signal-to-noise ratio determined by various link parameters, including Bit Error Ratio (BER) and Signal, Noise and Distortion (SINAD). • Example: 70/70
Signal Level	Wi-Fi signal strength, in dBm
Management Tunnel Info	
Management Tunnel Status	Status of management tunnel (secure VPN that AMM can use to access MG90) • UP • DOWN
Management Tunnel Local Address	IPv4 addresses of both ends of the management tunnel When a WAN link is established, the MG90 initiates the management VPN tunnel to the remote address. The VPN server authenticates the initiation request and issues a local address to the MG90. • Local Address—Issued by the VPN server to the MG90. • Remote Address—The AMM Tunnel IP Address specified in Table 17-15 on page 160.
Management Tunnel Remote Address	
IPsec VPN Info (Details repeat for each defined VPN associated with the device)	
IpsecVPN 1 Name	VPN descriptive name This is the Friendly Name field from the IPsec VPN Configuration screen.
IpsecVPN 1 Status	VPN status • UP • DOWN
IpsecVPN 1 Local Address	VPN gateway IP address This is the Server Address Field from the IPsec VPN Configuration screen.
Data Statistics	
RX Bytes Received	Total number of bytes received from the network since the link became active
TX Bytes Transmitted	Total number of bytes transmitted to the network since the link became active
RX Packets Received	Total number of packets received from the network since the link became active
TX Packets Transmitted	Total number of packets transmitted to the network since the link became active
RX Packet Errors	Number of packets received with errors since the link became active
TX Packet Errors	Number of packets transmitted with errors since the link became active
RX Packet Dropped	Number of received packets dropped since the link became active
TX Packet Dropped	Number of transmitted packets dropped since the link became active

General Information

The General Information screen (Status > General) displays basic details about the MG90's hardware, operating software, and GPS details, as shown in Figure 13-3.

Note: This screen is read-only, none of the information displayed can be updated from this screen.

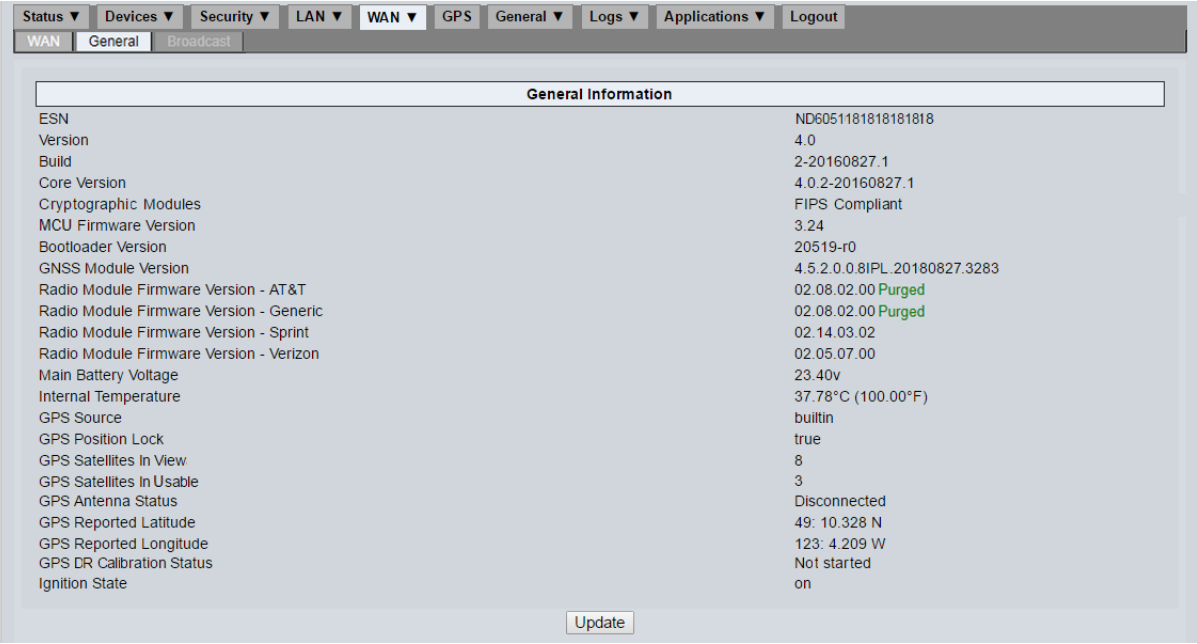

Figure 13-3: General Information screen (Status > General)

Table 13-3: General Information screen fields

Field	Description
ESN	MG90 serial number *Note: The ESN is also printed on a label on the bottom of the MG90.*
Version	Main version number
Build	Hardware build version
Core Version	Software version number
Cryptographic Modules	Indicates the router is "FIPS Compliant". This appears only if the MG90 is configured for FIPS.
MCU Firmware Version	MCU firmware version number
Bootloader Version	Bootloader version number

Table 13-3: General Information screen fields (Continued)

Field	Description
GNSS Module Version	GNSS module version number
Radio Module <type> Firmware Version <fw_type>	Radio module firmware versions present on the MG90.
Main Battery Voltage	Power supply voltage (Vehicle battery, AC power supply, etc.)
Internal Temperature	MG90 device's internal temperature
GPS Source	Device type providing GPS functionality: • builtin—The internal GPS device included with the MG90. • ethernet—GPS device connected to an Ethernet port. • serial—GPS device connected to the serial port (DB-9 connector).
GPS Position Lock	Status of the GPS fix: • false—No GPS fix • true—GPS fix acquired *Note: Four or more satellites must be found to get a position lock.*
GPS Satellites In View	Number of satellites detected by the GPS device
GPS Satellites Usable	Number of satellites usable by the GPS device
GPS Antenna Status	Current status of GPS antenna connector on MG90's rear panel: • Connected • Disconnected
GPS Reported Latitude	Last reported GPS fix position
GPS Reported Longitude	
GPS DR Calibration Status	Status of Dead Reckoning calibration process • Not started • In progress • Complete
Ignition State	Vehicle ignition state: • on • off

Broadcast

The Status Broadcast Configuration screen (Status > Broadcast) allows broadcasting of a selection of MG90 status information over UDP to be enabled/ disabled and customized as shown in Figure 13-4.

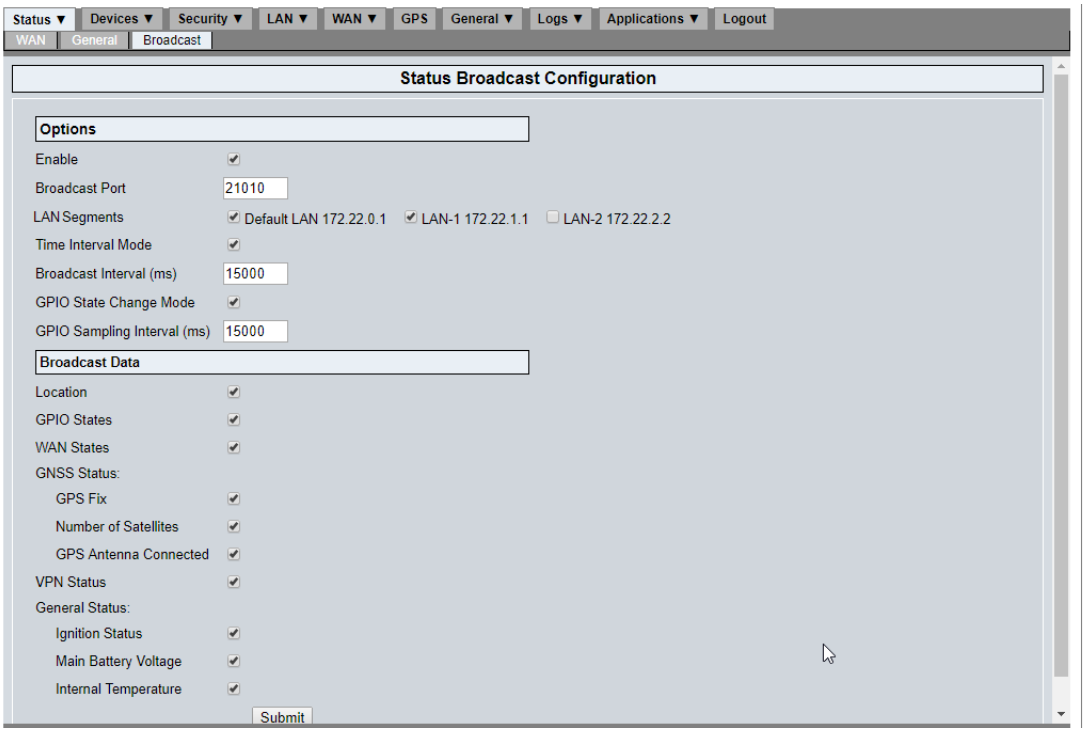

Figure 13-4: Status Broadcast Configuration screen (Status > Broadcast)

Table 13-4: Status Broadcast Configuration screen fields

Field	Description
Options	
Enable	Status Broadcast state: • Selected—Enabled. Status details will broadcast at the specified Broadcast Interval, GPIO Sampling Interval (if state changes occur), or both. • Not selected—Disabled *Note: One or both of Time Interval Mode and GPIO State Change Mode must be selected.*
Broadcast Port	UDP port to use for broadcasting
LAN Segments	LAN segments to use for broadcasting
Time Interval Mode	Enable/disable time interval broadcasting
Broadcast Interval (ms)	Broadcast frequency in milliseconds (used for Time Interval Mode only)

Table 13-4: Status Broadcast Configuration screen fields (Continued)

Field	Description
GPIO State Change Mode	Enable/ disable broadcasting triggered by GPIO state changes
GPIO Sampling Interval (ms)	GPIO sampling frequency in milliseconds (used for GPIO State Change Mode only)
Broadcast Data	
Location	Include latitude and longitude coordinates
GPIO States	Include input and output states for all five GPIOs
WAN States	Include details for each WAN link: • Friendly name • Status: 0 (link is down) or 1 (link is up) • Active (true or false) • Signal strength (in dBm)
GNSS Status	
GPS Fix	Include Fix availability (true or false)
Number of Satellites	Include number of usable satellites
GPS Antenna Connected	Include GPS antenna connected state (true or false)
VPN Status	Include VPN status 0 (No VPNs established) or 1 (at least one VPN established)
General Status	
Ignition Status	Include vehicle ignition status (true or false)
Main Battery Voltage	Include main battery voltage (in Volts)
Internal Temperature	Include internal MG90 temperature (in °C)

14: Devices Tab

This chapter describes the Devices tab, which is used to configure the devices installed in (or connected to) the MG90 that provide network connectivity.

The Devices tab includes the following sub-tabs:

- Cellular—Display the installed LTE radios, and configure them for WAN use or idle them. See Devices > Cellular on page 93.
- Ethernet—Display the pre-installed Ethernet ports, and configure them for WAN or LAN use, or idle them. See Devices > Ethernet on page 94.
- Wi-Fi—Display the installed Wi-Fi radios, and configure them for WAN or LAN use, or idle them. See Devices > Wi-Fi on page 95.
- Serial Modem—Add an optional Harris Land Mobile Radio, and configure it for WAN use, or idle it. See Devices > Serial Modem on page 96.
- Serial—Configure the MG90's DB9 serial port for console access or application (external device) use. See Devices > Serial on page 97.
- Bluetooth—Configure the internal Bluetooth device. See Devices > Bluetooth on page 98.

Devices > Cellular

The Cellular devices tab lists the cellular radios that are currently installed in the MG90, and any that were previously installed and have since been removed.

From this tab, you can configure the radios' display names and make them available for WAN connections or idle them.

Note: WAN-enabled radios will appear on the Status > WAN screen.

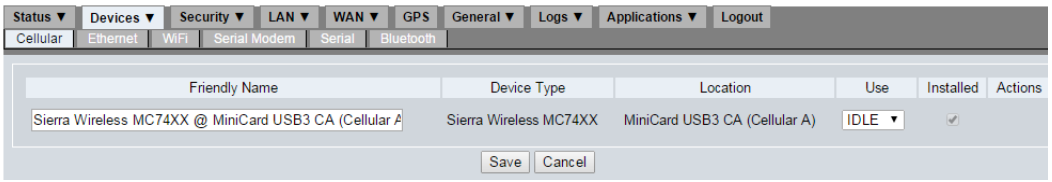

Figure 14-1: LCI: Devices > Cellular—Sample screen

Table 14-1: Devices > Cellular screen fields

Field	Description
Friendly Name	Enter a descriptive name for the LTE radio. This name identifies the radio in other LCI screens (e.g. Status > WAN).
Device Type	LTE radio's model name/number
Location	Internal position of the LTE radio For example: • MiniCard USB3 CA (Cellular A)—Uses the Cellular A antenna connectors. • MiniCard USB3 CB (Cellular B)—Uses the Cellular B antenna connectors.

Table 14-1: Devices > Cellular screen fields (Continued)

Field	Description
Use	Select the current usage mode of the LTE radio. • IDLE—Radio cannot be used for WAN connection at this time. • WAN—Radio can be used for a WAN connection. To check its connection status, see WAN Link Status Tab on page 83. To change the usage mode, select a different value and click Save.
Installed	LTE radio installation status • Selected—Radio is installed in the MG90. • Not selected—Radio has been removed from the MG90.
Actions	Not applicable

Devices > Ethernet

The Ethernet devices tab lists the pre-installed Ethernet ports located on the MG90's rear panel.

From this tab, you can configure the ports' display names and make them available for WAN connections, LAN connections, or idle them.

Note: WAN-enabled ports will appear on the Status > WAN screen.

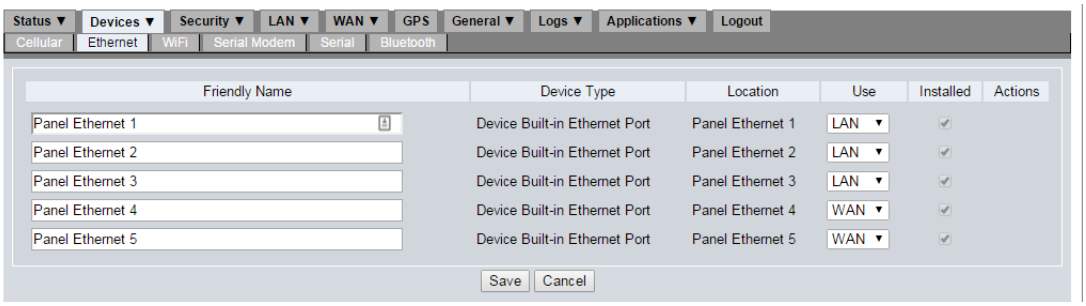

Figure 14-2: LCI: Devices > Ethernet—Sample screen

Table 14-2: Devices > Ethernet screen fields

Field	Description
Friendly Name	Enter a descriptive name for the Ethernet port. This name identifies the port in other LCI screens (e.g. Status > WAN and LAN > LAN Segments).
Device Type	All Ethernet ports are listed as "Device Built-in Ethernet Port".
Location	Connector position (1–5) on the MG90's rear panel

Table 14-2: Devices > Ethernet screen fields (Continued)

Field	Description
Use	Select the current usage mode of the Ethernet port. • IDLE—Port cannot be used for WAN or LAN connection at this time. • WAN—Port can be used for WAN connection. To check its current connection status, see WAN Link Status Tab on page 83. • LAN—Port can be used to connect a device (such as a notebook) to the MG90's LAN. To change the usage mode, select a different value and click Save.
Installed	Ethernet port installation status • Selected—Port is installed in the MG90. • Not selected—Port has been removed from the MG90 or is not functioning.
Actions	Not applicable

Devices > Wi-Fi

The Wi-Fi devices tab lists the Wi-Fi radios that are currently installed in the MG90, and any that were previously installed and have since been removed.

From this tab, you can configure the radios' display names and make them available for WAN connections, LAN connections (acting as an access point for other devices), or idle them.

Note: WAN-enabled Wi-Fi radios will appear on the Status > WAN screen.

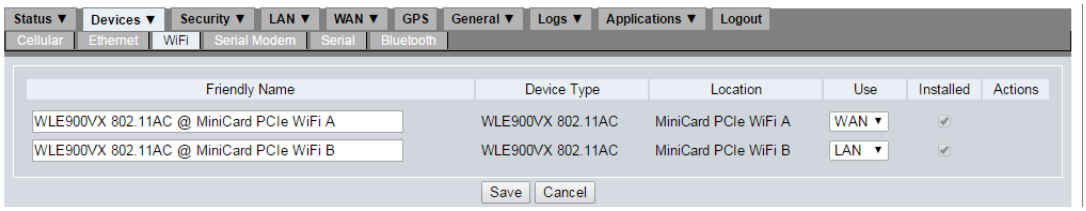

Figure 14-3: LCI: Devices > Wi-Fi—Sample screen

Table 14-3: Devices > Wi-Fi screen fields

Field	Description
Friendly Name	Enter a descriptive name for the Wi-Fi radio. This name identifies the radio in other LCI screens (e.g. Status > WAN and LAN > LAN Segments).
Device Type	Wi-Fi radio's model name
Location	Internal position of the Wi-Fi radio: • MiniCard PCIe WiFi A—Uses the Wi-Fi A antenna connectors. • MiniCard PCIe WiFi B—Uses the Wi-Fi B antenna connectors.

Table 14-3: Devices > Wi-Fi screen fields (Continued)

Field	Description
Use	Select the current usage mode of the Wi-Fi radio. • IDLE—Wi-Fi radio cannot be used for WAN or LAN connections at this time. • WAN—Wi-Fi radio can be used for a WAN connection. To check its current connection status, see WAN Link Status Tab on page 83. • LAN—Wi-Fi radio can be used as an access point to provide LAN connections for other devices (such as notebooks, smartphones, etc.). To change the usage mode, select a different value and click Save.
Installed	Wi-Fi radio installation status • Selected—Radio is installed in the MG90. • Not selected—Radio has been removed from the MG90.
Actions	Not applicable

Devices > Serial Modem

If a serial modem (Harris Land Mobile Radio) is used with your MG90, it appears on the Serial Modem device tab (after you have added it).

From this tab, you can configure the serial modem's display name and make it available for a WAN connection, or temporarily idle it.

Note: A WAN-enabled serial modem will appear on the Status > WAN screen.

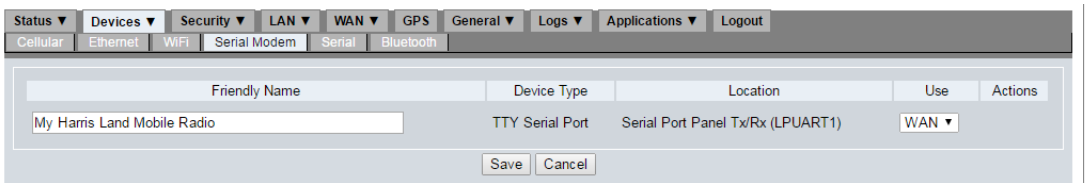

Figure 14-4: LCI: Devices > Serial Modem—Sample screen

Table 14-4: Devices > Serial Modem screen fields

Field	Description
Friendly Name	Enter a descriptive name for the serial modem device. This name identifies the device in other LCI screens (e.g. Status > WAN).
Device Type	The MG90 supports the Harris Land Mobile Radio as a serial modem. The serial modem is always listed as "TTY Serial Port".
Location	Position of the serial port connector The serial port location always appears as Serial Port Panel Tx/Rx (LPUART1), which is the DB-9 serial connector on the MG90's rear panel.

Table 14-4: Devices > Serial Modem screen fields (Continued)

Field	Description
Use	Select the current usage mode of the serial modem. • IDLE—Serial modem cannot be used for a connection at this time. • WAN—Serial modem can be used for a WAN connection, and will appear in the Status > WAN screen. To change the usage mode, select a different value and click Save.
Actions	Not applicable

Devices > Serial

The MG90 has a built-in DB-9 serial port on the rear panel. This port can be used by a computer to access the MG90's Linux console, or can be used to connect an external device (application) such as a serial modem or external GPS device.

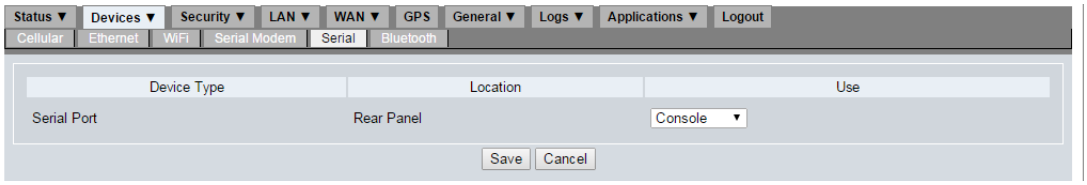

Figure 14-5: LCI: Devices > Serial—Sample screen

Table 14-5: Devices > Serial screen fields

Field	Description
Device Type	The MG90 has a single built-in serial port (RS-232 DB9 connector) on the rear panel). The port is always listed as "Serial Port".
Location	Serial port location The location always appears as "Rear Panel".
Use	Select the current usage mode of the serial port: • Console—A computer will be able to connect to the MG90's Linux console. • Application—An external device (serial modem, GPS device, etc.) can be connected to the MG90. Additional setup is required for external devices. For example, see Devices > Serial Modem on page 96 for serial modem setup, and Setting up GPS connectivity on page 70 for external GPS device setup. To change the usage mode, select a different value and click Save. The change takes effect after you reboot the MG90 (you can press and release the Reset button on the front panel).

Devices > Bluetooth

The MG90 has an internal Bluetooth adapter for connecting multiple Bluetooth-enabled devices to the MG90's Bluetooth network. The internal adapter is disabled by default and must be enabled before devices can pair with it.

Note: This screen is read-only, none of the information displayed can be updated from this screen.

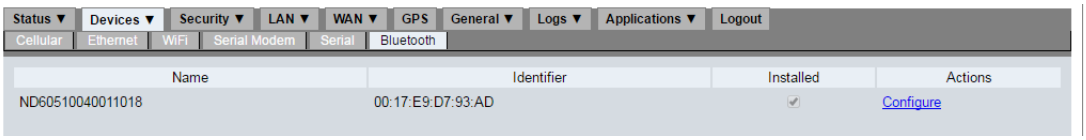

Figure 14-6: LCI: Devices > Bluetooth—Sample screen

Table 14-6: Devices > Bluetooth screen fields

Field	Description
Name	Descriptive name for the internal Bluetooth adapter that appears when a Bluetooth-enabled device discovers the MG90.
Identifier	Bluetooth device address code
Installed	Bluetooth adapter status • Selected—Adapter is functioning. • Not selected—Adapter is not functioning.
Actions	• Configure—Click to modify the Bluetooth adapter's name, PIN, and profile. See Bluetooth Adapter Configuration (Devices > Bluetooth > Configure) on page 98.

Bluetooth Adapter Configuration (Devices > Bluetooth > Configure)

This screen is used to configure the internal Bluetooth adapter's descriptive name and its access options.

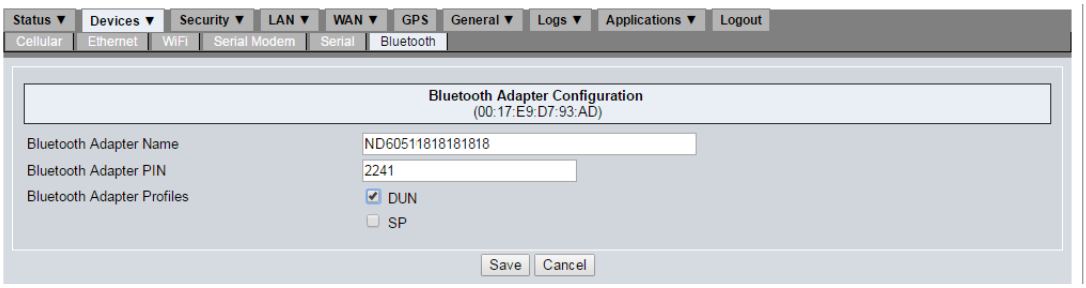

Figure 14-7: LCI: Devices > Bluetooth > Configure—Sample screen

Table 14-7: Devices > Bluetooth > Configure screen fields

Field	Description
Bluetooth Adapter Name	Enter a descriptive name for the internal Bluetooth adapter. This name identifies the MG90 when a Bluetooth-enabled device discovers its Bluetooth adapter. For example, the name could identify the vehicle carrying the MG90, such as “Truck25”.
Bluetooth Adapter PIN	Pairing code Enter the pairing code that a device needs to connect to the MG90’s Bluetooth adapter. *Note: By default, this code is blank. A user-selected code must be entered before the screen can be saved with either Bluetooth Adapter Profile selected.*
Bluetooth Adapter Profiles	Bluetooth connection method Select the appropriate method that devices need to connect to the Bluetooth adapter: • DUN—Device connects using a TCP/IP dial-up connection profile (e.g. Zoll, Phillips). • SP—Device connects using a serial port profile. If both methods are deselected, the adapter is disabled and devices cannot pair with it. *Note: By default, the adapter is disabled (both profiles are deselected). If enabling either profile, a Bluetooth Adapter PIN must also be assigned before the screen can be saved.*

15: Security Tab

This chapter describes the Security tab, which is used to manage user and root access to the MG90.

The Security tab includes the following sub-tabs:

- Users—Add, edit (update), and delete user accounts. See Security > Users on page 100.
- Change Root Password—Change the default root access password. See Security > Change Root Password on page 101.

Security > Users

The Users tab is used to display and configure the names, passwords, and access methods for users that can access the LCI.

Figure 15-1: LCI: Security > Users—Sample screen

Table 15-1: Security > Users screen fields/buttons

Field	Description
Add/Edit User (Top half of screen)	
User Name	Unique user name Enter a unique name for the user account that is being added/updated.
Password	User password Enter a non-blank password for the user account.
Role	User type Select the access level for the user account: • User—User can access Status > WAN screen only. • Administrator—User can access all LCI screens.
Add User (button) or **Edit User** (button)	Button to add a new user or edit an existing user • Add User—Default button when page is displayed. Click to add a new user with the name, password, and role entered above. • Edit User—Button appears when you click the 'Edit' link for a user in the users list. Change any of the fields above, and click to save the changes.

Table 15-1: Security > Users screen fields / buttons (Continued)

Field	Description
Users List (Bottom half of screen)	
User Name	Unique name of an existing user
Role	User type • User—User can access the LCI WAN Link Status screen only. • Administrator—User has full access to all LCI screens.
Action	Click these optional links to perform actions on the associated users: • Edit—Display the user details (name and role), enter a new password, and optionally change the user role. • Delete—Remove the user from the system. When prompted, click OK to confirm the deletion.

Security > Change Root Password

The Change Root Password tab is used to change the root password. When the screen appears, all fields are blank.

See Changing the Root Password on page 27 for details.

Important: *If you forget the root password, it cannot be recovered. Perform a factory reset to restore it to the default value (the MG90's serial number). To perform the factory reset, press and hold the Reset button on the MG90's front panel until all the LEDs turn solid white. Release the button, and the LEDs remain white while the factory reset is in progress. The LEDs return to their normal behavior when the factory reset finishes.*

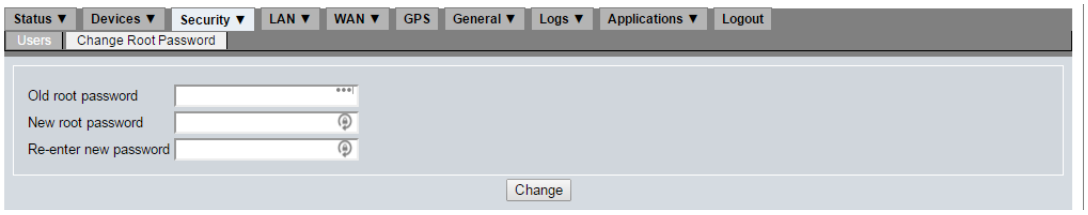

Figure 15-2: LCI: Security > Change Root Password—Sample screen

Table 15-2: Security > Change Root Password screen fields

Field	Description
Old root password	Enter the current root password • Factory default password is the MG90's serial number.
New root password	Enter a new, non-blank password, minimum 8 characters.
Re-enter new password	Re-enter the new password to confirm.
Change (button)	Click to save the new password.

16: LAN Tab

This chapter describes the LAN tab, which is used to manage the MG90's LAN.

The LAN tab includes the following sub-tabs:

- Ethernet Links—Configure the MG90's Ethernet ports for LAN use. See LAN > Ethernet Links on page 102.
- Access Points—Configure the MG90's Wi-Fi radios as access points for devices to connect to the MG90's LAN. See LAN > Access Points on page 105.
- LAN Segments—Configure the LAN as one or more segments for advanced networking scenarios. See LAN > LAN Segments on page 115.
- Virtual LANs—Configure virtual LANs for security purposes, VLAN tagging, etc. See VLAN Configuration (LAN > Virtual LANs) on page 118.
- Networking Rules—Configure rules to block or permit specific devices on the LAN, and to ensure quality of service. See LAN > Networking Rules, and LAN > LAN Segments > Networking Rules on page 119.
- LAN Throughput—Configure LAN throughput reporting. See LAN > LAN Throughput on page 125.
- Captive Portal—Configure captive portals for Wi-Fi access points. See LAN > Captive Portal on page 126.

LAN > Ethernet Links

This screen lists the Ethernet ports ('links') that are currently selected for LAN in Devices > Ethernet, and the available Actions for configuring them.

For example, Figure 16-1 does not show "Panel Ethernet 1" because that port is currently configured for WAN use.

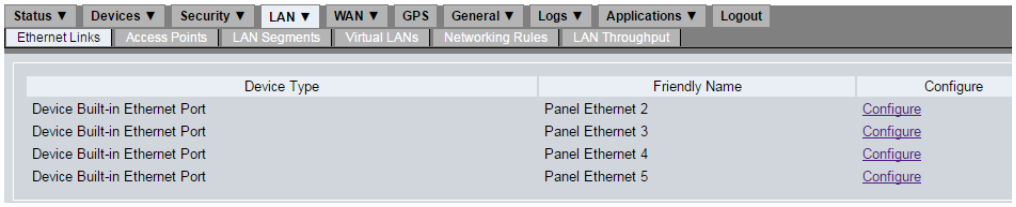

Figure 16-1: LCI: LAN > Ethernet Links—Sample screen

Table 16-1: LAN > Ethernet Links screen fields

Field	Description
Device Type	Hardware device type (cannot be modified). Always appears as "Device Built-in Ethernet Port"
Friendly Name	Friendly name defined in Devices > Ethernet
Configure	Click to configure the LAN connection options. See LAN Ethernet Configuration (LAN > Ethernet Links > Configure) on page 103.

LAN Ethernet Configuration (LAN > Ethernet Links > Configure)

This screen is used to enable (or disable) and configure 802.1x network access control for a LAN-enabled Ethernet port.

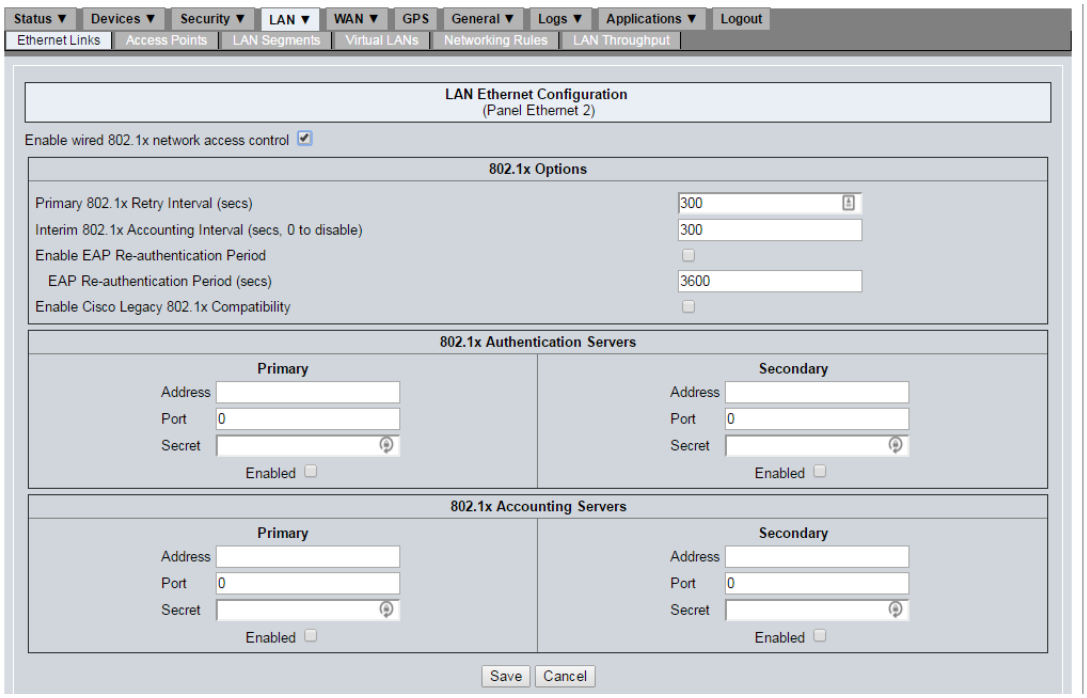

Figure 16-2: LCI: LAN > Ethernet Links > Configure—Sample screen

Table 16-2: LAN > Ethernet Links > Configure screen fields

Field	Description
Enable wired 802.1x network access control	802.1x network access control state • Selected—Enable 802.1x network access control and display the configuration fields. • Not selected—Disable network access control. Any device physically connected to the port can access the network. *Note: If this is enabled, at least one Authentication server must be entered and enabled.*
802.1x Options (These fields appear only if Enable wired 802.1x network access control is selected.)	
Primary 802.1x Retry Interval (secs)	Number of seconds the system waits after the primary authentication server has failed over to the secondary server before trying to reconnect to the primary server. • Default: 300 (5 minutes) *Note: The system sends to the secondary only if the primary fails.*

Table 16-2: LAN > Ethernet Links > Configure screen fields (Continued)

Field	Description
Interim 802.1x Accounting Interval (secs, 0 to disable)	Number of seconds that the system waits between submissions of interim accounting data. • 0—Disable • 1 or higher—Wait this number of seconds between submissions • Default: 300 (5 minutes) *Note: Data transmits automatically when a login session starts and stops.*
Enable EAP Re-authentication Period	Select to force system to periodically renegotiate connection credentials. • Selected—System automatically re-authenticates (renegotiates connection credentials) after the EAP Re-authentication Period. • Not selected—Full re-keying is required each time the MG90 moves into an area served by a different authenticator.
EAP Re-authentication Period (secs)	Number of seconds between authentications (if Enable EAP Re-authentication Period is selected) • Default: 3600 (60 minutes) *Note: Use a long re-authentication period (e.g. the default period—3600 seconds) to delay the need to re-authenticate when a WAN connection is interrupted.*
Enable Cisco Legacy 802.1x Compatibility	Select to enable for systems that use lower case MAC addresses in the calling station ID field. This is recommended for interoperability with the Cisco RADIUS implementation.
802.1x Authentication Servers (These fields appear only if Enable wired 802.1x network access control is selected.)	
Note: At least one authentication server must be enabled.	
Primary (To access these fields, select Enabled.)	
Address	IP address or host name of the primary RADIUS authentication server
Port	Port number used to access the authentication server
Secret	Shared secret code required to access the authentication server from the MG90. If the shared secret is incorrect, the server ignores authentication requests.
Enabled	Select to enable access to the primary authentication server.
Secondary (To access these fields, select Enabled.)	
Address	IP address or host name of the secondary RADIUS authentication server
Port	Port number used to access the authentication server
Secret	Shared secret code required to access the authentication server from the MG90. If the shared secret is incorrect, the server ignores authentication requests.
Enabled	Select to enable access to the secondary authentication server. *Note: The secondary server is used only if the primary is not enabled, or the primary fails.*

Table 16-2: LAN > Ethernet Links > Configure screen fields (Continued)

Field	Description
802.1x Accounting Servers (These fields appear only if Enable wired 802.1x network access control is selected.)	
Note: Accounting servers are optional.	
Primary (To access these fields, select Enabled.)	
Address	IP address or host name of the primary RADIUS accounting server
Port	Port number used to access the accounting server
Secret	Shared secret code required to access the accounting server from the MG90. If the shared secret is incorrect, the server ignores accounting requests.
Enabled	Select to enable access to the primary accounting server
Secondary (To access these fields, select Enabled.)	
Address	IP address or host name of the secondary RADIUS accounting server
Port	Port number used to access the accounting server
Secret	Shared secret code required to access the accounting server from the MG90. If the shared secret is incorrect, the server ignores accounting requests.
Enabled	Select to enable access to the secondary authentication server. *Note: The secondary server is used only if the primary is not enabled, or the primary fails.*

LAN > Access Points

The Access Points tab lists all devices that can be configured as Wi-Fi access points.

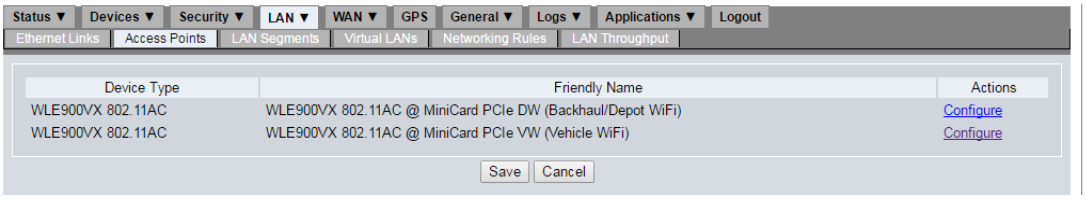

Figure 16-3: LCI: LAN > Access Points—Sample screen

Table 16-3: LAN > Access Points screen fields

Field	Description
Device Type	Device type identification The device type shown is a combination of the Wi-Fi module type and the network access control type (802.1x) used by the AP.

Table 16-3: LAN > Access Points screen fields (Continued)

Field	Description
Friendly Name	Descriptive name for the Wi-Fi device. To change the description, see Devices > Wi-Fi on page 95.
Actions	Click these optional links to perform actions on the associated access points: • Configure—Click to configure the device as an access point. See Access Point Configuration (LAN > Access Points > Configure) on page 106.

Access Point Configuration (LAN > Access Points > Configure)

This screen is used to configure a Wi-Fi device as an access point.

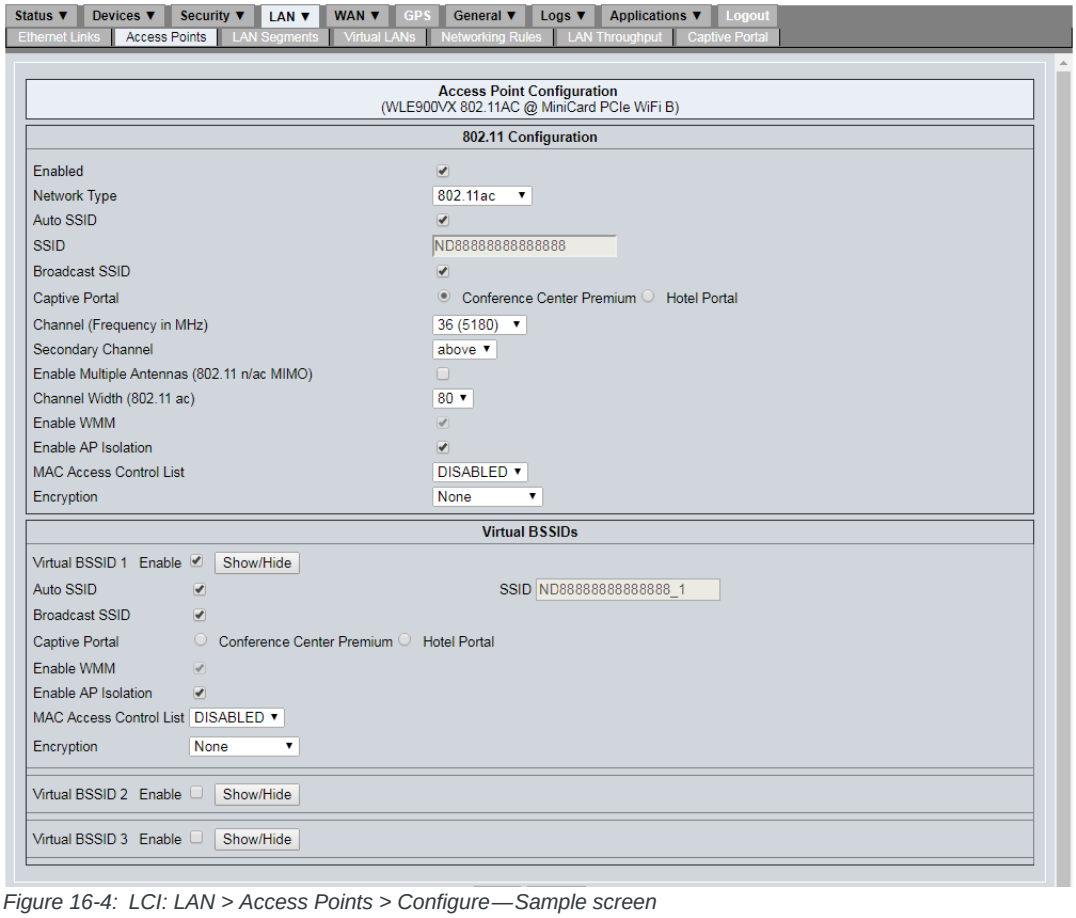

Figure 16-4: LCI: LAN > Access Points > Configure—Sample screen

Table 16-4: LAN > Access Points > Configure screen fields

Field	Description
802.11 Configuration	
Enabled	Access Point state • Selected—Enabled • Not selected—(Default) Disabled *Note: Disabling the Access Point does not affect any configuration settings, it only prevents the Access Point from being used.*
Network Type	802.11 network access control protocol used by the access point • 802.11a/b/g • 802.11n • 802.11ac (Default)
Auto SSID	Automatically generate the primary SSID (Basic Service Set Identifier) and virtual SSIDs • Selected—The MG90's serial number is used for the primary SSID, and the serial number followed by an underscore and a digit (i.e. <ESN>_1) is used for virtual SSIDs (BSSID 1, BSSID 2, BSSID 3). • Not selected—SSID field is set manually.
SSID	Basic Service Set Identifier This identifier appears when a device scans for access points and detects the MG90. • Default value: MG90's serial number *Note: This field is accessible only if Auto SSID is not selected.*
Broadcast SSID	Broadcast the SSID • Selected (Default)—Devices will see the SSID when scanning for access points. • Not selected—SSID is not visible to devices scanning for access points.
Captive Portal	Captive portal that users must connect through when using the access point. Only one portal can be selected at any time. • No portal selected—Access point is not restricted by a captive portal • Portal selected—Wi-Fi access is controlled by the captive portal as defined in LAN > Captive Portal > Configure on page 127. • "not defined"—No portals are defined in LAN > Captive Portal > Configure on page 127. *Note: Captive Portal support requires that only one Wi-Fi module is configured as an access point.*
Channel (Frequency in MHz)	Wi-Fi channel/frequency (i.e. the center frequency) within the spectrum to be used The list of available channels varies depending on the selected Network Type. *Note: When choosing the channel, consider other devices that may interfere with the channel (including other Wi-Fi devices in the MG90).*

Table 16-4: LAN > Access Points > Configure screen fields (Continued)

Field	Description
Secondary Channel	Secondary channel position for increased bandwidth A secondary channel is combined with the primary channel to provide a 40 MHz channel (for 802.11n) or 80 MHz channel (for 802.11ac) instead of 20 MHz or 40 MHz, respectively. The available options depend on the primary channel. For some primary channels, the secondary channel can only be below the primary; for others, it can only be above; for others it can be either. If set, the secondary channel's position will be relative to (i.e. below or above) the primary channel in the spectrum. Options: • none • above • below *Note: This field is not available when the Network Type is 802.11a/b/g.*
Enable Multiple Antennas (802.11n/ac MIMO)	MIMO (multiple antennas) support for 802.11n or 802.11ac. • Selected—MIMO is supported • Not selected—MIMO is not supported
Channel Width (802.11 ac)	Bandwidth for 802.11ac • 20 MHz • 40 MHz (Default) • 80 MHz
Enable WMM	WMM (Wireless MultiMedia extensions) support Make sure that this value is always selected.
Enable AP Isolation	Access Point Isolation • Selected—Clients on the access point cannot access each other. • Not selected—Clients on the access point can access each other.

Table 16-4: LAN > Access Points > Configure screen fields (Continued)

Field	Description

MAC Access Control List	Enable or disable MAC access control (whitelist or blacklist) of devices attempting to connect to the access point. (Also known as 'MAC filtering.)
	• DISABLED (default)—Disable MAC address filtering.
	• ACCEPT—"Whitelist" mode. Only devices with MAC addresses in the whitelist file (described below) can connect to the access point.
	• DENY—"Blacklist" mode. Devices with MAC addresses in the blacklist file (described below) are not allowed to connect to the access point.
	The whitelist and blacklist files should be created as described below, and issued to devices via the AMM.
	File requirements:
	• Whitelist location: /opt/inmotiontechnology/config/global.accept.txt
	Blacklist location: /opt/inmotiontechnology/config/global.deny.txt
	• Plain ASCII text
	• Comment lines may be used and will start with the octothorpe ('#') character
	• Blank lines are permitted
	• MAC addresses:
	  • One address per line
	  • Format: hh:hh:hh:hh:hh:hh (Six hexadecimal digit pairs)
	• Lines with malformed addresses are ignored. When a malformed address is encountered, it is logged in /opt/inmotiontechnology/logs/YYYY-MM-DDlan.log.
	Example (blacklist shown, whitelist uses identical format):
	`# List of MAC addresses that are not allowed to authenticate (IEEE 802.11) with the AP.`
	`00:20:30:40:50:60`
	`00:ab:cd:ef:12:34`
	`00:00:30:40:50:60`

Encryption	Encryption type used by the access point Depending on the encryption type, various configuration fields will appear. • None—Access point is unsecured. • WEP—Secure access via WEP • WPA/TKIP—Secure access via WPA/TKIP • WPA2/CCMP—Secure access via WPA2/CCMP
WEP-specific configuration fields (These fields appear only if Encryption type is "WEP".)	
WEP Key Length	WEP Key length • 40-bit • 104-bit
Change WEP Key	Select to access the next three fields. *Note: This field appears only if you are updating an existing AP configuration that has WEP encryption.*
Previous WEP Key	The current WEP key being used. *Note: This field appears only if you are updating an existing AP configuration that has WEP encryption.*

Table 16-4: LAN > Access Points > Configure screen fields (Continued)

Field	Description
WEP Key or **New WEP Key**	WEP security key Enter the key that devices must use to connect to the access point. • Hexadecimal characters only ('0'–'9','a'–'f','A'–'F') • Fill in all 'white' blocks (each block is 8 bits (two hexadecimal characters))
Retype WEP Key or **Retype New WEP Key**	Re-enter the WEP key to ensure it was entered correctly.
WEP Re-key Interval (sec)	Specifies how often (in seconds) to re-negotiate the keys to be used for WEP security
WPA2 (/TKIP and /CCMP)-specific configuration fields (These fields appear only if Encryption type is "WPA2/TKIP" or "WPA2/CCMP".)	
WPA Key Management	Key management protocol • WPA-PSK—Devices use a pre-shared key for authentication. • WPA-EAP—Devices are authenticated by a RADIUS authentication server.
Change WPA Key	Select to access the next three fields. *Note: This field appears only if you are updating an existing AP configuration that has WPA Key Management type WPA-PSK.*
Previous WPA Pre-Shared Key	The current WPA pre-shared key being used. *Note: This field appears only if you are updating an existing AP configuration that has WPA Key Management type WPA-PSK.*
WPA Pre-Shared Key or **New WPA Pre-Shared Key**	Pre-shared key that devices must use to authenticate to the access point. Format: • 8-63 ASCII characters or • 64 hexadecimal characters *Note: This field appears only if WPA Key Management type is WPA-PSK.*
Retype WPA Pre-Shared Key or **Retype New WPA Pre-Shared Key**	Re-enter the WPA pre-shared key to ensure it was entered correctly. *Note: This field appears only if WPA Key Management type is WPA-PSK.*
WPA GTK Rekey Interval (secs)	Specifies how often (in seconds) to renegotiate the Group Temporal Key • Default: 300 • Valid range: 1–99999 *Note: This field appears only if WPA Key Management type is WPA-PSK.*
WPA GMK Rekey Interval (secs)	Specifies how often (in seconds) to renegotiate the Group Master Key. • Default: 86400 • Valid range: 1–99999 *Note: This field appears only if WPA Key Management type is WPA-PSK.*

Table 16-4: LAN > Access Points > Configure screen fields (Continued)

Field	Description
Enable 802.1x	Select to enable 802.1x network access control and display the configuration fields. *Note: This field appears only if WPA Key Management type is WPA-EAP.*
Enable Cisco Legacy 802.1x Compatibility	Select to enable for systems that use lower case MAC addresses in the calling station ID field. This is recommended for interoperability with the Cisco RADIUS implementation. *Note: This field appears only if Enable 802.1x is selected.*
Primary 802.1x Retry Interval (secs)	Number of seconds the system waits after the primary authentication server has failed over to the secondary server before trying to reconnect to the primary server. • Default: 300 (5 minutes) *Note: The system sends to the secondary only if the primary fails.* *Note: This field appears only if Enable 802.1x is selected.*
Interim 802.1x Accounting Interval (secs, 0 to disable)	Number of seconds that the system waits between submissions of interim accounting data. • 0—Disable • 1 or higher—Wait this number of seconds between submissions • Default: 300 (5 minutes) *Note: Data transmits automatically when a login session starts and stops.* *Note: This field appears only if Enable 802.1x is selected.*
Enable EAP Re-authentication Period	Select to force system to periodically renegotiate connection credentials. • Selected—System automatically re-authenticates (renegotiates connection credentials) after the EAP Re-authentication Period. • Not selected—Full re-keying is required each time the MG90 moves into the area served by a different authenticator.) *Note: This field appears only if Enable 802.1x is selected.*
EAP Re-authentication Period (secs)	Number of seconds between authentications (if Enable EAP Re-authentication Period is selected) • Default: 3600 (60 minutes) *Note: Use a long re-authentication period (e.g. the default period—3600 seconds) to delay the need to re-authenticate when a WAN connection is interrupted.* *Note: This field appears only if Enable 802.1x is selected.*
802.1x Authentication Servers (These fields only appear if Enable 802.1x is selected.)	
Note: At least one authentication server must be enabled.	
Primary (To access these fields, select Enabled.)	
Address	IP address or host name of the primary RADIUS authentication server.
Port	Port number used to access the authentication server.
Secret	Shared secret code required to access the authentication server from the MG90. If the shared secret is incorrect, the server ignores authentication requests.

Table 16-4: LAN > Access Points > Configure screen fields (Continued)

Field	Description
Enabled	Select to enable access to the primary authentication server.
Secondary (To access these fields, select Enabled.)	
Address	IP address or host name of the secondary RADIUS authentication server.
Port	Port number used to access the authentication server.
Secret	Shared secret code required to access the authentication server from the MG90. If the shared secret is incorrect, the server ignores authentication requests.
Enabled	Select to enable access to the secondary authentication server. *Note: The secondary server is used only if the primary is not enabled, or the primary fails.*
802.1x Accounting Servers (These fields only appear if Enable 802.1x is selected.)	
Note: Accounting servers are optional.	
Primary (To access these fields, select Enabled.)	
Address	IP address or host name of the primary RADIUS accounting server.
Port	Port number used to access the accounting server.
Secret	Shared secret code required to access the accounting server from the MG90. If the shared secret is incorrect, the server ignores accounting requests.
Enabled	Select to enable access to the primary accounting server.
Secondary (To access these fields, select Enabled.)	
Address	IP address or host name of the secondary RADIUS accounting server.
Port	Port number used to access the accounting server.
Secret	Shared secret code required to access the accounting server from the MG90. If the shared secret is incorrect, the server ignores accounting requests.
Enabled	Select to enable access to the secondary authentication server. *Note: The secondary server is used only if the primary is not enabled, or the primary fails.*
Virtual BSSIDs	
Up to three virtual BSSIDs (Basic SSIDs) can be configured for a particular access point (AP). This means that the AP can appear to clients as up to four different APs, each with its own SSID and security configuration.	
Virtual BSSID 1	
Enable	Select to make this virtual BSSID available, using the configuration settings below.
Show/Hide (button)	Click to show/hide the configuration Virtual BSSID's configuration fields.

Table 16-4: LAN > Access Points > Configure screen fields (Continued)

Field	Description
Auto SSID	Automatically generate the SSID: • Selected—Set the SSID to the primary SSID followed by an underscore and a digit (e.g. <primarySSID>_1 is used for Virtual BSSID 1). • Not selected—SSID field is set manually.
SSID	Basic Service Set Identifier The identifier that appears to a device when it scans for access points. *Note: This field is accessible only if Auto SSID is not selected.*
Broadcast SSID	Broadcast the SSID • Selected—Devices will see the SSID when scanning for access points. • Not selected—SSID is not visible to devices scanning for access points. • Default: Selected
Captive Portal	Captive portal that users must connect through when using the access point. Only one portal can be selected at any time. • No portal selected—Access point is not restricted by a captive portal • Portal selected—Wi-Fi access is controlled by the captive portal as defined in LAN > Captive Portal > Configure on page 127. • "not defined"—No portals are defined in LAN > Captive Portal > Configure on page 127. *Note: Captive Portal support requires that only one Wi-Fi module is configured as an access point.*
Enable WMM	WMM (Wireless MultiMedia extensions) support Make sure that this value is always selected.
Enable AP Isolation	Access Point Isolation • Selected—Clients on the access point cannot access each other. • Not selected—Clients on the access point can access each other.

Table 16-4: LAN > Access Points > Configure screen fields (Continued)

Field	Description

MAC Access Control List	Enable or disable MAC access control (whitelist or blacklist) of devices attempting to connect to the access point. (Also known as 'MAC filtering.)
	• DISABLED (default)—Disable MAC address filtering.
	• ACCEPT—"Whitelist" mode. Only devices whose MAC addresses are in the whitelist file (described below) can connect to the access point.
	• DENY—"Blacklist" mode. Devices whose MAC addresses are in the blacklist file (described below) are not allowed to connect to the access point.
	The whitelist and blacklist files should be created as described below, and issued to devices via the AMM.
	File requirements:
	• Whitelist location: /opt/inmotiontechnology/config/global.accept.txt
	Blacklist location: /opt/inmotiontechnology/config/global.deny.txt
	• Plain ASCII text
	• Comment lines may be used and will start with the octothorpe (#) character
	• Blank lines are permitted
	• MAC addresses:
	• One address per line
	• Format: hh:hh:hh:hh:hh:hh (Six pairs of hexadecimal digits)
	• Lines with malformed addresses are ignored. When a malformed address is encountered, it is logged in /opt/inmotiontechnology/logs/YYYY-MM-DDlan.log.
	Example (blacklist shown, whitelist uses identical format):
	`# List of MAC addresses that are not allowed to authenticate (IEEE 802.11) with the AP.`
	`00:20:30:40:50:60`
	`00:ab:cd:ef:12:34`
	`00:00:30:40:50:60`

Encryption	Encryption type used by the access point Depending on the encryption type, various configuration fields will appear. • None—Access point is unsecured. • WEP—Secure access via WEP • WPA/TKIP—Secure access via WPA/TKIP • WPA2/CCMP—Secure access via WPA2/CCMP
Virtual BSSID 2	Same fields as Virtual BSSID 1
Virtual BSSID 3	Same fields as Virtual BSSID 2

LAN > LAN Segments

This screen is used to assign LAN-capable devices to LAN segments.

For details on LAN segmentation, see Configuring LAN Segments on page 53.

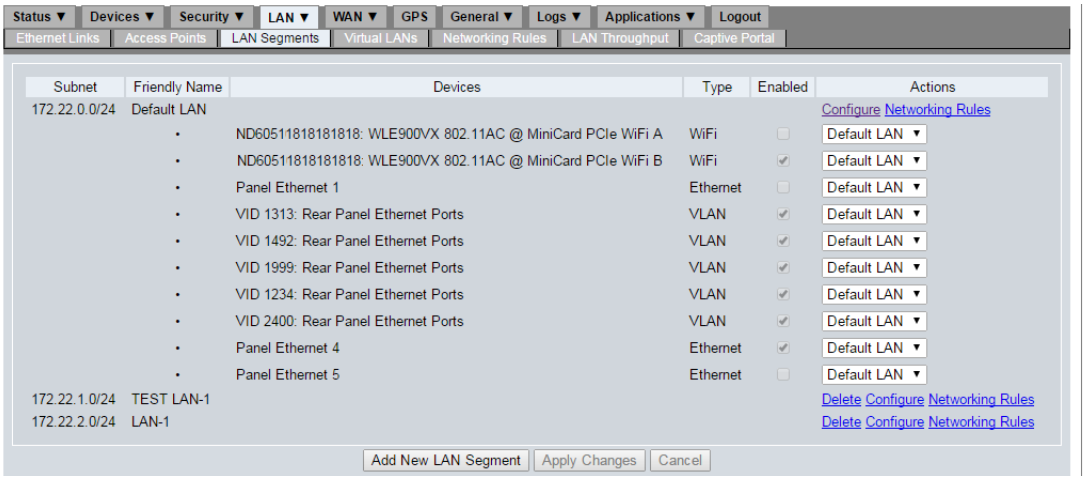

Figure 16-5: LCI: LAN > LAN Segments—Sample screen

Table 16-5: LAN > LAN Segments screen fields/buttons

Field	Description
Subnet	LAN segment address subnet
Friendly Name	Descriptive name for the LAN segment.
Devices	Descriptive names of devices that are associated with each LAN segment • Wi-Fi devices—Combination of the device's SSID and Friendly Name. • Ethernet devices—The device's Friendly Name. • Virtual LANs—VID number.
Type	Device type • Ethernet—Pre-installed Ethernet port • VLAN—Virtual LAN on an Ethernet port • Wi-Fi—Wi-Fi radio

Table 16-5: LAN > LAN Segments screen fields/buttons (Continued)

Field	Description
Enabled	Device enabled state • Selected—The device is currently enabled for LAN usage. • Not selected—The device is not currently enabled for LAN usage, or is not currently installed in the MG90. To enable the device for LAN use, see Devices > Cellular on page 93, Devices > Ethernet on page 94, or VLAN Configuration (LAN > Virtual LANs) on page 118.
Actions	Click these optional links to perform actions on the associated LAN segments: • Delete—Delete the associated LAN segment. (This option is not available for the default LAN segment.) • Configure—Configure the associated LAN segment. See LAN Segment Configuration (LAN > LAN Segments > Configure) on page 116 for details. • Networking Rules—Create networking rules (access granting, access blocking, QoS prioritizing) for the associated LAN segment. See LAN > Networking Rules, and LAN > LAN Segments > Networking Rules on page 119 for details. • Pull downs for devices—When the screen displays, all devices will show their associated LAN segment in the pull-down. To move a device from one segment to another: a. Select the desired segment from the pull-down. b. Click Apply Changes. *Note: Each device that can be enabled on a LAN segment is linked to a specific segment. If you delete a segment, the devices that were associated with it switch automatically to the Default LAN segment.*

LAN Segment Configuration (LAN > LAN Segments > Configure)

This screen is used to configure a LAN segment.

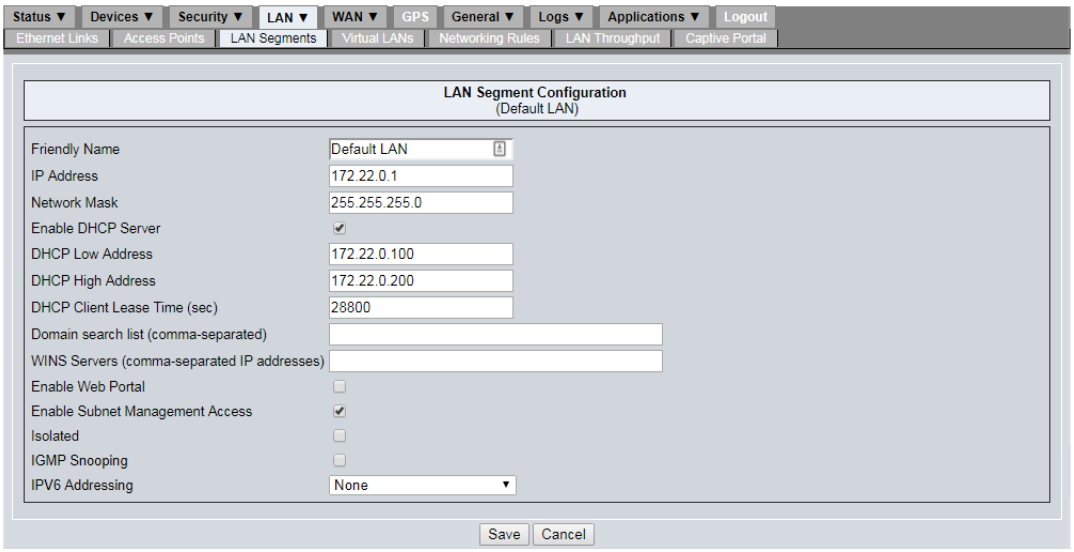

Figure 16-6: LCI: LAN > LAN Segments > Configure—Sample screen

Table 16-6: LAN > LAN Segments > Configure screen fields

Field	Description
Friendly Name	Enter a descriptive name for the LAN segment. This name identifies the segment in other LCI screens.
IP Address	IP address of the LAN bridge
Network Mask	Network mask of the LAN bridge Recommendation: Limit this network to a class C or smaller network. (e.g. “255.255.255.0” is the netmask for a class C (/24) network).
Enable DHCP Server	DHCP Server state • Selected—DHCP enabled • Not selected—DHCP disabled.
DHCP Low Address	Enter the starting IP address of the address pool used for DHCP.
DHCP High Address	Enter the ending IP address of the address pool used for DHCP.
DHCP Client Lease Time (sec)	Number of seconds that the IP address assigned from the address pool will be valid for the client
Domain search list (comma-separated)	List of domain name servers (DNS) to be used by the client • One or more DNS server addresses, comma-separated • IPv4 address format (e.g. xxx.xxx.xxx.xxx) or FQDN
WINS Servers (comma-separated IP addresses)	List of Windows Internet Name Service (WINS) servers to be used by the client • One or more WINS server addresses, separated by commas • IPv4 address format (e.g. xxx.xxx.xxx.xxx) or FQDN
Enable Web Portal	Web portal state If the web portal feature is enabled, the MG90 can be used as a web port for clients accessing the Internet. When a client accesses the MG90’s Wi-Fi network, the client must use a browser to view and agree to terms and conditions on a splash page before continuing. • Selected—Enabled. Clients will see the web portal splash page • Not selected—Disabled. Clients can access the Wi-Fi network without going through the portal. The web portal UI consists of customizable HTML and image files. Some configuration options are available in Applications > Web Portal.
Enable Subnet Management Access	Subnet Management state • Selected—MG90 management functions (e.g. LCI, SSH, command line) can be blocked, while allowing clients to access required resources (e.g. DNS, proxy) • Not selected—MG90 management functions cannot be blocked.
Isolated	LAN segment isolation • Selected—Segment is isolated (other segments cannot see it, but the isolated segment can still see other segments) • Not selected—Segment is not isolated (can be seen by other segments)

Table 16-6: LAN > LAN Segments > Configure screen fields (Continued)

Field	Description
IGMP Snooping	Enable/disable IGMP (Internet Group Management Protocol) snooping • Not selected—(Default) IGMP snooping disabled. • Selected—IGMP snooping enabled.
IPV6 Addressing	IPv6 Address support • None—IPv6 addresses not used • Unique Local Addressing—IPv6 equivalent of IPv4 private addresses. Address is unique and routable within a site, but is not globally routable. • WAN Prefix Pass through—Globally routable IPv6 address that uses the carrier prefix and appends the MAC address interface. *Note: If Enable IPV6 is not selected in WAN > Links > Configure (Cellular), then this option is ignored.*

VLAN Configuration (LAN > Virtual LANs)

In the Virtual LANs tab, you can configure and enable Ethernet ports for use as Virtual LANs.

Virtual LANs (VLAN) can be used when devices inside the vehicle require VLAN tagging for their operation, or when the vehicle LAN has a switch with VLAN tagging enabled. If a vehicle has VLANs configured, or requires additional Ethernet ports, they can be added by using a switch and VLAN tagging.

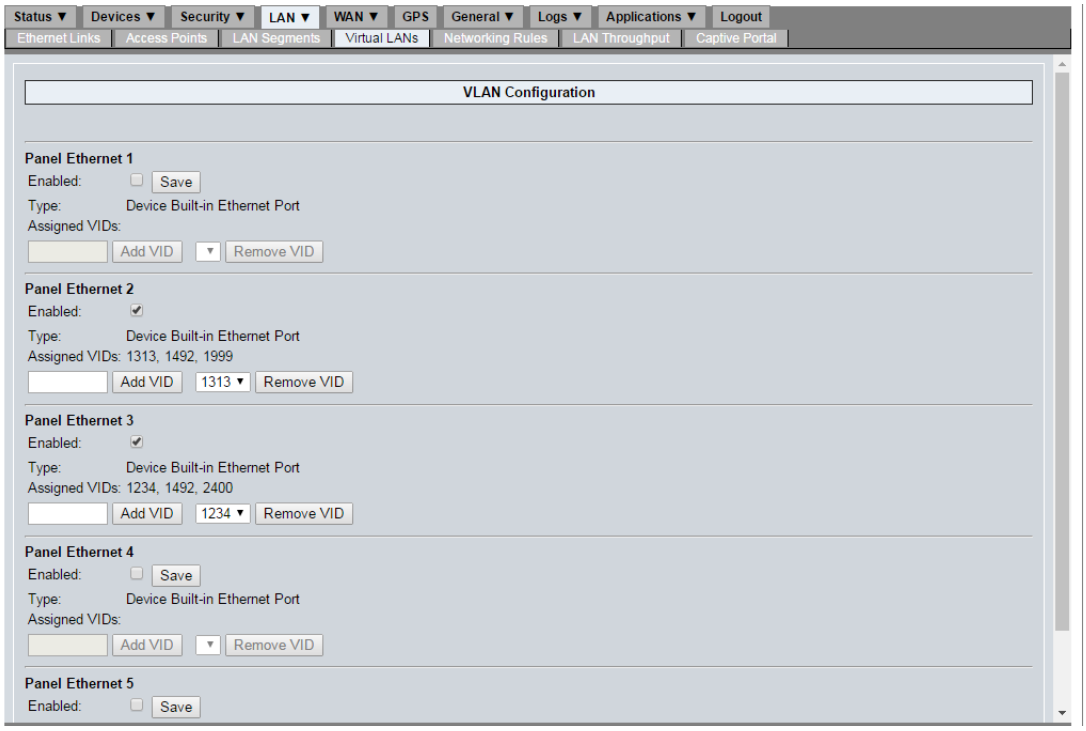

Figure 16-7: LCI: LAN > Virtual LANS—Sample screen

Table 16-7: LAN > Virtual LANs screen fields

Field	Description
Panel Ethernet 1	
Enabled	Select to use the device as a virtual LAN. • Selected—Device is used as a virtual LAN. • Not selected—Device is not used as a virtual LAN. *Note: To add or remove VIDs, select Enabled to make the Add VID and Remove VID buttons available.*
Type	Device type
Assigned VIDs	List of VIDs currently assigned to the VLAN
Add VID (button)	Enter a new VID and click to add it to the associated VLAN. • Valid range: 2–4094 • Valid range 2–4094.
Remove VID (button)	Enter one of the Assigned VIDs to remove and click to remove it from the associated VLAN.
Panel Ethernet 2 (Same options as Panel Ethernet 1)	
Panel Ethernet 3 (Same options as Panel Ethernet 1)	
Panel Ethernet 4 (Same options as Panel Ethernet 1)	
Panel Ethernet 5 (Same options as Panel Ethernet 1)	

LAN > Networking Rules, and LAN > LAN Segments > Networking Rules

The LAN Networking Rules tab is used to defined ‘global’ networking rules that apply to all LAN connections, and ‘segment’ networking rules that apply only to connections on specific LAN segments. These rules include:

- Access Blocking
- Access Granting
- QoS Prioritizing

Note: There are three ‘levels’ of networking rules—LAN segment, WAN link, and Global (LAN). If there is a conflict between any of these rules, LAN segment rules override WAN link and global rules, and WAN link rules override global rules.

Note: The LAN Networking Rules and WAN Networking Rules use similar setup parameters. For WAN networking rules, see WAN > Networking Rules on page 179.

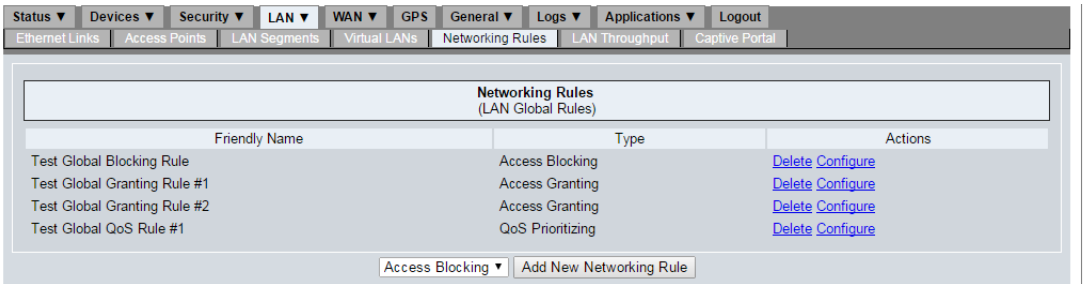

Figure 16-8: LCI: LAN > Networking Rules—Sample screen

Table 16-8: LAN > Networking Rules screen fields

Field	Description
Friendly Name	Descriptive name for the networking rule
Type	Rule type: • Access Blocking—Block incoming or outgoing traffic. See Access Blocking Rules on page 120. • Access Granting—Permit incoming or outgoing traffic. See Access Granting Rules on page 122. • QoS Prioritizing—Assign traffic priority. See QoS Priority Rules on page 123.
Actions	Click these optional links to perform actions on the associated rules: • Delete—Delete the associated networking rule. (This option is not available for the default LAN segment.) • Configure—Configure the associated networking rule.
Add New Networking Rule	From the drop-down, select the type of rule to add to the LAN segment, and click Add New Networking Rule. For usage details, see Setting up the LAN Firewall on page 56.

Access Blocking Rules

Add an Access Blocking rule to block incoming or outgoing traffic (from the MG90's perspective) for a specific IP address, based on the criteria in Table 16-9 on page 121.

Tip: *Fields that are left blank are treated as "wildcards". Limit the use of wildcards (fill fields with appropriate values) to make sure your rule works as intended.*

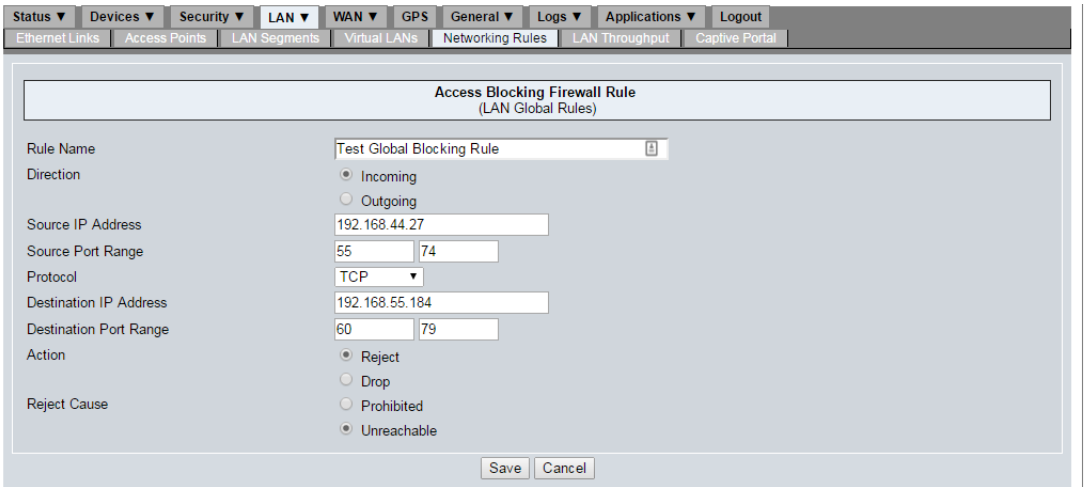

Figure 16-9: LCI: LAN > Networking Rules > Add Rule (Access Blocking)—Sample screen

Table 16-9: LAN > Networking Rules > Add Rule (Access Blocking) screen fields

Field	Description
Rule Name	Descriptive name for the networking rule
Direction	Traffic direction relative to the MG90 • Incoming—The Source IP Address will be blocked. • Outgoing—The Destination IP Address will be blocked.

Source IP Address	Source IP address
	• Format: xxx.xxx.xxx.xxx[/xx]
	• Examples:
	  • Address without netmask—192.168.4.17. Applies to the stated IP address.
	  • Address with netmask—192.168.4.0/24. Applies to the IP address range 192.168.4.0–192.168.4.255.

Source Port Range	Starting and ending source port numbers • Valid values: 0–65535 • Start port must be less than or equal to the end port
Protocol	Communications protocol • TCP • UDP • TCP/UDP • ICMP (Internet Control Message Protocol)
Destination IP Address	Destination IP address • Format: xxx.xxx.xxx.xxx[/xx]
Destination Port Range	Starting and ending source port numbers • Valid values: 0–65535 • Start port must be less than or equal to the end port

Table 16-9: LAN > Networking Rules > Add Rule (Access Blocking) screen fields

Field	Description
Action	Action to take when traffic matches the rule's specifications: • Reject—Send the Reject Cause to the sender. • Drop—Drop the traffic packets without notice. *Note: The 'Drop' rule is useful when attempting to prevent hacking.*
Reject Cause	Reason that user receives when Action is set to 'Reject' • Prohibited—Inform user that site is banned. • Unreachable—Inform user that site is unreachable.

Access Granting Rules

Add an Access Granting rule to permit incoming or outgoing traffic (from the MG90's perspective) for a specific IP address, based on the criteria in Table 16-10 on page 122.

Tip: *Fields that are left blank are treated as "wildcards". Limit the use of wildcards (fill fields with appropriate values) to make sure your rule works as intended.*

Note: By default, all ports (except ports 22 and 2222 (SSH) to the MG90 from the WAN side are blocked. Access granting rules will not open additional ports to the MG90 but are designed to act as exceptions to access blocking rules.

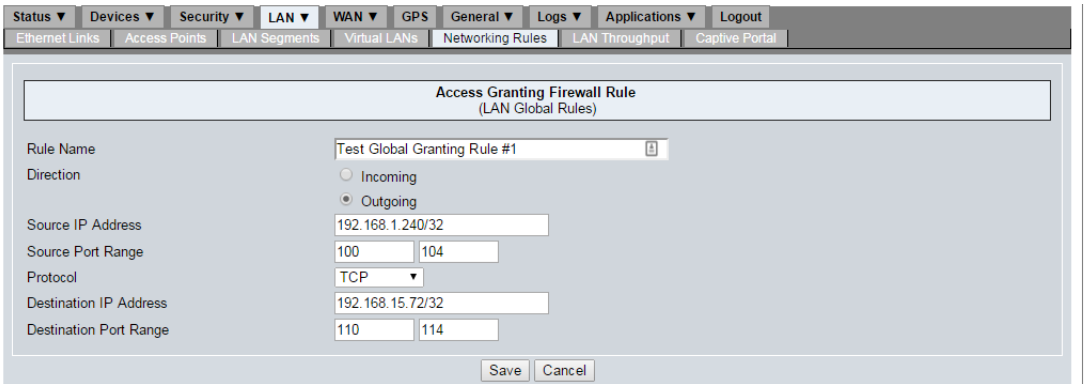

Figure 16-10: LCI: LAN > Networking Rules > Add Rule (Access Granting)—Sample screen

Table 16-10: LAN > Networking Rules > Add Rule (Access Granting) screen fields

Field	Description
Rule Name	Descriptive name for the networking rule.
Direction	Traffic direction relative to the MG90 • Incoming—The Source IP Address will be blocked. • Outgoing—The Destination IP Address will be blocked.

Table 16-10: LAN > Networking Rules > Add Rule (Access Granting) screen fields

Field	Description

Source IP Address	Source IP address
	• Format: [!]xxx.xxx.xxx.xxx[/xx]
	Note: The optional '!' means "anything other than this address (or range)".
	• Examples:
	  • Address without netmask—192.168.4.17. Applies to the stated IP address.
	  • Address with netmask—192.168.4.0/24. Applies to the IP address range 192.168.4.0–192.168.4.255.

Source Port Range	Starting and ending source port numbers • Valid values: 0–65535 • Start port must be less than or equal to the end port
Protocol	Communications protocol • TCP • UDP • TCP/UDP • ICMP (Internet Control Message Protocol)
Destination IP Address	Destination IP address • Format: [!]xxx.xxx.xxx.xxx[/xx] Note: The optional '!' means "anything other than this address (or range)".
Destination Port Range	Starting and ending source port numbers • Valid values: 0–65535 • Start port must be less than or equal to the end port

QoS Priority Rules

Add QoS Priority rules to various applications used by the customer and guarantee a certain level of performance to data flow.

Tip: *Fields that are left blank are treated as "wildcards". Limit the use of wildcards (fill fields with appropriate values) to make sure your rule works as intended.*

For applications that do not have a predetermined destination IP address such as Voice-over-IP, using the Source IP Address and Source Port is supported.

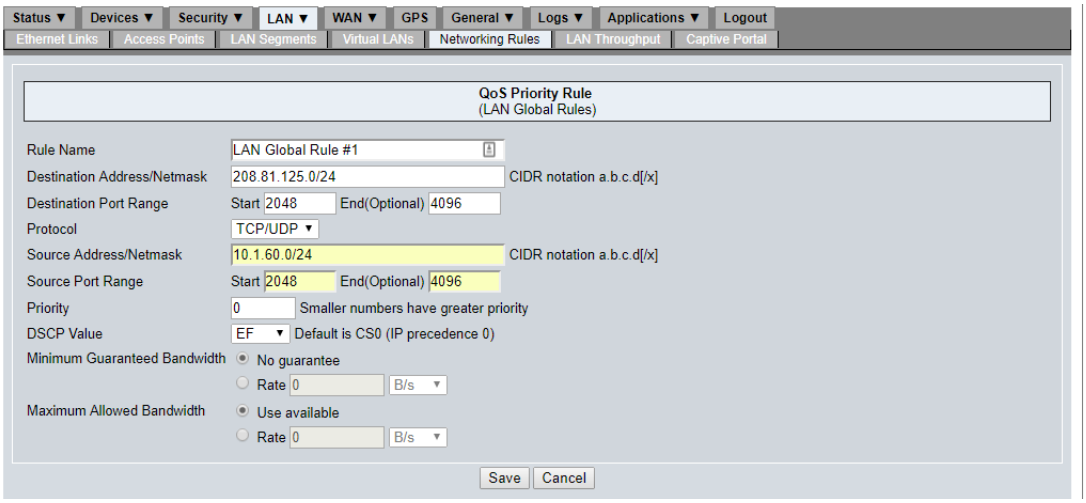

Figure 16-11: LCI: LAN > Networking Rules > Add Rule (QoS Prioritizing)—Sample screen

Table 16-11: LAN > Networking Rules > Add Rule (QoS Prioritizing) screen fields

Field	Description
Rule Name	Descriptive name for the networking rule
Destination Address/Netmask	Application server IP address • Format: [!]xxx.xxx.xxx.xxx[/xx] (CIDR notation) Note: The optional '!' means "anything other than this address (or range)". • Leaving this field blank gives priority to all traffic on this port, based on existing firewall rules.
Destination Port Range	Destination port number (For TCP, UDP, TCP/UDP Protocols) • Single port used for data transport (Start), or range of ports (Start/End) • End port is Optional • Valid values: 0–65535 *Note: This field is available only if Protocol type is TCP, UDP, or TCP/UDP.*
Protocol	Data transport protocol • ALL • TCP/UDP • TCP • UDP • ICMP
Source Address/ Netmask	Source IP address (used for applications that do not have a predetermined IP address (e.g. VoIP) • Format: [!]xxx.xxx.xxx.xxx[/xx] (CIDR notation) Note: The optional '!' means "anything other than this address (or range)".

Table 16-11: LAN > Networking Rules > Add Rule (QoS Prioritizing) screen fields

Field	Description
Source Port Range	Source port number (used for applications that do not have a predetermined IP address (e.g. VoIP) • Single port used for data transport (Start), or range of ports (Start/End) • End port is Optional • Valid values: 0–65535 *Note: This field is available only if Protocol type is TCP, UDP, or TCP/UDP.*
Priority	Traffic priority Traffic to the WAN in the specified port and destination IP address is prioritized using this value. • Format: Integer • Minimum value: 0 (Highest priority) • Higher values are lower priority
DSCP Value	DSCP (Differentiated Services Code Point), also known as PNTM[a] (Private Network Traffic Management) for Verizon • Select appropriate DSCP value from list. For DSCP details, refer to RFC 2597 and RFC 3260. • Values in the list are sorted from lowest priority (CS0) to highest priority (EF). • Value is used to prioritize traffic for end-to-end QOS across all devices in the path (if DSCP is supported).
Minimum Guaranteed Bandwidth	Minimum data transfer rate • No guarantee—No minimum data transfer rate. (Default) • Rate—Specify the minimum data rate (including the transfer unit) that should be provided *Note: If minimum bandwidth is specified for some rules, consider adding it to all rules. When the sum of the minimum guaranteed bandwidths for all transmissions is greater than the available bandwidth, transmissions with no guarantee will be stalled.*
Maximum Allowed Bandwidth	Maximum data transfer rate • Use available—No maximum data rate. (Default) • Rate—Specify the maximum data rate (including the transfer unit) that can be used. The maximum allowed bandwidth is used to ensure that traffic matching the condition specified by the rule does not exceed this bandwidth.

a. Pending Verizon PNTM certification.

LAN > LAN Throughput

The LAN Throughput tab is used to configure throughput event reporting for specific ports. These event reports are sent to AMM, which then uses them for various reports.

A throughput report event is generated when:
- The throughput Threshold has been reached and the Minimum Report Interval has elapsed
- The Maximum Report Interval has elapsed

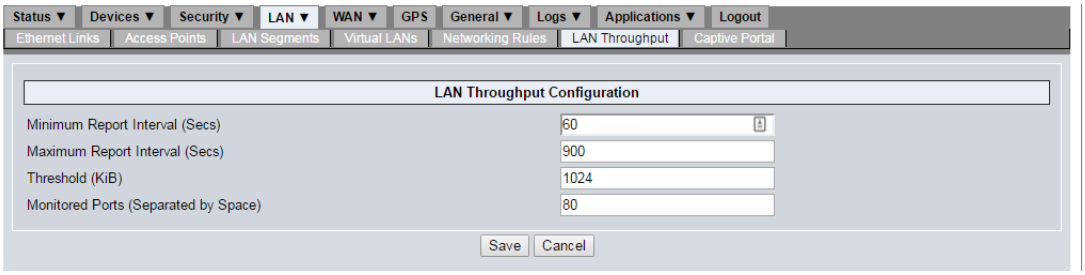

Figure 16-12: LCI: LAN > LAN Throughput—Sample screen

Table 16-12: LAN > LAN Throughput screen fields

Field	Description
Minimum Report Interval (Secs)	Minimum time between throughput report events Reports are not generated more often than this value. • Default: 60 seconds (1 minute)
Maximum Report Interval (Secs)	Maximum time between throughput report events A report will be generated after this interval even if the throughput Threshold limit has not been reached. • Default: 900 seconds (15 minutes)
Threshold (KiB)	Throughput report event threshold Throughput report event is generated when this threshold has been reached **and** the Minimum Report Interval has passed. • Default: 1024 KiB (1 MB)
Monitored Ports (Separated by Space)	Ports being monitored for throughput Throughput on the listed ports is monitored and reported based on the other throughput configuration fields. • Default port: 80 • Multiple ports must be separated by spaces

LAN > Captive Portal

The Captive Portal tab lists all defined captive portals. For a description of the Captive Portal feature, see Setting up Captive Portals on page 57.

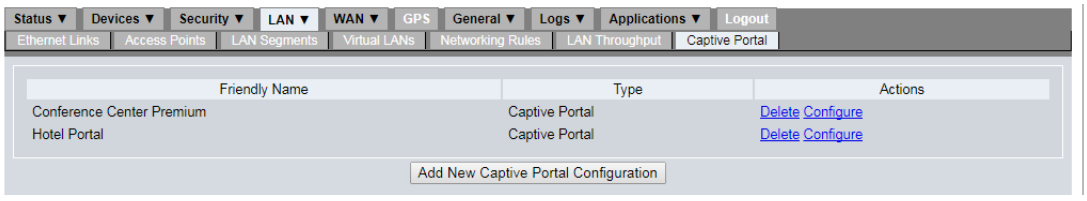

Figure 16-13: LCI: LAN > Captive Portal—Sample screen

Table 16-13: LAN > Captive Portal screen fields

Field	Description
Friendly Name	Descriptive name for the captive portal. To change the description, see LAN > Captive Portal > Configure on page 127.
Type	"Captive Portal" (No other value will appear)
Actions	Click these optional links to perform actions on the associated captive portal: • Delete—Delete the associated captive portal. • Configure—Click to configure the captive portal. See LAN > Captive Portal > Configure on page 127.

LAN > Captive Portal > Configure

The Captive Portal Configuration screen is used to configure and enable/disable a captive portal hotspot ("walled garden"). A Wi-Fi module on the MG90 that has been set up as an access point can be configured (if desired) to use any one of the defined captive portals.

Captive Portal support requires that only one Wi-Fi module is configured as an access point.

Captive portals can be hosted by an external portal server, or by the MG90 using its built-in 'miniportal'.

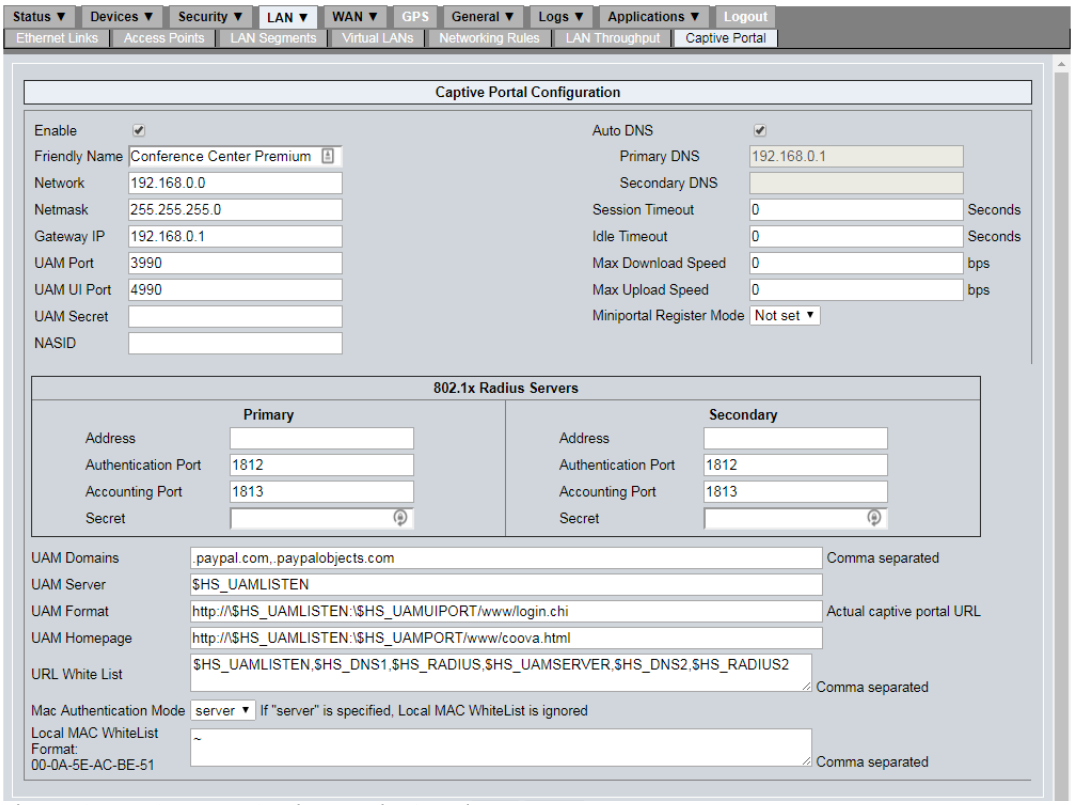

Figure 16-14: LCI: LAN > Captive Portal—Sample screen

Table 16-14: LAN > Captive Portal screen fields

Field	Description
Enable	Enable/disable this Captive Portal When a user connects to an access point associated with this portal (LAN > Access Points on page 105), if this option is: • Selected—The captive portal is enabled, and users are automatically directed through it. • Not selected—The captive portal is disabled, and users connect directly to the WAN.
Friendly Name	Descriptive name that identifies the portal in LAN > Access Points.
Network	Internal IP address of the captive portal on the MG90. Example: 192.168.0.0 *Note: Internally, this value is assigned to the variable $HS_UAMLISTEN.*
Netmask	Netmask that defines the LAN segment based on the Network Example: 255.255.255.0 is a "/24" netmask. If the Network field is 192.168.0.0 and the Gateway IP is 192.168.0.1, devices connecting to the captive portal will be assigned addresses in the range 192.168.0.2 – 192.168.0.255.
Gateway IP	Captive portal's IP address on subscriber network. The address is limited to a value in the range defined by the Network and Netmask. Example: If Network is 192.168.0.0 and Netmask is 255.255.255.0, the Gateway IP must be in the range 192.168.0.1 through 192.168.0.255.
UAM Port	Captive portal's UAM (Universal Access Mode) port on subscriber network. Use the default value (3990) unless otherwise instructed.
UAM UI Port	Captive portal's UAM "UI" port on subscriber network, for embedded portal. Use the default value (4990) unless otherwise instructed.
UAM Secret	(External portals only) Password assigned by the external portal server that hosts the captive portal.
NASID	(External portals only) Unique value assigned to the MG90 by the external portal server to identify the device to backend systems.
Auto DNS	DNS (Domain Name Server) used for the captive portal • Selected—MG90's DNS is used. (Primary DNS and Secondary DNS fields are ignored.) • Not selected—External DNS server is used.
Primary DNS	IP address of preferred DNS server to use *Note: This field is available only if Auto DNS is selected.*
Secondary DNS	IP address of alternate DNS server to use if Primary DNS is unavailable *Note: This field is available only if Auto DNS is selected.*
Session Timeout	Maximum time a session can stay open before automatically ending • 0—No time limit • ≥1—Session times out after this many seconds

Table 16-14: LAN > Captive Portal screen fields (Continued)

Field	Description
Idle Timeout	Maximum time a session can remain idle before automatically ending • 0—No time limit • ≥1—Session times out after being idle for this many seconds
Max Download Speed	Maximum download speed • 0—No limit (can use all available bandwidth) • ≥1—Maximum download speed in bits per second
Max Upload Speed	Maximum upload speed • 0—No limit (can use all available bandwidth) • ≥1—Maximum upload speed in bits per second
Miniportal Register Mode	Captive Portal provider • Not set—Use an external portal server • self—Use the MG90's built-in 'miniportal' server
802.1x Radius Servers RADIUS (Remote Authentication Dial-In User Service) servers used to authenticate and authorize users who attempt to access the captive portal. If two servers are used, captive portal access can be authorized if one server becomes unavailable.	
Primary	
Address	IP address of the primary RADIUS authentication/accounting server
Authentication Port	Server port used for authentication. Use the default port (1812) unless instructed otherwise.
Accounting Port	Server port used for accounting. Use the default port (1813) unless instructed otherwise.
Secret	Shared secret code required to access the RADIUS server from the MG90. If the shared secret is incorrect, the server ignores authentication requests.
Secondary	
Address	IP address of the secondary authentication/accounting server
Authentication Port	Server port used for authentication. Use the default port (1812) unless instructed otherwise.
Accounting Port	Server port used for accounting. Use the default port (1813) unless instructed otherwise.
Secret	Shared secret code required to access the RADIUS server from the MG90. If the shared secret is incorrect, the server ignores authentication requests.
UAM Domains	Comma-separated list of domain names that can be accessed via the captive portal page before the user is approved. For example, if the captive portal has a paid tier of services, the user must be able to connect through to an appropriate payment site. If the payment site is not in this list, the portal would prevent it from being accessed. Use the default list (.paypal.com,.paypalobjects.com) to allow users to pay for service using paypal, or add additional domains to use other services.

Table 16-14: LAN > Captive Portal screen fields (Continued)

Field	Description
UAM Server	Hostname of captive portal server Use the default value unless otherwise instructed.
UAM Format	URL of captive portal Use the default value unless otherwise instructed.
UAM Homepage	Captive portal main page (e.g. login page) Use the default value unless otherwise instructed.
URL White List	Comma-separated list of URLs that user can be redirected to by the captive portal server for authentication, accounting, for free (unauthenticated) access, etc. Some examples include: • RADIUS servers must be included (if used). • Corporate page (for example, the public site for a hotel chain that is providing the hotspot) Use the default value unless otherwise instructed.
Mac Authentication Mode	Enable/disable authentication of specific devices using their MAC addresses • off—Device MAC addresses are not used to authenticate users. • local—Local MAC Whitelist is enabled. • server—MAC authentication is provided by the RADIUS server to allow access by specific devices (the list is maintained on the server).The Local MAC Whitelist is ignored
Local MAC Whitelist Format: 00-0A-5E-AC-BE-51	Comma-separated list of MAC addresses of devices that are automatically authenticated to access the portal.

17: WAN Tab

This chapter describes the WAN tab, which is used to configure the MG90's WAN interfaces—cellular, Wi-Fi, Ethernet, and serial modem.

The WAN tab includes the following sub-tabs:

- Links—Configure the MG90's WAN-capable devices for WAN use. See WAN > Links on page 131.
- Monitors—Configure monitors to detect and recover from communication failures. See WAN > Monitors on page 156.
- VPNs— Configure VPNs to allow LAN devices connected to the MG90 to access an enterprise network and vice-versa. See WAN > VPNs on page 158.
- Wi-Fi Networks—Configure the MG90 to access specific Wi-Fi networks/access points. See WAN > Wi-Fi Networks on page 167.
- Networking Rules—Configure rules to block or permit specific devices on the WAN, to perform port forwarding, and to ensure quality of service. See WAN > Networking Rules on page 179.
- Recovery—Configure the MG90 to recover from dead WAN connections. See WAN > Recovery on page 185.
- SIM Configuration—Indicate which SIM slots to use for the LTE radios. See WAN > SIM Configuration on page 186.

WAN > Links

Each device that can be, or has been used as a WAN connection is called a WAN 'link'. This screen displays all WAN links and the available Actions for configuring them.

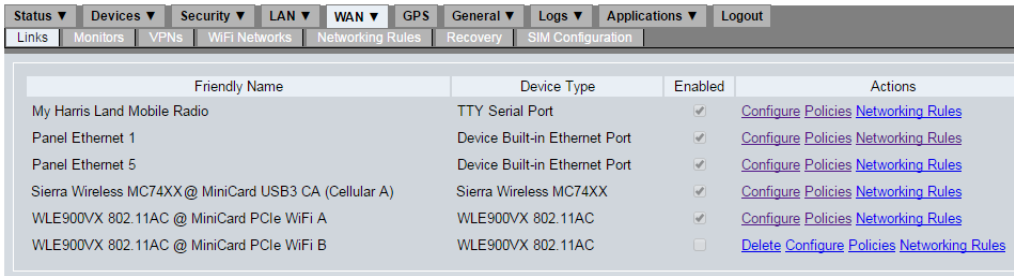

Figure 17-1: LCI: WAN > Links—Sample screen

Table 17-1: WAN > Links screen fields

Field	Description
Friendly Name	Descriptive device names defined in Devices tabs (Devices > Cellular, etc.)
Device Type	Hardware device type (cannot be modified)

Table 17-1: WAN > Links screen fields (Continued)

Field	Description
Enabled	Indicates whether the device is currently enabled as a WAN link: • Selected—Device is available and selected for WAN usage. • Not selected—Device is either currently assigned for LAN usage, idle, or has been removed from the MG90.
Actions	Click these optional links to perform actions on the associated WAN links: • Delete—Delete the associated WAN link (including its configuration details, policy assignments, and networking rules.). This option does not appear if the link is Enabled. *Caution: The link is deleted immediately. If you delete a link in error, you will have to re-enter any appropriate configurations, policies, and networking rules.* • Configure—Configure link-specific details (IP addresses, monitors, etc.). See WAN Link Configuration (WAN > Links > Configure) on page 132. • Policies—Configure link-specific policies used to determine which link is active. See WAN Link Policy Configuration (WAN> Links > Policies) on page 150. • Networking Rules—Create networking rules (access granting, access blocking, port forwarding, QoS prioritizing). See WAN > Networking Rules on page 179.

WAN Link Configuration (WAN > Links > Configure)

The WAN Link Configuration screen that appears when you click Configure in the WAN > Links screen depends on the associated WAN link type:

- Ethernet—See Ethernet WAN Link Configuration on page 133
- Cellular—See Cellular WAN Link Configuration on page 138
- Wi-Fi—See Wi-Fi WAN Link Configuration on page 143
- Serial modem—See Serial (modem) WAN Link Configuration on page 146

Note: Several options appear in more than one link type, but must be set independently.

Ethernet WAN Link Configuration

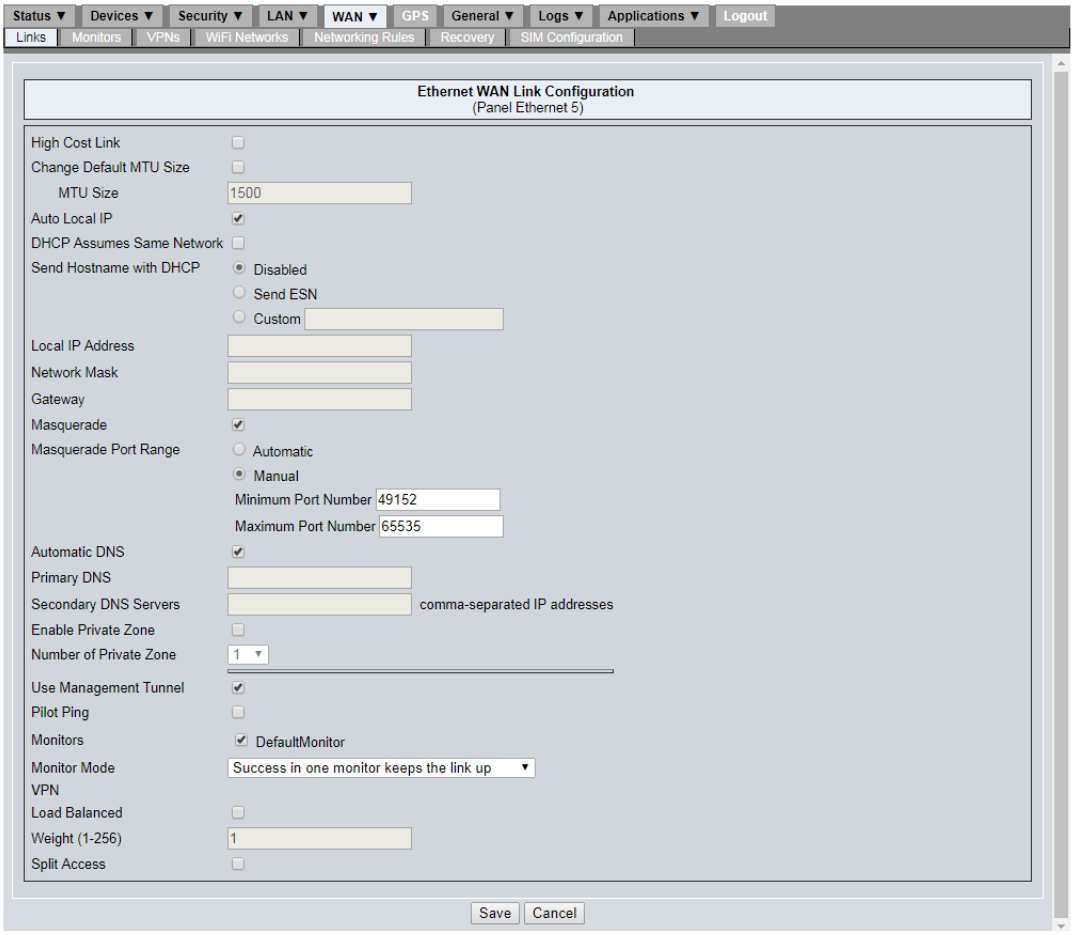

Figure 17-2: LCI: WAN > Links > Configure (Ethernet)—Sample screen

Table 17-2: WAN > Links > Configure (Ethernet) screen fields

Field	Description
High Cost Link	High Cost Link • Selected—High cost link. Transmission of management data (e.g. log files uploads, automatic software downloads, etc.) is limited, with most of the data being held until a low cost link is active. (Note: If required, you can allow Auto software updates and firmware updates over high cost links, by setting appropriate options. See Table 19-8, General > Auto Software Updates screen fields, on page 204 for details.) • Not selected—Not a high cost link. *Note: Ethernet links are typically not high cost, while cellular links would typically be high cost (depending on the data plan type).*
Change Default MTU Size	Use a different MTU Size than the default (1500 bytes) • Selected—MTU Size field can be edited. (Default) Deselect this checkbox to reset the MTU Size to the default value (the value resets when you click Save). • Not selected—MTU Size field cannot be edited. *Note: This may be required to accommodate some network configurations. Only change this value if instructed to by Sierra Wireless.*
MTU Size	Maximum Transmission Unit size (in bytes) • Valid range: 256–1500 • Default: 1500
Auto Local IP	Enable DHCP for this interface. • Selected—Enabled. The IP address will be assigned by a DHCP server connected to the access point network. • Not selected—Not enabled. Assign the Local IP Address, Network Mask, and Gateway manually.
DHCP Assumes Same Network	DHCP assignment when DHCP lease expires • Selected—Attempt to reconnect to same DHCP assignment when the lease expires. • Not selected—Gateway will request an IP address from a DHCP server in the available network when the lease expires. *Note: This field is available only if Auto Local IP is selected.*
Send Hostname with DHCP request	Enable/disable sending of MG90-identifying information with DHCP request • Disabled—Do not send identifying information • Send ESN—Send the MG90's ESN (Electronic Serial Number) • Custom—Send a custom hostname (for example, "Bus401") to identify the MG90 to the DHCP server. *Note: This field is available only if Auto Local IP is selected.*
Local IP Address	Statically-assigned Local IP Address • IPv4 address format (e.g. xxx.xxx.xxx.xxx) *Note: This field is available only if Auto Local IP is not selected.*

Table 17-2: WAN > Links > Configure (Ethernet) screen fields (Continued)

Field	Description
Network Mask	Network mask of the Local IP Address • IPv4 netmask format (e.g. xxx.xxx.xxx.xxx) *Note: This field is available only if Auto Local IP is not selected.*
Gateway	Default gateway to use for the Local IP Address • IPv4 address format (e.g. xxx.xxx.xxx.xxx) *Note: This field is available only if Auto Local IP is not selected.*
Masquerade	Network Address Translation for LAN-originated traffic leaving the MG90 WAN interface • Selected—Enabled. This is the typical setting. • Not selected—Disabled
Masquerade Port Range	Port range to use for masquerade (NAT) • Automatic—Enabled • Manual—Disabled (Default). This should be used in most cases to avoid using defined or reserved ports. *Note: This field is available only if Masquerade is selected.*

Minimum Port Number
Maximum Port Number
	Range of ports to use for masquerade (NAT)
	• Default range: 49152–65535
	• Valid range: 0–65535
	• If Minimum Port Number < 49152:
	  • traffic on ports lower than 512 is mapped to other ports lower than 512
	  • traffic on ports 512 to 1024 is mapped to ports lower than 1024
	  • traffic on ports greater than 1024 is mapped to ports greater than 1024
	Note: These fields are available only if Masquerade is selected and Masquerade Port Range is Manual.

Automatic DNS	DNS servers to be used • Selected—Use DNS servers specified by DHCP server. • Not selected—Use the DNS servers specified in Primary DNS or Secondary DNS. The fastest-responding server (regardless of whether named as Primary or Secondary) is chosen as the server to use. Periodically, the servers are re-evaluated to make sure the fastest-responding server is being used. If private DNS servers are used, set up DNS zones—see Configuring DNS Zones for Private DNS Server Use on page 67 for details. *Note: This must be disabled (not selected) if using a static IP address.*
Primary DNS	IP address of primary domain name server • Format: IPv4 address (xxx.xxx.xxx.xxx) • Required field (when Automatic DNS is not selected) *Note: This field is available only if Automatic DNS is not selected.*

Table 17-2: WAN > Links > Configure (Ethernet) screen fields (Continued)

Field	Description
Secondary DNS Servers	IP addresses of secondary domain name servers • Format: IPv4 addresses, comma-separated (e.g. xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy) • Optional field *Note: This field is available only if Automatic DNS is not selected.*
Enable Private Zone	Enables/disable DNS private zone use on this link. • Selected—Enabled. DNS private zones can be used on this link. • Not selected—Disabled. DNS private zones cannot be used on this link.
Number of Private Zone	Table of 1–10 private zone configuration entries
Private Zone <#>	Domain name to be resolved by the internal DNS server managing the private zone.
Private Zone IP <#>	IP address of the internal DNS server managing the private zone.
Use Management Tunnel	Management Tunnel usage The management tunnel is a dedicated secure VPN connection between the MG90 and the AMM. • Selected—AMM can access the MG90. (Default) • Not selected—Do not use the management tunnel. AMM cannot access the MG90. To configure the management tunnel, see WAN > VPNs > (Management Tunnel) > Configure on page 159.
Pilot Ping	Pilot ping • Selected—Enabled. Before a WAN link is identified as established, the MG90 attempts to pass ping traffic over the link. If the ping succeeds, the link is identified as established. If the ping fails, the link is not established. • Not selected—Disabled (Default). Ping traffic is not attempted, which could result in a WAN link being identified as established although it may not be able to pass traffic. *Note: After a WAN link has been established, ping monitors (next field) are used to monitor the link's connection.*
Monitors	Monitor(s) being used to monitor the link's connection state Select one or more monitors. • Factory-defined monitor—DefaultMonitor. This example should be replaced with your own monitor definition. To configure monitors, see WAN > Monitors > Configure on page 157.
Monitor Mode	Effect of selected monitors' state on link status • Success in one monitor keeps the link up— If at least one monitor is reporting as active, then the link should be considered 'up'. • Failure in one monitor declares the link down—If any one monitor is reporting as inactive, then the link should be considered 'down'. *Note: This field is meaningful only if one or more monitors are selected.*

Table 17-2: WAN > Links > Configure (Ethernet) screen fields (Continued)

Field	Description
VPN	VPNs that the WAN link can establish when the link is active • If multiple VPNs are selected, each must be LAN to LAN. To configure VPNs, see WAN > VPNs on page 158.
Load Balanced	Distribute traffic across active WAN links When load balancing is selected on two or more active WAN links, traffic can be distributed across these links (based on their Weight field values). • Selected—Distribute traffic across links, based on Weight field values. • Not selected—Do not load balance See Configuring Load Balancing on page 60 for usage.
Weight (1-256)	Load balancing 'weight' When load balancing is enabled on two or more links, their Weights are used to calculate the proportion of traffic each link will receive: Proportion (Link) = Weight (Link) / Total_Weight (All Links)) For example: Link A Weight = 50 Link B Weight = 100 Proportion (Link A) = 50 / (50+100) = 33.3% Proportion (Link B) = 100 / (50 + 100) = 66.7% Therefore, Link B will carry twice as many sessions as Link A. *Note: This field is available only if Load Balanced is selected.*
Split Access	Allow incoming session initiation on non-active connected link This allows an incoming session to initiate on a link even when the link is not the active (i.e. default route) link but is connected to the network. • Selected—Allowed • Not selected—Not allowed This is useful for test purposes on Ethernet links that have public IP addresses. It also enables applications such as live video look-in to an Ethernet interface even if the active connection is via another WAN (e.g. Wi-Fi). *Note: Users are encouraged to evaluate use of the Split Access feature from a security and system perspective prior to enabling. Depending on available links and routing rules, traffic may route from WAN to LAN or between WAN networks.*

Cellular WAN Link Configuration

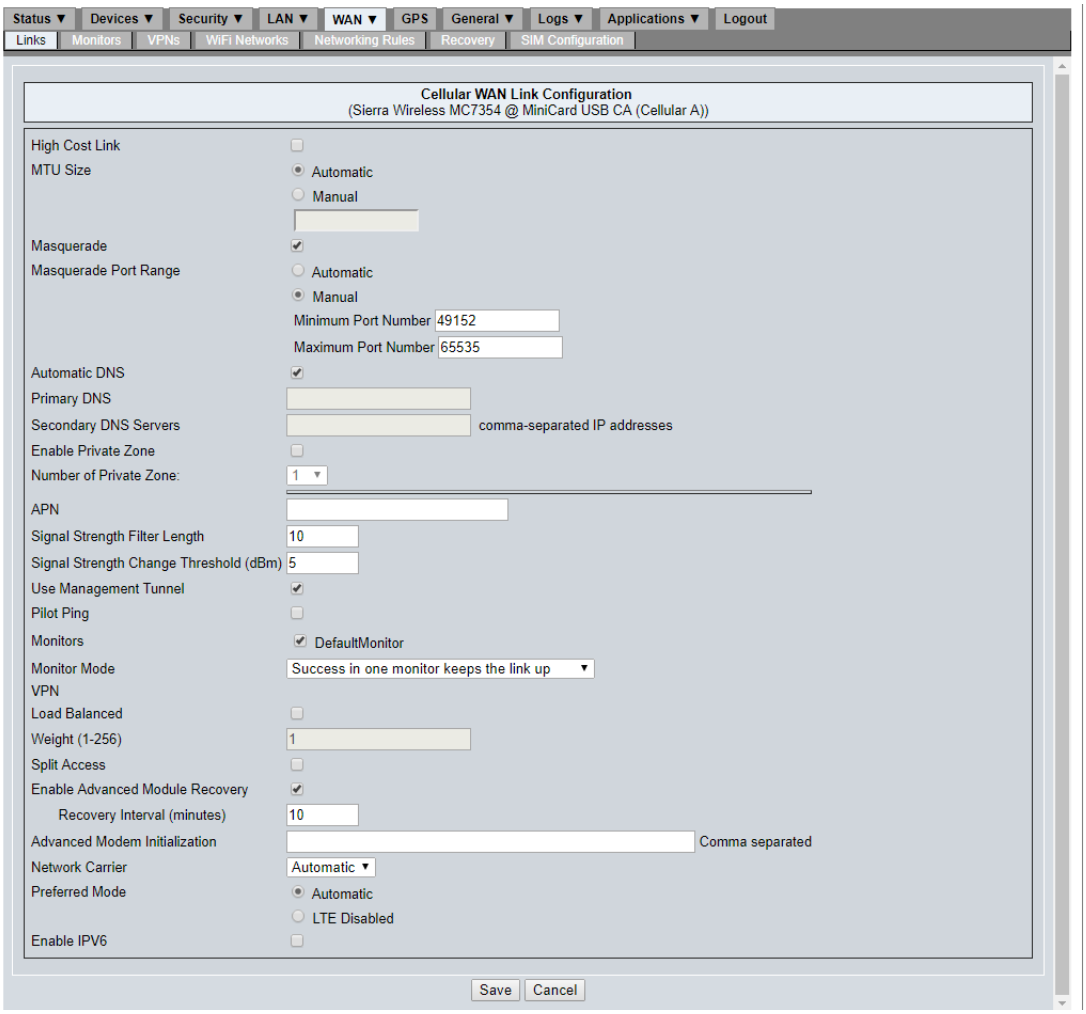

Figure 17-3: LCI: WAN > Links > Configure (Cellular)—Sample screen

Table 17-3: WAN > Links > Configure (Cellular) screen fields

Field	Description
High Cost Link	High Cost Link • Selected—High cost link. Transmission of management data (e.g. log files uploads, automatic software downloads, etc.) is limited, with most of the data being held until a low cost link is active. (Note: If required, you can allow Auto software updates and firmware updates over high cost links, by setting appropriate options. See Table 19-8, General > Auto Software Updates screen fields, on page 204 for details.) *Note: During initial testing, avoid enabling this feature to ensure all management events are emitted. If data plan costs are a concern, enable this after the MG90 is put into operation.* • Not selected—Not a high cost link. *Note: Cellular links are typically high cost (depending on the data plan type), while Ethernet links are typically not high cost.*
MTU Size	Maximum Transmission Unit size (in bytes) • Automatic—MTU size calculated by MG90 using radio module's configured MTU and the network carrier's default MTU • Manual—Enter the MTU size: • Valid range: 256–1500
Masquerade	Network Address Translation for LAN-originated traffic leaving MG90 WAN interface • Selected—Enabled. This is the typical setting, since many carriers will disconnect a cellular modem that emits IP datagrams bearing an address other than that of the cellular modem. • Not selected—Disabled
Masquerade Port Range	Port range to use for masquerade (NAT) • Automatic—Enabled • Manual—Disabled (Default). This should be used in most cases to avoid using defined or reserved ports. *Note: This field is available only if Masquerade is selected.*

Minimum Port Number
Maximum Port Number
	Range of ports to use for masquerade (NAT)
	• Default range: 49152–65535
	• Valid range: 0–65535
	• If Minimum Port Number < 49152:
	  • traffic on ports lower than 512 is mapped to other ports lower than 512
	  • traffic on ports 512 to 1024 is mapped to ports lower than 1024
	  • traffic on ports greater than 1024 is mapped to ports greater than 1024
	Note: These fields are available only if Masquerade is selected and Masquerade Port Range is Manual.

Table 17-3: WAN > Links > Configure (Cellular) screen fields (Continued)

Field	Description
Automatic DNS	DNS servers to be used • Selected—Use DNS servers specified by DHCP server. • Not selected—Use the DNS servers specified in Primary DNS or Secondary DNS. The fastest-responding server (regardless of whether named as Primary or Secondary) is chosen as the server to use. Periodically, the servers are re-evaluated to make sure the fastest-responding server is being used. If private DNS servers are used, set up DNS zones—see Configuring DNS Zones for Private DNS Server Use on page 67 for details. *Note: This must be disabled (not selected) if using a static IP address.*
Primary DNS	IP address of primary domain name server • Format: IPv4 address (xxx.xxx.xxx.xxx) • Required field (when Automatic DNS is not selected) *Note: This field is available only if Automatic DNS is not selected.*
Secondary DNS Servers	IP addresses of secondary domain name servers • Format: IPv4 addresses, comma-separated (e.g. xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy) • Optional field *Note: This field is available only if Automatic DNS is not selected.*
Enable Private Zone	Enables/disable DNS private zone use on this link. • Selected—Enabled. DNS private zones can be used on this link. • Not selected—Disabled. DNS private zones cannot be used on this link.
Number of Private Zone	Table of 1–10 private zone configuration entries
Private Zone <#>	Domain name to be resolved by the internal DNS server managing the private zone.
Private Zone IP <#>	IP address of the internal DNS server managing the private zone.
APN	Access Point Name Mobile Network Operator's Access Point Name • Verizon/AT&T/Sprint—Typically left blank. The APN is determined automatically when the carrier SIM is inserted and can be seen in Status > WAN > Extended Status. • Other carriers—Obtain from the service provider and enter the value in this field.
Signal Strength Filter Length	Number of samples used to determine signal strength Signal strength is calculated as the average value of the samples collected.
Signal Strength Change Threshold (dBm)	If signal strength increases or decreases by more than this threshold value in a 2 second period, send an event to the AMM. For example: a. Check signal strength X at time T. b. Check signal strength Y at time T+2. c. If abs[X - Y] > Threshold, send event report to the AMM.

Table 17-3: WAN > Links > Configure (Cellular) screen fields (Continued)

Field	Description
Use Management Tunnel	Management Tunnel usage The management tunnel is a dedicated secure VPN connection between the MG90 and the AMM. • Selected—AMM can access the MG90. (Default) • Not selected—Do not use the management tunnel. AMM cannot access the MG90. To configure the management tunnel, see WAN > VPNs > (Management Tunnel) > Configure on page 159.
Pilot Ping	Pilot ping • Selected—Enabled. Before a WAN link is identified as established, the MG90 attempts to pass ping traffic over the link. If the ping succeeds, the link is identified as established. If the ping fails, the link is not established. • Not selected—Disabled (Default). Ping traffic is not attempted, which could result in a WAN link being identified as established although it may not be able to pass traffic. *Note: After a WAN link has been established, ping monitors (next field) are used to monitor the link's connection.*
Monitors	Monitor(s) being used to monitor the link's connection state Select one or more monitors. Notes: • Factory-defined monitor—DefaultMonitor. This example should be replaced with your own monitor definition. To configure monitors, see WAN > Monitors > Configure on page 157.
Monitor Mode	Effect of selected monitors' state on link status • Success in one monitor keeps the link up— If at least one monitor is reporting as active, then the link should be considered 'up'. • Failure in one monitor declares the link down—If any one monitor is reporting as inactive, then the link should be considered 'down'. *Note: This field is meaningful only if one or more monitors are selected.*
VPN	VPNs that the WAN link can establish when the link is active • If multiple VPNs are selected, each must be LAN to LAN. To configure VPNs, see WAN > VPNs on page 158.
Load Balanced	Distribute traffic across active WAN links When load balancing is selected on two or more active WAN links, traffic can be distributed across these links (based on their Weight field values). • Selected—Distribute traffic across links, based on Weight field values. • Not selected—Do not load balance See Configuring Load Balancing on page 60 for usage.

Table 17-3: WAN > Links > Configure (Cellular) screen fields (Continued)

Field	Description
Weight (1-256)	Load balancing 'weight' When load balancing is enabled on two or more links, their Weights are used to calculate the proportion of traffic each link will receive: Proportion (Link) = Weight (Link) / Total_Weight (All Links)) For example: Link A Weight = 50 Link B Weight = 100 Proportion (Link A) = 50 / (50+100) = 33.3% Proportion (Link B) = 100 / (50 + 100) = 66.7% Therefore, Link B will carry twice as many sessions as Link A. *Note: This field is available only if Load Balanced is not selected.*
Split Access	Allow incoming session initiation on non-active connected link This allows an incoming session to initiate on a link even when the link is not the active (i.e. default route) link but is connected to the network. • Selected—Allowed • Not selected—Not allowed This is useful for test purposes on cellular links that have public IP addresses. It also enables applications such as live video look-in to a cellular interface even if the active connection is via another WAN (e.g. Wi-Fi). *Note: Users are encouraged to evaluate use of the Split Access feature from a security and system perspective prior to enabling. Depending on available links and routing rules, traffic may route from WAN to LAN or between WAN networks.*
Enable Advanced Module Recovery	Reboot cellular module (e.g. MC7354, MC74XX, EM75XX) if link down for too long • Not selected—Disabled (Default) When the link goes down, the module begins attempting to reconnect, with an increasing delay between connection attempts. ◦ 1st attempt—Immediately tries to reconnect. ◦ 2nd attempt—6 second delay before attempt. ◦ 3rd attempt—12 second delay ◦ 4th attempt—1 minute delay + random (0–15 seconds) ◦ 5th attempt—2 minute delay + random (0–30 seconds) ◦ 6th attempt—8 minute delay + random (0–60 seconds) ◦ 7th attempt (and onward)—15 minute delay + random (0–120 seconds) This method is useful when a large number of devices disconnect simultaneously (e.g. due to a carrier outage). Without the variable delays, all devices would attempt to reconnect at the same time. With the variable delays, the group of devices will attempt to reconnect at different times. • Selected—Enabled. The module reboots when the link goes down for longer than the Recovery Interval period.

Table 17-3: WAN > Links > Configure (Cellular) screen fields (Continued)

Field	Description
Recovery Interval (minutes)	Maximum link recovery period (in minutes) If the link goes down for longer than this period, the module (e.g. MC7354, MC74XX, ECM75XX) will reboot. • Default: 10 (600 seconds) • Minimum: 1 (60 seconds) *Note: This field is available only if Enable Advanced Module Recovery is selected.*
Advanced Modem Initialization	*Important: This field should only be used under the direction of Sierra Wireless Technical Support staff, or as described below.* • If the WAN link is a private network that requires a user name and password for access, enter the following command in the Advanced Modem Initialization String field: AT$QCPDPP=1\,1\,<password>\,<username> For example: AT$QCPDPP=1\,1\,3AD29482\,6045551234@static.carrier.ca
Network Carrier	Mobile network operator used for this link • Automatic—MG90 reads factory parameters from the modem to best determine how to connect to the selected network carrier. • Specific carrier (e.g. Verizon, AT&T, etc.)—MG90 will attempt to adjust the configuration on the modem accordingly.
Preferred Mode	Radio Access Technology (RAT) types that Link can connect to: • Automatic—Connect to any available RAT • LTE Disabled—Connect to 2G/3G RATs only (LTE is disabled)
Enable IPV6	Enable (or disable) use of IPv6 addresses if required by mobile network provider • Selected—IPv6 addresses supported • Not selected—IPv6 addresses not supported

Wi-Fi WAN Link Configuration

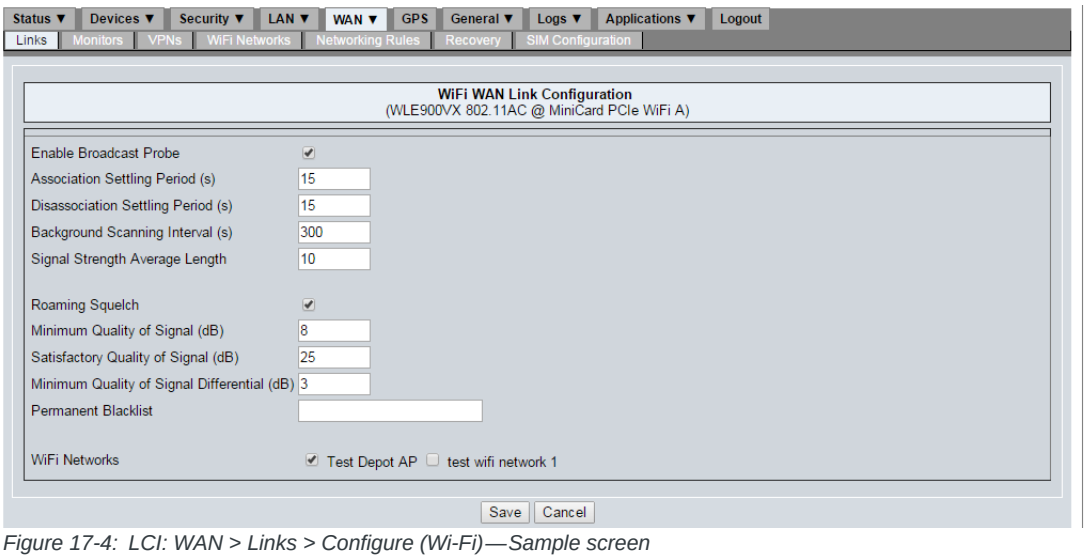

Figure 17-4: LCI: WAN > Links > Configure (Wi-Fi)—Sample screen

Table 17-4: WAN > Links > Configure (Wi-Fi) screen fields

Field	Description
Enable Broadcast Probe	Send periodic broadcast probe requests When enabled, a broadcast probe request is sent to all access points in the area. A probe request is sent by the client requesting information from either a specific access point or all access points in the area. • Selected—Probes enabled • Not selected—Probes not enabled
Association Settling Period (s)	Access Point Association Settling Period After connecting to a Wi-Fi access point, wait for this period (in seconds) before carrying traffic. This ensures that association to an AP with a marginal signal does not result in the link being selected for bearing default route traffic only to find it has disconnected. • Default: 15 • Recommended range: 1–60
Disassociation Settling Period (s)	Access Point Disassociation Settling Period When connected to a Wi-Fi access point and the link goes down, wait for this period (in seconds) before switching to another available link. The delay is intended to allow short interruptions to the Wi-Fi signal to be tolerated without provoking a link switch. • Default: 15 • Recommended range: 1–60
Background Scanning Interval (s)	Interval between background scans for suitable access points Before associating successfully, a scan is continuously executed to look for access points with the appropriate credentials. Once associated, a background scan is executed on the interval defined by this parameter. The background scan allows the MG90 to detect nearby eligible APs. This value should be set moderately (e.g. 60 seconds) when in a depot environment and aggressively (e.g. every 2 seconds) when operating in metropolitan networks. • Default: 300 (5 minutes)
Signal Strength Average Length	Number of background scan samples used to evaluate alternative APs This number of background scan samples are integrated to evaluate alternative APs. The default value of 10 readings is recommended for environments where there is only one access point with the appropriate credentials. For metropolitan networks, where the vehicle is expected to roam from access point to access point this value should be set to 1. • Default: 10
Roaming Squelch	Prevent Roaming (subject to signal quality) If selected, the MG90 stays associated with an AP (i.e. will not roam) unless the AP is disqualified by the signal quality settings in the next three fields. • Selected—Do not roam. Typically used in a depot environment. • Not selected—Roam. Typically used in metropolitan network where fast roaming is required.

Table 17-4: WAN > Links > Configure (Wi-Fi) screen fields (Continued)

Field	Description
Minimum Quality of Signal (dB)	Minimum Access Point Signal to Noise Ratio (SNR) to establish association The MG90 will not associate to an AP unless its SNR meets or exceeds this value. (A low SNR usually implies a low signal.) • SNR measured in dB *Note: This field is available only if Roaming Squelch is selected.*
Satisfactory Quality of Signal (dB)	Satisfactory Access Point Signal to Noise Ratio (SNR) to maintain association Once an MG90 has associated with an AP, it will remain associated unless the SNR drops below this value. • SNR measured in dB *Note: This field is available only if Roaming Squelch is selected.*
Minimum Quality of Signal Differential (dB)	Minimum Signal to Noise Ratio (SNR) differential to support switching APs When the Wi-Fi interface is considering a switch to a new access point, the difference in signal SNR between the current access point and the new one must be greater or equal to this value. • Differential measured in dB *Note: This field is available only if Roaming Squelch is selected.*
Permanent Blacklist	List of BSSIDs that the Wi-Fi interface should never connect to. • One or more BSSIDs, comma-separated *Note: This field is available only if Roaming Squelch is selected.*
Wi-Fi Networks	Wi-Fi networks that the link can connect to • Selected—Wi-Fi WAN link can connect to specified Wi-Fi network. • Not selected—Wi-Fi WAN link cannot connect to specified Wi-Fi network.

Serial (modem) WAN Link Configuration

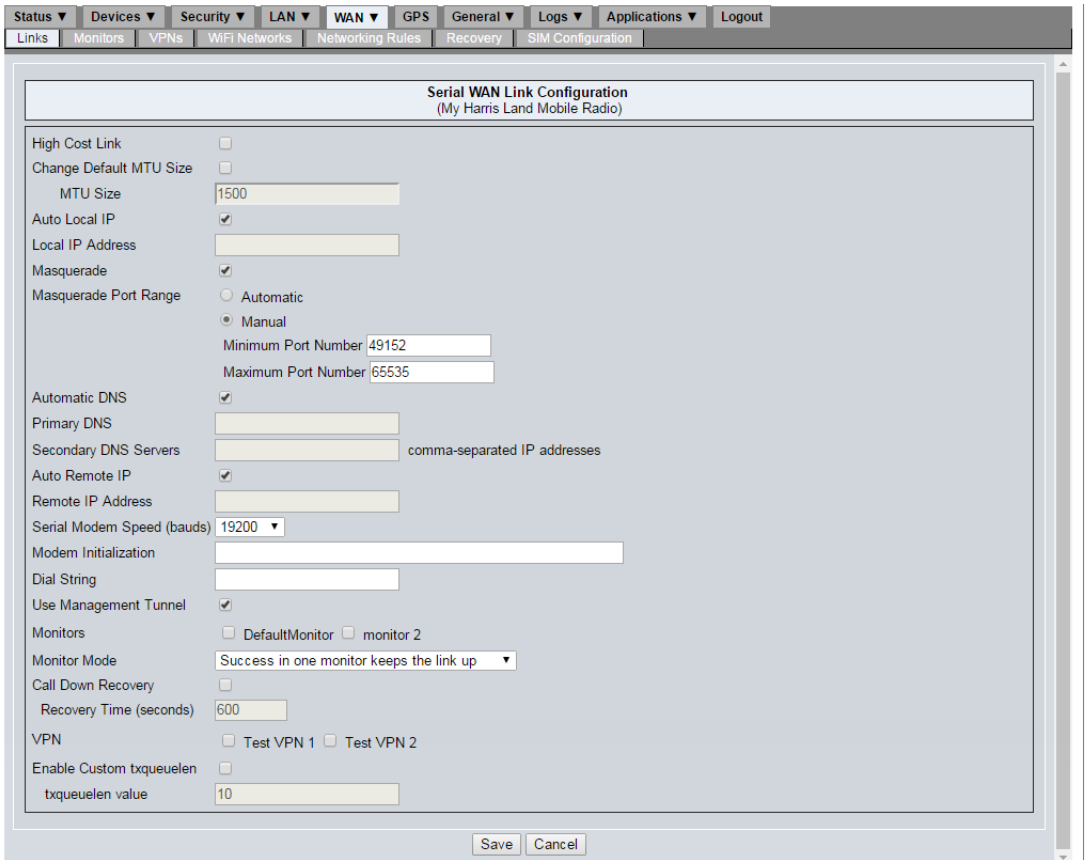

Figure 17-5: LCI: WAN > Links > Configure (Serial (modem))—Sample Screen

Table 17-5: WAN > Links > Configure (Serial (modem)) screen fields

Field	Description
High Cost Link	High Cost Link • Selected—High cost link. Transmission of management data (e.g. log files uploads, automatic software downloads, etc.) is limited, with most of the data being held until a low cost link is active. (Note: If required, you can allow Auto software updates and firmware updates over high cost links, by setting appropriate options. See Table 19-8, General > Auto Software Updates screen fields, on page 204 for details.) *Note: During initial testing avoid enabling this feature to ensure all management events are emitted. If data plan costs are a concern, enable this after the MG90 is put into operation.* • Not selected—Not a high cost link. *Note: Land mobile radio network (serial modem) links are typically very high cost and low bandwidth, while Ethernet links are typically not high cost.*
Change Default MTU Size	Use a different MTU Size than the default (1500 bytes). • Selected—MTU Size field can be edited. (Default) Deselect this checkbox to reset the MTU Size to the default value (the value resets when you click Save). • Not selected—MTU Size field cannot be edited. *Note: This may be required to accommodate some network configurations. Only change if instructed to by Sierra Wireless.*
MTU Size	Maximum Transmission Unit size (in bytes) • Valid range: 256–1500 • Default: 1500
Auto Local IP	Enable DHCP for this interface. • Selected—Enabled. The IP address will be assigned by a DHCP server connected to the access point network. (For most applications, the IP addresses should be obtained automatically from the network.) • Not selected—Not enabled. Assign the Local IP Address manually.
Local IP Address	Statically-assigned Local IP Address • IPv4 address format (e.g. xxx.xxx.xxx.xxx) *Note: This field is available only if Auto Local IP is not selected.*
Masquerade	Network Address Translation for LAN-originated traffic leaving MG90 WAN interface • Selected—Enabled. This is the typical setting, since many carriers will disconnect a cellular modem that emits IP datagrams bearing an address other than that of the cellular modem. • Not selected—Disabled
Masquerade Port Range	Port range to use for masquerade (NAT) • Automatic—Enabled • Manual—Disabled (Default). This should be used in most cases to avoid using defined or reserved ports. *Note: This field is available only if Masquerade is selected.*

Table 17-5: WAN > Links > Configure (Serial (modem)) screen fields (Continued)

Field	Description

Minimum Port Number
Maximum Port Number
	Range of ports to use for masquerade (NAT)
	• Default range: 49152–65535
	• Valid range: 0–65535
	• If Minimum Port Number < 49152:
	  • traffic on ports lower than 512 is mapped to other ports lower than 512
	  • traffic on ports 512 to 1024 is mapped to ports lower than 1024
	  • traffic on ports greater than 1024 is mapped to ports greater than 1024
	Note: This field is available only if Masquerade is selected and Masquerade Port Range is Manual.

Automatic DNS	DNS servers to be used • Selected—Use DNS servers specified by DHCP server. • Not selected—Use the DNS servers specified in Primary DNS or Secondary DNS. The fastest-responding server (regardless of whether named as Primary or Secondary) is chosen as the server to use. Periodically, the servers are re-evaluated to make sure the fastest-responding server is being used. If private DNS servers are used, set up DNS zones—see Configuring DNS Zones for Private DNS Server Use on page 67 for details. *Note: This must be disabled (not selected) if using a static IP address.*
Primary DNS	IP address of primary domain name server • Format: IPv4 address (xxx.xxx.xxx.xxx) • Required field (when Automatic DNS is not selected) *Note: This field is available only if Automatic DNS is not selected.*
Secondary DNS Servers	IP addresses of secondary domain name servers • Format: IPv4 addresses, comma-separated (e.g. xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy) • Optional field *Note: This field is available only if Automatic DNS is not selected.*
Auto Remote IP	Enable DHCP for this interface. • Selected—Enabled. The IP address will be assigned by a DHCP server connected to the access point network. (For most applications, the IP addresses should be obtained automatically from the network.) • Not selected—Not enabled. Assign the Local IP Address manually.
Local IP Address	Statically-assigned Remote IP Address • IPv4 address format (e.g. xxx.xxx.xxx.xxx) *Note: This field is available only if Auto Remote IP is not selected.*

Table 17-5: WAN > Links > Configure (Serial (modem)) screen fields (Continued)

Field	Description
Serial Modem Speed (bauds)	Serial modem baud rate Select the speed of the connected serial modem device: • 9600 • 19200 • 38400 • 57600 • 115200
Modem Initialization	AT command sequence for initializing modem For specific settings, see source.sierrawireless.com or contact your mobile network operator.
Dial String	Dial string to connect to mobile network operator's network
Use Management Tunnel	Management Tunnel usage The management tunnel is a dedicated secure VPN connection between the MG90 and the AMM. • Selected—AMM can access the MG90. (Default) • Not selected—Do not use the management tunnel. AMM cannot access the MG90. To configure the management tunnel, see WAN > VPNs > (Management Tunnel) > Configure on page 159.
Monitors	Monitor(s) being used to monitor the link's connection Select one or more monitors. • Factory-defined monitor—DefaultMonitor. This example should be replaced with your own monitor definition. To configure monitors, see WAN > Monitors > Configure on page 157.
Monitor Mode	Effect of selected monitors' state on link status • Success in one monitor keeps the link up— If at least one monitor is reporting as active, then the link should be considered 'up'. • Failure in one monitor declares the link down—If any one monitor is reporting as inactive, then the link should be considered 'down'. *Note: This field is meaningful only if one or more monitors are selected.*
Call Down Recovery	Reboot the router if link is down for too long When this option is enabled, the serial modem will reboot when the link goes down for longer than the Recovery Interval period. • Selected—Enabled • Not selected—Disabled (Default)
Recovery Time (seconds)	Maximum link recovery period If the link goes down for longer than this period (in seconds), the serial modem will reboot. • Default: 600 • Minimum: 1 *Note: This field is available only if Call Down Recovery is selected.*

Table 17-5: WAN > Links > Configure (Serial (modem)) screen fields (Continued)

Field	Description
VPN	VPNs that the WAN link can establish when the link is active • If multiple VPNs are selected, each of the VPNs must be LAN to LAN. To configure VPNs, see WAN > VPNs on page 158.
Enable Custom txqueuelen	Allow customized transmission buffer size When enabled, the specified number of packets (txqueuelen value) will be held in the transmit buffer of the WAN interface. This helps to prevent packets from being dropped on slower WAN connections. • Selected—Enabled. Set the buffer size to the txqueuelen value (next field). • Not selected—Disabled (Default). Use the default txqueuelen value. *Note: This field should not be changed without assistance from Sierra Wireless.*
txqueuelen value	Customized transmission buffer size • Default: 10 *Note: This field is available only if Enable Custom txqueuelen is selected.*

WAN Link Policy Configuration (WAN> Links > Policies)

The WAN Link Policy Configuration screen displays the policy types that are available for the selected WAN link type.

The example in Figure 17-6 shows the policies available for Cellular devices. Other device types will show some or all of these policies.

For details on setting up policies, see Setting up WAN Link Policies on page 42.

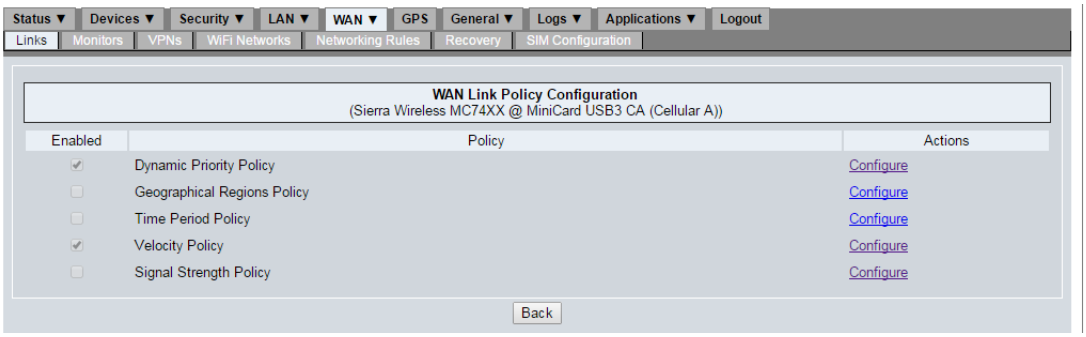

Figure 17-6: LCI: WAN > Links > Policies—Sample screen

Table 17-6: WAN > Links > Policies screen fields

Field	Description
Enabled	Indicates whether the associated policy is currently enabled for the WAN link • Selected—Policy is enabled for the WAN link. • Not selected—Policy is not enabled. To enable/disable a policy, click Configure.
Policy	Policy types that can be enabled for the WAN link (available policy types vary by WAN link type): • Dynamic Priority Policy—See Dynamic Priority Policy on page 151 for details. • Geographical Regions Policy—See Geographical Regions Policy on page 152 for details. • Time Period Policy—See Time Period Policy on page 153 for details. • Velocity Policy—See Velocity Policy on page 154 for details. • Signal Strength Policy—See Signal Strength Policy on page 155 for details.
Actions	The only available action type for policies is Configure. • Configure—Click to configure link-specific policy details

WAN > Links > Policies > Configure

Dynamic Priority Policy

The Dynamic Priority Policy Configuration allows you to assign a base score adjustment, and to assign an adjustment that dynamically changes based on the solidity of the connection.

See Dynamic Priority Policy Overview on page 43 for details.

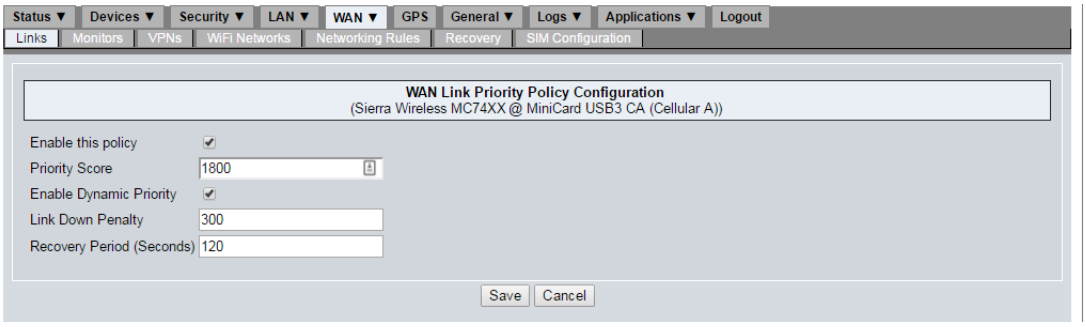

Figure 17-7: LCI: WAN > Links > Policies > Configure (Dynamic) — Sample screen

Table 17-7: WAN > Links > Policies > Configure (Dynamic) screen fields

Field	Description
Enable this policy	Enable/disable the policy for the WAN link • Selected—Enabled • Not selected—Disabled. If you disable a policy after configuring it, the configuration settings do not reset to default values, so they can still be used if you re-enable the policy.
Priority Score	Base priority score adjustment All links start with a base score of 1000. Use this field to adjust this link's base score. (The link with the highest score will be the active link when multiple links are available.) For example, if this field is 100, the link's adjusted base score before applying any other policy adjustments is 900 (1000 - 100).
Enable Dynamic Priority	Enable/disable dynamic priority score recovery When a down link is restored, a dynamic priority policy will determine the next suitable active link over a period of time to avoid unnecessary switching caused by instability of the recovered link. This is accomplished by gradually incrementing the recovered link's score over the recovery period. • Selected—Enabled. Use the Link Down Penalty and Recovery Period to gradually restore the link's base priority score. • Not selected—Disabled. When a down link is restored, its priority score is immediately set to its normal value.
Link Down Penalty	Priority score reduction applied to 'down' link When a down link recovers, this value is immediately subtracted from its base priority score. This penalty is removed linearly over the specified Recovery Period. Examples: • Penalty=60, Recovery Period=120 seconds When the down link first recovers, apply this penalty then begin decreasing it by 0.5 points/second. • Penalty=240, Recovery Period =120 seconds When the down link first recovers, apply this penalty then begin decreasing it by 2 points/second. *Note: This field applies only if Enable Dynamic Priority is selected.*
Recovery Period (seconds)	Link Down Penalty recovery period Period of time, in seconds, over which the Link Down Penalty decreases until it is completely removed. • Default: 0 • Recommended range: 0–600 *Note: If the link disconnects again during the recovery period, the Link Down Penalty and Recovery Period are re-applied when the link comes back online.* *Note: This field applies only if Enable Dynamic Priority is selected.*

Geographical Regions Policy

Use the geographical regions policy to consider the vehicle's location when determining which network to use. Up to three regions can be defined. When the vehicle travels into a defined region, an adjustment is applied to the link's score.

Each region is a rectangular area defined by:

- Upper-left latitude and longitude
- Lower-right latitude and longitude

See Geographical Regions Policy Overview on page 46 for details.

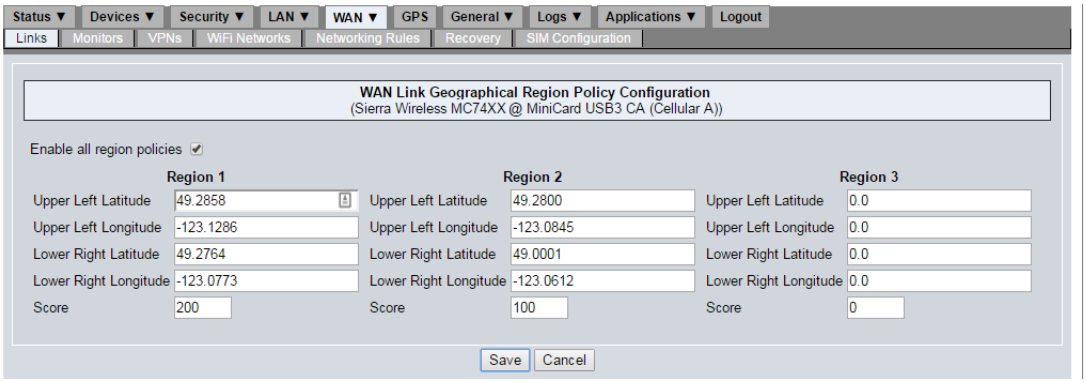

Figure 17-8: LCI: WAN > Links > Policies > Configure (Geographical)—Sample screen

Table 17-8: WAN > Links > Policies > Configure (Geographical) screen fields

Field	Description
Enable all region policies	Enable/disable the geographical region policies for the WAN link • Selected—Enabled. All three region policies are used. To use only one or two policies, set the latitude and longitude values for the unused regions to 0.0. • Not selected—Disabled. None of the region policies are used. *Note: If you disable the policies after configuring them, the configuration settings do not reset to default values, so they can still be used if you re-enable the policies.*

Upper Left Latitude
Upper Left Longitude
Lower Right Latitude
Lower Right Longitude
	Latitude/longitude coordinates of rectangular region
	• Format: Decimal (decimal portion rounds to four places)
	• Example:
	  • Upper Left Latitude: 49.2858 (49° 17’ 08” N)
	  • Upper Left Longitude: -123.1286 (123° 07’ 42” W)
	  • Lower Right Latitude: 49.2764 (49° 16’ 35” N)
	  • Lower Right Longitude: -123.0773 (123° 04’ 38” W)

Score	Score adjustment value The value that will be added to the link’s score for determining network selection.

Time Period Policy

Use the time period policy to consider the time of day when determining which network to use. Up to three time periods can be defined. Each period score is added to determine the network selection when the current time falls within the period.

Important: *Ensure the time periods do not overlap.*

See Time Period Policy Overview on page 47 for details.

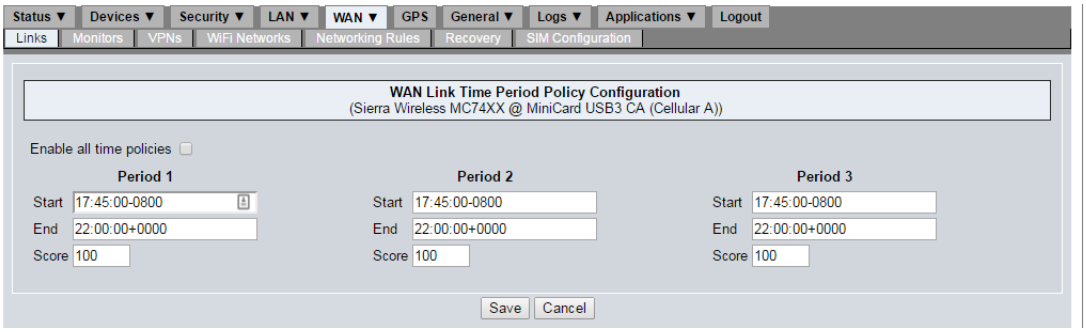

Figure 17-9: LCI: WAN > Links > Policies > Configure (Time Period)—Sample screen

Table 17-9: WAN > Links > Policies > Configure (Time Period) screen fields

Field	Description
Enable all time policies	Enable/disable the time period policies for the WAN link • Selected—Enabled. All three time period policies are used. To use only one or two policies, set the start and end values for the unused periods to 00:00:00+0000. • Not selected—Disabled. None of the time period policies are used. *Note: If you disable the policies after configuring them, the configuration settings do not reset to default values, so they can still be used if you re-enable the policies.*

Start
End
	Starting and ending times for the period
	• Format: HH:mm:ss±hhmm (where hhmm is the offset from UTC)
	• For example, the following values all represent the same time:
	  • 10:15:00+0000
	  • 14:15:00+0400
	  • 06:45:00-0330

Score	Score adjustment value The value that will be added to the link's score for determining network selection.

Velocity Policy

Use the velocity policy to allow for proactive network switching based on vehicle velocity instead of relying only on network outage switching. For example, you may prefer to give Wi-Fi a preference while stationary (e.g. in a depot) and cellular a preference while moving.

See Velocity Policy Overview on page 47 for details.

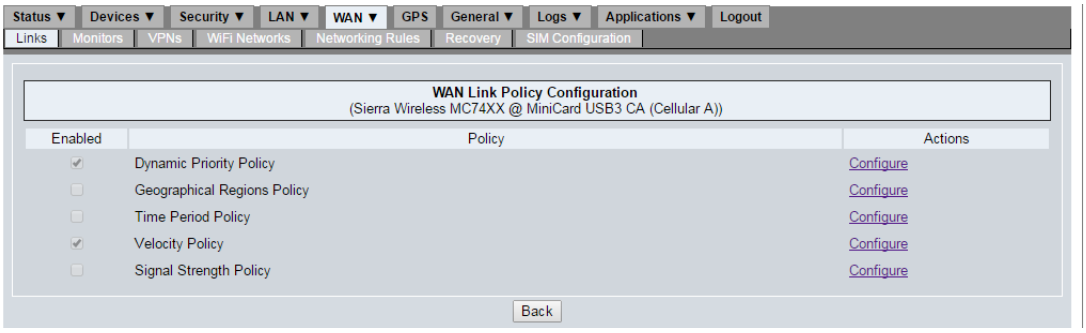

Figure 17-10: LCI: WAN > Links > Policies > Configure (Velocity)—Sample screen

Table 17-10: WAN > Links > Policies > Configure (Velocity) screen fields

Field	Description
Enable this policy	Enable/disable the policy for the WAN link: • Selected—Enabled. • Not selected—Disabled. *Note: If you disable the policy after configuring it, the configuration settings do not reset to default values, so they can still be used if you re-enable the policy.*
Threshold	Maximum velocity before Penalty is applied If the vehicle's velocity exceeds this value, the Penalty is applied to the link's score. • Select the appropriate velocity unit (mph or km/h) for the threshold value that you entered.
Penalty	Score adjustment value This value is immediately subtracted from the link's score when the velocity exceeds the threshold. When the velocity decreases below the threshold, the penalty is removed linearly over the specified Recovery Period. Examples: • Penalty=60, Recovery Period=120 seconds When velocity decreases below the threshold, the penalty begins to decrease by 0.5 points/second. • Penalty=240, Recovery Period =120 seconds When velocity decreases below the threshold, the penalty begins to decrease by 2 points/second.
Recovery Period (Seconds)	Period of time (in seconds) the vehicle's velocity must remain below the Threshold before the Penalty is completely removed • Default: 120 (2 minutes) *Note: If the velocity exceeds the threshold during the recovery period, the Penalty and Recovery Period are re-applied*

Signal Strength Policy

Use the signal strength policy to allow for proactive network switching based on WAN connection signal strength instead of relying only on network outage switching.

See Signal Strength Policy Overview on page 48 for details.

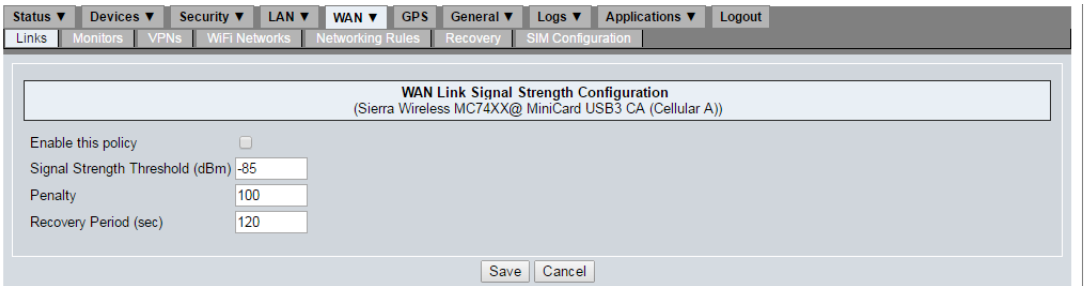

Figure 17-11: LCI: WAN > Links > Policies > Configure (Signal Strength)—Sample screen

Table 17-11: WAN > Links > Policies > Configure (Signal Strength) screen fields

Field	Description
Enable this policy	Enable/disable the policy for the WAN link • Selected—Enabled. • Not selected—Disabled. *Note: If you disable the policy after configuring it, the configuration settings do not reset to default values, so they can still be used if you re-enable the policy.*
Signal Strength Threshold (dBm)	Signal strength below which Penalty should be applied If the signal strength is lower than this value, the Penalty is applied to the link's score. • Default: -85 dBm *Note: The default threshold of -85 dBm is typically sufficient to drop bad connections that may not cause ping monitor failures, while also ensuring the MG90 does not unnecessarily switch to a lower throughput link that has a stronger signal.*
Penalty	Score adjustment value This value is immediately subtracted from the link's score when the signal strength falls below the Signal Strength Threshold. When the signal strength increases above the threshold, the penalty is removed linearly over the specified Recovery Period. Examples: • Penalty=60, Recovery Period=120 seconds When signal strength increases above the threshold, the penalty begins to decrease by 0.5 points/second. • Penalty=240, Recovery Period =120 seconds When signal strength increases above the threshold, the penalty begins to decrease by 2 points/second.
Recovery Period (Seconds)	Period of time (in seconds) the signal strength must remain above the threshold before the penalty is completely removed. • Default: 120 (2 minutes) *Note: If the signal strength drops below the threshold during the recovery period, the Penalty and Recovery Period are re-applied*

WAN > Monitors

The Monitors tab is used to create and configure monitors to detect and recover from high-level communication failures.

Note: A 'DefaultMonitor' is provided. Each time you add a new monitor, it uses the same initial default settings (so if you delete the DefaultMonitor by accident, you can simply use Add New WAN Monitor to recreate it).

See Using WAN Monitors to Detect Lost Connections on page 40 for details.

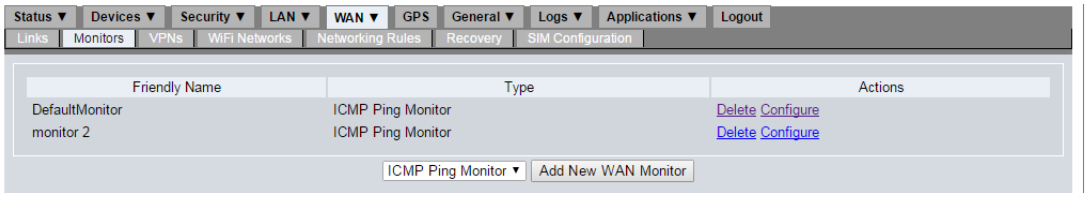

Figure 17-12: LCI: WAN > Monitors—Sample screen

Table 17-12: WAN > Monitors screen fields

Field	Description
Friendly Name	Descriptive name for the monitor
Type	Monitor type (cannot be modified). Always appears as “ICMP Ping Monitor”.
Actions	Click these optional links to perform actions on the associated monitors: • Delete—Delete the associated monitor. *Caution: The monitor deletes immediately, even if it is in use by any of the WAN links. If you delete the monitor by mistake, you will have to recreate it and then enable it in each of the affected WAN links.* • Configure—Configure monitor-specific details. See WAN > Monitors > Configure on page 157.
Add new WAN Monitor (button)	Click to display the configuration screen, using default values for all fields. The new monitor is added when you click Save after editing the configuration fields. See WAN > Monitors > Configure on page 157.

WAN > Monitors > Configure

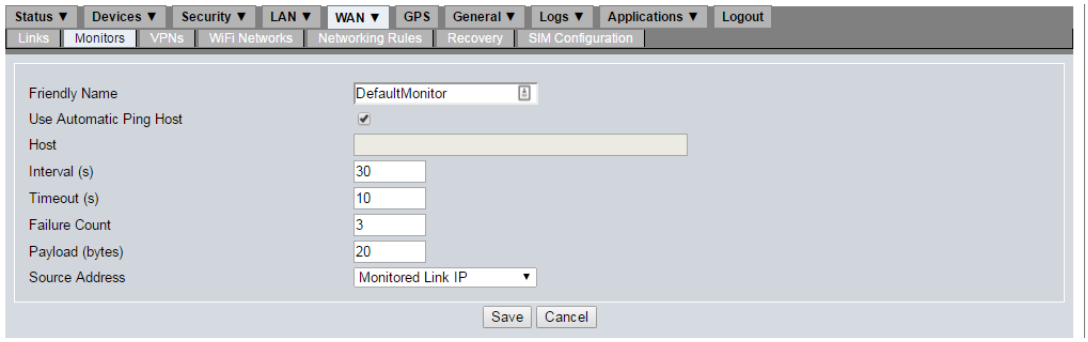

Figure 17-13: LCI: WAN > Monitors > Configure (or Add)—Sample screen

Table 17-13: WAN > Monitors > Configure (or Add) screen fields

Field	Description
Friendly Name	Descriptive name for the monitor This is the name that identifies the monitor on the WAN Link Configuration pages.
Use Automatic Ping Host	Use the default ping host, or specify a different host • Selected—Send pings to <ESN>.ping.omgservice.com (where <ESN> is the MG90's serial number, shown in the title bar of the LCI, and in Status > General). (Note—If you select this option and save the monitor, the Host field is cleared.) • Not selected—Specify a ping host in the Host field.
Host	IP address or URL of the host to ping. • IPv4 address format (e.g. xxx.xxx.xxx.xxx) *Note: This field applies only if Use Automatic Ping Host is not selected.*
Interval (s)	Ping interval Ping the host to confirm the link is active. Wait this number of seconds between sending each ping. • Default: 30
Timeout (s)	Ping response timeout Number of seconds to wait for a response to a ping. If a response is not received, increase the number of consecutive ping failures. • Default: 10
Failure Count	Maximum allowed consecutive ping failures If this number of consecutive pings fail, restart the WAN link. • Default: 3
Payload (bytes)	Ping packet size Number of bytes sent in a single ping request. • Default: 20
Source Address	VPN source address Select a different source address when configuring the VPN Ping Monitor. This will be populated with the LAN segments available, along with the Link IP. For the ICMP datagram to be allowed through the VPN, it *must* have the source address used to specify the VPN connection.

WAN > VPNs

The VPNs tab is used to create and configure VPN profiles that allow access to Virtual Private Networks (VPNs).

See How to configure a VPN on page 63 for details.

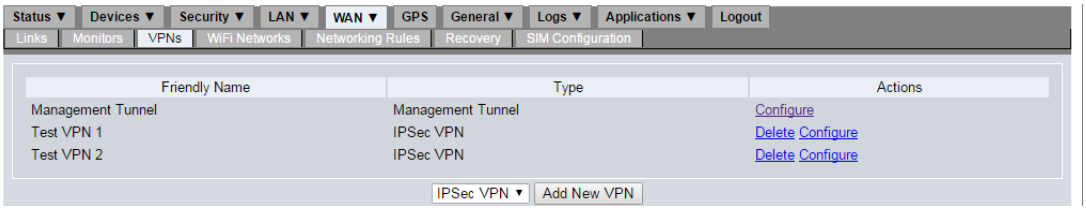

Figure 17-14: LCI: WAN > VPNs—Sample screen

Table 17-14: WAN > VPNs screen fields

Field	Description
Friendly Name	Descriptive name for the VPN, defined in the Configure screen.
Type	VPN type • Management Tunnel—Dedicated secure VPN connection between the MG90 and the AMM. • IPSec VPN—User-defined VPN
Actions	Click these optional links to perform actions on the associated VPN profiles: • Delete—Delete the associated VPN. (Note—This option is not available for the Management Tunnel.) *Caution: The VPN is deleted immediately, even if it is in use by any of the WAN links. If you delete the VPN by mistake, you will have to recreate it and then enable it in each of the affected WAN links.* • Configure—Configure VPN-specific details. See IPSec VPN Configuration (WAN > VPNs > Add New VPN, and WAN > VPNs > (IPSec VPN) > Configure) on page 161.
Add New VPN (button)	Click to display the configuration screen, using default values for all fields. The new VPN is added when you click Save after editing the configuration fields. *Note: The drop-down includes one option only—IPsec VPN.*

WAN > VPNs > (Management Tunnel) > Configure

The management tunnel is a dedicated secure VPN connection between the MG90 and the AMM. It provides secure remote console access, remote LCI, mass configuration, and event notification.

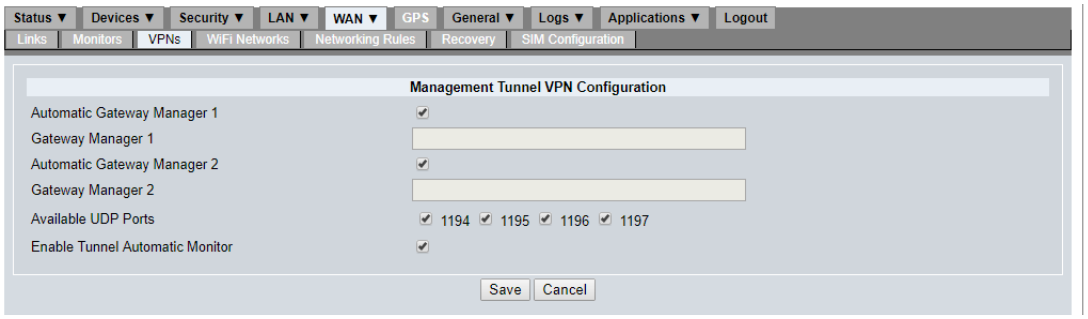

Figure 17-15: LCI: WAN > VPNs > Configure—Sample screen

Table 17-15: WAN > VPNs > (Management Tunnel) > Configure screen fields

Field	Description
Automatic Gateway Manager 1	Use first default gateway manager (<ESN>.dels.omgservice.com, where <ESN> is the MG90's serial number)
Gateway Manager 1	Gateway Manager • IPv4 address or FQDN of your first private AMM server *Note: This field applies only if Automatic Gateway Manager 1 is not selected.*
Automatic Gateway Manager 2	Use second default gateway manager (<ESN>.dels.omgservice.com, where <ESN> is the MG90's serial number)
Gateway Manager 2	Gateway Manager • IPv4 address or FQDN of your second private AMM server *Note: This field applies only if Automatic Gateway Manager 2 is not selected.*
Available UDP Ports	UDP Ports for Management Tunnel Select the UDP port(s) that the management tunnel can be brought up on. If more than one port is selected, the management tunnel will be brought up on one of the ports randomly. *Note: If AMM 2.15 or earlier is being used, select UDP port 1194.*
Enable Tunnel Automatic Monitor	Enable/disable Management Tunnel Monitor • Selected—Enabled. A ping monitor is enabled which will periodically ping the AMM to test for connectivity. • Not selected—Disabled.

IPSec VPN Configuration (WAN > VPNs > Add New VPN, and WAN > VPNs > (IPSec VPN) > Configure)

The IPsec VPN Configuration screen is used to add or update VPN profiles.

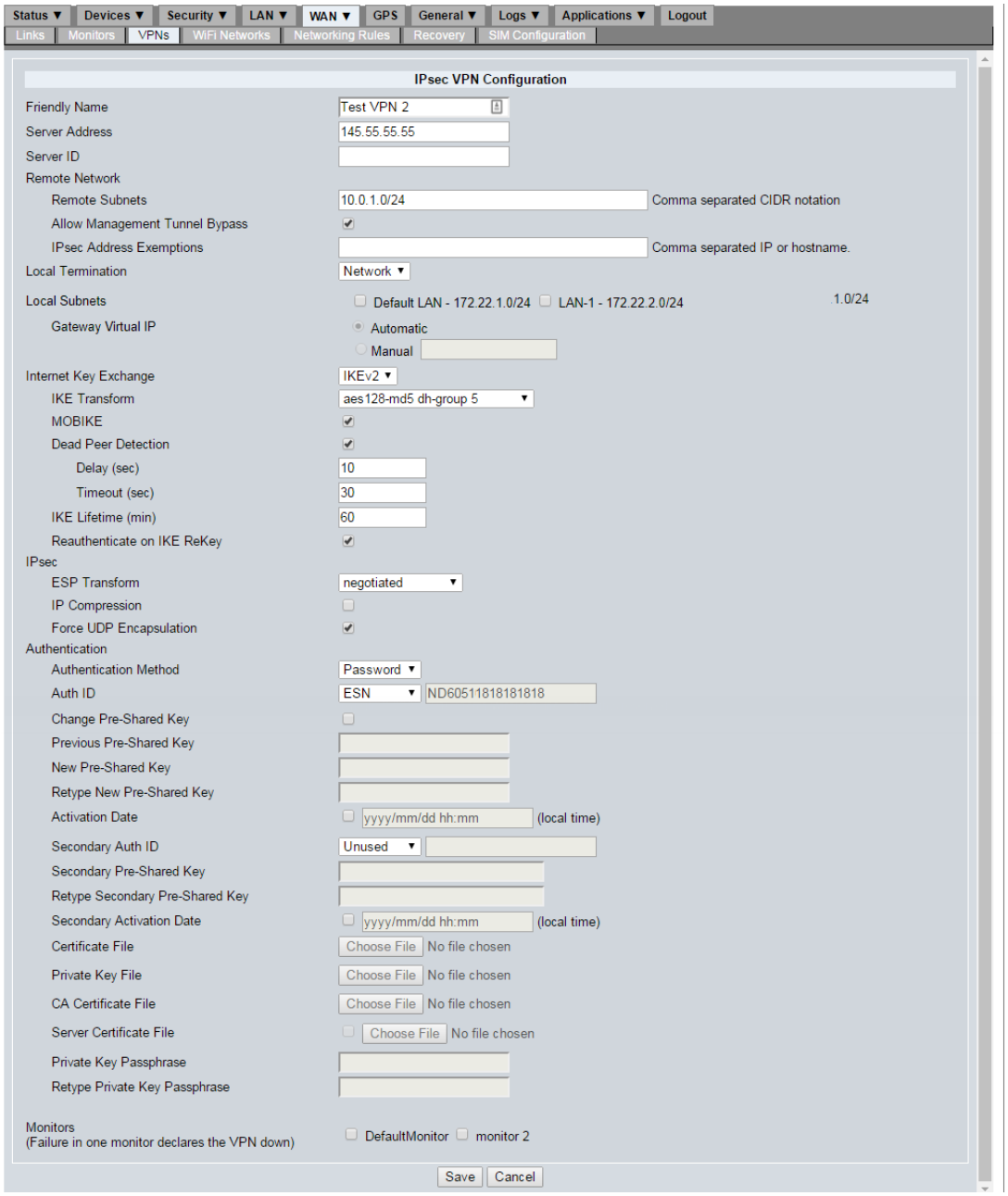

Figure 17-16: LCI: WAN > VPNs > Add New VPN—Sample screen

Table 17-16: WAN > VPNs > Add New VPN screen fields

Field	Description
Friendly Name	Enter a descriptive nickname for the VPN. This name identifies the VPN in other LCI screens (e.g. WAN > Links > Configure).
Server Address	Enter the VPN Gateway IP Address (IP address or FQDN) • IPv4 address format (e.g. xxx.xxx.xxx.xxx) • FQDN format (e.g. test.mycompany.net)
Server ID	Enter the IP address, hostname, domain name, or fully qualified domain name that the VPN server will use to identify itself to the gateway while negotiating the VPN tunnel. The value should be provided by the VPN server administrator. Examples: • Blank—Use the Server Address • 192.168.45.3 • test.yourcompany.net • Test1 *Note: If using certificate authentication, the Server ID mus be unique (must contain a valid Host DN (Distinguishable Name) value with a distinguishable CN (Canonical Name) parameter.*
Remote Network	
Remote Subnets	Destination IP network and destination IP network mask in CIDR notation. • IPv4 CIDR address format addresses, comma-separated (e.g. xxx.xxx.xxx.xxx/yy) • Example: 192.168.254.0/24
Allow Management Tunnel Bypass	Management Tunnel usage The management tunnel is a dedicated secure VPN connection between the MG90 and the AMM. • Selected—AMM can access the MG90. (Default) • Not selected—Do not use the management tunnel. AMM cannot access the MG90. To configure the management tunnel, see WAN > VPNs > (Management Tunnel) > Configure on page 159.
IPsec Address Exemptions	Traffic generated on the MG90 to the IP addresses (or Fully Qualified Domain Names (FQDNs)) in this list is sent directly to the Internet (it is not sent through the IPsec VPN tunnel). • IPv4 addresses and/or FQDNs, comma-separated
Local Termination	Local termination type • Host—Host to LAN configuration • Network—Network terminated
Local Subnets	Local subnets (LAN Segments) Select the LAN segments to use for this VPN. *Note: LAN segments are configured in LAN > LAN Segments.*

Table 17-16: WAN > VPNs > Add New VPN screen fields (Continued)

Field	Description

Gateway Virtual IP	IP address of the gateway (VPN peer)
	• Automatic—Receive virtual IP address dynamically from the VPN server.
	• Manual—Manually assign the virtual IP address based on the Local Termination type:
	  ◦ Host—Use the gateway virtual IP address (i.e. a host address to use for the VPN, not an IP address on the LAN segment)
	  ◦ Network—IP address that the MG90 has on one of the selected LAN segments (Local Subnets) selected on the VPN.
	  ◦ IPv4 address format (e.g. xxx.xxx.xxx.xxx)
	Note: This field is not used for IKEv1. This feature is supported only when Internet Key Exchange (IKE) V2 is used. Multiple VPN is not supported if any of the VPN profiles are using automatic Virtual IP addresses.

Internet Key Exchange	Select the Internet Key Exchange (IKE) protocol version used for this VPN. • IKEv1 • IKEv2
IKE Transform	Select the appropriate IKE transform for this VPN. *Note: The list of available transforms varies depending on the selected Internet Key Exchange version.* *Note: The IKE Transform must be a supported configuration on the VPN server.*
MOBIKE	Use the MOBIKE (IKEv2 Mobility and Multihoming) protocol • Selected—Enabled. (Note—Use this option only when using a VPN server (ACM or other appliance) that supports MOBIKE.) • Not selected—Not enabled. *Note: This field is available only if the Internet Key Exchange value is IKEv2. If MOBIKE is used for any VPN, all VPNs on the system must also use the IKEv2 transform*
Dead Peer Detection	Enable/disable Dead Peer Detection If enabled, dead peer detection can detect when an IKE peer is unavailable. *Note: Do not select this option if MOBIKE is enabled.* • Selected—Enabled. Detection attempts are based on the Delay and Timeout values. • Not selected—Disabled. *Note: Do not rely solely on DPD. Sierra Wireless recommends the use of VPN link monitors to ensure reliable failure detection and recovery.*
Delay (sec)	Number of seconds between contact attempts. • Default: 10 *Note: This field is available only if Dead Peer Detection is selected.*
Timeout (sec)	Number of seconds to wait for the IKE peer to respond to a contact attempt. • Default: 30 *Note: This field is available only if Dead Peer Detection is selected.*

Table 17-16: WAN > VPNs > Add New VPN screen fields (Continued)

Field	Description
IKE Lifetime (min)	Lifetime for IKE Security Association (SA) Number of minutes before a new SA will be negotiated. • Default: 60 *Note: Either end may initiate the negotiation; both ends need not agree.*
Reauthenticate on IKE ReKey	Require re-authentication when rekeying IKE security association. • Selected—Re-authentication required • Not selected—Re-authentication not required *Note: This field is available only if the Internet Key Exchange value is IKEv2.*
IPsec	
ESP Transform	ESP Transform used for IPsec security Select the appropriate ESP transform for this VPN. To enhance security, PFS (Perfect Forward Secrecy) can be enabled. This causes unique keys to be used when generating the SAs (Security Association) between the MG90/client device and VPN server. If any one key is compromised, only that specific SA is compromised. If PFS is disabled, however, the same key is used for all SAs and if the key is compromised, all SAs using that key are compromised. PFS is enabled/disabled by choosing an appropriate ESP transform: • Enable PFS—Select a transform that includes a dh-group (e.g. “aes256-sha2_256 dh-group 2”). • Disable PFS—Select a transform that does not include a dh-group (e.g. “aes256-sha2_256”). *Note: The ESP Transform must be a supported configuration on the VPN server.*
IP Compression	Enable/disable IP packet compression • Selected—Enabled • Not selected—Disabled *Note: This field must be disabled if the VPN server (Server Address field) doesn't support compression.*
Force UDP Encapsulation	Enable/disable UDP encapsulation • Selected—Enabled (Default). This is the recommended setting. When the VPN server is behind a firewall, firewall configuration is simplified as the firewall only has to allow ports 500 (IKE) and 4500 (UDP-encapsulated ESP). • Not selected—Disabled. When this setting is used, port 50 must also be allowed for the ESP protocol to pass.
Authentication	
Authentication Method	Network authentication method Select the method the VPN uses to authenticate client devices. • Password—Use a pre-shared key • Certificate—Use a digital certificate

Table 17-16: WAN > VPNs > Add New VPN screen fields (Continued)

Field	Description
Auth ID	Host authentication ID string Select an ID type and enter the ID string that will be used to identify the host. • ESN—The MG90's serial number (as displayed in Status > General) • ip address—IP address of the active WAN link • custom—A custom string. (Note: Do not include spaces in the string.)
Change Pre-Shared Key	Select to access the next three fields. *Note: This field appears only when updating an existing VPN that has the Authentication Method as "Password".*
Previous Pre-Shared Key	Enter the current password (pre-shared key). (Note that the value is obfuscated for security reasons.) *Note: This field appears only when updating an existing VPN that has the Authentication Method as "Password".*
Pre-Shared Key or **New Pre-Shared Key** **Retype Pre-Shared Key** or **Retype New Pre-Shared Key**	Enter a new non-blank password (pre-shared key), and re-enter it in the 'Retype' field to verify. (Note that the values are obfuscated for security reasons.). • The key cannot contain the following special characters: '$', '|' *Note: These fields are available only when the Authentication Method is "Password".*
Activation Date	Activation date for Auth ID and Pre-Shared Key. Select this option if using a rotating credential system, and enter the date that the Auth ID and Pre-Shared Key become the active credentials. • Date format: yyyy/mm/dd hh:mm *Note: This field is available only when the Authentication Method is "Password".*
Secondary Auth ID	Host authentication secondary ID string Select an ID type and enter the ID string, or select "Unused" to not use secondary authorization. This field is used as a backup to the Auth ID field. For more information contact Sierra Wireless Support. • Unused—Secondary authorization is not used • ESN—The MG90's serial number (as displayed in Status > General) • ip address—IP address of the active WAN link • custom—A custom string. (Note: Do not include spaces in the string.)
Change Secondary Pre-Shared Key	Select to access the next three fields. *Note: This field appears only when updating an existing VPN that has the Authentication Method as "Password", and a secondary pre-shared key is in use.*
Previous Secondary Pre-Shared Key	Enter the current secondary password (pre-shared key). (Note that the value is obfuscated for security reasons.) *Note: This field is accessible only when Change Secondary Pre-Shared Key is selected.*

Table 17-16: WAN > VPNs > Add New VPN screen fields (Continued)

Field	Description
Secondary Pre-Shared Key or **New Secondary Pre-Shared Key**	Enter a new non-blank password (pre-shared key), and re-enter it in the 'Retype' field to verify. (Note that the values are obfuscated for security reasons.). • The key cannot contain the following special characters: '$', '|' *Note: These fields are available only when Change Secondary Pre-Shared Key is selected.*
Retype Pre-Shared Key or **Retype New Pre-Shared Key**	
Secondary Activation Date	Activation date for Secondary Auth ID and Secondary Pre-Shared Key. Select this option if using a rotating credential system, and enter the date that the Auth ID and Pre-Shared Key become the active credentials. • Date format: yyyy/mm/dd hh:mm *Note: This field is available only when the Authentication Method is "Password" and the Secondary Auth ID is not "Unused".*
Certificate File	Click Browse/Choose File and select the identify certificate (.pem) file to use. *Note: This field is available only when the Authentication Method is "Certificate".*
Private Key File	Click Browse/Choose File and select the generated key (.pem) file to use. *Note: This field is available only when the Authentication Method is "Certificate".*
CA Certificate File	Click Browse/Choose File and select the CA server certificate (.pem) file to use. *Note: This field is available only when the Authentication Method is "Certificate".*
Server Certificate File	Use a server certificate file • Not Selected—Use a CA certificate server. • Selected—Select only when a CA certificate server is not available, then click Browse/Choose File to select the server certificate file to use. *Note: This field is available only when the Authentication Method is "Certificate".*
Change Private Key Passphrase	Select to access the next three fields. *Note: This field appears only when updating an existing VPN that has the Authentication Method as "Certificate", and a private key passphrase has been specified.*
Current Private Key Passphrase	Enter the current secondary password (pre-shared key). (Note that the value is obfuscated for security reasons.) *Note: This field is accessible only when Change Private Key Passphrase is selected.*

Table 17-16: WAN > VPNs > Add New VPN screen fields (Continued)

Field	Description
Private Key Passphrase or **New Private Key Passphrase**	Enter the non-blank passphrase used when creating the RSA Key file, and re-enter it in the 'Retype' field to verify. (Note that the values are obfuscated for security reasons.) *Note: This field is available only when the Authentication Method is "Certificate".*
Retype Private Key Passphrase or **Retype New Private Key Passphrase**	
Monitors	Monitor(s) being used to monitor the VPN connection Select one or more monitors. Notes: • Factory-defined monitor—DefaultMonitor. This example should be replaced with your own monitor definition. To configure monitors, see WAN > Monitors > Configure on page 157.

WAN > Wi-Fi Networks

The Wi-Fi Networks tab is used to create and maintain configuration details for the Wi-Fi networks (access points) that the MG90 can connect to.

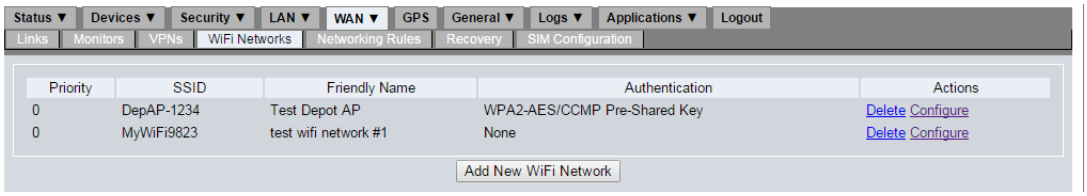

Figure 17-17: LCI: WAN > Wi-Fi Networks—Sample screen

Table 17-17: WAN > Wi-Fi Networks screen fields

Field	Description
Priority	Network Priority When more than one Wi-Fi network (access point) is defined, the network with the highest priority is connected first.
SSID	Basic Service Set Identifier The identifier broadcast by the access point.
Friendly Name	Descriptive name of the access point

Table 17-17: WAN > Wi-Fi Networks screen fields (Continued)

Field	Description
Authentication	Authentication method used by the access point
Actions	Click these optional links to perform actions on the associated VPN profiles: • Delete—Delete the associated access point configuration. • Configure—Configure the details for the associated access point. See WAN > Wi-Fi Networks > Add New Wi-Fi Network/Configure Network on page 169.

WAN > Wi-Fi Networks > Add New Wi-Fi Network/Configure Network

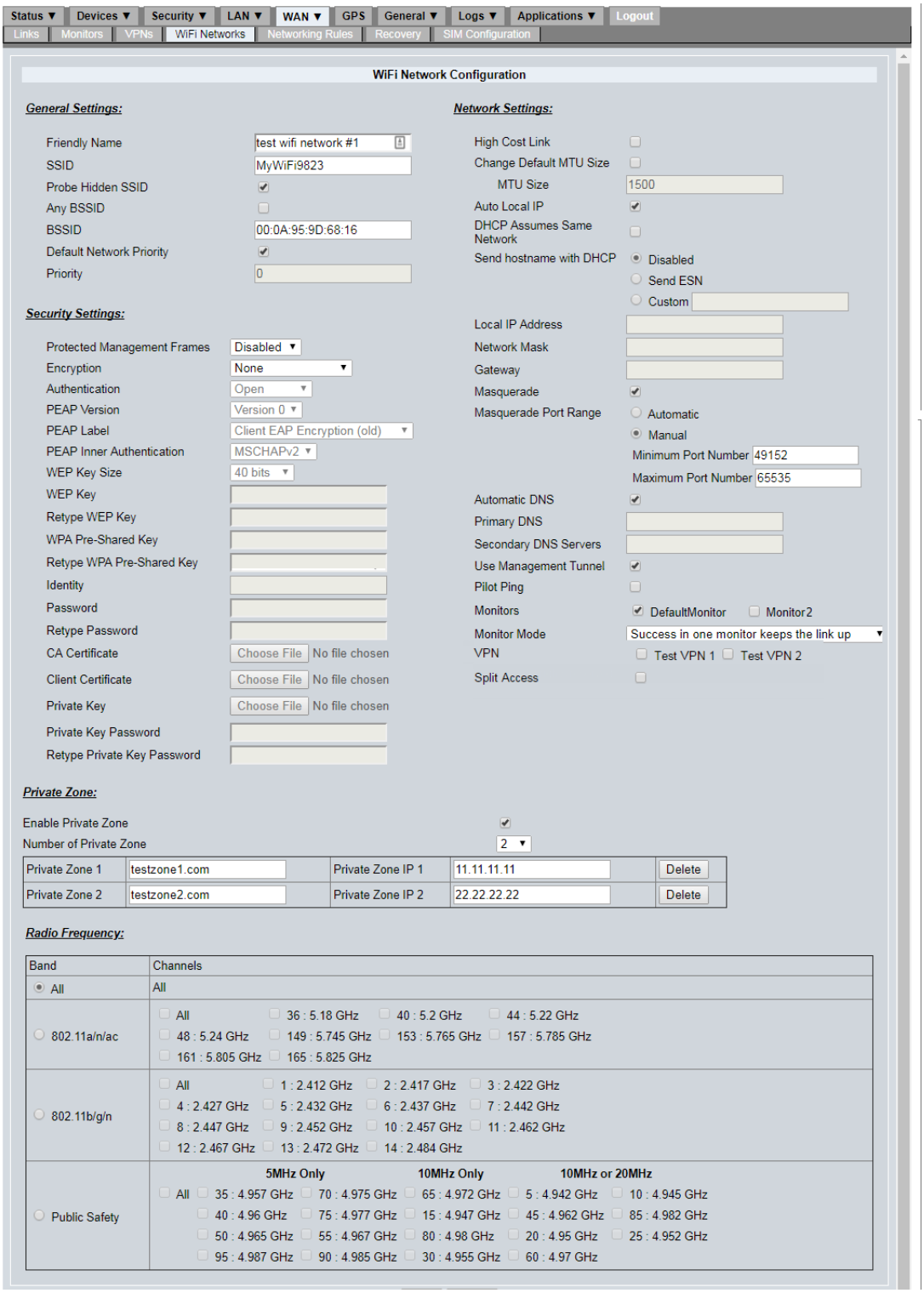

Figure 17-18: LCI: WAN > Wi-Fi Networks > Add New Wi-Fi (or Configure) Network—Sample screen

Table 17-18: WAN > Wi-Fi Networks > Add New Wi-Fi Network (or Configure) screen fields

Field	Description
General Settings	
Friendly Name	Enter a descriptive nickname for the Wi-Fi network. This name identifies the network in other LCI screens (e.g. WAN > Links > Configure for a Wi-Fi radio that is provisioned to be used on WAN).
SSID	Wi-Fi network's Basic Service Set Identifier (Network display name) Enter the SSID of the Wi-Fi network to which the MG90 should connect.
Probe Hidden SSID	Connection requests allowed to access points not broadcasting SSIDs • Selected—If an access point is not broadcasting the SSIDs for its Wi-Fi networks, the MG90 can still request a connection using the SSID in the previous field (SSID). • Not selected—The MG90 cannot request a connection to an AP's Wi-Fi network if the SSID is not being broadcast.
Any BSSID	Connect to any access point broadcasting the SSID value (above0. • Selected—MG90 will connect to any access point device with a broadcast SSID (BSSID) that matches the SSID field above. • Not selected—The MG90 will connect to an access point device that is broadcasting the SSID (from the field above) if the AP's MAC address is listed in the BSSID field below. This approach is more secure (will connect only to 'approved' APs).
BSSID	Enter the MAC address of the access point that the MG90 can connect to. *Note: This field is available only if Any BSSID is not selected.*
Default Network Priority **Priority**	Network priority of this AP When a Wi-Fi WAN link has more than one AP (with different SSIDs) selected, the AP network priorities are compared, and the link will connect to the AP with the highest priority. (Note—If multiple APs have the same (highest) priority, the MG90 uses the first one that is available.) • Selected—Use 0 (default value) for the network priority. • Not selected—Enter the network priority in the Priority field.

Table 17-18: WAN > Wi-Fi Networks > Add New Wi-Fi Network (or Configure) screen fields (Continued)

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td colspan="2">Security Settings</td></tr>
<tr><td>Protected Management Frames</td><td>Protected Management Frames for augmented WPA2 privacy
Set the PMF option to work with the option used by the external Access Point to which the MG90's Wi-Fi network connects:
<table>
<tr><th rowspan="2">MG90 PMF</th><th colspan="3">External access point PMF</th></tr>
<tr><th>Disabled</th><th>Optional</th><th>Required</th></tr>
<tr><td>Disabled</td><td>Connection allowed, PMF not used</td><td>Connection allowed, PMF not used</td><td>Connection not allowed</td></tr>
<tr><td>Optional</td><td>Connection allowed, PMF not used</td><td>Connection allowed, PMF may or man not be used</td><td>Connection allowed, PMF used</td></tr>
<tr><td>Required</td><td>Connection not allowed</td><td>Connection allowed, PMF used</td><td>Connection allowed, PMF used</td></tr>
</table>
Note: When enabled (Optional/Required), the Encryption is automatically set to WPA2-AES/CCMP.</td></tr>
<tr><td>Encryption</td><td>Encryption method MG90 must use to connect to this network
• None—No encryption, all Security Settings fields are disabled.
• WEP
• WPA-RC4/TKIP
• WPA-AES/CCMP
• WPA2-RC4/TKIP
• WPA2-AES/CCMP (Default)
Note: If Protected Management Frames is enabled, Encryption is automatically set to WPA2-AES/CCMP.</td></tr>
<tr><td>Authentication</td><td>Authentication protocol for the selected Encryption method
• Open—Note that this option is not available if Protected Management Frames are enabled.
• WPA-PSK
• EAP-TLS—Note that you must ensure you select a valid CA Certificate when using this protocol.
• EAP-PEAP
Note: Protocol availability depends on the selected encryption method. See Table 17-19 on page 178 for details.
Note: Security options required depend on the protocol. See Table 17-20 on page 178 for details.</td></tr>
<tr><td>PEAP Version</td><td>Version of PEAP (Protected Extensible Authentication Protocol) to use.
• Version 0 (Note—No other versions are supported.)
Note: This field is available only when Authentication method is EAP-PEAP.</td></tr>
</table>

Table 17-18: WAN > Wi-Fi Networks > Add New Wi-Fi Network (or Configure) screen fields (Continued)

Field	Description
PEAP Label	Client encryption type to use. • Client EAP Encryption (old) • Client PEAP Encryption (new) *Note: This field is available only when Authentication method is EAP-PEAP.*
PEAP Inner Authentication	PEAP inner authentication algorithm to use. • MSCHAPv2 • GTC *Note: This field is available only when Authentication method is EAP-PEAP.*
WEP Key Size	Size of key to use. • 40 bits • 104 bits *Note: This field is available only when Encryption Method is WEP and Authentication protocol is Open.*
Change WEP Key	Select to access the next three fields *Note: This field appears only when Encryption method is WEP, and a WEP key is already in use.*
Previous WEP Key	Enter the current WEP Key being used. (Note that the value is obfuscated for security reasons.) *Note: This field is available only when Change WEP Key is selected.*
WEP Key or **New WEP Key** **Retype WEP Key** or **Retype New WEP Key**	Enter the WEP Key (5 or 13 pairs of hexadecimal digits, no spaces), and re-enter it in the 'Retype' field to verify. (Note that the values are obfuscated for security reasons.). • If WEP Key Size = 40, enter 5 pairs of hexadecimal digits • If WEP Key Size = 104, enter 13 pairs of hexadecimal digits *Note: These fields are available only when Encryption method is WEP.*
Change WPA Pre-Shared Key	Select to access the next three fields. *Note: This field appears only when using a form of WPA encryption, the Authentication method is WPA-PSK, and a WPA Pre-Shared Key is already in use.*
Previous WPA Pre-Shared Key	Enter the current WPA Pre-Shared Key. (Note that the value is obfuscated for security reasons.) *Note: This field is available only when Change WPA Pre-Shared key is selected.*

Table 17-18: WAN > Wi-Fi Networks > Add New Wi-Fi Network (or Configure) screen fields (Continued)

Field	Description
WPA Pre-Shared Key or **New WPA Pre-Shared Key**	Enter the WPA Pre-Shared Key provided by the Wi-Fi network's administrator, and re-enter it in the 'Retype' field to verify. (Note that the values are obfuscated for security reasons.). Valid formats: • 8–63 printable ASCII characters • 64 hexadecimal digits *Note: These fields are available only when Authentication method is WPA-PSK.*
Retype WPA Pre-Shared Key or **Retype New WPA Pre-Shared Key**	
Identity	Identity (for EAP protocol) needed to log on to this Wi-Fi network • Format: ASCII string • Required field *Note: These field is meaningful only when Authentication method is EAP-PEAP. Do not enter a value if Authentication method is EAP-TLS.*
Change Password	Select to access the next three fields. *Note: This field appears only when Authentication method is EAP-PEAP or EAP-TLS, and a Password is already in use.*
Previous Password	Enter the current Password. (Note that the value is obfuscated for security reasons.) *Note: This field is available only when Change Password is selected.*
Password or **New Password**	Enter the Password that the user Identity needs to log on to this Wi-Fi network, and re-enter it in the 'Retype' field to verify. (Note that the values are obfuscated for security reasons.). • Format: ASCII string *Note: These fields are available only when Authentication method is EAP-PEAP.*
Retype Password or **Retype New Password**	
CA Certificate	Click Browse/Choose File to locate and open a CA certificate file (.pem) for the network, if supplied by the Wi-Fi network administrator. *Note: You can upload the file from a device connected to the LAN.* *Note: This field is available only when Authentication method is EAP-PEAP or EAP-TLS.*
Client Certificate	Click Browse/Choose File to locate and open a Client certificate file (.pem) for the network, if supplied by the Wi-Fi network administrator. *Note: You can upload the file from a device connected to the LAN.* *Note: This field is available only when Authentication method is EAP-PEAP.*
Private Key	Click Browse/Choose File to locate and open a private key file (.key) for the network, if supplied by the Wi-Fi network administrator. *Note: You can upload the file from a device connected to the LAN.* *Note: This field is available only when Authentication method is EAP-TLS.*

Table 17-18: WAN > Wi-Fi Networks > Add New Wi-Fi Network (or Configure) screen fields (Continued)

Field	Description
Change Private Key Password	Select this option to change the current Private Key Password. *Note: This field is available only when Authentication method is EAP-TLS.*
Previous Private Key Password	(This field is available only when Change Password is selected.) Enter the current Password. (Note that the value is obfuscated for security reasons.) *Note: This field is available only when Change Private key Password is selected.*
Private Key Password or **New Private Key Password**	Enter the Password that the user Identity needs to log on to this Wi-Fi network, and re-enter it in the 'Retype' field to verify. (Note that the values are obfuscated for security reasons.). • Format: ASCII string *Note: These fields are available only when Authentication method is EAP-TLS.*
Retype Private Key Password or **Retype New Private Key Password**	
Network Settings	
High Cost Link	High Cost Link • Selected—High cost link. Transmission of management data (e.g. log files uploads, automatic software downloads, etc.) is limited, with most of the data being held until a low cost link is active. (Note: If required, you can allow Auto software updates and firmware updates over high cost links, by setting appropriate options. See Table 19-8, General > Auto Software Updates screen fields, on page 204 for details.) • Not selected—Not a high cost link. *Note: Public Wi-Fi links are often declared as High Cost if the mobile network operator charges per MB.*
Change Default MTU Size	Use a different MTU Size than the default (1500 bytes). • Selected—MTU Size field can be edited. (Default) Deselect this checkbox to reset the MTU Size to the default value (the value resets when you click Save). • Not selected—MTU Size field cannot be edited. *Note: This may be required to accommodate some network configurations. Only change if advised by Sierra Wireless.*
MTU Size	Maximum Transmission Unit size (in bytes) • Valid range: 256–1500 • Default: 1500
Auto Local IP	Enable DHCP for this interface. • Selected—Enabled. The IP address will be assigned by a DHCP server connected to the access point network. • Not selected—Not enabled. Assign the Local IP Address, Network Mask, and Gateway manually.

Table 17-18: WAN > Wi-Fi Networks > Add New Wi-Fi Network (or Configure) screen fields (Continued)

Field	Description
DHCP Assumes Same Network	DHCP assignment when lease expires • Selected—Attempt to reconnect to same DHCP assignment when DHCP lease expires. • Not selected—Router will request an IP address from a DHCP server in the available network when the lease expires *Note: This field is available only when Auto Local IP is selected.*
Send Hostname with DHCP request	Enable/disable sending of MG90-identifying information with DHCP request • Disabled—Do not send identifying information • Send ESN—Send the MG90's ESN (Electronic Serial Number) • Custom—Send a custom hostname (for example, "Bus401") to identify the MG90 to the DHCP server. *Note: This field is available only if Auto Local IP is selected.*
Local IP Address	Statically-assigned Local IP Address • IPv4 address format (e.g. xxx.xxx.xxx.xxx) *Note: This field is available only when Auto Local IP is not selected.*
Network Mask	Network mask of the Local IP Address • IPv4 netmask format (e.g. xxx.xxx.xxx.xxx) *Note: This field is available only when Auto Local IP is not selected.*
Gateway	Default gateway to use for the Local IP Address • IPv4 address format (e.g. xxx.xxx.xxx.xxx) *Note: This field is available only when Auto Local IP is not selected.*
Masquerade	Network Address Translation for LAN-originated traffic leaving the MG90 WAN interface • Selected—Enabled. This is the typical setting. • Not selected—Disabled
Masquerade Port Range	Port range to use for masquerade (NAT) • Automatic—Enabled • Manual—Disabled (Default). This should be used in most cases to avoid using defined or reserved ports. *Note: This field is available only when Masquerade is selected.*

Minimum Port Number
Maximum Port Number
	Range of ports to use for masquerade (NAT)
	• Default range: 49152–65535
	• Valid range: 0–65535
	• If Minimum Port Number < 49152:
	  • traffic on ports lower than 512 is mapped to other ports lower than 512
	  • traffic on ports 512 to 1024 is mapped to ports lower than 1024
	  • traffic on ports greater than 1024 is mapped to ports greater than 1024
	Note: These fields are available only when Masquerade is selected and Masquerade Port Range is Manual.

Table 17-18: WAN > Wi-Fi Networks > Add New Wi-Fi Network (or Configure) screen fields (Continued)

Field	Description
Automatic DNS	DNS servers to be used • Selected—Use DNS servers specified by DHCP server. • Not selected—Use the DNS servers specified in Primary DNS or Secondary DNS. The fastest-responding server (regardless of whether named as Primary or Secondary) is chosen as the server to use. Periodically, the servers are re-evaluated to make sure the fastest-responding server is being used. If private DNS servers are used, set up DNS zones—see Configuring DNS Zones for Private DNS Server Use on page 67 for details. *Note: This must be disabled (not selected) if using a static IP address.*
Primary DNS	IP address of primary domain name server • Format: IPv4 address (xxx.xxx.xxx.xxx) • Required field (when Automatic DNS is not selected) *Note: This field is available only when Automatic DNS is not selected.*
Secondary DNS Servers	IP addresses of secondary domain name servers • Format: IPv4 addresses, comma (e.g. xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy) • Optional field *Note: This field is available only when Automatic DNS is not selected.*
Use Management Tunnel	Management Tunnel usage The management tunnel is a dedicated secure VPN connection between the MG90 and the AMM. • Selected—AMM can access the MG90. (Default) • Not selected—Do not use the management tunnel. AMM cannot access the MG90. To configure the management tunnel, see WAN > VPNs > (Management Tunnel) > Configure on page 159.
Pilot Ping	Pilot ping • Selected—Enabled. Before a WAN link is identified as established, the MG90 attempts to pass ping traffic over the link. If the ping succeeds, the link is identified as established. If the ping fails, the link is not established. • Not selected—Disabled (Default). Ping traffic is not attempted, which could result in a WAN link being identified as established although it may not be able to pass traffic. *Note: After a WAN link has been established, ping monitors (next field) are used to monitor the link's connection.*
Monitors	Monitor(s) being used to monitor the link's connection Select one or more monitors. Notes: • Factory-defined monitor—DefaultMonitor. This example should be replaced with your own monitor definition; it is commonly blocked within enterprise networks. Use an enterprise-specific network. To configure monitors, see WAN > Monitors > Configure on page 157.

Table 17-18: WAN > Wi-Fi Networks > Add New Wi-Fi Network (or Configure) screen fields (Continued)

Field	Description
Monitor Mode	Effect of selected monitors' state on link status • Success in one monitor keeps the link up— If at least one monitor is reporting as active, then the link should be considered 'up'. • Failure in one monitor declares the link down—If any one monitor is reporting as inactive, then the link should be considered 'down'. *Note: This field is meaningful only when one or more monitors are selected.*
VPN	VPNs that the WAN link can establish when the link is active • If multiple VPNs are selected, each of the VPNs must be LAN to LAN. • To configure VPNs, see WAN > VPNs on page 158.
Split Access	Allow incoming session initiation on non-active connected link This allows an incoming session to initiate on a link even when the link is not the active (i.e. default route) link but is connected to the network. • Selected—Allowed • Not selected—Not allowed This is useful for applications such as live video look-in to a Wi-Fi interface even if the active connection is via another WAN (e.g. cellular). *Note: Users are encouraged to evaluate use of the Split Access feature from a security and system perspective prior to enabling. Depending on available links and routing rules, traffic may route from WAN to LAN or between WAN networks.*
Private Zone	
Enable Private Zone	Enables/disable DNS private zone use on this link. • Selected—Enabled. DNS private zones can be used on this link. • Not selected—Disabled. DNS private zones cannot be used on this link.
Number of Private Zone	Table of 1–10 private zone configuration entries
Private Zone <#>	Domain name to be resolved by the internal DNS server managing the private zone.
Private Zone IP <#>	IP address of the internal DNS server managing the private zone.

Table 17-18: WAN > Wi-Fi Networks > Add New Wi-Fi Network (or Configure) screen fields (Continued)

Field	Description
Radio Frequency	
Band	Supported Wi-Fi bands Select the radio band this Wi-Fi network operates on—the MG90 will search these bands for the SSID to connect. Choose one of the following: • All—MG90 searches all bands for the SSID. (Default) • 802.11a/n/ac • 802.11b/g/n • Public Safety
Channels	Supported Channels for selected Bands Select the channels (frequencies) used by the Wi-Fi network on the selected Band—select 'All' or any combination of the listed channels. • All—All listed channels are supported. (Default) • Other channels—Select any combination of channels. (Note—You must deselect All before you can select any of the other channels.)

The following table summarizes the authentication methods available for each encryption option:

Table 17-19: Summary of available authentication options

Encryption	Open	WPA-PSK	EAP-TLS	EAP-PEAP
none	-	-	-	-
WEP	X	-	X	X
WPA-RC4/TKIP	-	X	X	X
WPA-AES/CCMP	-	X	X	X
WPA-RC4/TKIP	-	X	X	X
WPA2-AES/COMP	-	X	X	X

The following table summarizes the applicable security fields for each authentication method:

Table 17-20: Summary of required security options for each authentication method

Authentication	PEAP			WEP		WPA			Certificate		Private Key	
	Version	Label	Inner Authentication	Key Size	Key	Pre-Shared Key	Identity	Password	CA	Client	Key	Password
Open	-	-	-	-	-	-	-	-	-	-	-	-
WPA-PSK	-	-	-	-	-	X	-	-	-	-	-	-
EAP-TLS	-	-	-	-	-	-	X	-	X	X	X	X
EAP-PEAP	X	X	X	-	-	-	X	X	X	-	-	-

WAN > Networking Rules

The WAN Networking Rules tab is used to defined ‘global’ networking rules that apply to all WAN connections. The WAN rules include:

- Access Blocking
- Access Granting
- Port Forwarding
- QoS Prioritizing

Note: There are three ‘levels’ of networking rules—LAN segment, WAN link, and Global (LAN). If there is a conflict between any of these rules, LAN segment rules override WAN link and global rules, and WAN link rules override global rules.

Note: The WAN Networking Rules and LAN Networking Rules use similar setup parameters. For LAN networking rules, see LAN > Networking Rules, and LAN > LAN Segments > Networking Rules on page 119.

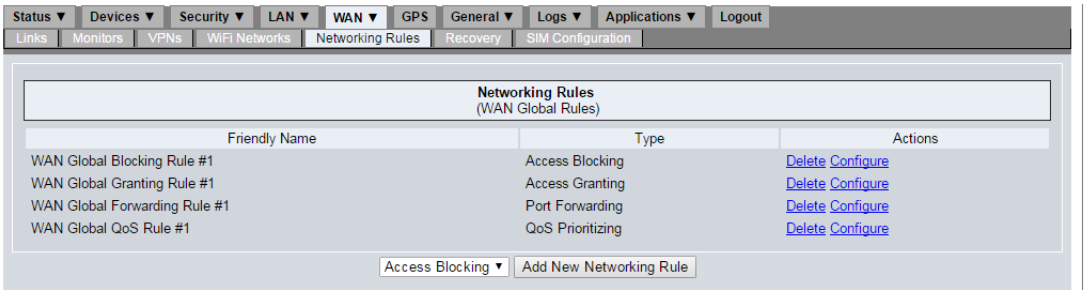

Figure 17-19: LCI: WAN > Networking Rules—Sample screen

Table 17-21: WAN > Networking Rules screen fields

Field	Description
Friendly Name	Descriptive name for the networking rule
Type	Rule type: • Access Blocking—Block incoming or outgoing traffic. See Access Blocking Rules on page 180. • Access Granting—Permit incoming or outgoing traffic. See Access Granting Rules on page 181. • Port Forwarding—Permit port forwarding. See Port Forwarding Rules on page 182. • QoS Prioritizing—Assign traffic priority. See QoS Priority Rules on page 183.
Actions	Click these optional links to perform actions on the associated rules: • Delete—Delete the associated networking rule. • Configure—Configure the associated network rule.
Add New Networking Rule	From the drop-down, select the type of rule to add, and click Add New Networking Rule. For usage details, see Setting up the WAN Firewall on page 50.

Access Blocking Rules

Add an Access Blocking rule to block incoming or outgoing traffic (from the MG90's perspective) for a specific IP address, based on the criteria in Table 17-22 on page 180.

Tip: *Fields that are left blank are treated as "wildcards". Limit the use of wildcards (fill fields with appropriate values) to make sure your rule works as intended.*

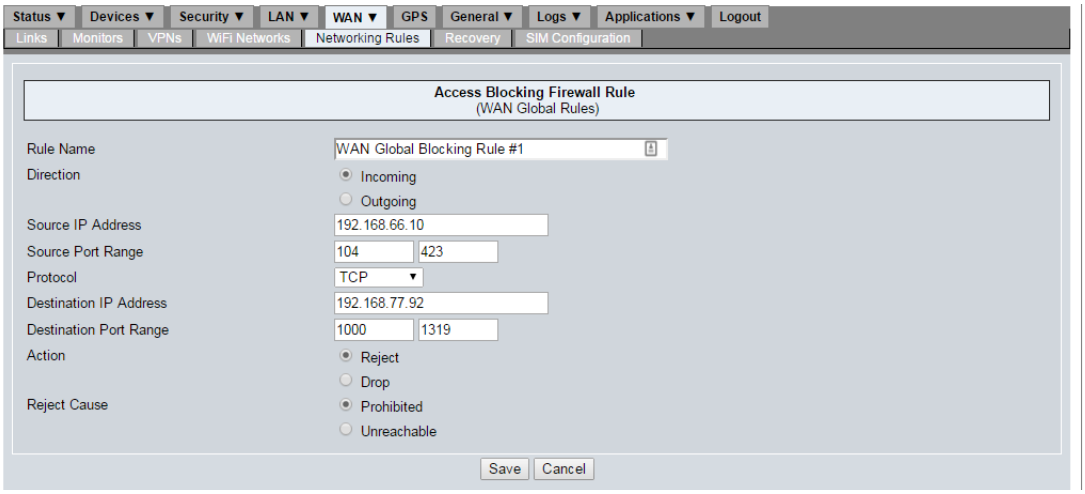

Figure 17-20: LCI: WAN > Networking Rules > Add Rule (Access Blocking)—Sample screen

Table 17-22: WAN > Networking Rules > Add Rule (Access Blocking) screen fields

Field	Description
Rule Name	Descriptive name for the networking rule.
Direction	Traffic direction relative to the MG90 • Incoming—The Source IP Address will be blocked. • Outgoing—The Destination IP Address will be blocked.

Source IP Address	Source IP address
	• Format: [!]xxx.xxx.xxx.xxx[/xx]
	Note: The optional '!' means "anything other than this address (or range)".
	• Examples:
	  • Address without netmask—192.168.4.17. Applies to the stated IP address.
	  • Address with netmask—192.168.4.0/24. Applies to the IP address range 192.168.4.0–192.168.4.255.

Source Port Range	Starting and ending source port numbers • Valid values: 0–65535 • Start port must be less than or equal to the end port

Table 17-22: WAN > Networking Rules > Add Rule (Access Blocking) screen fields

Field	Description
Protocol	Communications protocol • TCP • UDP • TCP/UDP • ICMP (Internet Control Message Protocol)
Destination IP Address	Destination IP address • Format: xxx.xxx.xxx.xxx[/xx]
Destination Port Range	Starting and ending source port numbers • Valid values: 0–65535 • Start port must be less than or equal to the end port
Action	Action to take when traffic matches the rule's specifications: • Reject—Send the Reject Cause to the sender. • Drop—Drop the traffic packets without notice. *Note: The 'Drop' rule is useful when attempting to prevent hacking.*
Reject Cause	Reason that user receives when Action is set to 'Reject' • Prohibited—Inform user that site is banned. • Unreachable—Inform user that site is unreachable.

Access Granting Rules

Add an Access Granting rule to permit incoming or outgoing traffic (from the MG90's perspective) for a specific IP address, based on the criteria in Table 17-23 on page 182.

Tip: *Fields that are left blank are treated as "wildcards". Limit the use of wildcards (fill fields with appropriate values) to make sure your rule works as intended.*

Note: By default, all ports (except ports 22 and 2222 (SSH)) to the MG90 from the WAN side are blocked. Access granting rules will not open additional ports to the MG90 but are designed to act as exceptions to access blocking rules.

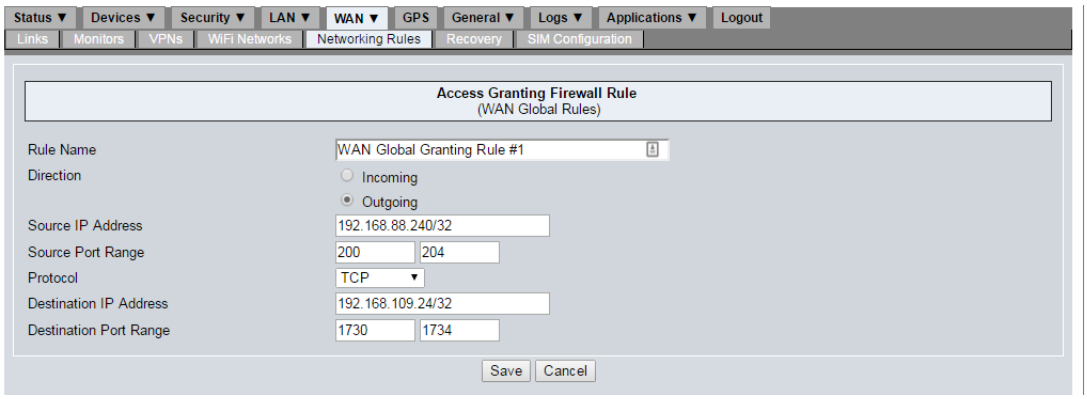

Figure 17-21: LCI: WAN > Networking Rules > Add Rule (Access Granting)—Sample screen

Table 17-23: WAN > Networking Rules > Add Rule (Access Granting) screen fields

Field	Description
Rule Name	Descriptive name for the networking rule.
Direction	Traffic direction relative to the MG90 • Incoming—The Source IP Address will be blocked. • Outgoing—The Destination IP Address will be blocked.

Source IP Address	Source IP address
	• Format: [!]xxx.xxx.xxx.xxx[/xx]
	Note: The optional '!' means "anything other than this address (or range)".
	• Examples:
	  • Address without netmask—192.168.4.17. Applies to the stated IP address.
	  • Address with netmask—192.168.4.0/24. Applies to the IP address range 192.168.4.0–192.168.4.255

Source Port Range	Starting and ending source port numbers • Valid values: 0–65535 • Start port must be less than or equal to the end port
Protocol	Communications protocol • TCP • UDP • TCP/UDP • ICMP (Internet Control Message Protocol)
Destination IP Address	Destination IP address • Format: [!]xxx.xxx.xxx.xxx[/xx] Note: The optional '!' means "anything other than this address (or range)".
Destination Port Range	Starting and ending source port numbers • Valid values: 0–65535 • Start port must be less than or equal to the end port

Port Forwarding Rules

Add a Port Forwarding rule to permit traffic from the WAN interface (Source IP + Destination Port Range) to be forwarded to a specific IP address and port on the LAN interface (Forward to Host and Forward Port Range).

Tip: *Fields that are left blank are treated as "wildcards". Limit the use of wildcards (fill fields with appropriate values) to make sure your rule works as intended.*

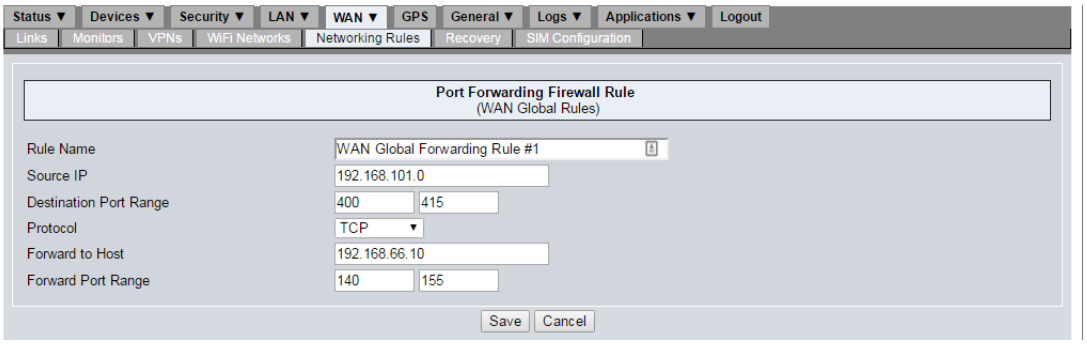

Figure 17-22: LCI: WAN > Networking Rules > Add Rule (Port Forwarding)—Sample screen

Table 17-24: WAN > Networking Rules > Add Rule (Port Forwarding) screen fields

Field	Description
Rule Name	Descriptive name for the networking rule.
Source IP	IP address of sender • Format: xxx.xxx.xxx.xxx[/xx] • If forwarding only based on the destination port(s), leave this field blank.
Destination Port Range	Starting and ending destination port numbers • Valid values: 0–65535 • Start port must be less than or equal to the end port
Protocol	Communications protocol • TCP • UDP • TCP/UDP
Forward to Host	Local IP Address of host. • Static IP address • Format: xxx.xxx.xxx.xxx
Forward Port Range	Starting and ending port numbers • Valid values: 0–65535 • Start port must be less than or equal to the end port

QoS Priority Rules

Add QoS priority rules to various applications used by the customer and guarantee a certain level of performance to data flow.

Tip: *Fields that are left blank are treated as "wildcards". Limit the use of wildcards (fill fields with appropriate values) to make sure your rule works as intended.*

For applications that do not have a predetermined destination IP address such as Voice-over-IP, using the Source IP Address and Source Port is supported.

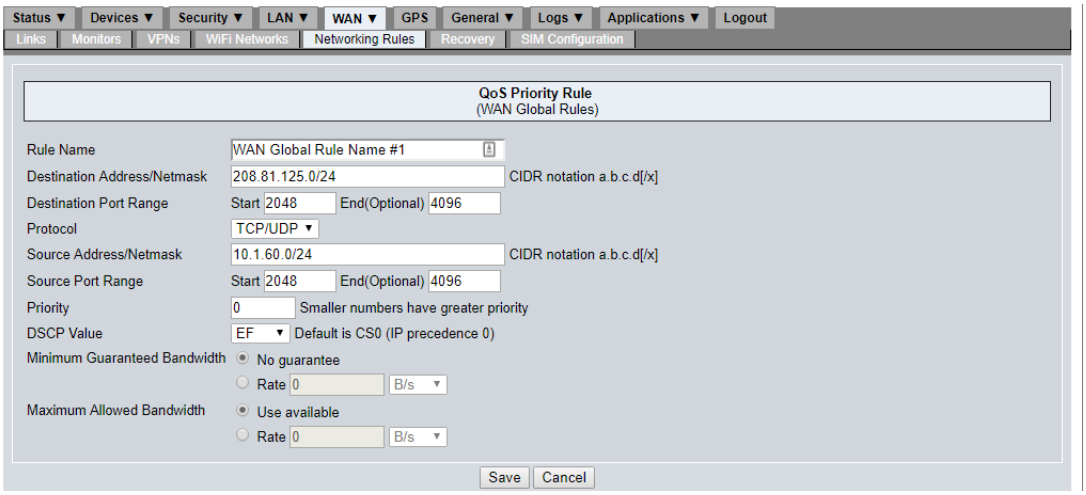

Figure 17-23: LCI: WAN > Networking Rules > Add Rule (QoS Prioritizing)—Sample screen

Table 17-25: WAN > Networking Rules > Add Rule (QoS Prioritizing) screen fields

Field	Description
Rule Name	Descriptive name for the networking rule.
Destination Address/Netmask	Application server IP address • Format: [!]xxx.xxx.xxx.xxx[/xx] (CIDR notation) Note: The optional '!' means "anything other than this address (or range)". • Leaving this field blank gives priority to all traffic on this port, based on existing firewall rules.
Destination Port Range	Destination port number (For TCP, UDP, TCP/UDP Protocols) • Single port used for data transport (Start), or range of ports (Start/End) • End port is Optional • Valid values: 0–65535 *Note: This field is available only if Protocol type is TCP, UDP, or TCP/UDP.*
Protocol	Data transport protocol • ALL • TCP/UDP • TCP • UDP • ICMP
Source Address/ Netmask	Source IP address (used for applications that do not have a predetermined IP address (e.g. VoIP) • Format: [!]xxx.xxx.xxx.xxx[/xx] (CIDR notation) Note: The optional '!' means "anything other than this address (or range)".

Table 17-25: WAN > Networking Rules > Add Rule (QoS Prioritizing) screen fields

Field	Description
Source Port Range	Source port number (used for applications that do not have a predetermined IP address (e.g. VoIP) • Single port used for data transport (Start), or range of ports (Start/End) • End port is Optional • Valid values: 0–65535 *Note: This field is available only if Protocol type is TCP, UDP, or TCP/UDP.*
Priority	Traffic priority Traffic to the WAN in the specified port and destination IP address is prioritized using this value. • Format: Integer • Minimum value: 0 (Highest priority) • Higher values are lower priority
DSCP Value	DSCP (Differentiated Services Code Point), also known as PNTM[a] (Private Network Traffic Management) for Verizon • Select appropriate DSCP value from list. For DSCP details, refer to RFC 2597 and RFC 3260. • Values in the list are sorted from lowest priority (CS0) to highest priority (EF). • Value is used to prioritize traffic for end-to-end QOS across all devices in the path (if DSCP is supported).
Minimum Guaranteed Bandwidth	Minimum data transfer rate • No guarantee—No minimum data transfer rate. (Default) • Rate—Specify the minimum data rate (including the transfer unit) that should be provided *Note: If minimum bandwidth is specified for some rules, consider adding it to all rules. When the sum of the minimum guaranteed bandwidths for all transmissions is greater than the available bandwidth, transmissions with no guarantee will be stalled.*
Maximum Allowed Bandwidth	Maximum data transfer rate • Use available—No maximum data rate. (Default) • Rate—Specify the maximum data rate (including the transfer unit) that can be used. The maximum allowed bandwidth is used to ensure that traffic matching the condition specified by the rule does not exceed this bandwidth.

a. Pending Verizon PNTM certification.

WAN > Recovery

The Recovery tab is used to configure the MG90 to reboot after a WAN link has been down for a specified time period, and to restore the MG90's configuration if an update pushed from the AMM caused the WAN link to go down.

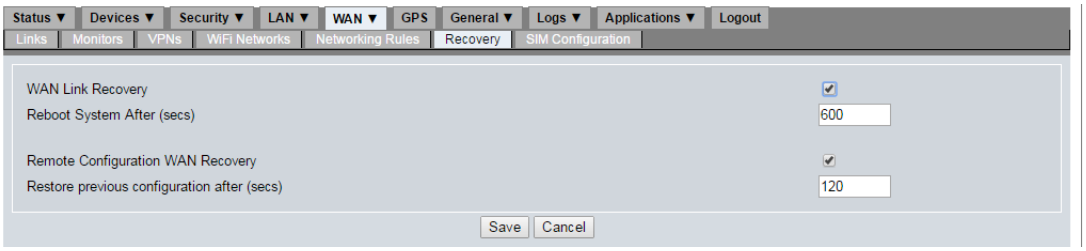

Figure 17-24: LCI: WAN > Recovery—Sample screen

Table 17-26: WAN > Recovery screen fields

Field	Description
WAN Link Recovery	Enable/disable automatic reboot to reestablish WAN link • Selected—Enabled. The MG90 will automatically reboot if there is no WAN communication (WAN links are down) for the period in Reboot System After. • Not selected—Disabled. MG90 will not automatically reboot.
Reboot System After (secs)	Interval to wait before automatic reboot Enter the amount of time (in seconds) that the MG90 waits after losing a WAN connection before automatically rebooting. *Note: This field is available only if WAN Link Recovery is selected.*
Remote Configuration WAN Recovery	Enable/disable configuration change reversion If enabled and the AMM pushes configuration changes that cause the MG90 to lose WAN connectivity, the changed configuration reverts to its original (pre-push) configuration. • Selected—Enabled. The MG90 discards AMM-pushed changes. • Not selected—Disabled. The MG90 does not discard AMM-pushed changes.
Restore previous configuration after (secs)	Interval to wait before restoring previous configuration Enter the amount of time (in seconds) that the MG90 keeps new configuration parameters pushed by the AMM that result in losing WAN connectivity. If the MG90 has no WAN connectivity after the timer expires, the MG90 will revert to the original configuration. *Note: This field is available only if Remote Configuration WAN Recovery is selected.*

WAN > SIM Configuration

The SIM Configuration tab is used to indicate which SIM slots are used for each installed cellular radio.

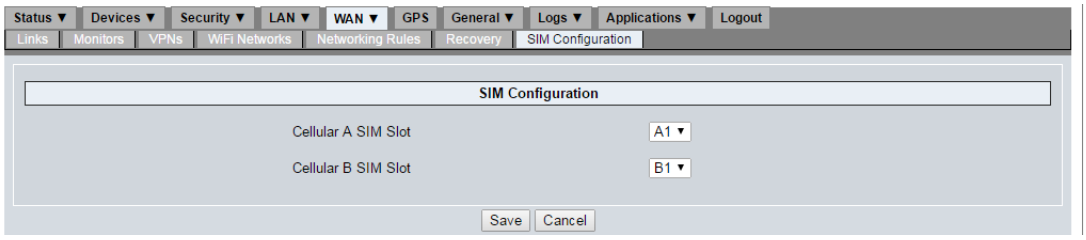

Figure 17-25: LCI: WAN > SIM Configuration—Sample screen

Table 17-27: WAN > SIM Configuration screen fields

Field	Description
Cellular A SIM Slot	Select the slot that contains the SIM for the Cellular A LTE radio. • A1 • A2
Cellular B SIM Slot	Select the slot that contains the SIM for the Cellular B LTE radio. • B1 • B2

18: GPS Tab

This chapter describes the GPS tab, which allows you to identify the GPS source the MG90 uses, and to configure GPS reporting options.

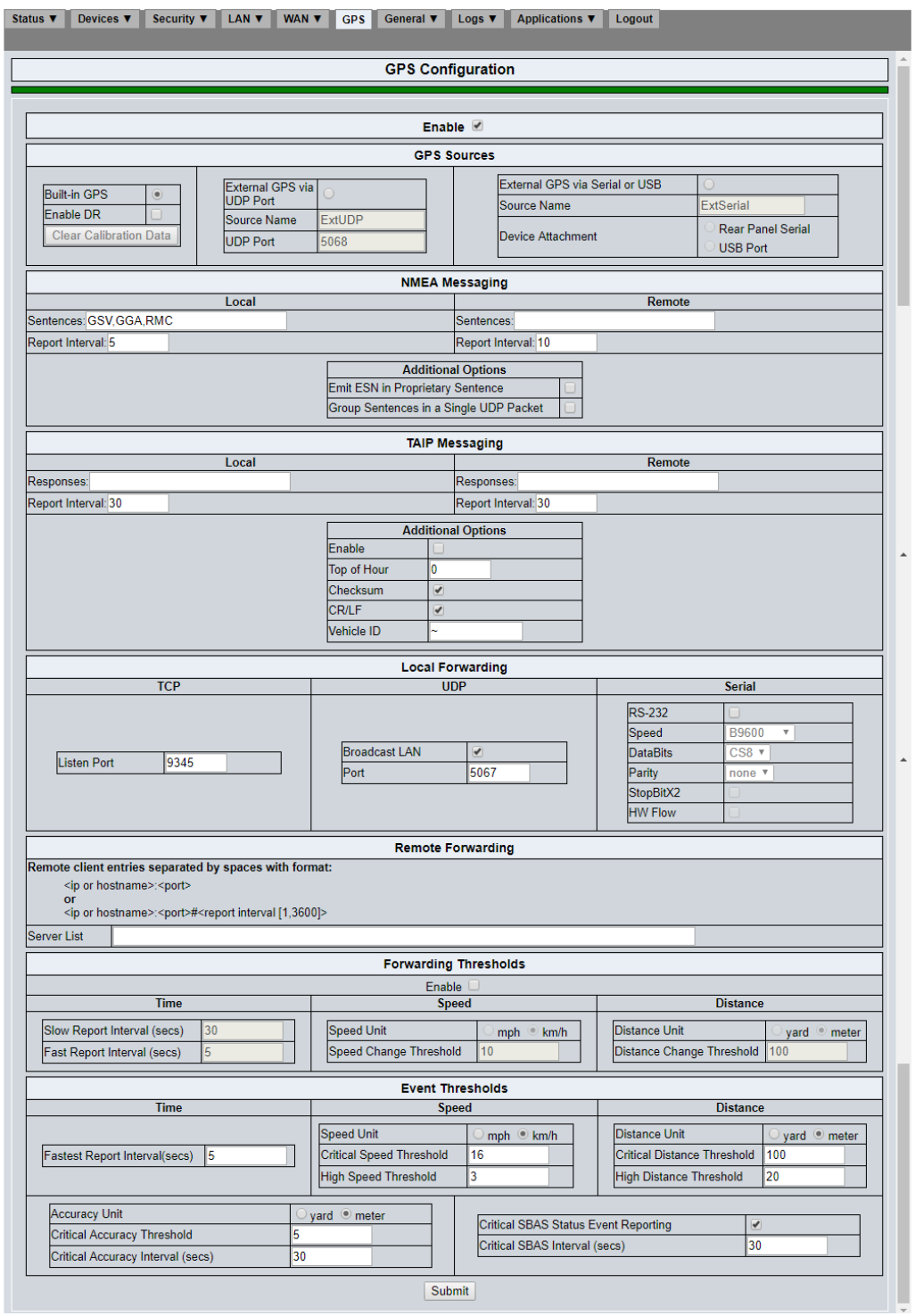

Figure 18-1: LCI: GPS—Sample screen

Note: The MG90 supports both National Marine Electronics Association (http://www.nmea.org/) and Trimble ASCII Interface Protocol (TAIP) messages. When configuring GPS, make sure to choose the correct NMEA and/or TAIP sentences for the applications that they will be sent to.

Table 18-1: GPS screen fields

Field	Description
Enable	Enable/disable custom GPS configuration • Selected—Enabled • Not selected—Disabled (Note—All fields on the screen are disabled.)
GPS Sources Select the appropriate GPS source—Built-in GPS, External GPS via UDP Port, or External GPS via Serial or USB. (Only one can be selected—Built-in GPS is the default.)	
Built-in GPS	Internal GPS • Selected—MG90 uses the internal GPS device. (Default) • Not selected—Not used
Enable DR	GPS Dead Reckoning • Selected—Enabled. Calibration will begin automatically when vehicle begins moving. See Configuring Dead Reckoning on page 73 for details. • Not selected—Disabled
Clear Calibration Data (button)	Clear previous Dead Reckoning calibration settings and immediately begin recalibrating. *Note: This button is available only if Enable DR is selected.*
External GPS via UDP Port	External GPS connected to UDP port • Selected—MG90 uses the external GPS device. • Not selected—Not used
Source Name	Descriptive name of the GPS device (appears in Status > General). • Default: ExtUDP *Note: This field is available only if External GPS via UDP Port is selected.*
UDP Port	UDP port used by external GPS • Default: 5068 *Note: This field is available only if External GPS via UDP Port is selected.*
External GPS via Serial or USB	External GPS connected to Serial or USB port • Selected—MG90 uses the external GPS device. *Note: Ensure the Serial Port in Devices > Serial is set to GPS in the Use field.* • Not selected—Not used
Source Name	Descriptive name of the GPS device (appears in Status > General). • Default: ExtSerial *Note: This field is available only if External GPS via Serial or USB is selected.*

Table 18-1: GPS screen fields (Continued)

Field	Description
Device Attachment	Physical port used by GPS device • Rear Panel Serial—The MG90's DB9 serial port. • USB Port—Either of the MG90's USB ports on the rear panel. *Note: This field is available only if External GPS via Serial or USB is selected.*
NMEA Messaging *Note: Local and remote consumers (devices 'listening' for GPS messages) can both be defined.*	
Local	
Sentences	Supported NMEA sentences for Local messages Enter a comma-separated list of supported NMEA sentences. Available sentences (as defined in the NMEA 0183 specification) are: • GGA: Global Positioning System Fix Data • GLL: Geographical Position, Latitude/Longitude • GSA: GPS DOP and active satellites • GSV: GPS Satellites in view • RMC: Recommended minimum specific GPS/TRANSIT data • VTG: Track Made Good and Ground Speed • ZDA: UTC Date/Time and Local Time Zone Offset
Report Interval	Interval between local NMEA message submissions Enter the number of seconds to wait between sending each NMEA message. • Default: 5
Remote	
Sentences	Supported NMEA sentences for Remote messages Enter a comma-separated list of supported NMEA sentences. Available sentences (as defined in the NMEA 0183 specification) are: • GGA: Global Positioning System Fix Data • GLL: Geographical Position, Latitude/Longitude • GSA: GPS DOP and active satellites • GSV: GPS Satellites in view • RMC: Recommended minimum specific GPS/TRANSIT data • VTG: Track Made Good and Ground Speed • ZDA: UTC Date/Time and Local Time Zone Offset
Report Interval	Interval between remote NMEA message submissions Enter the number of seconds to wait between sending each NMEA message. • Default: 10
Additional Options	
Emit ESN in Proprietary Sentence	Enable/disable sending a proprietary NMEA sentence with ESN • Selected—Enabled • Not selected—Disabled

Table 18-1: GPS screen fields (Continued)

Field	Description
Group Sentences in a Single UDP Packet	Enable/disable sending of all NMEA sentences in a single packet • Selected—Enabled • Not selected—Disabled
TAIP Messaging *Local and remote consumers (devices 'listening' for GPS messages) can both be defined.*	
Local	
Responses	Supported TAIP responses for Local messages Enter a comma-separated list of supported TAIP responses. Available responses are: • AL: Altitude/Up Velocity • CP: Compact Position Solution • ID: Identification Number • LN: Long Navigational Message • PV: Position/Velocity Solution • ST: Status • TM: Time/Date
Report Interval	Interval between local TAIP message submissions Enter the number of seconds to wait between sending each TAIP message. • Default: 30
Remote	
Responses	Supported TAIP responses for Remote messages Enter a comma-separated list of supported TAIP responses. Available responses are: • AL: Altitude/Up Velocity • CP: Compact Position Solution • ID: Identification Number • LN: Long Navigational Message • PV: Position/Velocity Solution • ST: Status • TM: Time/Date
Report Interval	Interval between remote TAIP message submissions Enter the number of seconds to wait between sending each TAIP message. • Default: 30
Additional Options	
Enable	Enable/disable additional TAIP Messaging options • Selected—Enabled • Not selected—Disabled
Top of Hour	N/A

Table 18-1: GPS screen fields (Continued)

Field	Description
Checksum	Enable/disable inclusion of checksum in TAIP messages Enable this option if the application that is receiving the data requires checksums to ensure data integrity. • Selected—Enabled. Include checksums. • Not selected—Disabled. Do not include checksums. *Note: This field is available only if Enable is selected.*
CR/LF	Enable/disable inclusion of CR/LF (Carriage Return and Line Feed) in TAIP messages Enable this option if the application that is receiving the data requires each reply on a new line. • Selected—Enabled. Include CR/LF. • Not selected—Disabled. Do not include CR/LF. *Note: This field is available only if Enable is selected.*
Vehicle ID	Unique vehicle identification code If required, enter a unique identification code that will be included with each TAIP response. This is useful in cases where a single monitoring system is receiving traffic from multiple devices. • Length—4 alpha-numeric characters (Note: If the code is 1–3 characters, it is automatically padded with spaces.) *Note: This field is available only if Enable is selected.*
Local Forwarding Data can be sent via TCP, UDP, and Serial (RS-232).	
TCP Use of TCP clients is discouraged since a poorly behaved client can block connections and impede operation of the GPS system. The MG90 does not enforce a minimum value (fastest forwarding) but intervals faster than five seconds are not recommended.	
Listen Port	Local consumer TCP listen port • Default port: 9345 • Valid range: 0–65535
UDP	
Broadcast LAN	Enable/disable UDP broadcast • Selected—Enabled • Not selected—Disabled (Default)
Port	UDP port • Default port: 5067 • A valid port value must be entered.

Table 18-1: GPS screen fields (Continued)

Field	Description
Serial To receive data via the serial port: a. Assign the serial port to GPS in Devices > Serial. b. Connect a null modem cable with a DB9 connector to the gateway and the terminal. c. Change the communication parameters below to match the terminal communication specification.	
RS-232	Enable/disable serial data forwarding via RS-232 port • Selected—Enabled • Not selected—Disabled (Default)
Speed	Serial port speed Select the appropriate speed from the drop-down.
DataBits	Serial port data bits Select the appropriate number of bits from the drop-down.
Parity	Serial port parity Select the appropriate parity from the drop-down.
StopBitX2	Serial port stop bits • Selected—2 stop bits • Not selected—1 stop bit
HW Flow	Serial port hardware flow control • Selected—Enabled • Not selected—Disabled
Remote Forwarding (...)	

Server List	Remote consumer server list
	• Space-separated list of IP addresses, ports, and report intervals (optional)
	• Format:
	  • <ip or hostname>:<port>
	  Example: 10.0.0.12:5777 10.0.0.15:5777
	  • <ip or hostname>:<port>#<report_interval[1,3600]>
	  Example: 10.0.0.12:5777 10.0.0.15:5777#30

Forwarding Thresholds Forwarding thresholds define the rules for enabling variable interval reporting for NMEA and TAIP messaging, based on speed, distance, and elapsed time.	
Time	
Slow Report Interval (secs)	Maximum interval between reports, regardless of speed and distance threshold limits.
Fast Report Interval (secs)	Minimum interval between reports, regardless of speed and distance threshold limits.
Speed	
Speed Unit	Unit of speed measurement (mph or km/h)

Table 18-1: GPS screen fields (Continued)

Field	Description
Speed Change Threshold	Speed increase/decrease (since last report) at which point report should be forwarded (subject to Fast Report Interval).
Distance	
Distance Unit	Unit of distance measurement (yard or meter)
Distance Change Threshold	Change in position (since last report) at which point report should be forwarded (subject to Fast Report Interval).
Event Thresholds Event thresholds affect when and how frequently the MG90 reports GPS events to the AMM. These thresholds are based on time, speed, and distance. High and Critical thresholds are defined for speed and distance. For low-cost WAN links, the MG90 sends GPS information when a High threshold is crossed; for high-cost WAN links, the MG90 sends GPS information when a Critical threshold is crossed.	
Time	
Fastest Report Interval (secs)	Minimum interval between GPS event reports Set the minimum interval (in seconds) between GPS report submissions. If a report is ready to be sent due to a speed or distance threshold being crossed, the report will not be sent until this minimum interval has been reached. *Note: The MG90 does not enforce a minimum value (fastest forwarding) but intervals faster than five seconds are not recommended.*
Speed	
Speed Unit	Unit of measurement for vehicle speed Select mph or km/h.
Critical Speed Threshold	High-cost WAN link critical speed threshold Speed at which a GPS event is reported for a high-cost WAN link.
High Speed Threshold	Low-cost WAN link high speed threshold Speed at which a GPS event is reported for a low-cost WAN link.
Distance	
Distance Unit	Unit of measurement for distance traveled Select yard or meter.
Critical Distance Threshold	High-cost WAN link critical distance threshold Distance traveled at which a GPS event is reported for a high-cost WAN link.
High Distance Threshold	Low-cost WAN link high distance threshold Distance traveled at which a GPS event is reported for a low-cost WAN link.
Accuracy Unit	Unit of measurement for the Critical Accuracy Threshold field (see below). Select yard or meter. • Default: meter

Table 18-1: GPS screen fields (Continued)

Field	Description
Critical Accuracy Threshold	Position change threshold If the GPS position changes by more than this distance within the Critical Accuracy Interval, a GPS event is reported. • Default: 5
Critical Accuracy Interval (secs)	Critical accuracy interval Number of seconds over which critical accuracy threshold is considered. • Minimum: >0 • Default: 30
Critical SBAS Status Event Reporting	Report SBAS events to AMM When enabled, SBAS (Satellite Based Augmentation System) events are reported to the AMM. • Selected—Enabled • Not selected—Not enabled
Critical SBAS Interval (secs)	Minimum interval between SBAS event reports Set the minimum interval (in seconds) between SBAS report submissions. • Minimum: 1 • Default: 30

19: General Tab

This chapter describes the General tab.

The General tab includes the following sub-tabs:

- Startup—Configure the MG90's startup behavior when ignition is turned on. See General > Startup on page 196.
- Shutdown—Configure the MG90's shutdown (and restart) behavior. See General > Shutdown on page 196.
- Services—Configure Event Reporting. See General > Services on page 198.
- Tools—Run a variety of diagnostic and other tools. See General > Tools on page 199.
- Backup/Restore—Backup and restore the MG90's current configuration. See General > Backup/Restore on page 201.
- Advanced Routing Rules—Enter custom scripts to run at specific times. See General > Advanced Routing Rules on page 201.
- Auto Software Updates—Configure the MG90's behavior for downloading software updates. See General > Auto Software Updates on page 203.

General > Startup

The Startup tab is used to control the MG90's startup behavior when power is applied.

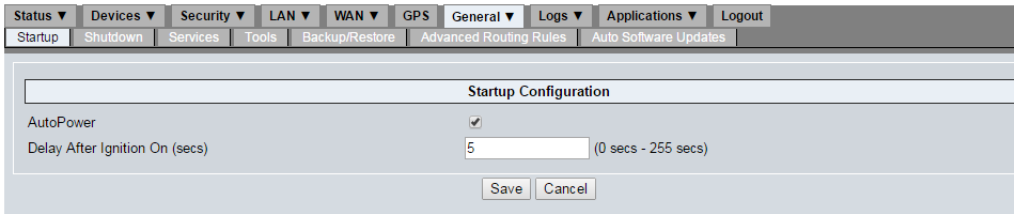

Figure 19-1: LCI: General > Startup—Sample screen

Table 19-1: General > Startup screen fields

Field	Description
AutoPower	MG90 startup behavior when power is applied • Selected—Start automatically. (Default) • Not selected—Start when Reset button is pressed.
Delay After Ignition On (secs)	Wait time between ignition on and power applied Enter the number of seconds of wait time before turning on the MG90's power after the ignition is turned on. • Range: 0–255 • Default: 5

General > Shutdown

The Shutdown tab is used to configure the MG90's shutdown behavior.

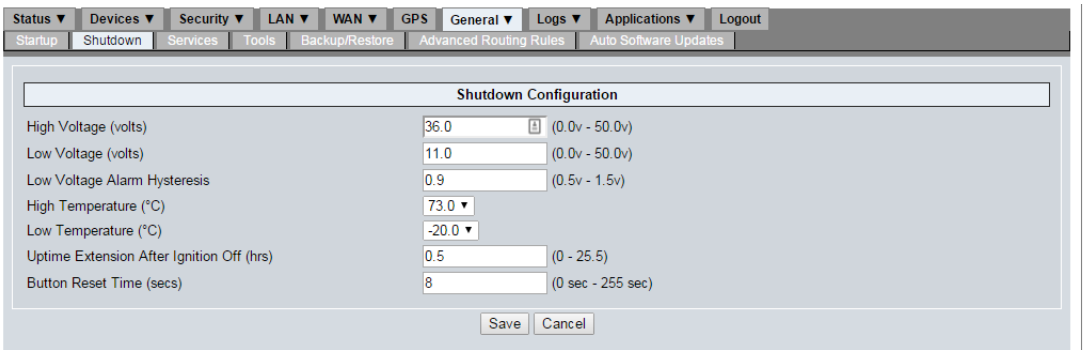

Figure 19-2: LCI: General > Shutdown—Sample screen

Table 19-2: General > Shutdown screen fields

Field	Description
High Voltage (volts)	Upper voltage threshold Enter the upper voltage threshold (in volts). The MG90 will shut down if the voltage exceeds this threshold. • Range: 0.0–50.0 • Default: 36.0 *Note: Voltage readings are subject to cable length and will always be slightly lower than the voltage measured at the source.*
Low Voltage (volts)	Lower voltage threshold Enter the lower voltage threshold (in volts). The MG90 will shut down if the voltage drops below this threshold to prevent further discharge of the vehicle battery. • Range: 0.0–50.0 • Default: 11.0 *Note: This is the "slow discharge" shutdown. When a vehicle cranks, the ignition system should conform to SAE J537. If it does not and the voltage spikes down below the SAE minimum, the MG90 will reboot, regardless of this setting. Also, voltage readings are subject to cable length and will always be slightly lower than the voltage measured at the source.*
Low Voltage Alarm Hysteresis	Low voltage hysteresis required for restart Enter the hysteresis value (in volts). After the MG90 shuts down due to low voltage, it will not restart until the input voltage exceeds Low Voltage + Low Voltage Alarm Hysteresis. This ensures the MG90 does not continually shutdown and restart when voltage is fluctuating around the low voltage value. • Range: 0.5–1.5 • Default: 0.9
High Temperature (°C)	Upper temperature threshold Select the upper temperature threshold (in °C). The MG90 will shut down if the internal temperature exceeds this threshold. • 85.0 • 73.0 (Default) • 60.0

Table 19-2: General > Shutdown screen fields (Continued)

Field	Description
Low Temperature (°C)	Lower temperature threshold Select the lower temperature threshold (in °C). The MG90 will shut down if the internal temperature drops below this threshold. • 0.0 • -20.0 (Default) • -30.0 • -40.0
Uptime Extension After Ignition Off (hrs)	Time before shutdown after turning off ignition Enter the time, in hours, that the MG90 stays on and remains communicating after turning off the vehicle ignition. • Range: 0–25.5 • 0.5 (Default) *Note: Choose this time carefully. If too much time is specified, the vehicle's battery may be drained.*
Button Reset Time (secs)	Required duration for Reset button press Enter the amount of time (in seconds) that the Reset button must be pressed to trigger a factory reset. • Range: 0–255 • 8 (Default)

General > Services

The Device Service Configuration screen is used to configure event reporting.

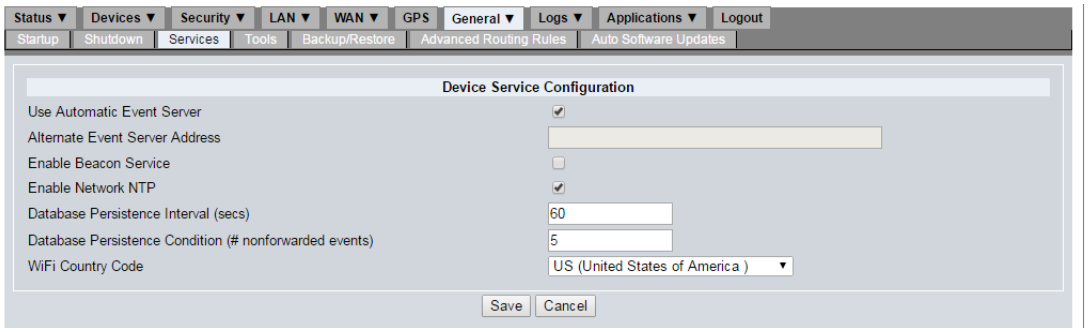

Figure 19-3: LCI: General > Services—Sample screen

Table 19-3: General > Services screen fields

Field	Description
Use Automatic Event Server	Enable/disable a default event server • Selected—Use the default event server (<ESN>.dels.omgservice.com) that was set up for the MG90 by Sierra Wireless, where <ESN> is the MG90's serial number. (Default) • Not selected—Use the specified Alternate Event Server Address
Alternate Event Server Address	Enter the address of the event server to be used. *Note: This field is available only if Use Automatic Event Server is not selected.*
Enable Beacon Service	N/A
Enable Network NTP	Enable/disable network NTP • Selected—Enabled (Default) • Not selected—Disabled
Database Persistence Interval (secs)	*Important: Do not change displayed values.*
Database Persistence Condition (# nonforwarded events)	
Wi-Fi Country Code	Wi-Fi country code Select the country code that the MG90 will broadcast.

General > Tools

The MG90 is equipped with a suite of diagnostic and device management 'command line' tools. The Tools tab allows you to choose the tools to run and enter their required command line arguments.

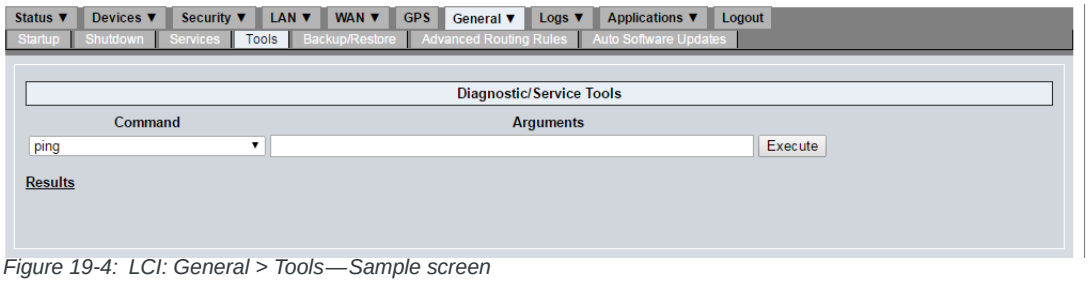

Figure 19-4: LCI: General > Tools—Sample screen

Table 19-4: General > Tools screen fields

Field	Description
Command	Select a diagnostic/service command, and then enter appropriate arguments and click Execute to run the command: • ping—Send an ICMP ping to network hosts. Can be used to determine if a particular host is reachable by the MG90. • dhcp-leases—Display the current DHCP leases assigned by the LAN Segment DHCP server. • traceroute—UNIX traceroute utility. Display a list of all gateways between the MG90 and the specified host. • route—Display the MG90's current routing table. • arp—Display the MG90's cached mappings between IP addresses and MAC addresses. • netstat—Display network connections, routing tables, interface statistics, masquerade connections and multicast memberships. • ifconfig—Display the configuration for each network interface. • iwconfig—Display the configuration of each wireless interface. • iwlist—Display additional information from a wireless network interface that is not displayed by iwconfig. The main argument is used to select a category of information while iwlist displays all detailed information related to this category, including information already shown by iwconfig. • ipsec-vpn-status—Display the output from the IPsec status command which shows statistics regarding your current IPsec VPN connection. • clean-local-software-update-cache—Clear the local cache. • verify-local-software-repository—Check for possible software repository problems prior to applying downloaded software updates. • download-new-software-updates— Manually download new software updates. • enable-fips-cryptographic-modules—Enable FIPS mode of operation on the MG90 (this option is only available on devices where FIPS is not already enabled). *Note: Be careful when enabling FIPS, as there is no option to revert from FIPS to non-FIPS.* • reboot-device— Reboot the MG90. • lsusb—Display information about the USB buses available and the devices currently connected to them. • enable-usb-bypass-PEM-CA—Allow a PC to directly access the Cellular A module via USB port B (the lower port on the rear panel). This could be used to allow a PC application (for example, Sierra Wireless' Skylight) to establish a network connection using the Cellular A module. • enable-usb-bypass-PEM-CB—Same as enable-usb-bypass-PEM-CA, but for the Cellular B module. • disable-usb-bypass—Stop the Cellular A or Cellular B bypass. • dmcapture—Capture the cellular chip's diagnostic log.
Arguments	Command arguments Enter appropriate arguments for the selected command.
Execute (button)	Click to execute the selected command and show the command output in Results.
Results	Output of selected command

General > Backup/Restore

The Backup/Restore tab is used to backup the MG90's configuration (multiple backups can be saved), and if required, restore a saved configuration.

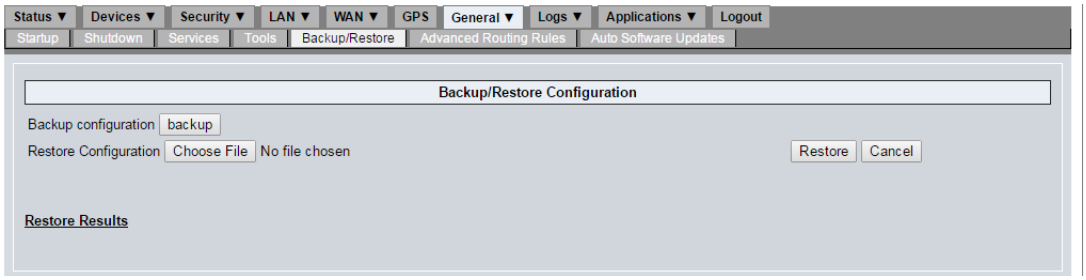

Figure 19-5: LCI: General > Backup/Restore—Sample screen

Table 19-5: General > Backup/Restore screen fields

Field	Description
Backup Configuration	Click backup to save the current MG90 configuration as a gzip file (config-<date>.tar.gz) in your default downloads folder.
Restore Configuration	Click Choose File/Browse and navigate to the folder containing the configuration file you want to restore (config-<date>.tar.gz).
Restore (button)	Click Restore to reconfigure the MG90 with the selected configuration file.
Restore Results	When the restoration is complete, comprehensive details appear in the Restore Results section.

General > Advanced Routing Rules

Advanced routing rules are custom scripts that can be executed at boot time, on WAN link activation, on LAN activation, or when a WAN connection changes from connected to disconnected.

Important: *These scripts should only be used under direction of Sierra Wireless Technical Support.*

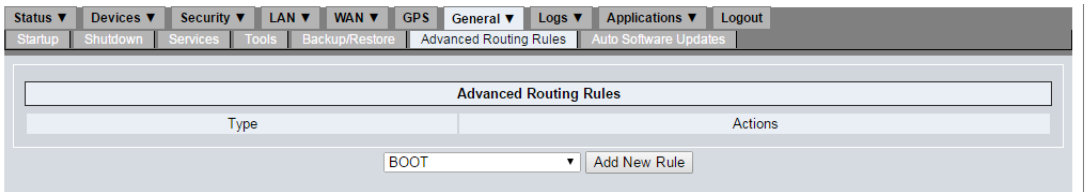

Figure 19-6: LCI: General > Advanced Routing Rules—Sample screen

Table 19-6: General > Advanced Routing Rules screen fields

Field	Description
Type	Script type: • BOOT: a boot file executes once on system boot. • LAN-Activation: this type of file executes after a bridge interface is brought up. The script argument uses the bridge name (e.g. br0). • WAN-Device State Change: this routing rule executes when a link changes state, for example from UP to DOWN and vice versa. Inputs include the interface IP address and the gateway IP address. • WAN-Activation: this file executes when a link becomes the active link. Inputs include the interface IP address and the gateway IP address.
Actions	Click these optional links to perform actions on the associated scripts: • Delete—Delete the associated script. • Configure—Configure the associated script. See General > Advanced Routing Rules > Add New Rule/Configure Rule on page 202.
Add New Rule (button)	Select the script type to add and click Add New Rule: • BOOT—Boot file that executes once on system boot. • LAN-Activation—Executes after a bridge interface is brought up. The script argument uses the bridge name (e.g. br0). • WAN-Device State Change—Routing rule that executes when a link changes state, for example from UP to DOWN and vice versa. Inputs include the interface IP address and the gateway IP address. • WAN-Activation—Executes when a link becomes the active link. Inputs include the interface IP address and the gateway IP address.

General > Advanced Routing Rules > Add New Rule/ Configure Rule

The Advanced Routing Rules screen is used to enter a custom script of the type that you selected in General > Advanced Routing Rules.

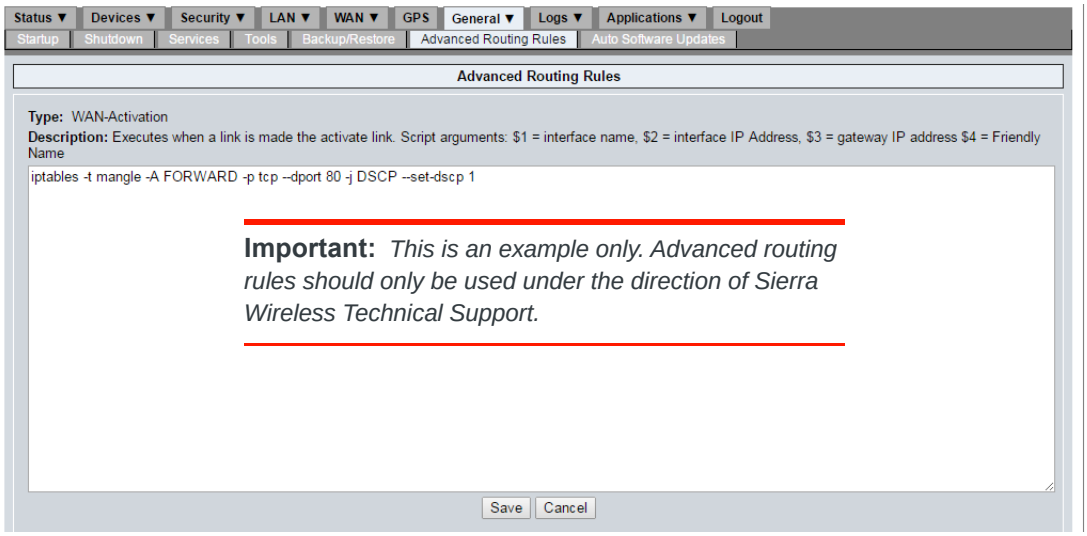

Figure 19-7: LCI: General > Advanced Routing Rules > Add New Rule/Configure Rule—Sample screen

Table 19-7: General > Advanced Routing Rules > Add New Rule (or Configure) screen fields

Field	Description
Type **Description**	Script type and description of when the script will execute • BOOT—Boot file that executes once on system boot. • LAN-Activation—Executes after a bridge interface is brought up. The script argument uses the bridge name (e.g. br0). • WAN-Device State Change—Routing rule that executes when a link changes state, for example from UP to DOWN and vice versa. Inputs include the interface IP address and the gateway IP address. • WAN-Activation—Executes when a link becomes the active link. Inputs include the interface IP address and the gateway IP address.
Script entry box	Enter the required script (series of commands)

General > Auto Software Updates

The Auto Software Updates tab is used to:
- Configure how software updates are downloaded and installed.
- Configure firmware switching and image management.

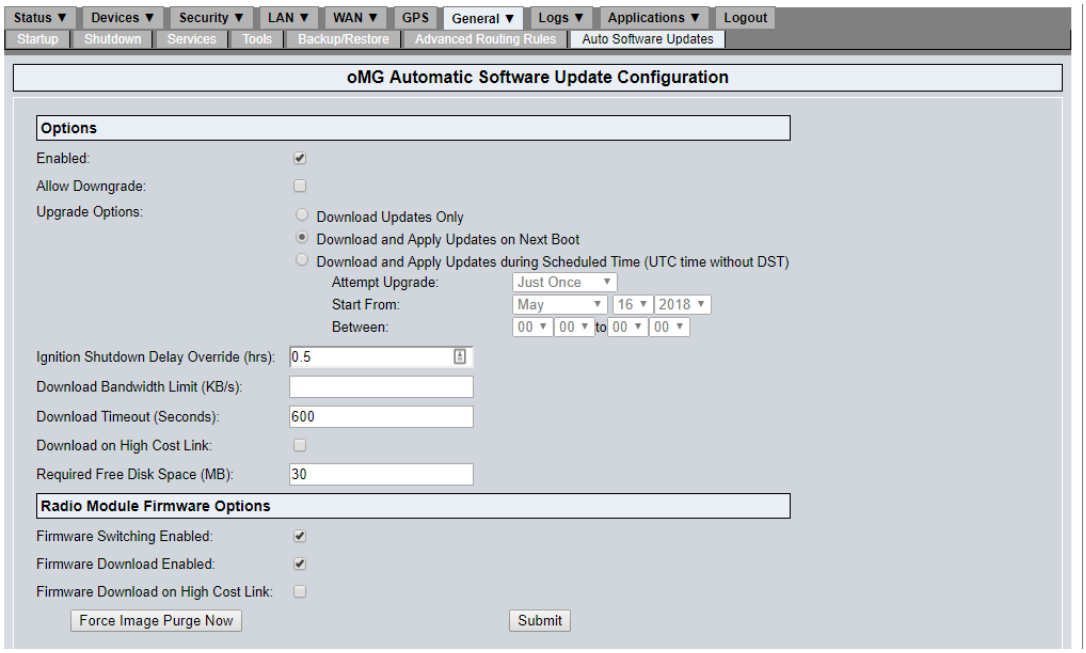

Figure 19-8: LCI: General > Auto Software Updates—Sample screen

Table 19-8: General > Auto Software Updates screen fields

Field	Description
Options The following options control MG90 firmware updates.	
Enabled	Enable/disable automatic software updates • Selected—Enabled (Default). The MG90 will check for any update(s) that have been published to Sierra Wireless' central repository, and automatically download and apply them based on the selected Upgrade Options. • Not selected—Disabled.
Allow Downgrade	Enable installation of software downgrades • Selected—Enabled. Software versions lower than that currently installed can be downloaded and applied as well as upgrades. • Not selected—Disabled (Default). Only higher versions can be downloaded and applied.

Upgrade Options	• Download Updates Only—The MG90 does not automatically apply any updates that have been downloaded. To apply updates, select one of the other two options. The updates will then be applied based on the rules for those selections.
	• Download and Apply Updates on Next Boot—(Default) When the MG90 boots, it automatically applies any updates that have been downloaded.
	• Download and Apply Updates during Scheduled Time (UTC time without DST)—If any updates have been downloaded, the MG90 applies them during the 'scheduled time':
	  ◦ Attempt Upgrade—How often upgrades can be installed:
	  ▪ Just Once—Only on the scheduled date and time slot
	  ▪ Every Day—Each day beginning on Start From
	  ▪ Every Week—Once per week beginning on Start From (e.g. 17 May 2017 is weekly attempts on Wednesdays)
	  ▪ Every Month—Once per month beginning on Start From (e.g. 17 May 2017 is monthly attempts on the 17th)
	  ◦ Start From—First day that updates can be applied. If date is last day of the month, 'every month' upgrades will be on the last day of each month.
	  ◦ Between—Time slot (UTC times) during which updates can be applied. (DST adjustments are not applied to the time slot.)
	Note: In cases where the unit is never shut off (i.e. when a vehicle is in operation 24 hours per day, 7 days per week), use the 'Scheduled Time' upgrade option to install updates.

Ignition Shutdown Delay Override (hrs)	Override ignition shutdown delay The MG90 performs updates only when the ignition is turned on. If the ignition is turned off during an update, this option overrides the Uptime Extension After Ignition Off shutdown option (seeTable 19-2 on page 197) by the number of hours specified. • Default: 0.5 *Note: Choose this override value carefully. If the time is too short, the MG90 may turn off before the update is complete. If the time is too long, the vehicle's battery may be drained.*

Table 19-8: General > Auto Software Updates screen fields (Continued)

Field	Description
Download Bandwidth Limit (KB/s)	Bandwidth available for downloading software updates Set the maximum bandwidth (in KB/s) available for downloading updates over the WAN link. This can be used to ensure that adequate bandwidth is available for regular communications over the WAN.
Download Timeout (Seconds)	Download timeout period Enter the amount of time (in seconds) after which failure to receive data causes the download to time out. The download will stop, and then continue when the gateway comes back online. This field is useful for slower links that may require larger values when dealing with large files, or when dealing with a bad link that frequently jumps between being offline and online. • Default: 600
Download on High Cost Link	Enable/disable software download on high cost WAN links • Selected—Enabled. The MG90 will download the update even when a high-cost WAN link is in use (e.g. a cellular connection). • Not selected—Disabled (Default). The MG90 downloads updates only on low-cost WAN links (e.g. Wi-Fi access point within a vehicle depot). *Tip: If bandwidth consumption is a concern (e.g. due to cost), set the cellular link to be a high cost link, and disable the Download on High Cost Link option.*
Required Free Disk Space (MB)	Default: 100mb (TBC)
Radio Module Firmware Options The following options control carrier-specific firmware image updates for the MG90's on-board MC7354/MC74XX/EM75XX cellular WAN module:	
Firmware Switching Enabled	Enable/disable carrier-based firmware image switching • Selected—Enabled (Default). The MG90 will detect the carrier based on the SIM card, and automatically install the appropriate image package for that carrier. *Note: When enabled, the gateway may require an additional 8 seconds to connect on boot.* • Not selected—Disabled.
Firmware Download Enabled	Enable/disable automatic firmware downloading • Selected—Enabled (Default). The MG90 will automatically download an image package when the carrier detected on the SIM card does not match the current carrier module image and the required image is not available for installation from the MG90's storage. • Not selected—Disabled
Firmware Download on High Cost Link	Enable/disable firmware downloads on high cost WAN links • Selected—Enabled. The MG90 will download the firmware image even when a high-cost WAN link is in use (e.g. a cellular connection). • Not selected—Disabled (Default). The MG90 downloads firmware images only on low-cost WAN links (e.g. Wi-Fi access point within a vehicle depot). *Note: If bandwidth consumption is a concern (e.g. due to cost), set the cellular link to be a high cost link, and disable the Firmware Download on High Cost Link option.*

Table 19-8: General > Auto Software Updates screen fields (Continued)

Field	Description
Purge Images on Next Boot	Purge images after installation • Selected—Enabled. All stored image packages on the MG90 will be deleted after the MG90 reboots and a connection has been made using the LTE radio. • Not selected—Disabled (Default). To purge image files manually, click Force Image Purge Now.
Force Image Purge Now (button)	Click to immediately purge (delete) all firmware image files currently stored on the MG90. If any radio modules need to install one of these images later, the image will need to be downloaded (or installed via USB stick).

20: Logs Tab

This chapter describes the Logs tab screens, which allow you to view system log (error/status) messages.

The Logs tab includes the following sub-tabs:

- Current Logs—Display logs that have not been uploaded to the AMM. See Logs > Current Logs on page 207.
- Archived Logs—Display logs that have been uploaded to the AMM. See Logs > Archived Logs on page 207.

Logs > Current Logs

The Current Logs tab lists all logs currently stored on the MG90 that will be uploaded to the AMM at the end of the day.

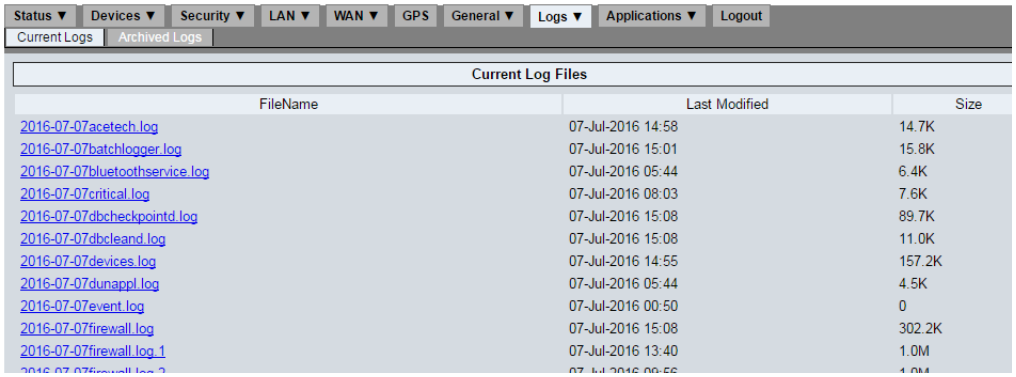

Figure 20-1: LCI: Logs > Current Logs—Sample screen

Table 20-1: Logs > Current Logs screen fields

Field	Description
FileName	Log name comprising the date it was created and the feature the log applies to.
Last Modified	Date and time the log was last updated.
Size	File size in KB.

Logs > Archived Logs

The Archived Logs tab lists the logs that have been uploaded to the AMM.

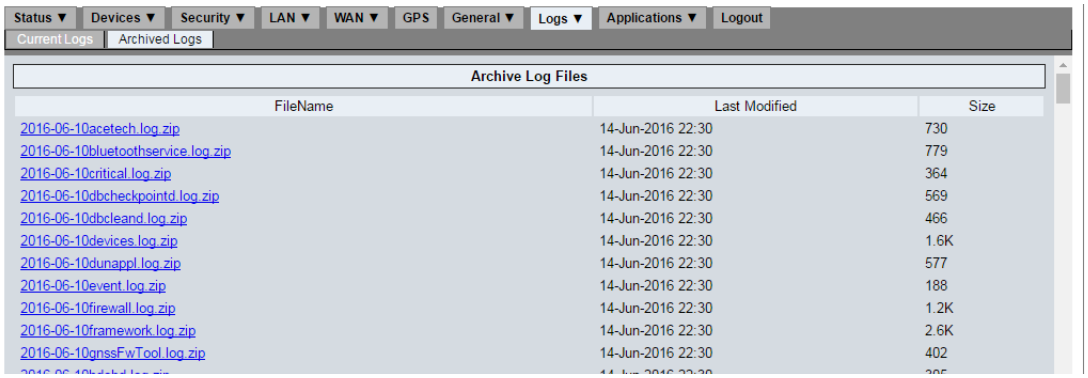

Figure 20-2: LCI: Logs > Archived Logs—Sample screen

Table 20-2: Logs > Archived Logs screen fields

Field	Description
FileName	Log name comprising the date it was created and the feature the log applies to.
Last Modified	Date and time the log was last updated.
Size	File size in KB.

21: Applications Tab

Several value added applications are available for the MG90 that enhance and extend the MG90's capabilities. Applications are purchased separately.

Examples of common applications include:

- Telemetry—Monitors and reports information about key vehicle telemetry parameters such as speed, acceleration etc.
- Asset Manager—Reports GPS locations of tracked assets to the AMM.

Each application requires configuration on both the MG90 and the AMM. Configuration settings are application specific and may include modifiable settings, status information or both. Documentation for each application and its configuration is available at source.sierrawireless.com.

Note: Contact your Sierra Wireless Account Manager or Channel Partner to inquire about Application Licensing options.

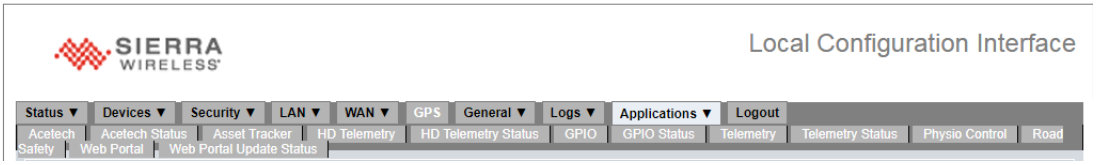

Figure 21-1: Applications Tab

General Purpose I/O Configuration

The MG90 GPIOs provides five GPIO (General Purpose I/O) signals that can be used to receive external sensor inputs or send data to external devices.

- Four GPIOs are provided on the DB9 serial connector
- One GPIO is provided on the power supply module.
- Each GPIO can be configured for Input or Output.

Note: Generic switch boxes can be used for GPIO testing.

This section describes the Applications GPIO tab, which allows you to configure the GPIOs.

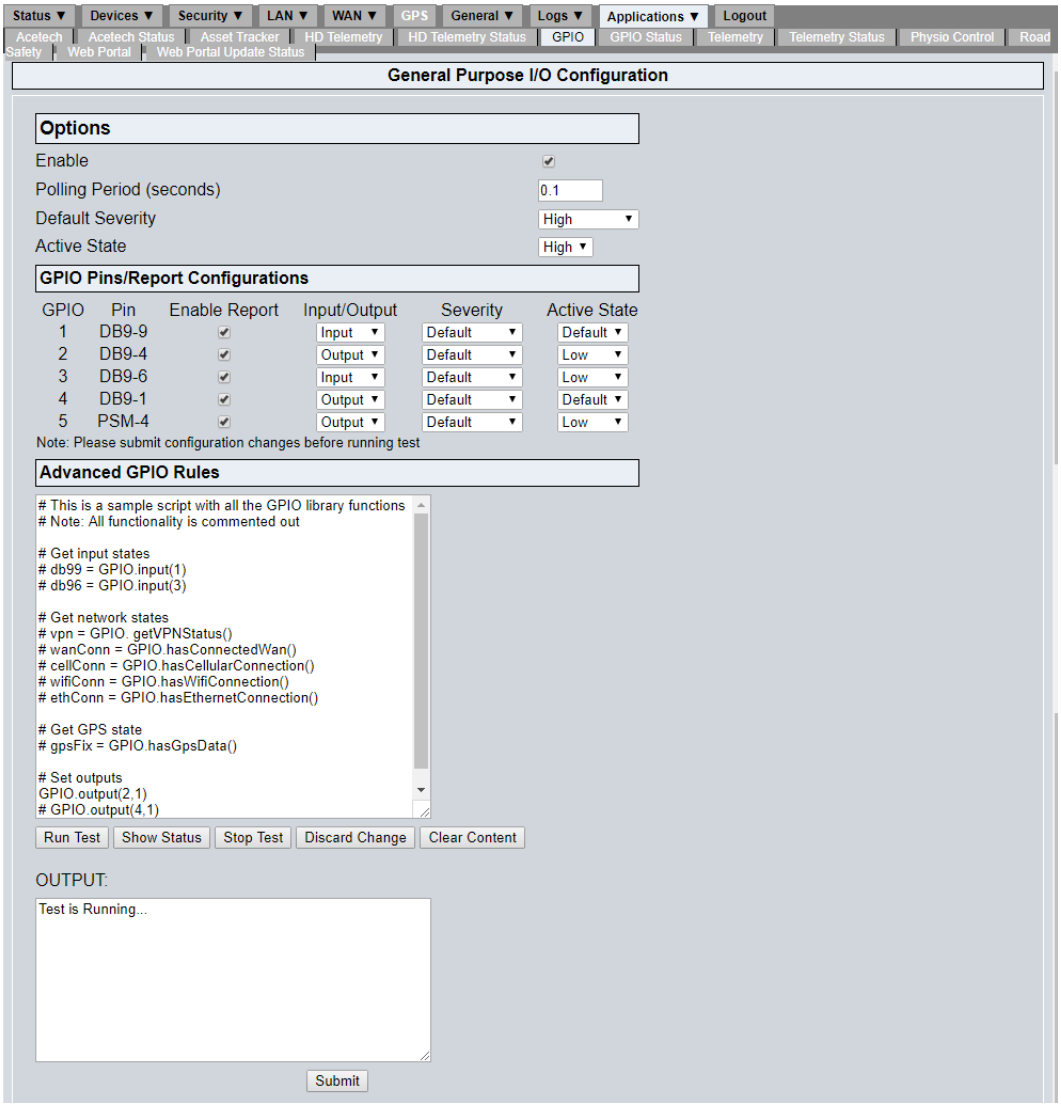

Figure 21-2: LCI: Applications > GPIO

Using GPIOs

This screen is used to configure the behavior of available GPIOs, and enter and store a script that can access the GPIOs and available GPIO API (library) functions.

Note: To view the past states of the available GPIOs, see GPIO Status on page 214.

To configure and use the GPIOs:

1. Select Enable to enable all GPIOs for use based on configuration settings on this screen.
2. Set a polling period measured in seconds. (e.g. if Polling Period is 0.1, all GPIOs are checked every 0.1 seconds)
3. Set a default DELS event severity level to be assigned to reportable events for any GPIO that is configured for Default severity.

4. Set the active state to be used for any GPIO that is configured for Default active state.
5. For each of the five available GPIOs:
   a. Select Enable Report if DELS events on the GPIO are to be sent to AMM.
   b. Select the GPIO direction (input to or output from the MG90).
   c. Select a DELS severity level to assign to events on this GPIO. To use the Default Severity from the Options section, select Default.
   d. Select the GPIO's active state (Low/High), or select Default to use the Active State from the Options section.
   e. Click Submit to commit the GPIO configuration settings.
   f. In the Advanced GPIO Rules editor pane, develop a script to process the GPIOs:
      i. Enter (or paste from a text editor) a Python script to process GPIO inputs, outputs, and API function calls.
      ii. While developing the script, use the editor buttons to test the script. (See Table 21-2 on page 212.)
      iii. When the script is complete and ready to be stored and run on the MG90, click Submit.

Table 21-1: Applications > GPIO screen fields

Field	Description
Options The following options are used to enable and set default details for all GPIOs.	
Enable	Enable / disable all GPIOs • Selected—Enabled (Default). GPIOs can be used as inputs or outputs depending on selected GPIO Pins/Report Configurations options. • Not selected—Disabled. GPIOs are not accessible. *Note: It is not possible to enable/disable individual GPIOs.*
Polling Period (seconds)	Interval between GPIO status checks, in seconds. • Minimum recommended interval—0.1 seconds (Default)
Default Severity	Default severity level assigned to DELS events (events that are forwarded to AMM) for GPIOs that have Severity (In the GPIO Pins/Report Configuration section) = Default
Active State	Active state of GPIOs that have Active State (in the GPIO Pins/Report Configuration section) = Default.
GPIO Pins/Report Configurations The following options define each available GPIOs direction, DELS event severity level, and active state.	
GPIO	GPIO number
Pin	Physical GPIO location • DB9-x—GPIO on DB9 connector, pin x • PSM-4—GPIO on Power Supply Module, pin 4

Table 21-1: Applications > GPIO screen fields (Continued)

Field	Description
Enable Report	Enable/disable DELS event reporting • Selected—Events (state change low→high or high→low) on this GPIO are reported to AMM. • Not selected—Events are not reported to AMM.
Input/Output	GPIO direction • Input • Output
Severity	Severity level assigned to DELS events for this GPIO If Default is selected, the Default Severity level in the Options section is used.
Active State	Active satate of GPIO If Default, then Active State in the Options section is used.
Advanced GPIO Rules Script to process GPIO inputs/outputs, use GPIO APIs, etc.	
Rule editor pane	Text pane to enter Python script used to process GPIOs (read inputs, write outputs) and access GPIO API functions to determine various system conditions. The MG90 supports a single script only. To save additional scripts for later use, save them on a computer. When Submit is clicked, the script in the pane is written to the MG90, replacing the existing script (if one was previously saved).
OUTPUT	Output message area displaying results of testing the script.

Table 21-2: GPIO Rule Editor Buttons

Button	Description
Run Test	Execute the script that is in the Rule Editor pane.
Show Status	Show the current status of all five GPIOs.
Stop Test	Stop executing the test.
Discard Changes	Remove all changes that have been made to the script since the last time Submit was clicked.
Clear Content	Clear the Rule editor.
Submit	Submit the script from the Rule editor to the MG90 to run in the background. The script will execute each time the gateway boots.

Table 21-3: GPIO API Functions

API	Parameters	Return Value	Notes
GPIO.output(Port, State)	Port: 1–5 State: 0 | 1	void	Set state of specified output GPIO (1 is high) e.g. GPIO.output(4,1)
GPIO.input(Port)	Port: 1–5	0 | 1	Get state (1 is active high) of specified input GPIO e.g. GPIO.input(4)
GPIO.getVPNStatus()		Boolean	Returns true when VPN is connected
GPIO.hasConnectedWan()		Boolean	Returns true when WAN is connected
GPIO.hasCellularConnection()		Boolean	Returns true when there is a Cellular WAN connection
GPIO.hasWiFiConnection()		Boolean	Returns true when there is a Wi-Fi WAN connection
GPIO.hasEthernetConnection()		Boolean	Returns true when there is an Ethernet WAN connection
GPIO.hasGpsData()		Boolean	Returns true when GPS data is available
GPIO.isWifiAccessPointEnabled()		Boolean	Returns true when Wi-Fi Access Point is enabled

Sample GPIO Rule Script

The following script (shown in Figure 21-2 on page 210) demonstrates how each GPIO API can be used:

```
# This is a sample script with all the GPIO library functions
# Note: All functionality is commented out

# Get input states
# db99 = GPIO.input(1)
# db96 = GPIO.input(3)

# Get network states
# vpn = GPIO. getVPNStatus()
# wanConn = GPIO.hasConnectedWan()
# cellConn = GPIO.hasCellularConnection()
# wifiConn = GPIO.hasWifiConnection()
# ethConn = GPIO.hasEthernetConnection()

# Get GPS state
# gpsFix = GPIO.hasGpsData()

# Set outputs
GPIO.output(2,1)
# GPIO.output(4,1)
# GPIO.output(5,1)
```

GPIO Status

Displays the values of the GPIOs at each polling interval.

This section describes the Applications GPIO tab, which allows you to configure the GPIOs.

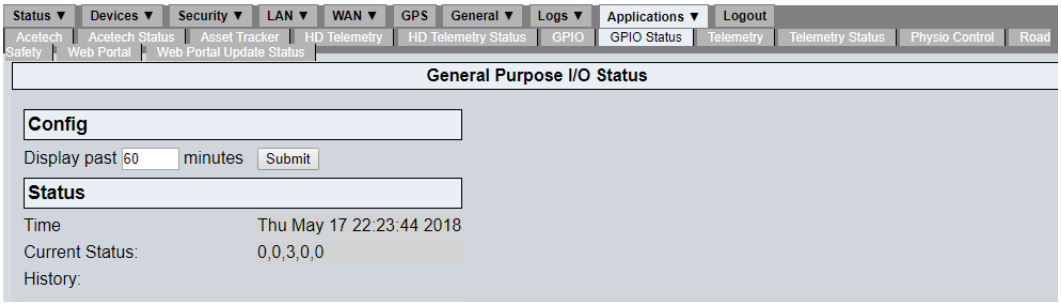

Figure 21-3: LCI: Applications > GPIO Status

Table 21-4: Applications > GPIO Status screen fields

Field	Description
Config Display options	
Display past <...> minutes	Number of minutes of GPIO state history (DELS events) to display • No limit *Note: The MG90 cleans the events database on a regular basis. If the listing appears to be incomplete, check the event report on the AMM, or the GPIO log on the AMM or in the LCI (Logs > Current Logs).*
Submit (button)	Display all available GPIO state events recorded in the past number of minutes.
Status Current system time, most recent GPIO state, and GPIO state history	
Time	Current system time
Current Status	Most recent GPIO states • Format: <gpio_1_state>,<gpio_2_state>,<gpio_3_state>,<gpio_4_state>,<gpio_5_state> where <gpio_#_state> is 0 (low) or the gpio_# (high) • e.g. 0,0,3,0,0 indicates: ◦ GPIO1 low ◦ GPIO2 low ◦ GPIO3 high ◦ GPIO4 low ◦ GPIO5 low
History	GPIO states reported in the past number of minutes.

22: Logout Tab

Click the Logout tab to end your LCI session.

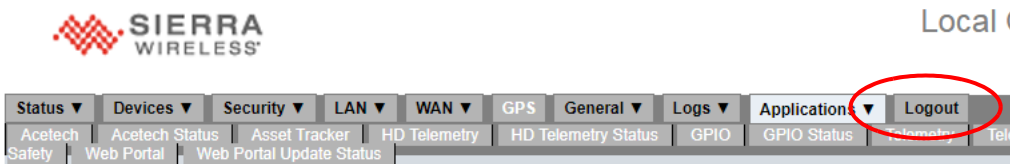

Figure 22-1: Logout Tab

23: LEDs

The MG90 uses six LEDs to indicate its current operational status. The table below describes the behavior for each LED.

LED Behavior

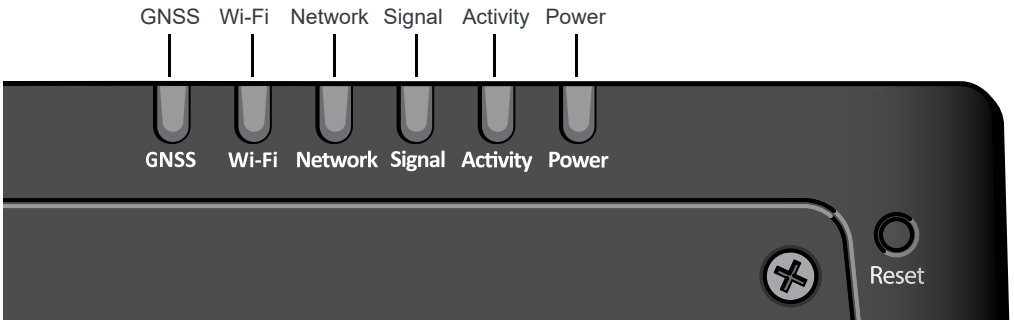

Figure 23-1: MG90 LED Status Indicators (front panel)

Table 23-1: LED Behavior

LED	Color/Pattern	Description
GNSS	**Solid Green**	Satellite fix is available, and Dead Reckoning is inactive (disabled, or not calibrated)
	Solid Blue	Satellite fix available, and Dead Reckoning is active
	Flashing Blue	No satellite fix is available, and Dead Reckoning is active
	Flashing Amber	No satellite fix is available, and Dead Reckoning is inactive (disabled, or not calibrated)
	Off	GNSS is off/disabled
Wi-Fi	**Solid Green**	Wi-Fi enabled (any mode), and not connected to an access point
	Flashing Green	Transmitting/receiving over Wi-Fi while not connected to an access point
	Solid Amber	Wi-Fi connected to an access point (i.e. Network state is “Network Ready - Wi-Fi”
	Flashing Amber	Transmitting/receiving over Wi-Fi while connected to an access point
	Off	Wi-Fi is off
Network	**Flashing Amber**	Connecting to a network
	Flashing Green	Connected to WAN (over cellular, Wi-Fi, or Ethernet)
	Solid Green	Connected to VPN
	Off	No network connection

Table 23-1: LED Behavior (Continued)

LED	Color/Pattern	Description
Signal	*Note: If the active WAN link is:* *• Cellular—Signal shown is for the cellular radio for that link.* *• Other (Wi-Fi, Ethernet, etc.)—Signal shown is for the strongest cellular radio.*	
	Solid Green	Good signal (≥85 dBm; equivalent to 4–5 bars)
	Solid Amber	Average signal (≥ -100 dBm, <-85 dB; equivalent to 2–3 bars)
	Red	Poor signal (<-100 dBm; equivalent to 1 bar)
Activity	**Flashing Green**	Transmitting/receiving over the WAN interface
	Off	No WAN activity
Power	**Solid Green**	Power is present, normal operation
	Flashing Green	Power is present, MG90 is booting
	Solid Amber	Standby mode
	Flashing Red	• Slow blink (1 per second)—Temperature out of operating range • Fast blink (4 per second)—Voltage out of operating range
	Off	No power
ALL LEDS *Note: A 'chase' is all LEDS blinking in sequence.*	**Green LED chase**	Radio module update or GNSS firmware update is in progress
	Amber LED chase	Software update is in progress
	Blue LED chase	MCU firmware update is in progress **Important:** *Do not turn off the power while the update is in progress.*
	Solid White	Factory default reset is in progress When the factory reset finishes, the MG90 will power off and, if AutoPower is enabled (LCI General > Startup tab), will reboot.

24: JSON Data

This chapter describes the JSON schema used for to broadcast the MG90 router status, and provides an example broadcast. For usage details, see Broadcast Router Status on page 24.

Broadcast Router Status—JSON Schema

```
{
    "$schema": "http://json-schema.org/schema#",
    "title": "gatewayStateBeacon",
    "type": "object",
    "required": ["timestamp", "vehicleID"],
    "properties": {
        "timestamp": {
            "type": "object",
            "properties": {
                "date": {
                    "type": "string"
                },
                "time": {
                    "type": "string"
                }
            }
        },

        "vehicleID": {
            type": "string"
        },

        "location": {
            "type": "object",
            "properties": {
                "latitude": {
                    "type": "number"
                },
                "longitude": {
                    "type": "number"
                }
            }
        },

        "gpInputStates": {
            "type": "array",
            "items": {
                "type": "number"
            }
        },

        "gpOutputStates": {
            "type": "array",
            "items": {
                "type": "number"
            }
        },

        "wanState": {
            "type": "array",
            "items": {
                "type": "object",
```

```
                    "properties": {
                        "friendlyName": {
                            "type": "string"
                        },
                        "status": {
                            "type": "number"
                        },
                        "active": {
                            "type": "boolean"
                        },
                        "signalStrength": {
                            "type": "number"
                        }
                    }
                }
            },

            "gnssStatus": {
                "type": "object",
                "properties": {
                    "fix": {
                        "type": "boolean"
                    },
                    "numberSatellites": {
                        "type": "number"
                    },
                    "antennaConnected": {
                        "type": "boolean"
                    }
                }
            },

            "vpnState": {
                "type": "array",
                "items": {
                    "type": "object",
                    "properties": {
                        "friendlyName": {
                            "type": "string"
                        },
                        "status": {
                            "type": "number"
                        }
                    }
                }
            },

            "generalInformation": {
                "type": "object",
                "properties": {
                    "ignitionOn": {
                        "type": "boolean"
                    },
                    "mainBatteryVoltage": {
                        "type": "number"
                    },
                    "internalTemperature": {
                        "type": "number"
                    }
                }
            }
        }
    }
```

Router Status Broadcast—Example Data


```
{
    "timestamp": {
        "date": "11082018",
        "time": "0506"
    },
    "vehicleID": "11028",
    "location": {
        "latitude": 49.172096,
        "longitude": -123.070115
    },
    "gpInputStates": [
        0,
        0,
        0,
        0,
        0
    ],
    "gpOutputStates": [
        0,
        0,
        0,
        0,
        0
    ],
    "wanState": [
        {
            "friendlyName": "WLE900VX 802.11AC @ MiniCard PCIe WiFi B",
            "status": 1,
            "active": false,
            "signalStrength": -68.000000
        },
        {
            "friendlyName": "Panel Ethernet 5",
            "status": 1,
            "active": true,
            "signalStrength": -200.000000
        },
        {
            "friendlyName": "Sierra Wireless MC74XX @ MiniCard USB3 CB (Cellular B)",
            "status": 1,
            "active": false,
            "signalStrength": -79.000000
        }
    ],
    "gnssStatus": {
        "fix": true,
        "numberSatellites": 3,
        "antennaConnected": true
    },
    "vpnState": {
        "status": 1
    },
    "generalInformation": {
        "ignitionOn": true,
        "mainBatteryVoltage": 13.600000,
        "internalTemperature": 35.555556
    }
}
```