G520 Series IoT Cellular Gateway User Guide

Part Number PMD-00123
Revision G September 2025

Intellectual Property

© 2025 Lantronix, Inc. All rights reserved. No part of the contents of this publication may be transmitted or reproduced in any form or by any means without the written permission of Lantronix.

Lantronix is a registered trademark of Lantronix, Inc. in the United States and other countries.

Patented: www.lantronix.com/legal/patents/. Additional patents pending.

Windows and *Internet Explorer* are registered trademarks of Microsoft Corporation. *Firefox* is a registered trademark of the Mozilla Foundation. *Chrome* is a trademark of Google Inc. All other trademarks and trade names are the property of their respective holders.

Warranty

For details on the Lantronix warranty policy, please go to our web site at www.lantronix.com/technical-support/warranty/

Contacts

Lantronix, Inc.
48 Discovery, Suite 250
Irvine, CA 92618, USA
Toll Free:800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support
Online: www.lantronix.com/technical-support/

Sales Offices
For a current list of our domestic and international sales offices, go to the Lantronix web site at www.lantronix.com/about-us/contact/

Disclaimer

All information contained herein is provided “AS IS.” Lantronix undertakes no obligation to update the information in this publication. Lantronix does not make, and specifically disclaims, all warranties of any kind (express, implied or otherwise) regarding title, non-infringement, fitness, quality, accuracy, completeness, usefulness, suitability or performance of the information provided herein. Lantronix shall have no liability whatsoever to any user for any damages, losses and causes of action (whether in contract or in tort or otherwise) in connection with the user’s access or usage of any of the information or content contained herein. The information and specifications contained in this document are subject to change without notice.

Revision History

Date	Rev.	Comments
December 2021	A	Initial document for G520 series cellular gateway
July 2022	B	Updated for firmware release 2.0.0.0R9. ◆ Added rating, power, and battery information. ◆ Added PoE specification and statement. ◆ Updated last gasp service and Tunnel BT SPP configuration. ◆ Added network 5G cellular interface protocol settings. ◆ Added cable diagnostics.
January 2023	C	Updated for firmware release 2.0.0.0R28. ◆ Updated quick setup and status based on UI enhancements, ◆ Updated ConsoleFlow client configuration options. ◆ Added country code selection for Wi-Fi operation. ◆ Added custom APN option to cellular interface configuration. ◆ Added two accessory POE power supplies. ◆ Updated compliance information and temperature specification for Taiwan.
August 2023	D	Updated for firmware release 2.1.0.0. ◆ Added support for G526RP transport pack gateway models ◆ Added Vehicle features: configure information, ignition, geofences, areas, parking area, alerts and CAN Bus. ◆ Added WireGuard VPN configuration. ◆ Added password prompt for backup and flash firmware. ◆ Added firmware upgrade from SD card/USB device. ◆ Added restoring installed IPKs after firmware upgrade. ◆ Added Audit Log option to ConsoleFlow client configuration.
October 2023	E	Updated for firmware release 2.2.0.0. ◆ Added Versatile IOs configuration. ◆ Renamed ConsoleFlow client to Percepxion ◆ Updated Percepxion configuration options: user audit log and send dynamic update ◆ Created Industrial Protocols chapter. ◆ Added Running Commands details. ◆ Updated product label

Date	Rev.	Comments
January 2025	F	Updated for firmware releases 2.3.0.0 and 2.4.0.0. ◆ Added firmware selection and wireless country selection to Quick Setup ◆ Added PDU enable to SMS configuration ◆ Updated SSH access ◆ Updated Cellular QMI Protocol configuration. Added enable IP passthrough, firmware selection, use DNS servers advertised by peer, band selection, and advanced configuration. Removed Cid ◆ Updated Wireless Interface configuration. Added isolate clients, 802.11w, and updated encryption. Removed enable key reinstallation ◆ Added 464XLAT (CLAT) network interface protocol ◆ Added discover channel to Bluetooth SPP configuration ◆ Added management console option to mode in Serial configuration ◆ Modified Lantronix sever URL in opkg commands ◆ Added industrial protocol IEC 104 MQTT ◆ Added serial section to Tunnel configuration ◆ Added SCEP client to Services ◆ Added use SCEP client to IPsec general settings ◆ Added route configuration to Vehicle Updated package contents and accessories details Changed the value for number of Wi-Fi clients in AP mode for G526RP Removed part number ACC-U301 from list of accessories
September 2025	G	Updated for firmware release 2.5.0.0 ◆ Added Modbus to MQTTS support ◆ Added Modbus to DNP3 conversion ◆ Added Crash Log to Status ◆ Added versatile input/output details to Status Overview ◆ Updated Information section in Vehicle. Added driving behavior and trip report, and driving behavior thresholds ◆ Updated IPsec General Settings configuration parameters Added option X.509 Certificate(scep certificate) to authentication method, and support for multiple remote subnets ◆ Updated IPsec Advanced Settings configuration parameters ◆ Updated Events section with new events and actions Removed Lantronix Connectivity Services and related content.

For the latest revision of this product document, please check our online documentation at www.lantronix.com/support/documentation.

Contents

1: About this Guide 20

Purpose 20
Summary of Chapters 20
Additional Documentation 22

2: Introduction 23

Key Features 23
- Hardware Variants 23
- InfiniShield™ Security 23
- Software Features 23
- Lantronix Software Services 24

Applications 24
SKU Information 25
Hardware Components 27
- General Specification 27
- Model-Dependent Features 29
- Front Panel 30
- Back Panel 31
- LEDs 32
  - Top Panel LEDs 32
- Cellular 33
- SIM Slots 34
- Antenna Connections 34
- Certified Antennas 35
  - Antenna Selection 35
- Ethernet Ports (LAN/WAN) 36
- RS-232 Serial Port 37
- RS-485 Serial Port 37
  - RS-485 Wiring diagram 38
- Input / Output Connections 38
- Power Input 40
- Power Consumption 40
- Reset Button 41
- Power over Ethernet (PSE-PoE+) 41
- Product Label 41

3: Installation 42

Package Contents 42
Accessory Bundles 42
Compatible Accessories 42

Statement 44
Add-ons 44
Preparing to Install 44
Enabling DHCP Client on Your Computer 44
SIM Card Installation 45
Insert the SIM Card 45
Connect the Antennas 46
Connect the AC Power 47
Connect the Gateway to a Computer 48
Connect using Wi-Fi 48
Connect using Ethernet 48
Default Configuration 49
Web Admin Page 49
Wireless Access Point SSID 49
Default Interface Configuration 49

4: Web Administration Interface 50

Logging In 52
Change Passwords After Initial Login 52
Logging Out 53

5: Using Lantronix Provisioning Manager 54

Installing Lantronix Provisioning Manager 54
Accessing the G520 Using Lantronix Provisioning Manager 54

6: Quick Setup 55

Quick Setup 55

7: Status 58

Overview (Page) 58
System 58
Percepxion 59
Memory 60
Digital Input/Output 60
Versatile Input/Output 60
Network 60
Cellular 60
Network 62
Active DHCP and DHCPv6 Leases 62
Wireless 63
Dynamic DNS 63
Firewall 64

Routes 65
System Log 66
Kernel Log 66
Crash Log 66
Processes 66
Realtime Graphs 68
Load 68
Traffic 69
Wireless 70
Connections 71
Load Balancing 72
Interface 72
Detail 72
Diagnostics 72
Troubleshooting 72

8: System 73

System 73
General Settings 73
Logging 74
Time Synchronization 75
Language and Style 76
Administration 77
Router Password 77
SSH Access 77
SSH-Keys 78
Software 79
List the Packages 80
Update the List of Packages 80
Install a Package 80
Upgrade a Package 81
Remove a Package 82
Configure OPKG 82
Startup 83
Initscripts 83
Local Startup 84
Scheduled Tasks 85
LED Configuration 86
Backup / Flash Firmware 88
Backup and Restore 89
Reset to Defaults 89
Factory Reset using Reset Button 89
Firmware Upgrade 90

Restoring IPKs after Firmware Upgrade on the Device 90
Configuration 91
Firmware and Configuration Upgrade from SD Card / USB Device 91
Custom Commands 92
Write Custom Shell Command 92
Run Custom Shell Command 92
Reboot 93
Schedule a Reboot 93

9: VPN 94

IPsec (Internet Protocol Security) 94
OpenVPN 100
OpenVPN Instances 100
Template-based Configuration 101
Predefined templates 101
Edit the template-based configuration 101
OpenVPN Configuration File 101
Edit the OVPN Configuration File 101
WireGuard VPN 102
Install WireGuard IPKs to the Device 102
Generate Private and Public Keys for WireGuard 102
Create the WireGuard VPN Interface 103
Configure a Firewall Rule to Allow WireGuard Traffic 103
Monitor Status 104
Create a WireGuard Interface on the Peer Device 104

10: Services 105

CAN Bus 105
Global Settings 105
CAN Standard 106
OBDII - Current Data 108
OBDII - Diagnostics 110
CANOpen - Gateway 110
CANOpen - Commands 111
CANopen Command Syntax 111
Upload SDO 111
Download SDO 111
Command specified node in the Gateway 111
DOTA 112
Lantronix Server 112
Custom Server 113
Dynamic DNS 114
Events 116

External Filesystems 118
GPS 119
Description of NMEA Messages 120
GPGGA Format 121
GPRMC Format 122
GPGSV Format 123
GPGSA Format 124
GPVTG Format 125
Keepalived 127
Keepalived Configuration 127
Last Gasp 130
Logs Information 131
Reporting Agent 131
Sending Data 132
Data Format 133
SCEP Client 134
Service Actions 135
SMS 136
SMS Configuration 136
SMS AT Commands 136
Ethernet SMS 139
Live Message 140
SNMPD 141
SNMP Architecture 141
SNMP Versions 141
SNMP Configuration 142
Agent Behavior 142
View-based Access Control Model (VACM) 142
SNMPv3 with User-based Security Model (USM) 143
System Information and Monitoring 143
Active Monitoring 143
Configure SNMPv1 or SNMPv2 144
Configure SNMPv3 with USM 144
SNMPTRAPD 152
SNMP-TRAP Configuration 152
uHTTPd 154
Web Server Configuration 154
Self-Signed SSL Certificate Parameters 156
Versatile IOs 157

11: Industrial Protocols 158

Industrial Protocol Converters 158
Data Send Applications 158

DLMS Client 159
EtherCAT 160
IEC 104 to MQTT 160
IEC 104 MQTT Configuration 160
IEC 104 to IEC 104 Multimaster 161
IEC 104 Multimaster Configuration 161
IEC 101 to 104 162
Modbus Master 163
Serial Transmission Mode 163
Ethernet Transmission Mode 164
Modbus Master Configuration 164
Data Window 165
Modbus Download 165
Modbus RTU to DNP3 165
Configure DNP3 Outstation for Modbus RTU to DNP3 conversion 165
Modbus Configuration File for DNP3 Outstation 166
Modbus to DNP3 167
Configure DNP3 for Modbus to DNP3 conversion 168

12: Network 169

Interfaces 169
Interfaces Overview 169
Interface Status 171
Interface Protocols 172
Protocol Descriptions 173
Static Address 173
DHCP Client 175
DHCPv6 Client 177
PPPoE 178
QMI Cellular 179
464XLAT (CLAT) 181
CELLULAR Interface 182
LAN Interface 183
DHCP Server 183
WAN and WAN6 Interface 185
WWAN and WWAN6 Interface 187
Add Virtual Interface 188
Relay Bridge 190
Wireless 191
Wireless Network Configuration 192
Default Wireless Client Profile 195
DHCP and DNS 196
General Settings 196

Resolv and Host Files 197
TFTP Settings 197
Advanced Settings 198
Static Leases 199
Hostnames 200
Static Routes 200
Static IPv4 Routes 200
Static IPv6 Routes 201
Diagnostics 203
Firewall 204
General Settings 204
Firewall Global Settings 204
Firewall Zones 205
Port Forwards 206
Add Port Forwarding Rule 207
Traffic Rules 208
Add Traffic Rule 209
Custom Rules 210
PoE 211
QoS 212
Load Balancing 214
How it works 214
Globals 214
Interfaces 215
Members 217
Policies 218
Rules 220
Notification 221

13: Bluetooth 222

Bluetooth Settings 222
Configure Bluetooth settings 222
Scan for and Pair a Device 222
Bluetooth SPP 223
Configure Bluetooth SPP Connection 224
Configure Tunnel SPP Slave 224
Configure Tunnel SPP Master 225

14: Percepxion 226

Client 226
Percepxion Line 228

15: Discovery 229

Query Port 229

16: Serial 230

Serial Line Statistics 230
Serial Line Configuration 230

17: SSL 232

Credentials 232
Trusted Authorities 234

18: Vehicle 235

Information 235
- Driving Behavior and Trip Report 235
- Driving Thresholds 236
- Configuration 236

Ignition 237
Routes 238
- Overview 238
- 240
- Geo-Fences Overview Page 240
- Add a Geofence 241
- Areas Overview Page 243
- Add an Area 243
- Routes Overview Page 245
- Add a Route 245

Parking 247
Alerts 249

19: Tunnel 251

Tunnel Statistics 251
Tunnel Modbus RTU to Modbus TCP 251
Tunnel Accept 252
Tunnel Connect 255
- Hosts 256
- Connecting Multiple Hosts 258

Tunnel Disconnect 258
Tunnel Serial 258

A: Compliance Information 260

FCC Statement 261

Federal Communication Commission Interference Statement 261
ISED Statement 262
EU Declaration of Conformity 263
EU Statements 264

B: Power Cable Schematic 270

Power Cable Schematic 270

C: List of Acronyms and Protocols 271

D: Running Commands 274

Types of Commands 274
Bash Commands 274
Usage 274
Bash Command Examples 274
Example 274
Example 275
Example 275
Example 276
Example 276
opkg Commands 277
Example 277
UCI Commands 278
Example 278

D: Lantronix Technical Support 279

List of Figures

Figure 2-1 G526/G527/G528 Front View 30
Figure 2-2 G526/G527 Back View 31
Figure 2-3 G526RP Back View 31
Figure 2-4 G528 Back View 32
Figure 2-5 Dual SIM Operation 34
Figure 2-6 Ethernet Port 36
Figure 2-7 RS-232 DB9F Interface 37
Figure 2-8 RS-485 and I/O Connections 37
Figure 2-9 RS-485 Wiring Diagram 38
Figure 2-10 DC Input Interface 40
Figure 2-11 Sample Product Label (G526GP1AS shown) 41
Figure 4-1 Web Admin Interface 50
Figure 4-2 Web Admin Login Page 52
Figure 7-1 IPv4 Firewall Status 64
Figure 7-2 Realtime CPU Load Graph 68
Figure 7-3 Realtime Network Traffic Graph (eth1) 69
Figure 7-4 Realtime Wireless Usage Graph (client) 70
Figure 7-5 Realtime Connections Traffic Graph 71
Figure 10-1 Reporting Agent Data Format (excerpt) 133
Figure 10-2 Service Actions 135
Figure 10-3 VACM Configuration Model 143
Figure 12-1 Interfaces Overview (partial view) 170
Figure 12-2 WAN Interface Status 171
Figure 12-3 Cellular Interface Configuration 182
Figure 12-4 LAN Interface (Static Address) Configuration 184
Figure 12-5 WAN Interface (Static Address) Configuration 186
Figure 12-6 WWAN Interface (DHCP client) Configuration 187
Figure 12-7 Network Add New Interface 188
Figure 12-8 Wireless Overview 191
Figure 18-1 Rectangular Geofence 238
Figure 18-2 Geographic Area Composed of Overlapping Geofences 239
Figure 18-3 Route 240
Figure 18-4 Parking Area 240
Figure A-1 EU Declaration of Conformity 263
Figure B-1 3-pin Power Cable 270

List of Tables

Table 2-1 G520 Series Models 25
Table 2-2 General Specification 27
Table 2-3 G520 Series Model-Dependent Features 29
Table 2-4 Top Panel LEDs 32
Table 2-5 G520 Series Cellular Data Rates 33
Table 2-6 G520 Series Cellular Bands 33
Table 2-7 Certified Antennas 35
Table 2-8 Ethernet RJ45 Connector Pin Assignment and LEDs 36
Table 2-9 RS-232 Pin Assignment 37
Table 2-10 RS-485 Pin Assignments 37
Table 2-11 RS-485 Options 38
Table 2-12 Digital I/O Pin Assignments 38
Table 2-13 Versatile I/O Pin Assignments 39
Table 2-14 Digital I/O and Versatile I/O Pin Assignments 39
Table 2-15 Power Input and PoE Output 40
Table 2-16 G520 Series Power Consumption 40
Table 3-1 Lantronix Accessory Bundles 42
Table 3-2 Lantronix Accessories 42
Table 3-3 Add-ons 44
Table 3-4 Default Web Admin Page Credentials 49
Table 3-5 Default Wireless Access Point SSID 49
Table 3-6 Default Network Interface Configuration 49
Table 6-1 Quick Setup Network Configuration 55
Table 7-1 System Status Overview 58
Table 7-2 System Status Overview 59
Table 7-3 Memory Status Overview 60
Table 7-4 Cellular Status Overview 61
Table 7-5 Network Status Overview 62
Table 7-6 Active DHCP Leases Status Overview 62
Table 7-7 Wireless Status Overview 63
Table 7-8 Firewall Status 64
Table 7-9 Routes Status 65
Table 7-10 Processes Status 66
Table 8-1 System General Settings 73
Table 8-2 Syslog Configuration 74
Table 8-3 System Time Synchronization Configuration 75

Table 8-4 Language and Style Configurations 76
Table 8-5 SSH Access Configuration 78
Table 8-6 Software Page 79
Table 8-7 OPKG Package Manager Configuration 82
Table 8-8 Initscripts Actions 83
Table 8-9 Cron Shortcuts 85
Table 8-10 LED Configuration 86
Table 8-11 Trigger Descriptions 86
Table 8-12 Backup and Restore / Flash Firmware Operations 88
Table 8-13 Custom Commands Configuration 92
Table 8-14 Schedule Reboot Time Specification 93
Table 9-1 IPsec General Settings 94
Table 9-2 IPsec Advanced Settings 96
Table 10-1 CAN Bus Global Settings 105
Table 10-2 CAN Standard Configuration 106
Table 10-3 OBDII- Current Data Configuration 108
Table 10-4 CANOpen Gateway Configuration 110
Table 10-5 DOTA using Lantronix Server 112
Table 10-6 DOTA Custom Server Configuration 113
Table 10-7 Dynamic DNS Client Configuration 114
Table 10-8 Events Configuration 117
Table 10-9 External Filesystems Configuration 118
Table 10-10 GPS Service Configuration 119
Table 10-11 GGA Data Format 121
Table 10-12 RMC Data Format 122
Table 10-13 GPGSV Data Format 123
Table 10-14 GSA Data Format 124
Table 10-15 VTG Data Format 125
Table 10-16 Keepalived Configuration 128
Table 10-17 Last Gasp Message Configuration 130
Table 10-18 Reporting Agent Configuration 131
Table 10-19 Reporting Agent Data Send Configuration 132
Table 10-20 SCEP Client page Overview 134
Table 10-21 SCEP Certificate Details 134
Table 10-22 SMS Service Configuration 136
Table 10-23 SMS AT Command Syntax 137
Table 10-24 Ethernet SMS Configuration 139
Table 10-25 SNMP Security Models and Levels 142

Table 10-26 SNMP General Settings Configuration 145
Table 10-27 SNMP v1/v2/USM VACM Settings 147
Table 10-28 SNMP VACM Settings Engine ID Configuration 149
Table 10-29 SNMP VACM Settings SNMPv3-USM 150
Table 10-30 SNMP Trap Settings Configuration 150
Table 10-31 SNMP-Trap Receiver Configuration 152
Table 10-32 uHTTPd Server Configuration 154
Table 10-33 uHTTPd Self-signed Certificate Configuration 156
Table 10-34 Versatile IOs Configuration 157
Table 11-1 DLMS Client Configuration 159
Table 11-2 DLMS Data Send Configuration 159
Table 11-3 IEC 101 Slave Configuration 162
Table 11-4 IEC-104 Master Configuration 162
Table 11-5 Modbus RTU Packet Data Structure 163
Table 11-6 Modbus Application Protocol Byte Header 164
Table 11-7 Modbus Master Configuration 164
Table 11-8 DNP3 Outstation and Modbus Master Configuration 166
Table 11-9 DNP3 Configuration 168
Table 12-1 Network Interfaces Overview 170
Table 12-2 Wireless Overview and Associated Stations 171
Table 12-3 Network Interface Protocols 172
Table 12-4 Static Address Protocol Settings 173
Table 12-5 DHCP Client Protocol Settings 175
Table 12-6 DHCPv6 Client Protocol Settings 177
Table 12-7 PPPoE Protocol Settings 178
Table 12-8 QMI Cellular Protocol Settings 179
Table 12-9 VPN Tunnel Protocols 189
Table 12-10 Wireless Overview and Associated Stations 191
Table 12-11 Wireless Device Configuration 193
Table 12-12 Wireless Interface Configuration 193
Table 12-13 General Configuration of DHCP Server and DNS-Forwarder 196
Table 12-14 Resolv and Host File Configuration for DHCP and DNS 197
Table 12-15 TFTP Configuration for DHCP and DNS 197
Table 12-16 Advanced Configuration for DHCP and DNS 198
Table 12-17 DHCP and DNS Static Leases 199
Table 12-18 Hostnames Configuration 200
Table 12-19 Static IPv4 Routes Configuration 200
Table 12-20 Static IPv6 Routes Configuration 201

Table 12-21 Diagnostics - Network Utilities 203
Table 12-22 Cable Diagnostics Status Messages 203
Table 12-23 Firewall Global Settings 204
Table 12-24 Firewall Zones Configuration (LAN) 205
Table 12-25 Firewall Port Forwards 207
Table 12-26 Port Forwarding Configuration for Firewall Zone 207
Table 12-27 Firewall Zone Traffic Rules 208
Table 12-28 Firewall Traffic Rule Configuration 209
Table 12-29 PoE Configuration 211
Table 12-30 QoS Configure Classes 212
Table 12-31 MWAN Globals Configuration 215
Table 12-32 MWAN Interface 215
Table 12-33 MWAN Interface Configuration 216
Table 12-34 MWAN Members 217
Table 12-35 MWAN Members Configuration 218
Table 12-36 MWAN Policy 219
Table 12-37 MWAN Policy Configuration 219
Table 12-38 MWAN Rules 220
Table 12-39 MWAN Rules Configuration 220
Table 13-1 Bluetooth Settings Configuration 222
Table 13-2 Bluetooth Scan Results 223
Table 13-3 Bluetooth SPP Line Configuration 224
Table 14-1 Percepxion Client Configuration 226
Table 14-2 Percepxion Line 228
Table 16-1 Serial Line Configuration 230
Table 17-1 SSL Credentials - Upload Certificate 232
Table 17-2 SSL Credentials - Create Self-Signed Certificate 233
Table 17-3 SSL Trusted Authority 234
Table 18-1 Driving Behavior and Trip Report Details 235
Table 18-2 Driving Thresholds 236
Table 18-3 Ignition Configuration 237
Table 18-4 Geofence Configuration 241
Table 18-5 Areas Configuration 244
Table 18-6 Route Configuration 246
Table 18-7 Parking Configuration 247
Table 18-8 Alerts Configuration 249
Table 19-1 Tunnel for Modbus RTU to Modbus TCP 251
Table 19-2 Tunnel Accept Mode Configuration 252

Table 19-3 Tunnel Connect Mode Configuration 255
Table 19-4 Host Configuration 257
Table 19-5 Tunnel Disconnect Configuration 258
Table A-1 Regional Certifications 260
Table A-2 Country Transmitter IDs 260
Table A-3 EU Statements 264

1: About this Guide

Purpose

This guide provides the information needed to install, configure, and use the Lantronix G520 series IoT cellular gateways using the web interface. The G520 series gateways are designed for IoT professionals for M2M and enterprise IoT applications requiring faultless connectivity.

The information in this document assumes the reader has knowledge of networking fundamentals and routing concepts for data communication, control, and management functions.

For additional support and product resources, please visit the Lantronix Technical Support portal (https://ltrxdev.atlassian.net/wiki/spaces/LTRXTS/overview).

Summary of Chapters

The remaining chapters in this guide include:

Chapter	Description
Chapter 2: Introduction	Describes the main features of the product and the protocols it supports.
Chapter 3: Installation	Instructions for installing the G520 series gateways. List of accessories for the gateway. Provides the default credentials for access to the web interface and wireless access point.
Chapter 4: Web Administration Interface	Instructions for accessing the web administration interface and using it to configure settings for the G520 series gateways. The configuration chapters (6 -17) provide detailed instructions for using the web interface.
Chapter 5: Using Lantronix Provisioning Manager	Instructions for using Lantronix Provisioning Manager to locate and configure the gateway.
Chapter 6: Quick Setup	Instructions for configuring the Quick Setup.
Chapter 7: Status	Overview of the gateway status pages.
Chapter 8: System	Instructions for configuring the system features, including clock, syslog, SSH access and keys, password, enabling startup scripts, scheduling cron jobs, LED behavior, and executing custom shell commands. Instructions for operations and maintenance, installing software packages, firmware upgrades, configuration backup, restoring configuration, reboot and factory reset.
Chapter 9: VPN	Instructions for configuring and enabling OpenVPN and IPsec tunneling.
Chapter 10: Services	Instructions for configuring and enabling router and gateway services, and for starting and stopping services.
Chapter 11: Industrial Protocols	Instructions for configuring industrial protocol services.

Chapter	Description
Chapter 12: Network	Instructions for configuring and enabling the wired, wireless, and cellular network interfaces. Instructions for configuring DHCP and DNS, static routes, firewall, QoS, and load balancing. Instructions for defining hostname and running network diagnostic commands.
Chapter 13: Bluetooth	Instructions for configuring and enabling Bluetooth SPP for serial data transmission.
Chapter 14: Percepxion	Instructions for configuring PercepXion client settings.
Chapter 15: Discovery	Instructions for enabling discovery on query port 0x77FE.
Chapter 16: Serial	Instructions for configuring serial settings on the RS-232 and RS-485 lines.
Chapter 17: SSL	Instructions for creating SSL credentials, uploading SSL certificates and private keys from a CA or self-signed, generating self-signed certificates, and uploading trusted authority certificates.
Chapter 18: Vehicle	Instructions for configuring vehicle, tracking and management features.
Chapter 19: Tunnel	Instructions for configuring and enabling serial Tunnel connections.
Appendix A: Compliance Information	Provides compliance information.
Appendix B: Power Cable Schematic	Provides information about accessories, cabling, and connectors.
Appendix C: List of Acronyms and Protocols	Provides a glossary of relevant acronyms and protocols.
Appendix D: Lantronix Technical Support	Provides instructions for contacting Latronix Technical Support.

Additional Documentation

Visit the Lantronix Product Index (https://www.lantronix.com/support/documentation) for the latest documentation for this product series.

Document	Description
G520 Series Quick Start Guide	Provides hardware installation instructions, directions to connect the G520 series gateway, and network IP configuration information.
Using the G520 Series SDK Application Note	Describes how to use the SDK to create custom packages and the Image Builder to build custom firmware images.
G520 Series Product Brief	Provides G520 series gateway product overview information and specifications.

2: Introduction

The G520 series offers LTE Cat 4 and 5G industrial-grade cellular gateways that address the demands of Industry 4.0, security, and transport applications.

With multiple variants providing vertical configuration and clear market differentiators, the G520 series cellular gateways make it possible to combine multiple application use cases in a compact, highly secure, industrial-grade platform.

Key Features

Hardware Variants

- Industrial Gateway – Ethernet, serial, I/O, Fieldbus conversion, other industrial protocols
- Security Gateway – Built-in cryptographic secure element and PSE-PoE

  Note: *The product is considered not likely to require connection to an Ethernet network with outside plant routing.*
- Transportation Gateway – dedicated high accuracy GNSS module, accelerometer, CAN Bus protocol, Ignition/over-speeding/harsh-braking alerts, tracking via geofences, areas and waypoints, ECO score

InfiniShield™ Security

- Built-in security framework for mission-critical applications
- Secure boot, secure firmware updates, secure storage
- Secure communications, secure network attach

Software Features

- Administration and network protocols
  - Web user interface, setup wizard, console log viewer, save/load configuration
  - NTP, SMS/OTA remote configuration, TR-069 capable, Lantronix Provisioning Manager
- Redundancy
  - Ethernet, Cellular, Wi-Fi (configurable as failover or load balancing)
- Resilience
  - Network connectivity watchdog (configurable), internal application watchdog
- Wi-Fi
  - Client or Access point, multiple SSID
  - WPA, WPA-PSK/WPA2-PSK/WPA3-PSK
  - Enterprise Security (WPA2-Enterprise/WPA3-Enterprise)
  - EAP-TLS, EAP-TTLS (MS-CHAPv2), EAP-PEAPv0/EAP-MS-CHAPV2, EAP-PEAPv1, EAP-FAST
  - Bluetooth and Wi-Fi coexistence

- Routing features and protocols
  - DHCP, static routing, port forwarding, traffic routing, static/dynamic DNS, DNS proxy, NAT, STP
  - VPN and tunneling protocols – PPTP client, L2TP, OpenVPN client/server/passthrough, GRE, IPsec up to 4 channels
  - Security – zone-based firewall, VLAN, DMZ, HTTPS local & remote connection, SIM PIN
- Performance and Fault Management
  - Real time processor load and interface (WAN/LAN/Wi-Fi), traffic analysis, ICMP, traceroute, NS lookup
- Essential IoT Applications
  - Serial and Bluetooth SPP to Network tunnels
  - Python runtime and packages available as IPKs for installation
  - Add your own IoT edge applications with the SDK and Image Builder
- Industrial protocols and protocol conversion suite
  - Modbus master, DLMS client, DNP3 outstation (client), EtherCAT, IEC 101, IEC 104
  - Modbus RTU to TCP, Modbus RTU to DNP3, IEC 101 to IEC 104 conversion, Modbus to DNP3

Lantronix Software Services

Lantronix Percepxion – secure cloud platform to manage remote IoT gateways through a single pane of glass

Applications

The G520 series cellular gateway is suitable for these application scenarios:

- Industry 4.0
- Security camera monitoring
- Banking application

SKU Information

Table 2-1 G520 Series Models

Lantronix Part Number	Description
INDUSTRY GATEWAY	
G526GP12S	INDUSTRY PACK LTE CAT 4 GATEWAY FOR EMEA, ASIA PACIFIC; ◆ LTE-3G-2G B28,20,8,3,1,7-B8,1-B8,3; ◆ 10.8 - 60 V DC; L. GASP; DI; ◆ DI-O X2; VI-O X2; ◆ RS-232; RS-485; USB; ◆ WI-FI 5; BT 5; ◆ ETHERNET X2; ◆ GNSS; DUAL SIM; ◆ MICROSD ◆ SW EPACK INDUSTRIAL SUITE
G526GP12SB01	**SLC Kit with G526GP12S Industry gateway**
G526GP1AS	INDUSTRY PACK LTE CAT 4 GATEWAY FOR CANADA, USA; ◆ LTE B71,12(17),13,14,26(5),66(10,4),25(2); ◆ 10.8 - 60 V DC; L. GASP; DI; ◆ DI-O X2; VI-O X2; ◆ RS-232; RS-485; USB; ◆ WI-FI 5; BT 5; ◆ ETHERNET X2; ◆ GNSS; DUAL SIM; ◆ MICROSD ◆ SW EPACK INDUSTRIAL SUITE
G526GP1AS1B01	**SLC Kit with G526GP1AS1 Industry gateway**
G526GP17S	INDUSTRY PACK LTE CAT 4 GATEWAY FOR JAPAN; ◆ LTE B18,5(19),8,21,3(9),1,7; ◆ 10.8 - 60 V DC; L. GASP; DI; ◆ DI-O X2; VI-O X2; ◆ RS-232; RS-485; USB; ◆ WI-FI 5; BT 5; ◆ ETHERNET X2; ◆ GNSS; DUAL SIM; ◆ MICROSD ◆ SW EPACK INDUSTRIAL SUITE
SECURITY GATEWAY	
G527GP22S	SECURITY PACK LTE CAT 7-13 GATEWAY FOR EMEA, ASIA PACIFIC; ◆ LTE-3G B28,20,8,32,3,1,7;40,41(38),42,43-B5,8,1; ◆ 10.8 - 60 V DC; L. GASP; DI; ◆ DI-O X2; VI-O X2; ◆ RS-232; RS-485; USB; ◆ WI-FI 5; BT 5; ◆ SECURITY ELEMENT; ◆ PSE-POE+ ETHERNET X2; ◆ GNSS; DUAL SIM; ◆ MICROSD ◆ SW EPACK SECURITY SUITE

Lantronix Part Number	Description
G527GP2AS	SECURITY PACK LTE CAT 7-13 GATEWAY FOR AMERICA; ◆ LTE-3G B71,12(17),13,14,26(5),66(10,4),25(2),7;41,42,48,43-B5,4,2; ◆ 10.8 - 60 V DC; L. GASP; DI; ◆ DI-O X2; VI-O X2; ◆ RS-232; RS-485; USB; ◆ WI-FI 5; BT 5; ◆ SECURITY ELEMENT; ◆ PSE-POE+ ETHERNET X2; ◆ GNSS; DUAL SIM; ◆ MICROSD ◆ SW EPACK SECURITY SUITE
G527GP27S	SECURITY PACK LTE CAT 7-13 GATEWAY FOR JAPAN; ◆ LTE-3G B18,5(19),8,3(9),1,41,42,43/B5(19,6),1; ◆ 10.8 - 60 V DC; L. GASP; DI; ◆ DI-O X2; VI-O X2; ◆ RS-232; RS-485; USB; ◆ WI-FI 5; BT 5; ◆ SECURITY ELEMENT; ◆ PSE-POE+ ETHERNET X2; ◆ GNSS; DUAL SIM; ◆ MICROSD ◆ SW EPACK SECURITY SUITE
G528GP2FS	SECURITY PACK 5G Sub 6 GHZ LTE CAT13 FB IOT GATEWAY WORLD; ◆ 10.8 - 60 V DC; L. GASP; DI; ◆ DI-O X2; VI-O X2; ◆ RS-232; RS-485; USB; ◆ WI-FI 5; BT 5; ◆ SEC. ELEM.; ◆ PSE-POE+ ETHERNET X2; ◆ GNSS; DUAL SIM; ◆ MICROSD ◆ SW EPACK SECURITY SUITE
TRANSPORTATION GATEWAY	
G526RP42S	◆ TRANSPORT PACK LTE CAT 4 ROUTER FOR EMEA, ASIA PACIFIC; ◆ LTE-3G-2G B28,20,8,3,1,7-B8,1-B8,3; ◆ 10.8 - 60 V DC; L. GASP; DI; ◆ DI-O X2; VI-O X2; ◆ RS-232; RS-485; USB; ◆ WI-FI 5; BT 5; ETHERNET X2; ◆ GNSS; DUAL SIM; ◆ MICROSD. ◆ SW EPACK TRANSPORT SUITE
G526RP47S	◆ TRANSPORT PACK LTE CAT 4 ROUTER FOR JAPAN; ◆ LTE B18,5(19),8,21,3(9),1,7; ◆ 10.8 - 60 V DC; L. GASP; DI; ◆ DI-O X2; VI-O X2; ◆ RS-232; RS-485; USB; ◆ WI-FI 5; BT 5; ETHERNET X2; ◆ GNSS; DUAL SIM; ◆ MICROSD SW EPACK TRANSPORT SUITE

Lantronix Part Number	Description
G526RP4AS	◆ TRANSPORT PACK LTE CAT 4 ROUTER FOR CANADA, USA; ◆ LTE B71,12(17),13,14,26(5),66(10,4),25(2); ◆ 10.8 - 60 V DC; L. GASP; DI; ◆ DI-O X2; VI-O X2; ◆ RS-232; RS-485; USB; ◆ WI-FI 5; BT 5; ETHERNET X2; ◆ GNSS; DUAL SIM; ◆ MICROSD SW EPACK INDUSTRIAL SUITE

Hardware Components

General Specification

Table 2-2 General Specification

Component	Specification
Physical	
Casing	Brushed aluminum alloy
Dimensions (W x D x H)	131.5 x 81.27 x 25 mm
Weight	334 grams
Environmental	
Operating temperature	-30 °C ~ +70 °C, up to 95% RH -30 °C ~ +50 °C, up to 95% RH for Taiwan applications
Storage temperature	-40 °C ~ +85 °C, up to 95% RH
Memory	
SPI Flash memory	8MB
NAND Flash memory	256MB
RAM	DDR2 SDRAM 256MB
Power	
Power	Input voltage: 10.8 ~ 60 V DC 3-pin Nano-Fit™ header Power over ethernet (PSE-PoE+) is available on select models. See *Model-Dependent Features*.
Last Gasp	100-second long, approximately Two (2) 96 mWh Li-ion batteries (not functional below -10 °C)
Digital Input (Ignition)	One (1) digital input, on the middle pin of the 3-pin header Input: 0 V DC ~ 2.5 V DC => ZERO; 3 V DC ~ 50 V DC => ONE
Power off Timekeeping	Dedicated RTC with 100-day data retention period, approximately 15 mWh lithium manganese battery (not functional below -20 °C)
Interfaces	

Component	Specification
Ethernet	10/100 BASE-T Two (2) ports (1 LAN, 1 WAN, configurable as LAN) Two (2) LEDs per port (link, activity)
Wi-Fi	IEEE 802.11ac/a/b/g/n 2x2 MIMO 2T2R Wi-Fi 5, with 2 RP-SMA antenna connectors Bluetooth 5.1, via Wi-Fi's rightmost RP-SMA antenna connector For the number of Wi-Fi clients in AP mode, see *Model-Dependent Features*.
Dual SIM operation	Dual SIM / Single standby Two (2) SIM slots (Mini - 2FF)
GNSS	Satellite systems support: BeiDou, Galileo, GLONASS, GPS One (1) SMA antenna connector
User data storage	Internal: via the 256MB of parallel NAND Flash memory External: One (1) microSD card slot (microSD card not provided)
USB	One (1) USB 2.0 host port, Type A
RS-232	One (1) RS-232 serial port with DB9F connector Software configurable baud rate options from 2400 bps to 921600 bps For RS-485 serial operation, see *Model-Dependent Features*.
Digital I/Os	Two (2) I/Os with common ground, with 3-pin COMBICON header and plug. ◆ Input: 0 V dc ~ 2.5 V dc => ZERO; 3 V dc ~ 50 V dc => ONE ◆ Output: open collector, 200 mA maximum, 50 V dc maximum CAN Bus – two pins, assigned as CANH and CANL, can be used to replace the Digital input / output. See *Model-Dependent Features*.
Versatile I/O	Two (2) I/Os with common ground, with 3-pin COMBICON header and plug. Each I/O is independently user-configurable as analog input, analog input suited to current loop (4 mA ~ 20 mA) sensors, or digital output. ◆ Analog input: 0 V dc ~ 48 V dc range; 12-bit resolution; capable of counting pulses at up to 10 Hz ◆ Analog input: 4 mA ~ 20 mA range, 12-bit resolution ◆ Output: open collector, 200 mA maximum, 50 V dc maximum
Status LEDs	Nine (9) LEDs on top panel for network activity and status
Reset button	Soft Reset (reboot): Short press more than one (1) second and less than 5 seconds Hard Reset (factory reset): Long press more than 5 seconds and less than 20 seconds

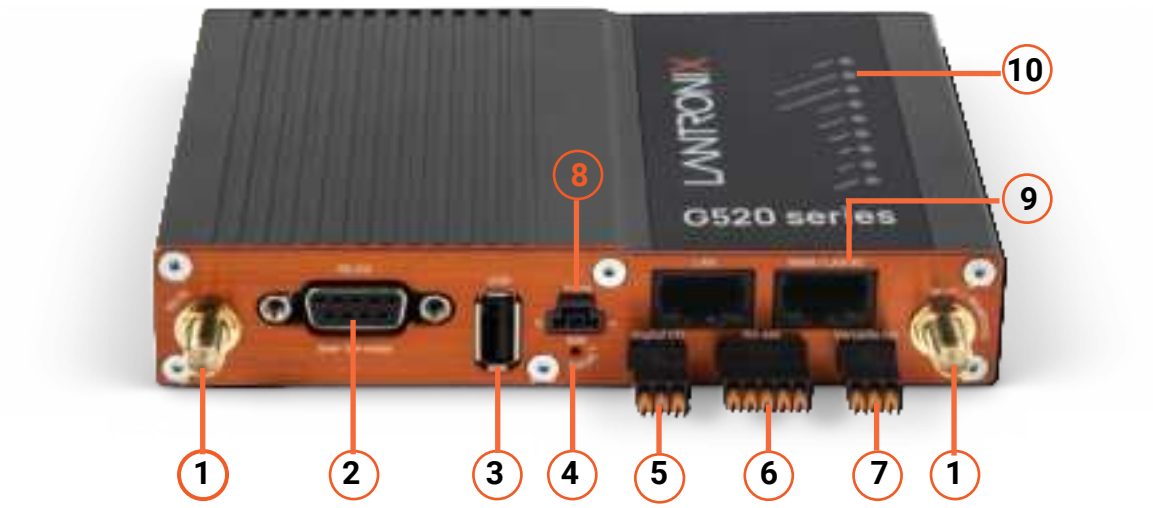
Model-Dependent Features

Table 2-3 G520 Series Model-Dependent Features

Feature	Description	Industry Gateway (G526)	Security Gateway (G527 / G528)	Transport Gateway (G526RP)
CAN Bus	Two pins, CANH and CANL, used to replace the digital I/Os	No	No	Yes
RS-485 operation (serial)	6kV (contact) and 8kV (air) ESD-protected, 2.5kV isolated, via 5-pin COMBICON header Half-duplex (factory setting) or Full-duplex mode (software configurable)	Yes	Yes	No
PSE-PoE+ (power over ethernet)	IEEE 802.3at standard-compliant 30 W per LAN port; requires PoE+ power supply accessory	No	Yes	No
Wi-Fi Operation	Number of Wi-Fi Clients in AP mode	12	12	12
4G Cellular and GNSS Operations	LTE Cat 4 with 3G or 3G/2G fallback mode; 2 SMA antenna connectors or LTE Cat 13/7 with 3G fallback mode; 2 SMA antenna connectors	LTE Cat 4	LTE Cat 13/ 7	LTE Cat 4
	Qualcomm® IZat™ location services or u-blox M8; 1 dedicated SMA antenna connector	Qualcomm IZat gen. 8c	Qualcomm IZat gen. 9c	u-blox M8
5G Cellular and GNSS Operations	Sub-6 GHz 5G, with both LTE Cat 13 (uplink) / Cat 20 (downlink) and 3G fallback modes	No	Yes	No
	Dual band GPS and Galileo; Single band GLONASS and BeiDou; 4 SMA antenna connectors, 2 Rx / Tx dedicated to cellular and 2 Rx-only shared between cellular and GNSS	No	Yes	No
3-axis accelerometer	STMicroelectronics LIS331DLH	No	No	Yes
Secure element	NXP EdgeLock SE050	No	Yes	No
User data storage	Internal via the 256MB of parallel NAND Flash memory	Yes	Factory option	Factory option

Front Panel

Figure 2-1 G526/G527/G528 Front View



ID	Connection Name	ID	Connection Name
1	Wi-Fi antenna (left) Wi-Fi / Bluetooth antenna (right)	**6**	RS-485
2	RS-232	**7**	Versatile I/O
3	USB	**8**	Power input
4	Reset button	**9**	Ethernet (LAN, WAN/LAN #2)
5	Digital I/O	**10**	LEDs

Back Panel

Figure 2-2 G526/G527 Back View

ID	Connection Name
1	Cellular diversity antenna (left)
	Cellular main antenna (right)
2	microSD card slot
3	Last Gasp switch (OFF by default)
4	GNSS antenna
5	SIM #1 / SIM # 2 Mini SIM slots

Figure 2-3 G526RP Back View

Note: *The location of the GNSS antenna on the G526RP model differs from the G526/G527 models as shown above.*

Figure 2-4 G528 Back View

ID	Connection Name
1	Cellular diversity antenna (left)
	Cellular main antenna (right)
2	microSD card slot
3	Last Gasp switch (OFF by default)
4	Cellular / GNSS antenna
5	Cellular / GNSS antenna
6	SIM #1 / SIM # 2 Mini SIM slots

LEDs

Top Panel LEDs

Table 2-4 describes the top panel LEDs as shown from top to bottom in *Figure 2-1*.

Table 2-4 Top Panel LEDs

Name	Color	Status	Description
Alert	Red	OFF	No alert, device is running smoothly
		Flashing	Cellular module reboot, Linux kernel booting
		ON	Hardware fault
User programmable #1	Blue	OFF	User configurable via software
		Flashing	User configurable via software
		ON	User configurable via software
User programmable #2	Blue	OFF	User configurable via software
		Flashing	User configurable via software
		ON	User configurable via software
Activity	Amber	OFF	Cellular data service is not connected
		Flashing	Data sent and received over cellular connection
		ON	Cellular data service is connected
Network	Amber	OFF	Device is not registered on a cellular network
		Flashing	Registered on roaming cellular network
		ON	Registered on home cellular network

Name	Color	Status	Description
Signal	Amber	OFF	No signal (CSQ=0 to 5, 97, 98, 99)
		Flashing	Weak signal (CSQ > 6 to 12)
		ON	Strong signal (CSQ ≥ 6 to 12)
SIM	Blue	OFF	SIM not in use
		Flashing	SIM2 in use
		ON	SIM1 is in use
Wi-Fi	Blue	OFF	Wi-Fi network is inactive
		Flashing	Wi-Fi network connection traffic
		ON	Wi-Fi network link is up and active
Power	Green	OFF	Power off
		ON	Power on

Cellular

Table 2-5 G520 Series Cellular Data Rates

Cellular Type	Uplink / Downlink Maximum Data Rate
2G	236.8 / 296 kbps
3G	5.76 / 42.2 Mbps
4G LTE Cat 4	FDD: 50 / 150 Mbps TDD: 35 / 130 Mbps
4G LTE Cat 13/7	FDD: 150 / 300 Mbps TDD: 35 / 130 Mbps

Table 2-6 G520 Series Cellular Bands

Model	Part Number	Cellular Type	Bands[1]	Fallback Mode	Bands[1]
Industry Gateway					
G526	G526GP12S	LTE Cat 4	28/20/8/3/1/7	3G, 2G	8/1; 8/3
	G526GP1AS	LTE Cat 4	71/12(17)/13/14/26(5)/ 66(10,4)/25(2)	–	–
	G526GP17S	LTE Cat 4	18/5(19)/8/21/3(9)/1/7	–	–
Security Gateway					
G527	G527GP22S	LTE Cat 13 (up)/LTE Cat 7 (down)	28/20/8/32/3/1/7; TDD 40/41(38)/42/43	3G	5/8/1
	G527GP2AS	LTE Cat 13 (up)/LTE Cat 7 (down)	71/12(17)/13/14/26(5)/ 66(10,4)/25(2)/7; TDD 41/42/48/43	3G	5/4/2
	G527GP27S	LTE Cat 13 (up)/LTE Cat 7 (down)	18/5(19)/8/3(9)/1; TDD 41/42/43	3G	5(19,6)/1

Model	Part Number	Cellular Type	Bands[1]	Fallback Mode	Bands[1]
G528	G528GP2FS	Sub-6 GHz 5G ---------- LTE Cat 13 (up) /LTE Cat 20 (down)	n71/n12/n28/n20/n5/ n8/**n3/n66/n2/n1/n7**; TDD **n41(n38)**/ **n77(n78)/n79**[2] ---------- 71/12(17)/28/29/13/14/ 20/26(18,5,19)/8/32/ **3/66(4)/25(2)/1/30/7**; TDD 39/34/**40/41(38)**/ **42/48**; LAA 46	3G	5(19,6)/8/4/9/ 2/1
Transport Gateway					
G526	G526RP42S	LTE Cat 4	28/20/8/3/1/7	3G, 2G	8/1; 8/3
	G526RP4AS	LTE Cat 4	71/12(17)/13/14/26(5)/ 66(10,4)/25(2)	–	–
	G526RP47S	LTE Cat 4	18/5(19)/8/21/3(9)/1/7	–	–

1. Ranked by increasing frequency
2. Bands with 4 x 4 MIMO support are shown in **bold orange characters**

SIM Slots

The G520 series gateway provides two SIM slots to accommodate two mini SIM cards (2FF), as shown in *Figure 2-5*. The SIM cards must be activated before use.

Figure 2-5 Dual SIM Operation

Antenna Connections

Wi-Fi / Bluetooth Antenna connectors:

- Two (2) Wi-Fi, RP-SMA connectors (all models, see *Figure 2-1*)

Note: *If you are using Bluetooth only (no Wi-Fi), one antenna may be attached to the connector on the right.*

WWAN Antenna connectors:

- 4G / GNSS (G526, G527 models, see *Figure 2-2*) - Two (2) cellular, RP-SMA connectors and one (1) GNSS, RP-SMA connector
- 5G / GNSS (G528 model only, see *Figure 2-4*) - Four (4) SMA connectors total, two (2) Rx / Tx dedicated to cellular, two (2) Rx only shared between cellular and GNSS

Certified Antennas

Table 2-7 lists the antennas that have been certified for the G520 series gateways.

Table 2-7 Certified Antennas

Purpose	Antenna type	Description	Lantronix Part Number	Approved Region
Wi-Fi Antenna	Dipole, swivel type antenna, with RP-SMA(M) connector	Peak gain: 2 dBi, 2.4 Ghz to 2.5 Ghz, 2 dBi, 5.15 Ghz to 5.85 Ghz RoHS compliant	A21H0	FCC, IC, EU, AUS/ NZS, JPN, China, Mexico
	Dipole, swivel type antenna, with RP-SMA(M) connector	Peak gain: 2 dBi, 2.4 Ghz to 2.5 Ghz, 2 dBi, 5.15 Ghz to 5.85 Ghz RoHS compliant	ACC-930-0299-00	FCC, IC, EU, AUS/ NZS, JPN, China, Mexico
WWAN Antenna	Dipole, 4G, swivel type blade antenna, with SMA connector, adhesive mount	Performance across LTE frequency bands 698-960, 1710-2170, 2500-2700 MHz Gain: Up to 2 dBi RoHS compliant	A33M0	N/A

Note: *Antenna gain listed above excludes cable loss.*

Antenna Selection

Use the following guidelines in Wi-Fi antenna selection:

- Dipole, peak gain less than 2 dBi @ 2.4 GHz ~ 2.5 GHz
- Use the same dipole antenna type as certified module and modem for FCC or external antenna with length greater than 20 cm.

Ethernet Ports (LAN/WAN)

Figure 2-6 Ethernet Port

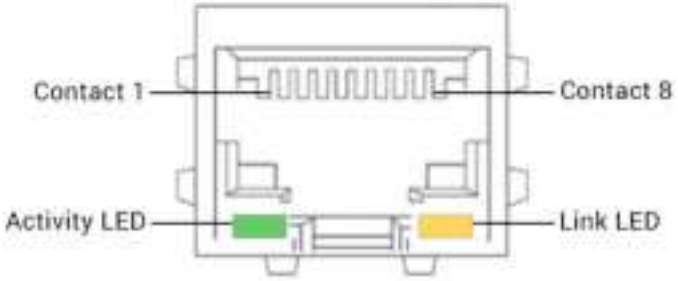


Table 2-8 Ethernet RJ45 Connector Pin Assignment and LEDs

Pin	Signal Name
1	ETX+
2	ETX-
3	ERX+
4	-
5	-
6	ERX-
7	-
8	-
Left LED (Green)	RX/TX Activity Flashing on: Activity Off: No activity
Right LED (Amber)	Link On: Link Off: No link

RS-232 Serial Port

Figure 2-7 RS-232 DB9F Interface

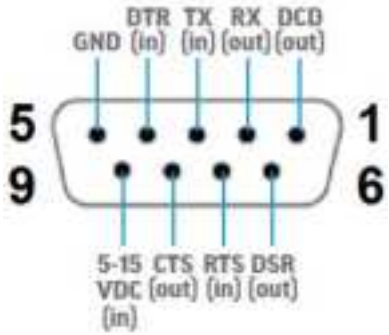


Table 2-9 RS-232 Pin Assignment

Pin	Description	Pin	Description
1	DCD out	6	DSR out
2	RX out	7	RTS in
3	TX in	8	CTS out
4	DTR in	9	NC
5	GND	–	–

RS-485 Serial Port

Figure 2-8 RS-485 and I/O Connections

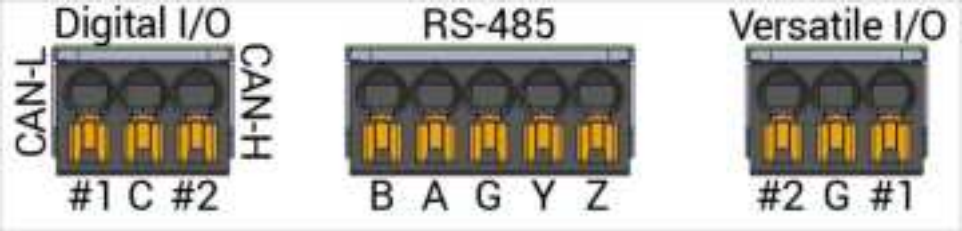


Table 2-10 RS-485 Pin Assignments

RS-485 Full-duplex

Pin	Description
B	B-
A	A+
G	Ground
Y	Y+
Z	Z-

RS-485 Half-duplex

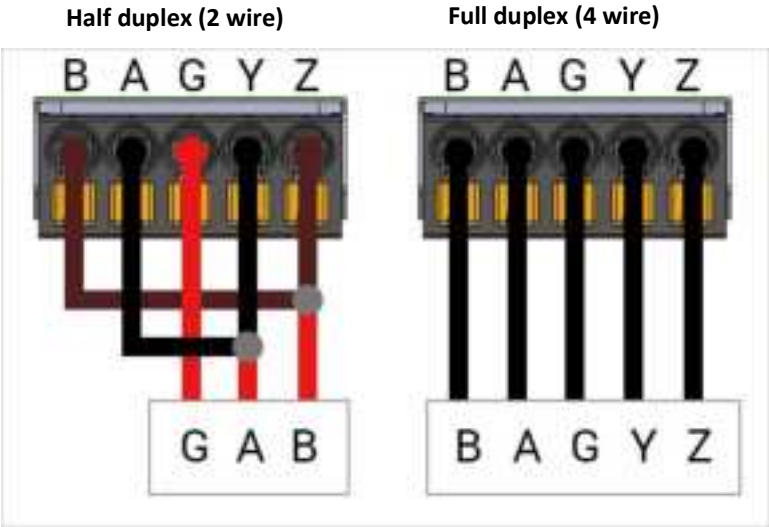
Pin	Description
A & Y	Data +
B & Z	Data -
G	Ground

Table 2-11 RS-485 Options

Interface	Description
RS-485 port	2.5 kV-isolated; half- or full-duplex RS-485 port on 5-pin COMBICON header and tool-less plug (supplied by user)
SNAP CAP™ RS-485 add-on connected to RS-232 serial port (not provided)	SNAPCAP RS-485 (SC485) converts G520 series RS-232 serial port into a 6 kV- (contact) or 8 kV- (air) ESD-protected, 2.5 kV-isolated, half- or full-duplex RS-485 port on a 5-pin 3.5 mm pitch, COMBICON header.

RS-485 Wiring diagram

Figure 2-9 RS-485 Wiring Diagram



Input / Output Connections

The G520 series gateway provides digital I/O and versatile I/O connections on 3-pin COMBICON headers and tool-less plugs (supplied by user). The connections are shown in *Figure 2-8*.

Table 2-12 Digital I/O Pin Assignments

Pin	Description
#1	◆ Digital input: 0 V dc ~ 2.5 V dc => ZERO; 3 V dc ~ 50 V dc => ONE ◆ Digital output: open collector, 200 mA maximum, 50 V dc maximum ◆ CAN-H
C	Common
#2	◆ Digital input: 0 V dc ~ 2.5 V dc => ZERO; 3 V dc ~ 50 V dc => ONE ◆ Digital output: open collector, 200 mA maximum, 50 V dc maximum ◆ CAN-L

Table 2-13 Versatile I/O Pin Assignments

Pin	Description
#1	◆ Digital output: open collector, 200 mA maximum, 50 V dc maximum ◆ Analog input: 0 V dc ~ 48 V dc range; 12-bit resolution; capable of counting pulses at up to 10 Hz ◆ Analog input: 4 mA ~ 20 mA range, 12-bit resolution
G	Ground
#2	◆ Digital output: open collector, 200 mA maximum, 50 V dc maximum ◆ Analog input: 0 V dc ~ 48 V dc range; 12-bit resolution; capable of counting pulses at up to 10 Hz ◆ Analog input: 4 mA ~ 20 mA range, 12-bit resolution

Table 2-14 Digital I/O and Versatile I/O Pin Assignments

Digital I/O

Pin	Description
#1	Input
C	Common
#2	Output

Versatile I/O

Pin	Description
#1	Input
G	Ground
#2	Output

Power Input

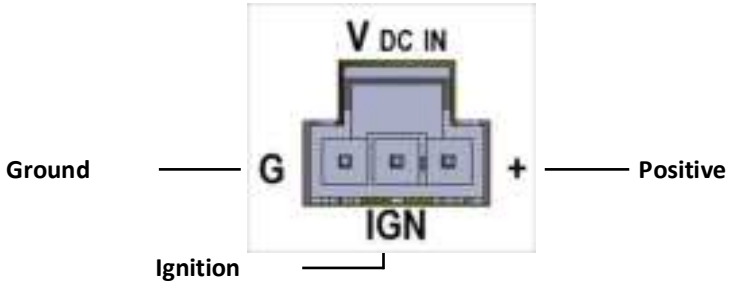
The power input interface is shown in *Figure 2-10*.

For the power cable schematic, see *Power Cable Schematic on page 270*.

Table 2-15 Power Input and PoE Output

Input Rated	PoE Output
46.75 - 60Vdc	Each PoE port loaded to 30W
10.8 - 46.74Vdc	No PoE output

Figure 2-10 DC Input Interface



Power Consumption

Table 2-16 G520 Series Power Consumption

Device State	Input Voltage		
	10V	12V	48V
Idle state (WAN, LAN, Wi-Fi, RS485, GPS & Cellular off)	210 mA	176 mA	83 mA
WAN connected (LAN, Wi-Fi, RS485, GPS & Cellular off)	245 mA	204 mA	96 mA
LAN connected (WAN, Wi-Fi, RS485, GPS & Cellular off)	240 mA	190 mA	95 mA
Wi-Fi on (WAN, LAN, RS485, GPS & Cellular off)	245 mA	190 mA	95 mA
RS485 connected (WAN, LAN, Wi-Fi, GPS & Cellular off)	–	–	–
GPS on (WAN, LAN, Wi–Fi, RS485 & Cellular off)	–	–	–
WAN, LAN, RS485 connected & Wi-Fi, GPS on (Cellular standby)	290 mA	245 mA	108 mA
WAN, LAN, RS485 connected & Wi-Fi, GPS on & Cellular on	295 mA	250 mA	110 mA

Reset Button

Using a paper clip or similar object to poke through the RESET hole, press the recessed Reset button as shown in *Figure 2-1*.

- To reboot the unit, press and hold the reset button for more than 1 second and less than 5 seconds.
- To reset to factory settings, press and hold the reset button for more than 5 seconds and less than 20 seconds.

Power over Ethernet (PSE-PoE+)

The G520 series gateway (Security gateway SKUs only) can be used as an IEEE 802.3at PoE+ compliant power source (PSE) to supply power to a device attached to the LAN port. Each LAN port supports a maximum output of 30 W. This requires a PoE+ power supply accessory, purchased separately. See *Lantronix Accessories on page 42*.

Input Rated	PoE Output
46.75 - 60Vdc	Each PoE port loaded to 30W
10.8 - 46.74Vdc	No PoE output

Product Label

Figure 2-11 Sample Product Label (G526GP1AS shown)

3: Installation

Package Contents

- G526, G526RP, G527, G528 IoT cellular gateway
- Power cord, part number: ACC-500-0420-00
- Quick Start Guide
- Percepxion promotional flyer

Other accessories are user supplied. Lantronix offers accessory bundles and other compatible accessories for purchase.

Accessory Bundles

For purchase information, go to https://www.lantronix.com/products/g520/.

Table 3-1 Lantronix Accessory Bundles

Part Number	Description
ACC-G526-1	BUNDLE, ACCESSORY, G526, Antenna A33M0, Antenna A21H0, Power supply ACC-520-0165-00,Din rail clip BR351
ACC-G527-MW	BUNDLE, ACCESSORY, G527, Antenna A33M0, Antenna A21H0, PoE Power supply SDR75-48, Din rail clip BR351
ACC-G528-MW	BUNDLE, ACCESSORY, G528, ANTENNA ACC-930-0296-00, ANTENNA A21H0, PoE Power supply SDR75-48, DIN RAIL CLIP BR351

Compatible Accessories

For purchase information, go to https://www.lantronix.com/products/g520/.

Table 3-2 Lantronix Accessories

Part Number	Description
Power Cords	
ACC-500-0420-00	POWER CORD WITH 3-PIN NANO-FIT PLUG; 2.5 A FUSE; TWO 1-METER-LONG AWG20 STRIPPED WIRES (RED, BLACK) FOR POWER
ACC-500-421-00	POWER CORD WITH 3-PIN NANO-FIT PLUG; 2.5 A FUSE; TWO 1-METRE-LONG AWG20 STRIPPED WIRES (RED, BLACK) FOR POWER; ONE 20-CENTIMETRE-LONG AWG20 WIRE (BLUE) FOR IGNITION
Power Supply and Adapters	

Part Number	Description
ACC-520-0165-00	WORLDWIDE. POWER SUPPLY, WALL CUBE, 12VDC 12W, 4 AC PLUGS, LEVEL 6, WITH PSE, 2X2 3.0MM LATCHED CONN OUTPUT
ACC-520-0166-00	US. POWER SUPPLY, WALL CUBE, 12VDC 12W, US, LEVEL 6, WITH PSE, 2X2 3.0MM LATCHED CONN OUTPUT
ACC-520-0199-00	PoE Power supply AC/DC CONVERTER, 54V, 96W, 196.0MM X 68.00MM X 38.8MM)
ACC-520-0200-00	PoE Power supply AC/DC CONVERTER, DIN RAIL, 48V, 77W, 102.0MM X 32.00MM X 125.2MM)
Wi-Fi Antenna	
ACC-930-0299-00	2.4/5.8GHZ DIPOLE ANTENNA FOR ISM & WLAN, RP-SMA(M) HINGED
A21H0	2.4/5.8GHZ DIPOLE ANTENNA FOR ISM & WLAN, RP-SMA(M) HINGED
4G / GNSS Antenna	
A33M0	THREE IN ONE LTE, 2*LTE+GPS/GLONASS/BD ANTENNA, 3*3000MM RG174 CABLE WITH 3*SMA MALE, ADHESIVE MOUNT
A33H0	THREE IN ONE LTE, 2*LTE+GPS/GLONASS/BD/GALILEO ANTENNA, 3*3000MM RG174 CABLE WITH 3*SMA MALE, ADHESIVE MOUNT.
A32M0	TWO IN ONE LTE, 2*LTE ANTENNA, 2*3000MM RG174 CABLE, SMA MALE
A32H0	TWO IN ONE LTE, 2*LTE ANTENNA, 2*3000MM CABLE, SMA MALE, ADHESIVE MOUNT.
A22H0	ANTENNA, 4G, ULTRA WIDEBAND, LTE/GPS/WIFI, HINGED 90 DEGREE SMA MALE.
A22H1	4G LTE ANTENNA, LTE/GPS/WIFI, HIGHED 90 DEGREE SMA MALE. (INCLUDING 450 MHZ)
5G / GNSS Antenna	
ACC-930-0296-00	'4-IN-1' 5G/GNSS ANTENNA, REMOTE, 3 m COAX, WATERPROOF (IP67-RATED), ADHESIVE MOUNT
MICRO COMBICON Plugs	
ACC-140-0985-00	3 PIN PLUGGABLE TERMINAL BLOCKS: FMC 0,5/3-ST2,54
ACC-140-0986-00	5 PIN PLUGGABLE TERMINAL BLOCKS FMC 0,5/5-ST2 54

Note: *The product is intended to be supplied by a UL Listed Power Unit marked "L.P.S." (or "Limited Power Source") and is rated 10.8-60Vdc, 1.6A min., Tma = 70 degree C. For assistance with purchasing the power source, please contact Lantronix Sales.*

Caution: ***Caution: Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.***

Note: *If Class I power supply is used, the power cord shall be connected to a socket outlet with earthing connection.*

Statement

- Replacement of a battery with an incorrect type that can defeat a safeguard (for example, in the case of some lithium battery types);
- Disposal of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery, that can result in an explosion;
- Leaving a battery in an extremely high temperature surrounding environment that can result in an explosion or the leakage of flammable liquid or gas;
- A battery subjected to extremely low air pressure that may result in an explosion or the leakage of flammable liquid or gas.
- GPS function is not intended to be used for location of persons.

Add-ons

To order Lantronix add-on parts, go to https://www.lantronix.com/about-us/contact/.

Table 3-3 Add-ons

Item	Description
SNAPCAP™ Converter	31.5 mm-wide, 17 mm-high, 9-pin sub-D plugs that convert G520 series' RS-232 DB9F serial port
SC485	38.2 mm-deep, 6 kV- (contact) or 8 kV- (air) ESD-protected, 2.5 kV-isolated, half- (factory setting) or full-duplex (user-configurable via a slide switch) RS-485 port; via a 5-pin, 3.5 mm pitch COMBICON header

Preparing to Install

Before starting installation, gather the necessary hardware, accessories, and documentation. Review and follow the safety information as described in the documentation.

Ensure that the computer used to access the web admin interface for gateway configuration is equipped with the following:

- Ethernet port or Wi-Fi connectivity and Internet service
- Web browser with recently updated version (Chrome, Safari, Firefox, Edge, Internet Explorer)
- DHCP client is enabled on the computer

Enabling DHCP Client on Your Computer

The DHCP client must be enabled on your computer to obtain a valid IP address from the gateway.

To enable DHCP on Windows 8 or 10:

1. Go to Start > Control Panel > Network and Internet > Network and Sharing Center.
2. Click the active network connection. The Network Connection Status box appears.
3. Click Properties and then select IPv4 (TCP/IPv4) and click Properties. The Internet Protocol Version 4 (TCP/IP) Properties will appear.

4. On the General tab, select the following options:
   - Obtain an IP address automatically
   - Obtain DNS server address automatically
5. Click OK to close the dialog.

To enable DHCP on Mac OS:

1. Launch System Preferences, and then choose Network.
2. Select Ethernet from the adapters list on the left.
3. Set the Configure IPv4 list to “Using DHCP.”

SIM Card Installation

Purchase a SIM card (region specific) from a cellular operator. Before using the SIM card, activate it according to the instructions provided by the vendor.

Insert the SIM Card

To insert a SIM card:

1. Select SIM slot #1 or #2 and slide the latch to the left.

2. Gently insert the SIM card (contact side down) into the slot and push to lock it in place. Release the latch.

Connect the Antennas

Ensure that the antenna used is suitable for the cellular frequencies in use, for both the main and auxiliary connectors.

To connect the antennas:

1. Attach the cellular antennas to the main and auxiliary connectors on the base unit and tighten them securely.
2. Attach and tighten the GNSS antenna to the GNSS connector.

   Note: *The G526 (G527 is similar) model is shown below. The G528 model is equipped with one additional cellular / GNSS antenna connector, for a total of four (4) connectors.*

3. Attach and tighten the Wi-Fi antennas to the Wi-Fi and Wi-Fi / Bluetooth connectors on the base unit. If you are using Bluetooth only but not Wi-Fi, then one antenna can be attached to

the Wi-Fi / Bluetooth connector on the right.

Wi-Fi **Wi-Fi / Bluetooth**

Connect the AC Power

To connect the AC power:

1. Connect the power cord to the power supply.
2. Attach the 3-pin connector end of the power cord to the DC input connector on the base unit.

DC input - 3-pin connector

3. Plug the AC plug on the power supply into a standard AC receptacle.

Connect the Gateway to a Computer

To log into the web administration interface, first connect to the gateway's Wi-Fi access point or connect an Ethernet cable from the gateway's LAN Ethernet port to the computer's LAN Ethernet port.

Connect using Wi-Fi

To connect using Wi-Fi:

1. On your computer, open the Wireless settings and connect to the gateway's Wi-Fi access point. The default access point SSID is:

Parameter	Details
SSID	Lantronix-<model>-<serial-number>
WPA/WPA2 TKIP Key	W1rele$$

2. Open the web browser to 192.168.1.1. The login page appears.
3. Log into the web admin interface. The default username and password credentials are:

User	Default Password
admin	admin
root	L@ntr0n1x

4. You will be required to change the root and user passwords after the first login. After changing the initial passwords, log in again to configure the network settings.

Connect using Ethernet

To connect using Ethernet:

1. Connect an RJ-45 terminated Ethernet cable between the LAN Ethernet port on the unit and the LAN Ethernet port on the computer.
2. Open the web browser to 192.168.1.1. The login page appears.
3. Log into the web admin interface. The default username and password credentials are:

User	Default Password
admin	admin
root	L@ntr0n1x

4. You will be required to change the root and admin user passwords after the first login. After changing the initial passwords, log in again to configure the network settings.

Default Configuration

All usernames and passwords are case sensitive.

Web Admin Page

Table 3-4 Default Web Admin Page Credentials

User	Default Password
admin	admin
root	L@ntr0n1x

Note: *Upon first login, you are required to change the factory default passwords before any other gateway configuration can be done. Both the admin and root passwords must be changed.*

Wireless Access Point SSID

Table 3-5 Default Wireless Access Point SSID

Parameter	Details
SSID	Lantronix-<model>-<serial-number>
WPA/WPA2 TKIP Key	W1rele$$

Default Interface Configuration

Table 3-6 Default Network Interface Configuration

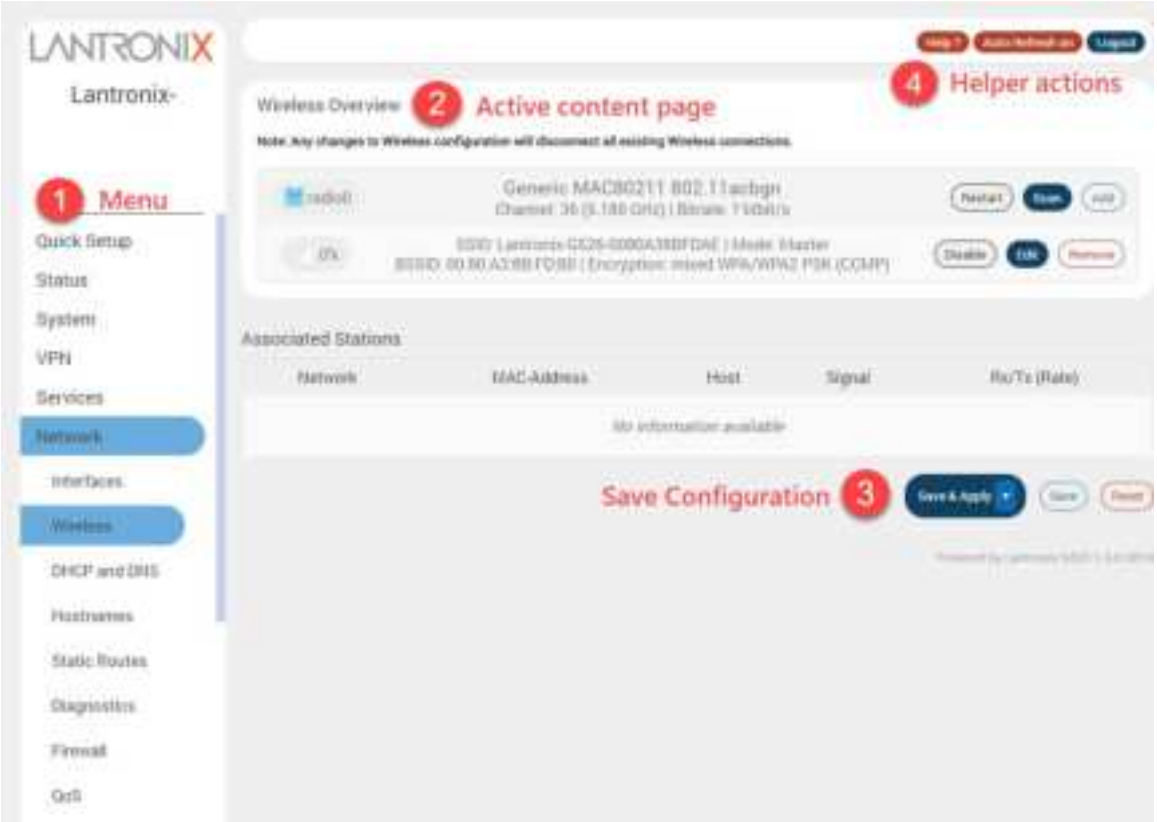
Interface	Details
WAN (Ethernet)	Automatic (DHCP client) Priority source of Internet with cellular backup
LAN (Ethernet)	Active DHCP with starting IP address 192.168.1.100 with pool of 100 clients.
Cellular	No PAP/CHAP authentication
Wireless (LAN)	Wi-Fi enabled as access point

4: Web Administration Interface

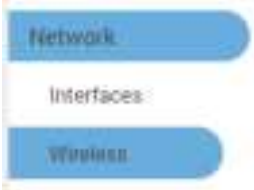
The web admin interface allows the administrator and other authorized users to configure and manage the G520 series gateways using most web browsers (Firefox, Internet Explorer or Safari web applications with the latest browser updates).

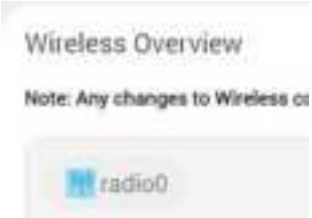
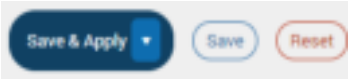
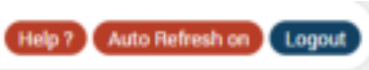
Figure 4-1 shows highlights key components on the web admin interface:

Figure 4-1 Web Admin Interface



How to interact with the web interface:

1	**Menu**  	The menu displays a list of options to configure and operate the gateway. Select a menu option to display the related status and configuration settings in the content pane.

2	**Active content**  	The content pane displays status, configuration settings, and options for interacting with the gateway. It lets you view status, and configure settings on the gateway, or perform maintenance or other operations.
3	**Save Configuration**  	These actions let you save configuration changes or reset unsaved changes on the active page ◆ **Save & Apply** - Applies and saves the changes on the web page to the gateway (in NVRAM) so that the settings will persist when the gateway is rebooted. After clicking this button, wait for the configuration to be applied before closing the browser, otherwise the old configuration will be restored. ◆ **Apply Unchecked** - Click the arrow on the Save & Apply button to reveal this option. Applies and saves the changes on the web page to the gateway (in NVRAM), but will not disrupt the active network interface. Use this if you are changing the interface parameters on which the session is active. ◆ **Save** - Saves the changes on the web page (to RAM) without committing the changes. All saved configuration will be lost when the gateway is rebooted if they are not saved and applied. ◆ **Reset** - Discards the unsaved changes on the page.
4	**Helper actions**  	These actions help you use the web interface. ◆ **Help?** - opens embedded help information for the active page ◆ **Auto Refresh on/off** - lets you enable or disable the UI auto refresh action ◆ **Unsaved changes: <#>** - shows the number of unsaved changes and lets you save & apply the changes to the gateway's configuration or revert the changes back to the saved configuration. ◆ **Logout** - logs you out of the web administration interface.

Logging In

The admin user or root user can log into the web admin interface.

If your gateway is new, please inspect and set up the gateway as described in *Chapter 3: Installation*.

To log into the web interface:

1. Open a web browser on the computer.
2. Enter the default LAN IP address 192.168.1.1. The login screen is displayed.

Figure 4-2 Web Admin Login Page

3. Enter the username and password. If you are logging in for the first time after installation or after factory reset, use the default credentials.

Change Passwords After Initial Login

After first login with a new device or after resetting the device to factory defaults, you are required to change the factory default passwords for both the admin user and root user before any other gateway configuration can be done.

The password requirements are the following:

- Password must consist of at least 8 characters and include a minimum of the following:
- 1 uppercase character
- 1 lowercase character
- 1 numerical character (0-9)
- 1 special character

Note: *Log in as root user to change both admin and root password at the same time.*

1. Log into the web admin interface as root user. This will allow you to change the passwords for both the root user and the admin user.
2. For the root user, enter the new password and then re-enter it to confirm it.
3. For the admin user, enter the new password and then re-enter it to confirm it.
4. If the country code selection for Wi-Fi operation is displayed, select the country code where the device is being used. This selection ensures that the device will only enable Wi-Fi radio settings that conform with the country's regulatory laws.
5. Click **Save & Apply**.

   This will log you out and return to the login page automatically.

Logging Out

To log off the web admin interface:

1. Click the **Logout** button located in the upper right part of the web admin interface page. When logout is complete, the login screen is displayed.

5: Using Lantronix Provisioning Manager

This chapter covers the steps for locating a device and viewing its properties and details. Lantronix Provisioning Manager is a free utility program provided by Lantronix that discovers, configures, upgrades, and manages Lantronix devices.

It can be downloaded from the Lantronix website at https://www.lantronix.com/products/lantronix-provisioning-manager/. For instructions on using the application, see the Lantronix Provisioning Manager online help.

Installing Lantronix Provisioning Manager

1. Download the latest version of Lantronix Provisioning Manager from https://www.lantronix.com/products/lantronix-provisioning-manager/.
2. In most cases, you can simply extract Lantronix Provisioning Manager from the archive and run the executable. For detailed instructions, see the Lantronix Provisioning Manager online help.

Accessing the G520 Using Lantronix Provisioning Manager

To discover a device on the local network:

1. Launch Lantronix Provisioning Manager
2. If this is the first time you have launched Lantronix Provisioning Manager, you may need to proceed through an initial setup.
3. Locate the G520 series gateway in the device list. The device's firmware version, serial number, IP address, and MAC address will be shown. Additional information can be obtained by clicking the **three dot menu** and clicking **Get Device Info**.
4. In order to perform operations on the G520 series gateway such as upgrading the firmware, updating the configuration, or uploading to the file system, click the **checkbox** next to the device and select the appropriate operation from the menu.

6: Quick Setup

Quick Setup lets you configure the IP network port so that you can configure other gateway settings. To bypass quick setup and directly configure the network interfaces using advanced settings, go to the Network page (see *Chapter 12: Network*).

Quick Setup

Quick Setup > Quick Setup

To configure the network settings:

1. On the Quick Setup page, enter the network and basic configuration of the gateway. See *Table 6-1*.

Table 6-1 Quick Setup Network Configuration

Parameters	Description
Local Area Network (LAN)	
IPv4-Address	Enter an IPv4 address for the LAN interface. This is the IP Address that must be used to access the gateway. The default LAN IPv4 Address is 192.168.1.1.
IPv4-Netmask	Enter the IPv4 netmask of the LAN interface. The default netmask is 255.255.255.0
Wide Area Network (Wired WAN)	
Enable Wan as Lan	Select to set up the WAN port to function as LAN.
Protocol	Select the protocol for the WAN interface: ◆ Manual – to set a static IPv4 address. If selected, enter the details for IPv4 address, IPv4 netmask, IPv4 gateway, and DNS server. ◆ Automatic – to use DHCP server to acquire the IP address. ◆ PPPoE (Point to Point Protocol over Ethernet) . If selected, enter the username and password. The default WAN protocol is Automatic (DHCP).
Cellular	
General Settings (tab)	Displays the primary SIM slot.
Primary SIM	Select the primary SIM slot as SIM1 or SIM2.
Firmware selection	Allows you to select the firmware that works best with SIM/Network carrier. ◆ Generic - Compatible with most carriers ◆ Automatic - Selects the firmware based on SIM/Network carrier used
SIM 1 settings/SIM 2 settings (tab)	Cellular SIM card settings for two SIM card slots.
Use Custom APN	Select this option to use a custom Access Point Name (APN) for the cellular data connection.
APN	If Use Custom APN is selected, enter the custom APN.

Parameters	Description
PIN	SIM card Personal Identification Number (PIN) is used to lock the card, preventing people from making unauthorized phone call or accessing cellular data services. Enter the PIN of the SIM card.
Authentication Type	The authentication method used for the cellular connection. If PAP, PAP/CHAP, or CHAP are selected, enter the username and password.
Username	Enter the PAP/CHAP username.
Password	Enter the PAP/CHAP password.
Enable Roaming	Select to enable data roaming on the cellular interface.
Wireless Network Options	
Country	Select country to enable WiFi channels and allowed power ratings. ***Note:*** *To ensure compliance, select only the country in which you are using the device.*
Wireless Network (LAN)	
Disable	Select the check box to disable the Wireless interface. By default, the Wireless interface is enabled. ***Note:*** *Only the default access point configuration can be modified from the Quick Setup page. To modify encryption or Wi-Fi client configuration, use the Wireless Configuration page. (Network > Wireless).*
Mode	Displays the Wireless network (LAN) mode. Mode can be ap (access point) or client.
SSID	Enter the Service Set Identifier (SSID) name. Leave the field blank to use the default SSID value. The default SSID is **Lantronix-<model>-<serial-number>**
Encryption	Displays the type of encryption.
Password	The default SSID password is **W1rele$$**.
Percepxion Client	
Enable	Select to enable or clear to disable the Percepxion client. For more configuration options, go to **Percepxion > Client**.
Device ID	Read only. Displays the gateway's Device ID. The Device ID is a 32-character string provisioned on the G520 series device at the factory. If the displayed Device ID is a 12-character string, it must be provisioned before using Percepxion. This can be done using the Lantronix Provisioning Manager software. ***Note:*** *Device ID can only be provisioned once. It will persist across resets.*
Serial Number	Read only. Displays the serial number of the device.
Connection 1	
Host	Enter the host name or IP address of the Percepxion server, used to register the device. It should start with "api."
SSH Access	
Enable	Select to enable or clear to disable SSH access. To configure SSH access, go to **System > Administration**.

Parameters	Description
Time Synchronization	
Enable NTP client	Select to enable the NTP client on the gateway to synchronize its internal clock every 60 minutes from an NTP server. Clear the check box to disable NTP client. For more configuration options, go to **System > System > Time Synchronization.**
NTP Server candidates	Enter the pool of NTP servers to poll the time from.
Timezone	Select the timezone of the gateway.

7: Status

Status provides a summary view of the vital configurations of the gateway. It includes the following pages (based on the standard firmware installation):

- *Overview (Page)*
- *The Versatile Input/Output allows configuration of certain pins as either analog inputs or digital outputs. In analog input mode, the pin reads and displays a voltage value. In digital output mode, the pin can be set to a logical state, ON (high) or OFF (low).*
- *Firewall*
- *Routes*
- *System Log*
- *Kernel Log*
- *Crash Log*
- *Processes*
- *Realtime Graphs*
- *Load Balancing*

Note: *Other Status pages may be available if additional software packages are installed.*

Overview (Page)

Status > Overview

The Status Overview page provides a listing of important system parameters.

To view the Status Overview page:

1. Go to Status > Overview.
2. Scroll the page to view the Status Overview sections. Click the following links for details about each of the subsections.

- *System*
- *Percepxion*
- *Memory*
- *Digital Input/Output*
- *Versatile Input/Output*

System

The System section provides the gateway's model and software related information.

Table 7-1 System Status Overview

Parameters	Description
Hostname	Name assigned to the gateway for addressing purposes

Parameters	Description
Model	Model number of the gateway
Part Number	Model part number Example: G526GP1AS
Secure Boot	Indicates if secure boot is enabled or disabled.
UbootVersion	U-Boot version number
Architecture	Architecture type
Firmware Version	Base firmware version number
Module Firmware	Modem firmware version
Kernel Version	Linux Kernel version number
Router Time	Day of the week, month, date, time and year configured on the unit. The format is Day Month Date hh:mm:ss Year. The time is displayed in 24-hour clock format.
Uptime	Displays the elapsed time since the unit last rebooted. The format is dd hh mm ss.
Load Average	Average CPU load time over periods of 1, 5, and 15 minute averages
Reboot Cause	Displays the last reboot cause and time whenever possible.
IMEI	15 digit IMEI number An IMEI number (International Mobile Equipment Identity) is a 15 or 17 digit unique number to identify GSM or UMTS mobile devices. It is used to prevent call initiation from a misplaced or stolen GSM or UTMS device, even if someone swaps out the device's SIM card. ***Note:*** *We recommend you record the IMEI number and secure it so that it can be quickly accessed in the event of theft or loss of the unit.*
PSE-PoE+	The G520 series gateway (Security gateway SKUs only) can be used as an IEEE 802.3 at PoE+ compliant power source (PSE) to supply power to a device attached to the LAN port.
SnapCap	Displays the installation status of the SnapCap accessory. ◆ Connected ◆ Not Connected
Ignition	Ignition feature is available on G526RP models (transport SKUs only). Indicates if ignition feature is On or Off.

Percepxion

This section describes the Percepxion client status.

Table 7-2 System Status Overview

Parameters	Description
Client State	Displays the current state of the Percepxion client. Displays a message if the device credentials are not configured.
Last Status Update	Displays the elapsed time since the Percepxion client sent its status to the server.

Parameters	Description
Last Content Check	Displays the elapsed time since the Percepxion client requested content check from the server.
Available Firmware Updates	Lists any available firmware updates.
Available Configuration Updates	Lists any available configuration updates.

Memory

The Memory section provides information about the available memory.

Table 7-3 Memory Status Overview

Parameters	Description
Total Available	Total available RAM memory. Total Memory is sum of used memory, free memory, buffered memory and cached memory.
Free	Free RAM memory. The bar graph shows the amount of free memory as a percentage of the total memory.
Buffered	Size of buffered memory. The bar graph shows the amount of buffered memory as a percentage of the total memory.
Cached	Size of cached memory. The bar graph shows the amount of cached memory as a percentage of the total memory.

Digital Input/Output

The Digital Input/Output section shows the state of the two digital input/digital output pins. The status is red when the pins are Low/Open, or green when the pins are High/Closed.

Versatile Input/Output

The Versatile Input/Output allows configuration of certain pins as either analog inputs or digital outputs. In analog input mode, the pin reads and displays a voltage value. In digital output mode, the pin can be set to a logical state, ON (high) or OFF (low).

Network

Status > Network

The Network Status page is subdivided into the following sections: cellular, network, active DHCP/DHCP6 leases, wireless, and dynamic DNS.

Cellular

The Cellular section provides the status of the SIM cards in the unit.

Table 7-4 Cellular Status Overview

Parameters	Description
Cellular Data	Displays the cellular data connection status. ◆ CONNECTED – Data communication is connected. ◆ DISCONNECTED – Data communication is not connected.
Signal Strength	Displays the current signal strength. The signal strength range is 0 to 32. ◆ 0: -113 dBm or less (none) ◆ 1: -111 dBm (poor) ◆ 2 to 30: -109 to -53 dBm (fair to good) ◆ 31: -51dBm or greater (excellent) ***Note:*** *Signal strength for a good cellular data connection must be 12 or above.*
Network Status	Displays the registration status of the unit on the current cellular network. ◆ Registered ◆ Not Registered
Operator Name	Name of the cellular operator in use
Operator Number	Number of the cellular operator in use
Operator Type	Operator type
Roaming Status	The roaming status of the unit: ◆ Home ◆ Roaming ◆ N/A
SIM 1/SIM 2 Status	Displays the availability of SIM card in SIM card slot. ◆ Error – SIM card is not inserted. ◆ READY – SIM card is inserted.
Active SIM	Displays the active SIM, SIM 1 or SIM 2.
IMSI	Displays the International Subscriber Identity (IMSI) number. In case of UMTS, it is read from the SIM card. The IMSI is a 15 digit unique mobile number associated with the cellular network and used to acquire the details of the mobile for identifying the user of a cellular network.
Configured Band	The configured radio frequency bands
Registered Band	The registered radio frequency band
Temperature	Internal temperature of the unit in degrees Celsius
ICCID	Integrated Circuit Card ID (ICCID) – unique serial number that identifies the SIM card.

Network

The Network section provides the IPv4 and IPv6 WAN status and the number of active connections.

Table 7-5 Network Status Overview

Parameters	Description
IPv4 Upstream	Displays status of IPv4 WAN connections with following details: ◆ Protocol – Static (manually addressed) or DHCP client (dynamically addressed) ◆ Address – IP address of the WAN interface. ◆ Gateway – IP address of the WAN interface gateway. ◆ DNS 1/2/3 – DNS IP addresses, in order of precedence. ◆ Connected: Duration since connection was established. ◆ Device: the physical interface, cellular, ethernet adapter and so on.
IPv6 Upstream	Displays status of IPv6 WAN connections with following details: ◆ Protocol – Static (manually addressed) or DHCPv6 client (dynamically addressed) ◆ Address – IPv6 addresses of the interface. ◆ Gateway – IP address of the gateway. ◆ DNS 1/2/3 – DNS IP addresses; in order of precedence. ◆ Connected: Duration since connection was established. ◆ Device: the physical interface, cellular, ethernet adapter and so on.

Active DHCP and DHCPv6 Leases

The Active DHCP Leases and DHCPv6 Leases section shows information about the devices connected to the gateway using a DHCP or DHCPv6 lease.

Table 7-6 Active DHCP Leases Status Overview

Parameters	Description
Host Name	Name of the device (laptop, mobile, etc.) that is connected to the gateway and has been leased an IPv4 address or an IPv6 address by the gateway's DHCP server.
IPv4 Address/IPv6 Address	IPv4 address or IPv6 address assigned to the device.
MAC Address	Applies to IPv4. MAC address of the device.
DUID	Applies to IPv6. DUID (Device Unique Identifier) of the device connected.
Leasetime remaining	The remaining time for which the device can use the DHCP server leased IPv4 address.

Wireless

The Wireless section describes the status of the Wi-Fi network used by the gateway and the Wi-Fi associated stations.

Table 7-7 Wireless Status Overview

Parameters	Description
Connection Name	Name of the connection and the details: ◆ Type – The wireless radio chipset ◆ Channel – Wi-Fi channel ◆ Bitrate – Data transfer rate ◆ SSID –Service Set Identifier (SSID) that uniquely names a wireless local area network (WLAN) ◆ Mode – Displays whether the WLAN interface is currently configured as an access point (Master) or as a client of a higher order Wi-Fi network. ***Note:*** *For Wi-Fi WAN (WWAN) operation, the connection mode should be 'Client'.* ◆ BSSID – Displays Basic Service Set Identification (BSSID); 24 bit MAC address of wireless device. ◆ Encryption – Displays the data encryption method. ◆ Associations – Displays the number of associated stations.
Associated Stations	
Network	Mode and name of the network to which the device is connected
MAC Address	MAC address of the computers and/or devices that are connected
Host	Host name of the associated station
Signal/Noise	Signal strength/noise in dBm
RX Rate/Tx Rate	The receive (RX) and transmission (TX) data rates of the associated client. Displays data transfer rate (Mbit/s), channel bandwidth (MHz), Modulation and Coding Scheme index (MCS), and GI time (Guard Interval, for TX rate).
Disconnect	Click to disconnect the associated station from the access point.

Dynamic DNS

The Dynamic DNS section shows the Dynamic DNS IPv4 and IPv6 configuration.

The details include configuration name, next update, lookup hostname, registered IP, and network.

Firewall

Status > Firewall

The Firewall Status page provides a listing of the IPv4 firewall or IPv6 firewall rule chains in the Filter, NAT, Mangle, and Raw firewall tables.

Use the buttons at the top of the page to complete the following actions:

Hide empty chains	Click to hide the chains that have no rules.
Show empty chains	Click to show all chains.
Reset Counters	Click to reset counters for number of packets and traffic.
Restart Firewall	Click to reload the existing firewall configuration of every interface.

Figure 7-1 shows a portion of the IPv4 Firewall status page, and *Table 7-8* describes the firewall details.

Figure 7-1 IPv4 Firewall Status

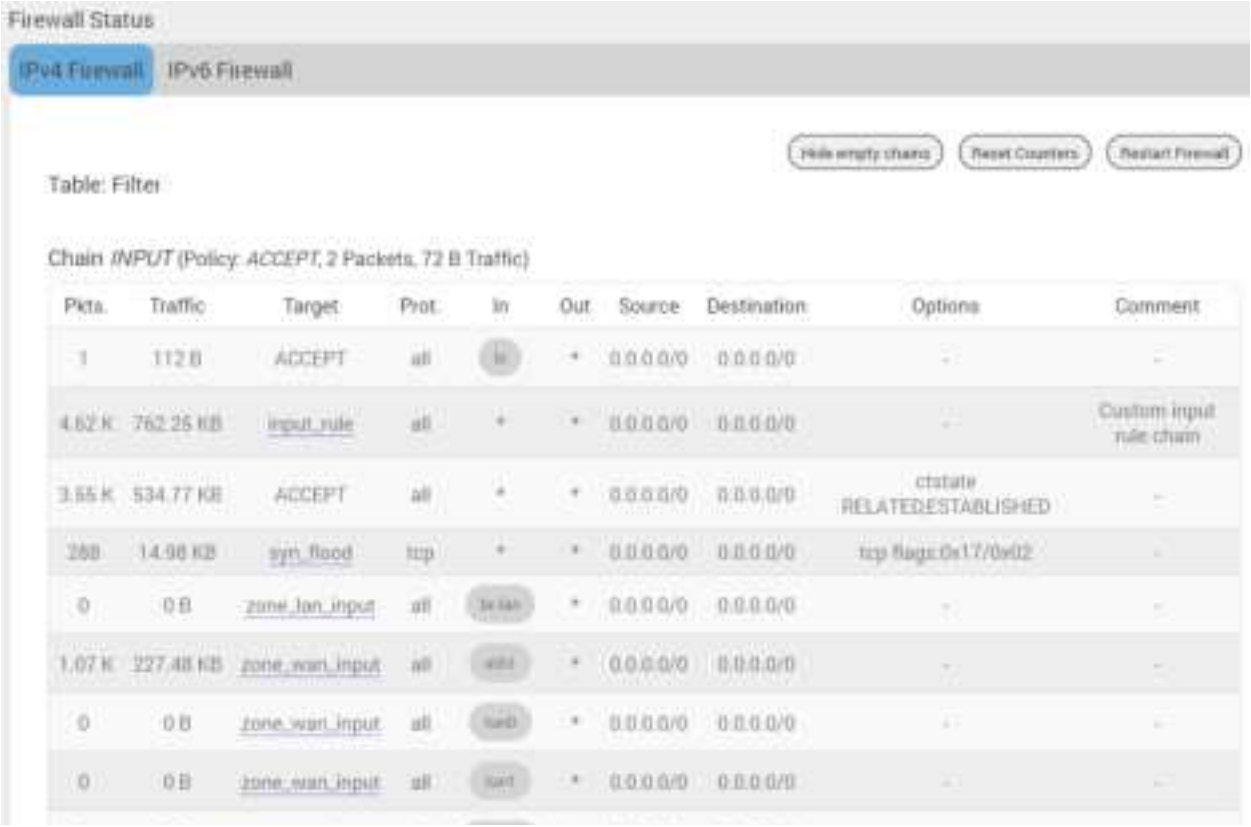


Table 7-8 Firewall Status

Parameters	Description
Rule Chain name and details	Displays the rule chain name, type, and policy details
Pkts	Displays the number of accepted packets.
Traffic	Displays the amount of traffic captured by the filter.
Target	Displays the target action for the traffic processed for a respective rule.

Parameters	Description
Prot.	Displays the protocols configured in the firewall rule.
In	Input interface.
Out	Output interface.
Source	Displays the source IPv4/IPv6 address.
Destination	Displays the destination IPv4/IPv6 Address.
Options	Displays option details
Comment	Displays comment details

Routes

Status > Routes

The Routes status page displays the ARP table and active IPv4 and IPv6 routes.

Table 7-9 Routes Status

Parameters	Description
ARP	
IPv4 Address	Displays the IPv4 address.
MAC Address	Displays MAC address of the peripheral device.
Interface	Displays the interface name connected to the peripheral device.
Active IPv4 Routes	
Network	Displays the network type used by the active IPv4 routes.
Target	Displays the destination IPv4 address and mask.
IPv4 gateway	Displays the IPv4 address gateway used for traffic routing.
Metric	Displays the routing metric assigned to the interface.
Active IPv6 Routes	
Network	Displays the network type used by the active IPv4 routes.
Target	Displays the destination IPv6 address.
Source	Displays the IPv6 address gateway used for traffic routing.
Metric	Displays the routing metric assigned to interface.

System Log

Status > System Log

The System Log displays detailed system, traffic, and network activity log information.

Syslog format is shown in the following example:

```
Tue Sep 15 22:33:38 2020 user.info Eventsms: BAND : All supported bands
```

where:

date = `Tue Sep 15 22.33.38 2020`

severity = `user.info`

event details = `Eventsms: BAND: All supported bands`

To configure the system logs, see *System > System > Logging*.

Kernel Log

Status > Kernel log

The Kernel log displays the Linux kernel log events. It shows information about hardware drivers, kernel information and status during boot up and more. It gets reset on every boot.

Crash Log

Status > Crash log

The Crash Log displays the Linux Kernel stack traces for crashes.

Processes

Status > Processes

The Processes log displays a list of active Linux system processes and their resource usage.

Use the buttons in the individual process rows to complete the following actions:

Hang up	Sends a hang up signal to terminate the process.
Terminate	Sends a terminate signal to terminate the process.
Kill	Sends a kill signal to immediately terminate the process. The process will not perform any cleanup operations.

Table 7-10 Processes Status

Parameters	Description
PID	Displays the Process identifier (PID) number associated with the process.
Owner	Displays the task owner

Parameters	Description
Command	Displays the command name
CPU usage %	The CPU usage of the process, displayed as a percentage of the total available CPU resources.
Memory usage %	The amount of the system's working physical memory that the process is currently using, displayed as a percentage.

Realtime Graphs

Status > Realtime Graphs

The Realtime graphs display the gateway's activities over time for CPU load, WAN network traffic, wireless usage, and network connections.

Load

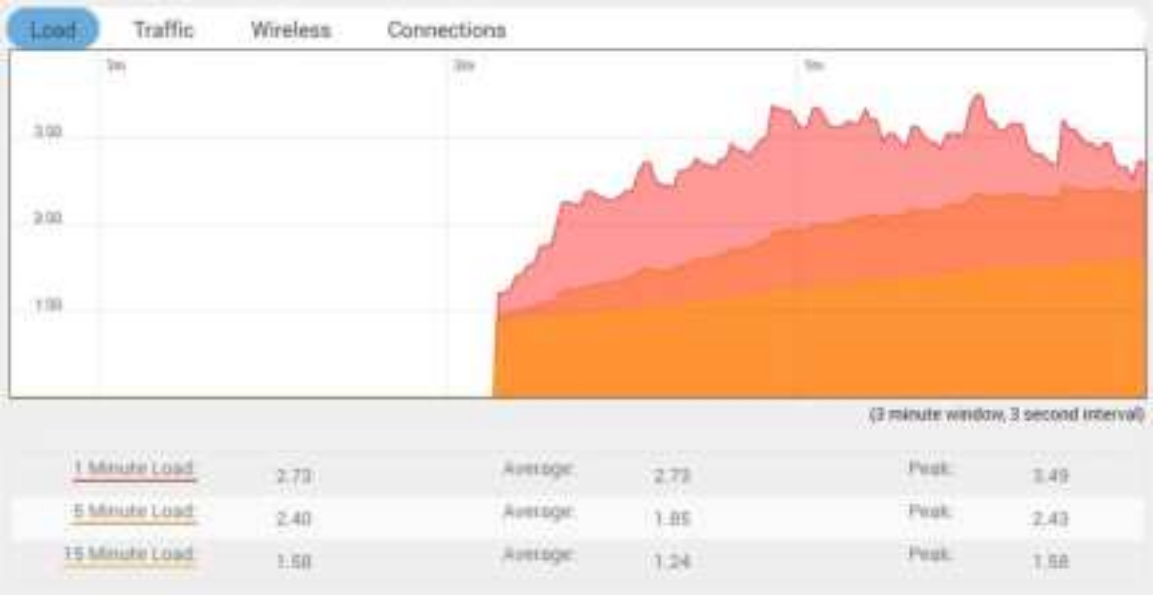
Status > Realtime Graphs > Load

The Load graph shows the CPU load average and peak (y-axis, % utilization) over time (x-axis).

Average loads are shown for 1-minute (red), 5-minute (orange), and 15-minute (yellow) load.

Figure 7-2 shows a CPU load graph.

Figure 7-2 Realtime CPU Load Graph



Traffic

Status > Realtime Graphs > Traffic

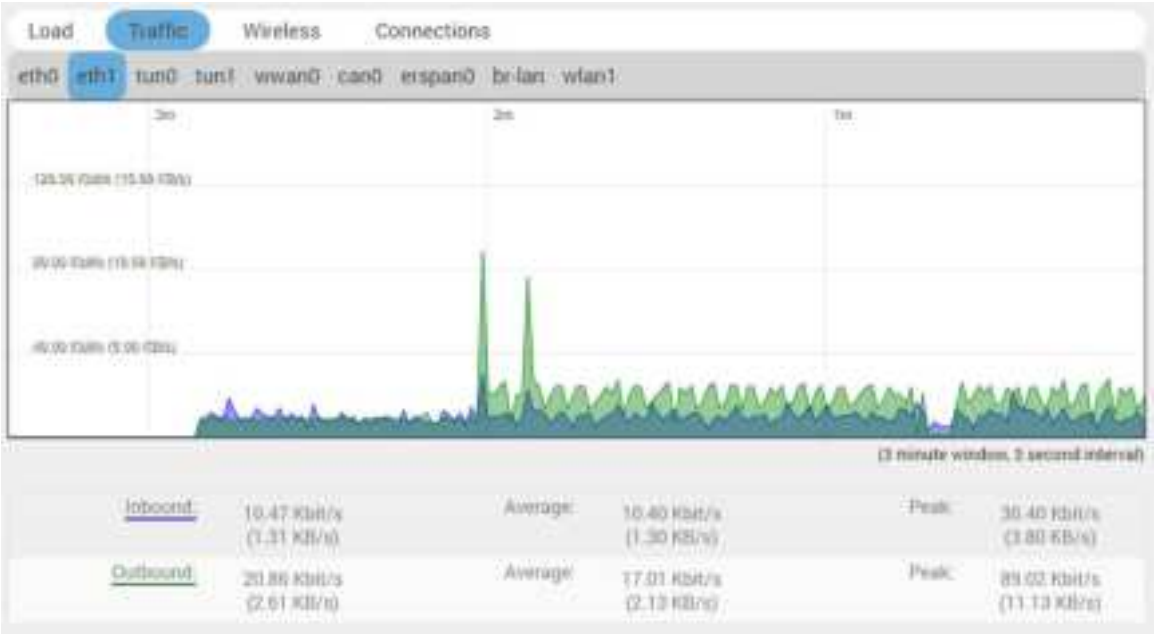
The Traffic graph indicates the WAN-side incoming and outgoing traffic rate (y-axis) on the different interfaces over time (x-axis). The graphs display the average and peak data transfer on the following interfaces (if configured for WAN traffic): eth0, eth1, tun0, tun1, wwan0, can0, erspan0, br-lan, and wlan1.

Average and peak rates are shown for inbound traffic (blue) and outbound traffic (green).

The WAN interface shows average and peak WAN and cellular traffic.

Figure 7-3 shows an example of network traffic for the eth1 interface:

Figure 7-3 Realtime Network Traffic Graph (eth1)



Wireless

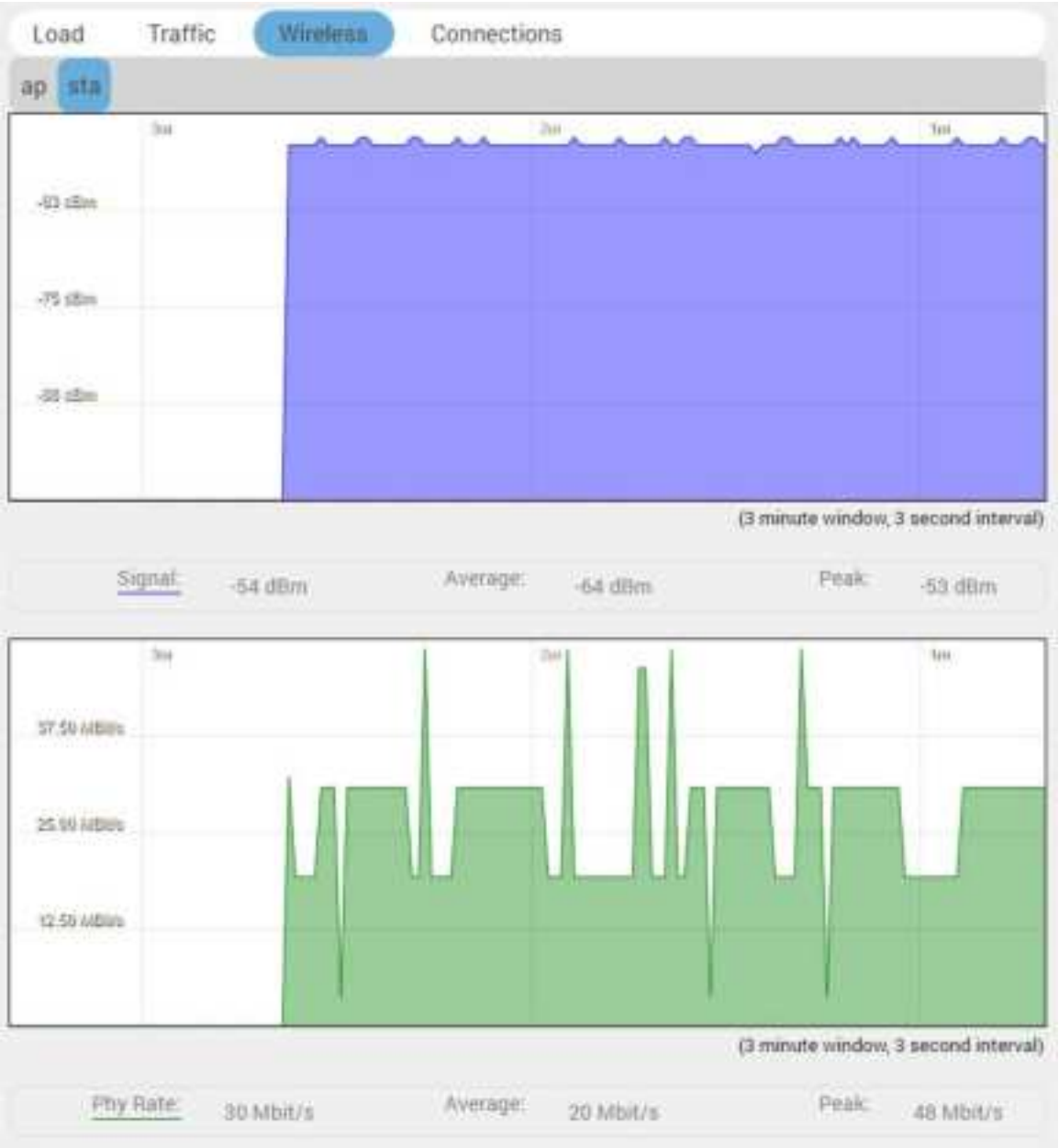
Status > Realtime Graphs > Wireless

The Wireless graph indicates Wi-Fi usage for the device configured as an access point or wireless client. including signal and noise levels (y-axis, dBm) and physical data transfer rate (y-axis, Mbit/sec) over time (x-axis).

The top graph displays signal (blue) and noise (red) levels. The bottom graph displays the physical data transfer rate (green) irrespective of WI-Fi being used as an access point or client.

Figure 7-4 shows the wireless usage graph for a G520 series device configured as Wi-Fi client (STA) and connected to an external access point.

Figure 7-4 Realtime Wireless Usage Graph (client)



Connections

Status > Realtime Graphs > Connections

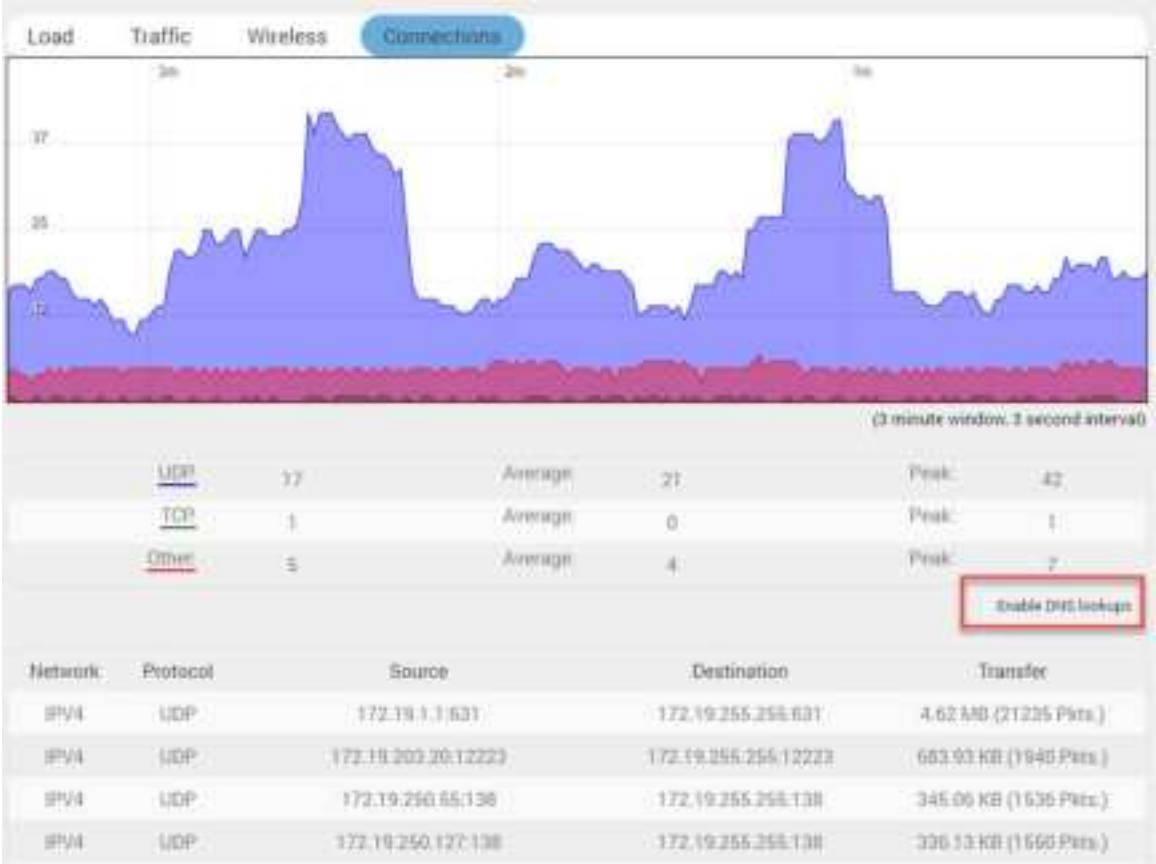
The Connections graph indicates the number of active network connections (x-axis) over time (y-axis). It includes connections originating from the gateway and also connections originating from the LAN or WAN.

The graph displays UDP (blue), TCP (green) and other (red) connections. The table below the graph displays connection details including IPv4/IPv6, protocol, source IP, destination IP, and amount of data transferred.

By default DNS lookup is disabled. You can enable it by clicking the link **Enable DNS lookups** below the graph.

Figure 7-5 shows a realtime connection graph for an idle gateway.

Figure 7-5 Realtime Connections Traffic Graph



Load Balancing

Status > Load Balancing

Interface

Status > Load Balancing > Interface

The Interface page shows the MWAN interfaces, with active interfaces shown in green and disabled interfaces shown in red. The uptime (hh:mm:ss) is displayed for active interfaces.

Detail

Status > Load Balancing > Detail

The Detail page shows MWAN interface (IPv4 and IPv6) details including interface status, current policies, directly connected networks, and active user rules.

Diagnostics

Status > Load Balancing > Diagnostics

The Diagnostics page provides diagnostic commands to check the health of the selected MWAN interface.

The following diagnostics commands are supported:

- Ping the default gateway
- Ping tracking IP
- Check IP rules
- Check routing table
- Hotplug ifup
- Hotplug ifdown

To run a diagnostics command, select the MWAN interface and the task and click **Execute**.

The results of the command are displayed in the results section below the diagnostics command.

Troubleshooting

Status > Load Balancing > Troubleshooting

The MWAN Status - Troubleshooting page runs the following IP commands and displays the output:

- ip a show
- ip route show
- ip route list table 1-250
- iptables -L -t mangle -v -n

It may take a couple minutes to process the commands and display the results.

8: System

The System pages provide configuration for secure local and remote management. The System menu contains the following sections:

- *System*
- *Administration*
- *Software*
- *Startup*
- *Scheduled Tasks*
- *LED Configuration*
- *Backup / Flash Firmware*
- *Custom Commands*
- *Reboot*

System

System > System

This section contains settings that apply to the basic operation of the system, including the hostname, time zone, and system log configuration.

General Settings

System > System > General Settings

General settings let you configure local time and router time, hostname, and time zone.

To configure general system settings:

1. Go to System > System > General Settings.
2. Enter the configuration settings. See *Table 8-1*.
3. Click **Save & Apply**.

Table 8-1 System General Settings

Parameters	Description
Local Time	Displays the local time of the user's computer. Sync the local time with browser or with an NTP server. Click **Sync with browser** button to synchronize the gateway's clock with the local computer browser. Click **Sync with NTP-Server** to synchronize the gateway's clock with an NTP server. ***Note:*** *The displayed time is dependent on the configuration of your local computer that is being used as an NTP server.*
Router Time	Displays the current router time according to the configured time zone.

Parameters	Description
Hostname	Displays the hostname for this unit. Do not include the period character "." in the hostname as only the string before the period will be used as the hostname.
Timezone	Select time zone according to the geographical region in which the unit is deployed. The default time zone is UTC.
Set Time Manually	Set the year, month, date, hour, minute and seconds. Click **Apply the time** to save the information.

Logging

System > System > Logging

The system logger provides important debugging and monitoring capabilities. The system logs capture traffic, system, and network activity. The logs are stored in RAM and are reset when the gateway is rebooted.

The system logs can be stored locally or sent to an external UDP or TCP syslog server for storage and archival purposes.

To configure the system log settings:

1. Go to System > System > General Settings.
2. Enter the configuration settings (see *Table 8-2*).
3. Click **Save & Apply**.

Table 8-2 Syslog Configuration

Parameters	Description
System log buffer size	Enter the size of the buffer in Kilobytes (KB) to save logs and status information details. The default system log buffer size is 64 KB. When the buffer is full, records will be overwritten on a first in, first out (FIFO) basis.
External system log server	Enter the IP address of an external syslog server to be used to save the real time logs. By default the logs are written to the local system.
External system log server port	Enter the UDP port number of the external syslog server. The default port is 514.
External system log server protocol	Protocol of the external syslog server. The protocol is UDP.
Write system log to file	File path and file name to write the log messages to. If an external filesystem (SD card or USB flash drive) is mounted, add the mount path and file name here. The logs display application (see *Services > Logs Information*) will download the files written to this file path. Example: /mnt/usbdevice/log.txt

Parameters	Description
Log output level	Select the log severity output level. The level of severity progresses from Info to Emergency. Lower severity levels are more verbose and will include messages from all higher severity levels. Log levels are listed in order of increasing severity: ◆ Debug – Provides debug messages used by the software developer for debugging the application. These logs are typically not useful during operations. ◆ Info – Provides normal operational information messages that are used for general purposes like reporting. ◆ Notice – Provides alerts for peculiar events that are not an error. These logs help to identify potential issues. Since these logs do not indicate errors, immediate action may/may not be necessary. ◆ Warning – Displays warning messages for a potential issue, indicating to take an action. An error may occur if no action is taken against the warning issued. ◆ Error – Displays the messages indicating an error condition. ◆ Critical – Indicates failure in secondary system and must be corrected immediately. ◆ Alert – Problems which should be corrected immediately. ◆ Emergency – System is unusable. ***Note:*** *For help with log errors, contact* Lantronix Technical Support.
Cron log level	Select the minimum level for cron messages to be logged to syslog. ◆ Debug – Helps to debug cron process which has failed during runtime. ◆ Normal – Displays informational messages ◆ Warning – Indicates some issues can happen or error could be generated in cron process. ***Note:*** *For help with Cron log warning messages, contact* Lantronix Technical Support.

Time Synchronization

System > System > Time Synchronization

Select the method that the gateway uses to synchronize its internal clock. The available methods are GPS, NTP, or GSM

Note: *If all three methods are enabled, the order of precedence is GPS, then NTP, then GSM.*

Table 8-3 System Time Synchronization Configuration

Parameters	Description
GPS Time Synchronization	Select this option for the gateway to synchronize its internal clock using GPS. ***Note:*** *To use this option, confirm the following: the gateway supports GPS, GPS is enabled, and a GPS antenna is installed.*
Interval	The time in seconds to update time from the GPS frame.

Parameters	Description
Enable NTP client	This option enables the NTP client on the gateway to synchronize its internal clock every 60 minutes from an NTP server. If enabled, enter the NTP options as needed. To use as NTP client, no change to the firewall is required. ***Note:*** *Enabling NTP Client consumes data.*
Provide NTP server	This option enables the NTP server on the gateway. The service will respond to the local network with the time of the gateway. To run as NTP server, open UDP port 123. Disabled by default.
Use DHCP advertised servers	Enables or disables the use of DHCP-provided NTP servers. Enabled by default.
NTP server candidates	Enter the pool of NTP servers to poll the time from.
GSM Time Synchronization	If enabled, the gateway will synchronize using GSM functionality.

Language and Style

System > System > Language and Style

The language and style settings are used to control the look and feel of the web interface.

Table 8-4 Language and Style Configurations

Parameters	Description
Language	Default value is auto.
Design	Default design of user interface is Rosy.
Auto refresh default poll interval in seconds	Sets the web interface auto refresh polling interval. The valid range is between 5 and 50 seconds. The default is 5 seconds. ***Note:*** *Auto refresh can be turned on or off using the Auto Refresh button on the UI.*

Administration

System > Administration

The Administration page allows you to configure the unit's password and SSH access to the device. You can configure various ports and login security.

Router Password

System > Administration > Router Password

This page allows you to change the login password of the current user. If you are logged in as administrator, you can change the administrator password, and if you are logged in as root, you can change the root password and the administrator password.

The password requirements are the following:

- Password must consist of at least 8 characters and include a minimum of the following:
- 1 uppercase character
- 1 lowercase character
- 1 numerical character (0-9)
- 1 special character

To change the password:

1. Go to System > Administration. The Router Password page is displayed.
2. Type the current password.
3. Type the new password and retype it to confirm.
4. Click **Save**.

SSH Access

System > Administration > SSH Access

Secure Shell (SSH) lets you securely and remotely access the gateway over the network from a terminal emulator to view and configure it. SSH provides strong password authentication and public key authentication, as well as encrypted data communication between your computer and the router. The router listens for SSH connections on TCP port 22 (default).

To set up SSH access, an SSH key is required. You can use the default SSH key or generate your own SSH key pair and upload the public key.

By default, remote SSH over WAN is disabled. You can enable it from the web interface by configuring the firewall with a rule to allow SSH traffic from the WAN (enable port 22), or by sending an SMS from a registered admin number.

To enhance security, it is recommended to disable SSH access on interfaces when it's not needed.

Note: *SSH requires password change on first login. Similar to web admin interface, SSH prompts you to change root and admin password on first login.*

To configure SSH access:

1. Go to System > Administration > SSH Access.
2. Enter the configuration settings (see *Table 8-5*).

Table 8-5 SSH Access Configuration

Parameters	Description
Interface	Select the interface. SSH listens only on the selected interface. ***Note:*** *Unspecified – If this option is selected, SSH listens on all interfaces.*
Port	Provide the listening port of the instance. Default port is 22.
Password Authentication	Select to allow SSH authentication using user name and password.
Allow root logins	Select to allow root user logins over SSH.
Allow root logins with password	Select to allow root logins using a password over SSH.
Gateway Ports	Select to allow remote hosts to connect to local SSH forwarded ports.
Add Instance	Click to add another SSH instance.

SSH-Keys

System > Administration > SSH-Key

Public SSH keys are used to authenticate with SSH public key authentication. One or more keys are provided by default or you can upload your own keys.

To add a new public SSH key:

1. Go to System > Administration > SSH-Keys.
2. Copy the public key from the host system and paste it in the input field. Alternatively, drag and drop the SSH key file (.pub) into the input field.
3. Click **Add key**.

Software

System > Software

The software package manager lets you upgrade the system by installing, upgrading, or removing additional software packages from package repositories that are local or on the Internet. The package manager (opkg utility) attempts to resolve dependencies with packages in the repositories. If it fails, it reports an error and aborts the installation of the package.

The software package manager is not used to upgrade system firmware (sysupgrade). For firmware upgrade, see *Backup / Flash Firmware*.

The Software page displays the list of all packages or the packages that match the Filter criteria according to the following categories (tabs).

- **Available** - when selected, the table lists all packages that are available in the configured repository. You can see if the package is installed, or if you have the option to install or upgrade it.
- **Installed** - when selected, the table lists the packages that are currently installed on the device. You can see the option to remove these packages.
- **Updates** - when selected, lists the packages where an updated version is available, as long as you use a supported version of OpenWRT. If none are found, displays “No packages”.

The Software page is described in *Table 8-6*:

Table 8-6 Software Page

Parameters	Description
Free space	Indicates the available memory on the flash memory, as both a percentage and size in MB. The darker line represents the portion of free space.
Filter	Filters the package list. Type part or all of the package name in the filter field.
Download and install package	Downloads and installs a package from the configured repository or from a custom feed. Enter the package name for a package in the configured repository or enter the URL for a package on a custom feed.
Actions	
Update lists	Click to update the package list. The package manager needs this information to install or upgrade packages or print information about them. Run the update command each time before you install a new package.
Upload Package	Click to select the package to upload from the local machine.
Configure opkg	Click to modify the opkg package manager configuration. See *Configure OPKG*.
Package List	
Package list	Displays the available, installed, or available for upgrade packages list.
Package name	Displays the name of package
Version	Displays the package version
Size (.ipk)	Displays the size of the installed package
Description	Displays the package description.

Parameters	Description
(Status) or action	Displays “Installed” to indicate the package is installed, or displays the relevant action. The options are: **Install** - click to install the package **Upgrade** - an upgrade package is available. Click to install the package. **Remove** - (on Installed tab). click to remove the package.

List the Packages

To view all packages in the configured repository:

1. Go to System > Software.
2. Click the Available tab. The packages are displayed. (Click the Installed tab to view the installed packages only.)
3. Click the page back and page forward arrows (<< and >>) to view the entire packages list if it spans more than one page.

To filter the package list by package name:

1. Go to System > Software.
2. Next to Filter, type part or all of the package name.
3. Click the Available, Installed or Updates tab. The packages that match the filter are displayed.
4. Click the page back and page forward arrows (<< and >>) to view the list of packages.

Update the List of Packages

The update command retrieves the list of packages. The package manager needs this information to install or upgrade packages or print information about them. You should run the update command before you install a new package.

To update the list of available packages:

1. Go to System > Software.
2. Click **Update lists**. The package manager updates the list of available packages.
3. Click **Dismiss**.
4. View the available packages.

Install a Package

To install a package:

1. Go to System > Software.
2. Click **Update lists** to refresh the list of available packages.
3. Do one of the following:
   - Click the Available tab, select the package (or filter the list and select the package) and click **Install**.
   - Under **Download and install package**, enter the package name for a package on the download server, or enter the URL for a package on a custom feed, and click **OK**.

- Click **Upload Package,** to select the package from the local machine, and click **Upload**.

4. The package manager displays the package details including the following:
   - version of the package
   - size of installed package
   - list of dependent packages, with installation status and size if not installed
   - package description
   - space required and the number of packages to install
   - A warning message is displayed if the installed packages are incompatible with the required packages.
   - The option to **Overwrite files from other package(s)**. By default, it is not selected.
5. Review the package details. Ensure the device has adequate space available to install the required packages. If desired, select **Overwrite files from other package(s)**.
6. Click **Install**.
7. The package manager displays the installation progress and error messages, if applicable. Click **Dismiss** when finished.
8. Refresh the web page and view that the package is listed as “Installed” in the list of Available packages. You may need to restart the device, depending on the package and its use.

Upgrade a Package

To upgrade a package:

1. Go to System > Software.
2. Click **Update lists** to refresh the list of packages.
3. Do one of the following:
   - Click the Available tab, select the package (or filter the list and select the package) and click **Upgrade**.
   - Under **Download and install package**, enter the package name for a package on the download server, or enter the URL for a package on a custom feed, and click **OK**.
   - Click **Upload Package** and browse to select the package from the local machine.
4. The package manager lists the package details including the following:
   - version of the package
   - size of installed package
   - package description
   - space required and the number of packages to install
   - A warning message is displayed if the installed packages are incompatible with the required packages.
5. Review the package details. If desired, select **Overwrite files from other package(s)**.
6. Click **Install**.
7. The package manager displays the installation progress and error messages, if applicable. Click **Dismiss** when finished.

8. To verify, refresh the web page and view that the package is listed as “Installed” in the list of Available packages. You may need to restart the device, depending on the package and its use.

Remove a Package

To remove a package:

1. Go to System > Software.
2. Click the Installed tab, select the package (or filter the list and select the package) and click **Remove**.
3. Review the package details, including the following:
   - version of the package
   - size of installed package
   - description of the package
   - The option to **Automatically remove unused dependencies** box (checked by default). To keep all dependent packages, clear this box.
4. To continue, click **Remove**.
5. The package manager displays the progress and error messages, if applicable. Click **Dismiss** to close the dialog.

Configure OPKG

The OPKG configuration files define the configuration and feed locations used by the OPKG package manager. It includes the following configuration files:

- opkg.conf – This configuration file sets the default folders.
- opkg/customfeeds.conf – This file is used to add your custom package feeds (repositories).
- opkg/distfeeds.conf – This file is used to set the feeds. By default, it provides the path to the Lantronix package server.

To modify the OPKG configuration:

1. Go to System > Software.
2. Click the **Configure opkg** button.
3. Modify the configuration (see *Table 8-7*).
4. Click **Save**.

Table 8-7 OPKG Package Manager Configuration

Parameters	Description
opkg.conf	The default configuration is shown: ◆ dest root / ◆ dest ram /tmp ◆ lists_dir ext /var/opkg-lists ◆ option overlay_root /overlay ◆ option check_signature The options can be left at the default value.

Parameters	Description
customfeeds.conf	Enter each custom package feed on its own line. The feed can be on a remote server, in a version control system, on the local file system, or in any location addressable by a single name (path/URL) over a protocol with a supported feed method. An example format is provided: # src/gz example_feed_name http://www.example.com/path/to/files Remove the "#" (hash symbol) at the start of the line.
distfeeds.conf	Displays the Lantronix package feeds repository. The feed can be on a remote server, in a version control system, on the local file system, or in any location addressable by a single name (path/URL) over a protocol with a supported feed method.

Startup

System > Startup

Initscripts

System > Startup > Initscripts

Init scripts are responsible for starting required processes during the boot process. The Initscripts page displays the installed init scripts in order of priority and lets you take action to enable, disable, start, restart or stop them.

Note: *Do not disable init scripts unless you understand the consequences of doing so, as disabling an essential script such as a network script may cause your device to become inaccessible.*

Table 8-8 describes the init scripts actions.

Table 8-8 Initscripts Actions

Parameters	Description
Start priority	Displays the priority of when the initscript is run during startup. Order of priority is from 00 to 99.
Initscript	Displays the name of the initscript
Enable/Disable	Displays the current state as Enabled or Disabled. Click the button to change the state from enabled to disabled or from disabled to enabled.
Start	Clicking the Start button starts the init script immediately. Reboot the router for changes to take effect.
Restart	Clicking the Restart button restarts the init script immediately. Reboot the router for changes to take effect.
Stop	Clicking the Stop button stops the init script immediately. Reboot the router for changes to take effect.

Local Startup

System > Startup > Local Startup

The local startup file (/etc/rc.local) contains custom commands that are run at the end of the boot process, after the system is initialized. By default, it is empty.

To configure the local startup file:

1. Go to System > Startup > Local Startup.
2. In the editor, type custom commands on any line before the line “exit 0”. Make sure that the file ends with the line “exit 0”.
3. Click **Save**.

Changes will take effect on the next reboot.

Scheduled Tasks

System > Scheduled Tasks

This page displays the cron configuration file, and lets you schedule cron jobs to run at a fixed time, date, or interval.

Each line in the cron configuration file represents a cron job. Enter each task on a separate line. Use the following format for the cron job entry:

```
* * * * * command to execute
- - - - -
| | | | •----day of the week (0-6) (Sunday=0)
| | | •------month (1-12)
| | •--------day of month (1-31)
| •----------hour (0-23)
•------------min (0-59)
```

To configure scheduled tasks:

1. Go to System > Scheduled Tasks.

   Note: *If the editor is empty, you must restart the cron service before creating a scheduled task. To restart the cron service, go to Services > Service Actions.*

2. Enter the cron task according to the syntax described above. *Table 8-9* lists available shortcuts.
3. Click **Save**.
4. Restart the cron service to apply the new cron job configuration.

Ensure that the commands specified in the cron job entries have the correct paths and permissions to execute successfully.

Table 8-9 Cron Shortcuts

Shortcut	Equivalent	Description
@reboot	(none)	At system startup
@yearly	0 0 1 1 *	Every year
@annually	0 0 1 1 *	Every year
@monthly	0 0 1 * *	Every month
@weekly	0 0 * * 0	Every week
@daily	0 0 * * *	Every day
@midnight	0 0 * * *	Every day
@hourly	0 * * * *	Every hour

LED Configuration

System > LED Configuration

The G520 series router provides 9 LEDs to indicate status and activity. Among these, there are 2 user-programmable LEDs. The other LEDs are not recommended to be modified. For a description of the default LED behaviors, see *LEDs.*

LED configuration should be done by experienced personnel. Use care when modifying the LEDs as incorrect configuration may cause consequences including but not limited to misleading status indications, loss of important system notifications, hardware or software malfunctions, and poor user experience.

Note: *When the user LED is configured for an alert (see Vehicle > Alerts), it must not be configured for any other applications. Do not configure the user LED if it is configured for an alert.*

To configure the user-programmable LED:

1. Go to System > LED Configuration.
2. Click **Add LED action** or click **Edit** next to the existing LED action that you want to modify.
3. Enter or modify the configuration settings. See *Table 8-10*.
4. Click **Save**.
5. Click **Save & Apply**.

Table 8-10 LED Configuration

Parameter	Description
Name	Displays the descriptive name of the LED.
LED Name	Displays the LED name by function.
Default state	Displays the default state of the LED before the trigger. Options are On or Off.
Trigger	Displays the trigger event that will toggle the LED state. For descriptions, see *Table 8-11*.

When configuring the LED, the trigger option determines which system events control the LED. Depending on the trigger, additional options must be specified. *Table 8-11* lists some trigger descriptions. The UI displays some triggers not listed in the table, but these are not recommended to be used.

Table 8-11 Trigger Descriptions

Trigger	Description	Examples
none	The LED is always in the default state. This is useful to declare an LED to be always ON.	LED always on: ◆ LED name: any LED ◆ Default: On ◆ Trigger: none

Trigger	Description	Examples
timer	The LED blinks with the configured On/ Off frequency. Options: ◆ On-state delay: time in milliseconds that the LED is On. ◆ Off-state delay: time in milliseconds that the LED is Off.	LED is 100ms On / 200ms Off: ◆ LED name: any LED ◆ Default: On ◆ Trigger: timer ◆ On-State Delay: 100 ◆ Off-State Delay: 200
defaulton	This trigger option is deprecated. Use trigger = none and default = On instead.	
heartbeat	The LED flashes to simulate actual heartbeat thump-thump-pause. The frequency is in direct proportion to 1-minute average CPU load.	LED blinks in heartbeat pattern: ◆ LED name: any LED ◆ Default: Off ◆ Trigger: heartbeat
netdev	Network Activity The LED flashes with link status and/or send and receive activity on the configured interface. Options: ◆ Device: name of the network interface whose status will be indicated ◆ Mode: link, transmit, receive. One or more can be selected	LED blinks when there is a link, transmit or receive activity on the configured network interface (WAN, WWAN, LAN, cellular). ◆ LED name: G520-wwanactivity, G520-lanactivity, G520-wanactivity, or G520-network ◆ Default: Off ◆ Trigger: netdev ◆ Device: select the configured interface (for example, “Ethernet adapter: eth1” for WAN) ◆ Mode: Link, Transmit, Receive
usbdev usbport	The LED turns on if a USB device is connected. It is recommended to use usbport rather than usbdev. Options for usbport: ◆ USB Port: select the configured USB port Options for usbdev: ◆ USB device: select the configured USP device	LED turns on if USB device is connected. ◆ LED name: ◆ Default: Off ◆ Trigger: usbport ◆ USP Port: Portusb1-port2

Backup / Flash Firmware

System > Backup / Flash Firmware

This page allows you to perform system operations such as backup and restore, reset, and flash firmware (system upgrade) to keep the device healthy.

The system operations are described in *Table 8-12*.

Table 8-12 Backup and Restore / Flash Firmware Operations

Parameters	Description
Backup/Restore	
Download Backup	Click **Generate archive** button to download an archive file of the current configuration files. Authentication - ◆ **Confirm user password -** enter the password of the logged in user. ◆ **Set Password** - enter a password to protect the backup archive.
Reset to defaults	Click **Perform Reset** button to reset the device to its initial configuration after flashing the firmware. This removes settings and user-installed software packages, which are stored on the overlayfs configuration partition. It works with any install with a squashfs / overlayfs setup. Authentication - ◆ **Confirm user password:** enter the password of the logged in user.
Restore backup	Click **Upload archive** button to upload a previously generated backup archive. Authentication - ◆ **Enter backup archive password** - Enter the password that was created to download the backup archive. The validity of the backup archive is checked and the files in the backup archive are listed. Review the list of files before you continue or cancel the restore operation.
Flash image	
Image	Click **Flash image** button to upload a sysupgrade compatible image for replacing the running firmware. *Warning:* ***Do not power off the device during the update.*** When the image file is uploaded, a file integrity check is done through the use of md5 algorithm. Verify the md5 value with the one given along with the firmware file. **Keep software packages, settings, and current configuration** - This is selected by default. To retain installed software packages (IPKs), settings, and current configuration, leave it selected. If you deselect it, the device configuration will be reset to factory setting after updating to the new firmware. *Warning:* ***Software packages are only restored from configured repositories. The device will automatically reboot when packages are restored.*** Authentication - ◆ **Confirm user password and continue** - Enter the password of the logged in user.

Backup and Restore

Download backups to keep the working configuration data. The backup consists of all policies and all other user related information.

Restore backups to restore configuration on the router or to configure a new router with the same settings.

To generate a backup archive:

1. Go to System > Backup/Flash Firmware > Actions.
2. Click the **Generate archive** to download a backup file.
3. At Confirm user password, enter the password of the logged in user. Click **Proceed**.
4. At Set Password, enter a password to protect the backup file. Click **Download**.
5. The backup archive is generated and downloaded to the local download folder.

To restore a backup archive:

1. Go to System > Backup/Flash Firmware > Actions.
2. Click **Upload archive** to restore a backup archive.
3. At Enter backup archive password, enter the password that was created to secure the backup archive. Click **Proceed**.
4. Select the backup archive file to upload. Click **Upload**.
5. The validity of the backup archive is checked and the files in the backup archive are listed. Review the list of files. Click **Continue** to proceed.

   The configuration is applied and the device reboots. If the restored configuration changes the current LAN IP address, you may need to reconnect manually.

Reset to Defaults

A factory reset erases all user-installed packages and settings and returns the device to its initial state after installing the firmware. The G520 series devices use a squashfs file system, as required for this feature.

To reset the firmware:

1. Go to System > Backup/Flash Firmware > Actions.
2. Click **Perform reset.**
3. At the Authentication prompt, enter the password of the logged in user. Click **Proceed.** The system erases the configuration partition and then reboots.
4. Access the device using the default configuration.

Factory Reset using Reset Button

The device has a physical reset button which can be used to reset the operating system to default settings without serial or SSH access. The recessed Reset button is located below the power input connector on the front panel of the device.

To reset the device using the reset button:

1. Using a paper clip or similar object to carefully poke through the RESET hole, press and hold the reset button for more than 5 seconds and less than 20 seconds.

2. Release the button. The device will do a factory reset and then reboot. This operation may take a few minutes to complete.
3. Connect to the device using the default configuration.

Note: *To reboot the device using the reset button, press and hold the reset button between 1 to 5 seconds.*

Firmware Upgrade

Flash firmware (system upgrade) optionally saves specified configuration files, wipes the entire file system, installs the new version, and then restores the saved configuration files. Any parts of the file system that are not specifically saved will be lost.

To retain the configuration, settings, and user-installed software packages, select “Keep software packages, settings, and current configuration” when you flash the firmware. For more details, see *Restoring IPKs after Firmware Upgrade on the Device*.

To do a firmware upgrade:

1. Go to System > Backup/Flash Firmware > Actions.
2. Click **Flash image**.
3. Select the file to upload and click **Upload**. The system confirms the upload and displays the flash image size and checksum. Verify the firmware image checksum.
4. **Keep software packages, settings, and current configuration** - This is selected by default. Leave it selected to retain installed software packages (IPKs), settings, and current configuration. If you deselect it, the device configuration will be reset to factory setting and user installed software packages will be removed after updating the firmware.
5. At the Authentication prompt, enter the user password.
6. Click **Continue** to proceed with flashing the image.
7. Do not power off the device while the upgrade is in progress. This may take a couple minutes. After the upgrade completes, the device will reboot. You may need to renew the IP address in your browser to reach the device again.

Restoring IPKs after Firmware Upgrade on the Device

To ensure that previously installed software packages and their configurations are retained when upgrading the firmware, follow the flash firmware procedure and make sure that “Keep software packages, settings, and current configuration” is selected.

The device will automatically reboot after packages are restored. To verify that the packages have been restored, go to System > Software > Installed to view the installed packages.

Note: *Software packages are only restored from configured repositories. Repositories can be configured from System > Software > Configuration. See* *Configure OPKG.*

Configuration

System > Backup / Flash Firmware > Configuration

Add files and directories that should be preserved during a system upgrade to the backup file list. Modified files in /etc/config/ directory and certain other configurations are automatically preserved.

To show the current backup file list, click **Open list...**

To modify the backup file list:

1. Go to System > Backup/Flash Firmware > Configuration.
2. In the editor, place the cursor below the last line.
3. Enter file path for each file or directory on a new line. The file path is relative to the top level directory.
4. Click **Save**.

Firmware and Configuration Upgrade from SD Card / USB Device

The external file system (SD card / USB storage device) can be used to upgrade the firmware and apply the configuration when the device boots. This option can be useful for initial setup of devices.

During the device boot, the firmware on the SD card or USB device will be applied only if the firmware in the external file system is newer than the current firmware in the device. If the firmware upgrade is successful, the system looks for a configuration file. If the configuration file is present, then the configuration will be applied. No version checks are done on the configuration file.

Note: *If the external file system has two firmware (.rom) files, the firmware upgrade will fail.*

Firmware File

Use a valid firmware image with .rom extension that is appropriate for the device model.

Use a released firmware image as provided (downloaded from the Lantronix Tech Support web stie) or an SDK built firmware image that adheres to the file name format below:

The file name format must be: ${devmodel}_<version>.rom

<version> format: a.b.c.dRx

a is major version number

b is minor version number

c is OEM version number (Example: 0) - to denote a version built specifically for OEM purposes

d is maintenance version number (Example: 0) - to denote a patch fix, no major or minor changes to firmware

Rx is (R) is release candidate and x is a number up to 4 digits indicating the revision number of the R build

Configuration File

The configuration file name format must be one of the following:

config-devicemodel-version.tar.gz

backup-devicemodel-version.tar.gz

The backup archive can be retrieved using the Generate Archive command on the System > Backup/Flash Firmware page. Note that the backup archive is password protected. If the backup archive is used, the password protection must be removed from the archive because there is no mechanism to supply or enter the password when upgrading from the SD card/USB device.

To upgrade the firmware and configuration file from the external file system:

1. Copy the firmware file (.rom) and configuration file (.tar.gz) onto the external file system (SD card / USB).
2. Connect the external file system to the G520 series device.
3. Reboot the device to upgrade the firmware and configuration files.
4. After upgrading the firmware and/or configuration, the device will reboot automatically to indicate that the installation is complete. Remove the SD card/USB from the device.

Custom Commands

System > Custom Commands

Write and execute custom shell commands from the web interface.

Write Custom Shell Command

This page lets you add or delete custom shell commands.

To write a custom shell command:

1. Go to System > Custom Commands > Configure.
2. Click **Add**.
3. Enter the command details. See *Table 8-13*.
4. Click **Save** or **Save & Apply**.

   The commands will be visible on the dashboard where you can run them.

Table 8-13 Custom Commands Configuration

Parameter	Description
Description	A short text description of the command.
Command	The command to execute on the shell terminal. To specify a file to be executed, the file must be copied to the /usr/sbin directory on the router. Files not in env PATH require the complete file path and should be executable.
Custom arguments	Check the box to allow user to provide additional command line arguments while running this command.
Public access	Check the box to allow the command to be executed and the output downloaded without prior authentication.

Run Custom Shell Command

Run custom shell commands. You also have the option to download the results of the command.

To run a custom command:

1. Go to System > Custom Commands > Dashboard.
2. Select the command to be run and click **Run.**

   The command, result, and return code are displayed in a box below the custom command.

Reboot

System > Reboot

Perform a reboot of the device. Any unsaved configuration will be lost when the device is rebooted.

To reboot the router:

1. Go to System > Reboot.
2. Click **Perform Reboot**.

The device restarts and reloads the configuration. After the device boots, the login page is displayed.

Schedule a Reboot

Schedule times when the router will reboot itself. You can set the frequency by time of day (hour and minute), day of week, and day of month.

To configure the reboot schedule:

1. Go to System > Reboot > Schedule Reboot.
2. Click **Add**.
3. Enter the schedule details (see *Table 8-14*). You may also enable the reboot schedule now or enable it later.
4. Click **Save**.
5. Click **Save & Apply**.

Table 8-14 Schedule Reboot Time Specification

Parameter	Description
Minute	Range: 0-59
Hour	Range: 0-23 0 = midnight
Day of week	Range: 0-6 0 = Sunday
Date	1-31
Month	Range: 1-12

9: VPN

This chapter describes how to establish a VPN connection for the following VPN protocols:

- *IPsec (Internet Protocol Security)*
- *OpenVPN*
- *WireGuard VPN*

Note: *The G520 series gateways support additional tunneling protocols. For L2TP, PPtP, or GRE protocol configuration, see Add Virtual Interface.*

IPsec (Internet Protocol Security)

VPN > IPsec

The IP Security (IPsec) suite of protocols are designed for cryptographically secure communication at the IP layer. The gateway uses standard IPsec protocol to protect traffic. The identity of communicating users is checked with the user authentication based on pre-shared keys (PSK) or X.509 certificates.

The IPsec connection can be started or stopped from the Web UI or by sending an SMS AT+VPN command. See *Table 10-23 SMS AT Command Syntax*.

You can configure up to 32 IPsec connections.

To configure an IPsec connection:

1. Go to VPN > IPsec, and click **Add new ipsec...**
2. Enter **Name** and select **Connection Mode** as Gateway to Gateway.
3. Click create **Create ipsec**, the configuration page displays.
4. Enter the VPN configuration details on the General Settings (*Table 9-1*) and Advanced Settings (*Table 9-2*) tabs.

Table 9-1 IPsec General Settings

Parameters	Description
Enable	Select to enable the IPsec.
Gateway type	Select the gateway type. ◆ Initiate - Acts as a VPN client, able to initiate a connection ◆ Respond only - Acts as a VPN server. Only responds to connection requests from clients
Connection type	Select connection type. Gateway to Gateway is the only option available.
IPsec Mode	Select IPsec mode. ◆ Tunnel ◆ Transport
Remote Gateway	Enter IP address of remote gateway.
Remote Subnet	Available when IPsec mode is Tunnel. Enter the subnet of remote gateway.

Parameters	Description
Route method	Select the route configuration method. ◆ Static – indicates that you will specify the interface to be used to establish the tunnel ◆ Auto – uses the interface that is active from the Load Balancer (MWAN) policies
Route interface	Available if Static is selected as Route method. Select the interface used to configure IPsec. ◆ Wan ◆ Wifi ◆ Cellular
Route policy	Available if Auto is selected as Route method. Select the MWAN policy to use. ◆ p1 ◆ p2
NAT traversal	Select to enable NAT over IPsec VPN for overlapping subnets.
NAT Subnet	Available if NAT traversal is enabled. Enter a virtual IP and subnet mask for overlapping subnets.
Left Subnet	Enter the gateway LAN IP and subnet mask.
Enable Router to Router Communication	Select to enable router to router communication.
Remote ID	Enter ID of the remote network as configured on the remote IPsec router server.
Local ID	Enter ID of the local router as configured on the remote IPsec router server. On the remote server, it may be displayed as “Remote ID”
Authentication method	Select the type of authentication to use for the VPN connection. ◆ Pre Shared Key ◆ X.509 Certificate ◆ X.509 Certificate (scep certificate)
Preshared-Key	Available if Pre shared Key is selected as Authentication method. Enter the key. The peer uses the key to authenticate each other from Internet Key Exchange.
Cert.	Available if X.509 Certificate is selected as Authentication method. The certificate file must be uploaded to the /etc/ipsec.d/certs directory. Click **Select file...** to browse the local drive and select the file. Click **Upload file...** to upload the file. After the file is uploaded, the Cert. field displays the file name and time stamp of the upload. To delete a file, click **Delete**.
Key	Available if X.509 Certificate is selected as Authentication method. The key file must be uploaded to the /etc/ipsec.d/private directory. Click **Select file...** to browse the local drive and select the file. Click **Upload file...** to upload the file. After the file is uploaded, the Key field displays the file name and time stamp of the upload. To delete a file, click **Delete**.

Parameters	Description
CA Cert.	Available if X.509 Certificate is selected as Authentication method. The CA certificate file must be uploaded to the /etc/ipsec.d/cacerts directory. Click **Select file...** to browse the local drive and select the file. Click **Upload file...** to upload the file. After the file is uploaded, the CA Cert. field displays the file name and time stamp of the upload. To delete a file, click **Delete**.
Key Type	Available if X.509 Certificate is selected as Authentication Method Select Key Type. ◆ RSA ◆ ECDSA
Certificate Name	Available if X.509 Certificate(scep certificate) is selected as Authentication method. Select certificate enrolled in Simple Certificate Enrollment Protocol (SCEP) client page.
Key type	Available if X.509 Certificate(scep certificate) is selected as Authentication method. Read only field. The value is obtained from the SCEP certificate selected.
Cert type	Available if X.509 Certificate(scep certificate) is selected as Authentication method. Select Cert type. ◆ PEM ◆ DER

Table 9-2 IPsec Advanced Settings

Parameters	Description
IKE Mode	Select the mode that Internet Key Exchange (IKE) protocol uses to authenticate and/or encrypt the peers. ◆ Main ◆ Aggressive
Key Exchange	Select the mode of encryption key exchange between two communicating peers: ◆ IKEV1 ◆ IKEV2 ◆ The default mode is IKEV1.

Parameters	Description
IKE Encryption	Select the cipher type to use for the Internet Key Exchange (IKE): ◆ Any ◆ AES ◆ AES-128 ◆ AES-192 ◆ AES-256 ◆ 3DES ◆ DES ◆ AES-128-GCM-64 ◆ AES-192-GCM-64 ◆ AES-256-GCM-64 ◆ AES-128-GCM-96 ◆ AES-192-GCM-96 ◆ AES-256-GCM-96 ◆ AES-128-GCM-128 ◆ AES-192-GCM-128 ◆ AES-256-GCM-128 The default cipher type is “Any”.
IKE Hash	The IKE hash is used for authentication of packets for the key exchange. Select the IKE Hash type to use for VPN connection: ◆ MD5 ◆ SHA1 ◆ SHA2 256 ◆ SHA2 384 ◆ SHA2 512 The default IKE hash type is “MD5”.
DH Group	Select the desired Diffie-Hellman group to use: ◆ ◆ Group1(768) ◆ Group2(1024) ◆ Group5(1536) ◆ Group14(2048) ◆ Group15(3072) ◆ Group16(4096) ◆ Group19(ecp256) ◆ Group20(ecp284) ◆ Group19(ecp256) ◆ Group20(ecp284) Higher-numbered groups are more secure but also require longer to generate the key. The default group is “Group1(768)”.

Parameters	Description
IPsec Encryption	Select the type of IPsec encryption for VPN connection: ◆ Any ◆ AES ◆ AES-128 ◆ AES-192 ◆ AES-256 ◆ 3DES ◆ DES ◆ AES-128-GCM-64 ◆ AES-192-GCM-64 ◆ AES-256-GCM-64 ◆ AES-128-GCM-96 ◆ AES-192-GCM-96 ◆ AES-256-GCM-96 ◆ AES-128-GCM-128 ◆ AES-192-GCM-128 ◆ AES-256-GCM-128 The default cipher type is “Any”.
IPsec Hash	The IPsec hash is used for authentication of packets for the key exchange. Select the IPsec Hash type to use for VPN connection: ◆ ◆ MD5 ◆ SHA1 ◆ SHA2 256 ◆ SHA2 384 ◆ SHA2 512 The default hash type is “MD5”.
DH Group	Select the desired Diffie-Hellman group to use: ◆ Any ◆ Group1(768) ◆ Group2(1024) ◆ Group5(1536) ◆ Group14(2048) ◆ Group15(3072) ◆ Group16(4096) ◆ Group19(ecp256) ◆ Group20(ecp384) Higher-numbered groups are more secure but also require longer to generate the key. The default group is “Any”.
DPD Keep Alive Time	Enter the time in seconds for interval between Dead Peer Detection keep alive messages.
DPD Timeout	Enter the time in seconds of no response from peer before Dead Peer Detection times out.
IKE Re-key Time	Enter the time in seconds between changes of the encryption key. To disable changing the key, set it to 0.
SA Life Time	Enter the time in seconds for the security association lifetime.

Parameters	Description
DPD Action	Select the desired Dead Peer Detection action. This action must be taken when a dead IKE peer is detected. ◆ None ◆ Clear ◆ Hold ◆ Restart
Single hop IP for watchdog	Enter the IP address to be used for monitoring purposes. The application will ping the IP defined here. If the ping fails, it will restart the device. This could be the LAN IP address of the IPsec router server.
Monitor interface ping failure	Select Yes to ping the IP address defined in Single hop IP for watchdog. Select No if you don't want the monitor interface to ping the single hop IP address. The default is No.
Force encaps	Enabled by defaut.It ensures host to host communication.
Strict cipher	Select to enable strict cipher. When selected, both peers should match ciphers.

5. Click **Save**. The instance is saved and displayed on the IPsec page.
6. After configuring the profile, click **Connect** to start the IPsec connection for the first time.

OpenVPN

VPN > OpenVPN

OpenVPN is an open-source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections. It uses the OpenSSL library to provide encryption of both the data and control channels. OpenVPN can run over UDP or TCP transports, multiplexing created SSL tunnels on a single TCP/UDP port.

OpenVPN fully supports IPv6 as the protocol of the virtual network inside a tunnel and the OpenVPN applications can also establish connections via IPv6. It has the ability to work through most proxy servers (including HTTP) and is good at working through network address translation (NAT) and getting out through firewalls. The server configuration has the ability to push certain network configuration options to the clients, including IP addresses, routing commands, and a few connection options.

The G520 series gateways support OpenVPN client, server, and pass through.

OpenVPN Instances

The OpenVPN client will attach itself to the configured OpenVPN server over any available WAN, LAN, or Cellular network interface. If the auto-connect function is enabled, OpenVPN will connect over available WAN, switch between WAN connections when one WAN fails-over to another, and also auto start on every reboot.

To create an OpenVPN instance:

1. Go to VPN > OpenVPN. The top of the page displays the status of OpenVPN profiles. The lower portion of the page displays the configured OpenVPN instances and their current state.
2. Under OpenVPN instances, select the method for the instance configuration:
   - **Template based configuration** – Select the instance name and the template (server or client templates are provided). Click **Add**.
   - **OVPN configuration file upload** – Select the instance name and then choose the OVPN configuration file. Click **Upload**.
3. The instance is added to the list under OpenVPN instances.
4. Choose from the following options:
   - To continue configuring the instance, click **Edit**. See *Template-based Configuration* or *OpenVPN Configuration File* for details respective to the configuration method.
   - To enable the instance, select **Enabled**.
5. Click **Save & Apply**.

Note: *You must manually enter the DNS from Network > DHCP and DNS.*

Template-based Configuration

Predefined templates

Use the following predefined server and client templates to create the initial configuration of the OpenVPN instance:

- Client configuration for an ethernet bridge VPN
- Client configuration for a routed multi-client VPN
- Simple client configuration for a routed point-to-point VPN
- Server configuration for an ethernet bridge VPN
- Server configuration for a routed multi-client VPN
- Simple server configuration for a routed point-to-point VPN

Note: *This document does not cover OpenVPN client/server configuration. Please consult your administrator for configuration details of your VPN or refer to the* OpenVPN online documentation *for information on how to configure the VPN.*

Edit the template-based configuration

After you add the template-based instance, you can edit the instance to configure the appropriate fields and values for the particular VPN connection.

Note the following about editing the template-based instances:

- Click the **Switch to advanced configuration** or **Switch to basic configuration** links at the top of the form to switch the view between basic and advanced configuration.
- Select **Additional Field** at the bottom of the form to select additional configuration fields to add to the form.
- Select **Client** to enable client mode, or leave it blank to enable server mode.
- You should add your CA, certificates, and keys for the instance.
- Click **Save & Apply** when you are finished.

OpenVPN Configuration File

If you use an OVPN configuration file to configure the OpenVPN instance, the configuration file should contain settings for either a server configuration or a client configuration with **.ovpn** as the file extension.

Note: *This document does not cover how to create OpenVPN configuration files. Please refer to the* OpenVPN online documentation *for sample server and client configuration files and information on how to create configuration files.*

Edit the OVPN Configuration File

After you upload the configuration file, you can use the OpenVPN configuration editor on the web interface to modify the configuration. The editor window contains two sections: one to modify the OVPN configuration file and one to add a user and password authentication file with your credentials.

Click **Save** to save changes to the configuration file and close the editor.

WireGuard VPN

The WireGuard® VPN feature is available as a sofware package (IPK), and is not part of the standard firmware. Install it using the software package manager.

WireGuard is an open source software VPN protocol that can be deployed for many different circumstances. It's intended to be fast, secure, and easy to deploy. WireGuard securely encapsulates IP packets over UDP. WireGuard relies on public key cryptography. It requires generating a private and public key for each peer and exchanging only the public keys. WireGuard is time sensitive and can refuse to pass traffic if the peer's clock is out of sync. It's recommended to rely on NTP for all peers.

Refer to the following procedures to establish a VPN connection using WireGuard VPN protocol. On successful connection, the devices in the selected firewall zone can communicate with peer devices using their WireGuard interface IP addresses.

Install WireGuard IPKs to the Device

Install the WireGuard VPN software packages (IPKs) using the software package manager.

To install the WireGuard VPN feature:

1. Go to System > Software.
2. Click **Update lists** to refresh the list of packages.
3. In the Filter field, type "wireguard". The WireGuard packages are listed under Available packages. The package names are as follows:
   - luci-app-wireguard
   - luci-proto-wireguard
   - wireguard-tools
   - kmod-wireguard
4. Select "luci-app-wireguard" from the list and click **Install**.
5. The package manager displays the package details. Review the package details and ensure that the device has adequate available memory to install the packages. Note that the other 3 WireGuard packages are listed under Dependencies as "not installed". The package manager will install all 4 packages.
6. Leave "Overwrite files from other package(s)" unchecked and click **Install**.
7. The package manager executes and displays the installation progress and results. Click **Dismiss** when finished.
8. Restart the device.

Generate Private and Public Keys for WireGuard

Generate a pair of private and public keys for the WireGuard server.

To generate the private and public keys, SSH to the device and execute the commands:

```
root@Lantronix-<hostname>:~# umask go=
root@Lantronix-<hostname>:~# wg genkey | tee wgprivate | wg pubkey >
wgpublic
root@Lantronix-<host-name>:~# cat wgprivate
<output of wgprivate key>
root@Lantronix-<host-name>:~# cat wgpublic
```

```
<output of wgpublic key>
```

Use the **wgprivate** key file to configure the WireGuard interface on this device.

Use the **wgpublic** key file to configure peers that will connect to this device through the WireGuard VPN.

Create the WireGuard VPN Interface

For details about configuring the WireGuard VPN protocol of the virtual interface, see Table 12-9, “VPN Tunnel Protocols,” on page 189.

To create the WireGuard VPN interface:

1. Go to Network > Interfaces. Click **Add new interface**.
2. Enter the following information on the General Settings tab:
   - Name: “wg0”
   - Protocol: select WireGuard VPN, then click **Create interface**.
   - Private key: <private key of the device> (enter the value of wgprivate)
   - Listen Port: 51820
   - IP Addresses: WireGuard interface IP addresses. (for example: 192.168.9.1/24)
3. Click the Firewall Settings tab. Enter the following information:
   - Create/Assign Firewall zone: Select the “lan” zone to allow peer devices to communicate with lan zone devices.
4. Click the Peers tab and click **Add Peer**. Enter the following information. (Repeat this step to add multiple peers):
   - Description: type “peer_1” (or a name you choose)
   - Public key: enter the public key of the peer device/host
   - Allowed IPs: “0.0.0.0/0”, “::/0”
   - Endpoint Host: IP address of the peer device/host (for example: 192.168.9.2/24)
   - Endpoint Port: 51820
   - Persistent Keep Alive: 25
5. To save the configuration, click **Save** and then click **Save & Apply**.

Configure a Firewall Rule to Allow WireGuard Traffic

The rule will allow access to the VPN server from the WAN zone.

To configure the firewall rule:

1. Go to Network > Firewall > Traffic Rules. Click **Add**.
2. Enter a name such as “allow_wireguard”.
3. Configure the rule to **accept** UDP traffic from any source address/port in the wan zone to UDP port 51820 (any destination address) in the lan zone.
   - Protocol: UDP
   - Source zone: wan
   - Source Address: any

- Source Port: any
- Destination zone: lan wg0
- Destination Address: any
- Destination Port: 51820
- Action: accept

4. To save the configuration, click **Save** and then click **Save & Apply**.

Monitor Status

To view information about the WireGuard VPN:

1. Go to Status > WireGuard Status.
2. View the client's information and connectivity status.

Create a WireGuard Interface on the Peer Device

Create a WireGuard interface on the peer device by providing the public key (wgpublic) created in *Generate Private and Public Keys for WireGuard* and the device's WAN IP address.

Ensure that the WireGuard interface IP address of the device and the WireGuard interface IP addresses of the peer devices are in the same subnet. (For example, IP of device is 192.168.9.1/24 and IP of peer device is 192.168.9.2/24.)

Repeat this step for all peers that were added in *Create the WireGuard VPN Interface*.

10: Services

The G520 series gateways are equipped with services that complement the routing features. These services include:

- *CAN Bus*
- *DOTA*
- *Dynamic DNS*
- *Events*
- *External Filesystems*
- *GPS*
- *Keepalived*
- *Last Gasp*
- *Logs Information*
- *Reporting Agent*
- *Reporting Agent*
- *SCEP Client*
- *Service Actions*
- *SMS*
- *SNMPD*
- *SNMPTRAPD*
- *uHTTPd*
- *Versatile IOs*

CAN Bus

Services > CAN Bus

CAN bus provides a reliable and efficient means of communication between electronic devices within a network. CAN bus allows multiple devices, such as sensors, actuators, and controllers, to communicate with each other over a shared bus. This feature is available only on G526RP (Transport Pack) models.

CAN Bus supports the following CAN protocols:

- CAN Standard
- OBDII - Current Data
- OBDII - Diagnostics
- CANOpen - Gateway

Note: *Only one protocol can be active at a time.*

Global Settings

To configure the global settings:

1. Go to Services > CAN Bus. The Global Settings page is displayed.
2. Configure the settings. See *Table 10-1*.
3. Click **Save & Apply**.

Table 10-1 CAN Bus Global Settings

Field	Description
Status	Displays the status as Enabled (Running) or Disabled (Not Running).

Field	Description
Enable	Select the check box to enable CAN Bus or clear it to disable.
Speed	Select the speed. This must match the baud rate of the configured device. The options are (in Kbps): 100, 125, 200, 250, 400, 500, 666, 800, 1000.
Protocol	Select the protocol. ◆ CAN Standard ◆ OBDII - Current Data ◆ OBDII - Diagnostics ◆ CANOpen - Gateway

CAN Standard

CAN Standard supports up to 10 configuration slots. The CAN Standard protocol subscribes to a particular identifier, which is saved in the slot. The data length can be single bit (Digital 0 or 1) or multiple bits (up to 4 bytes, or 32 bits). Whenever there is a broadcast message on the bus, an alert / event is triggered with:

- an event message with <Normal Message> if values fall under normal range
- alert messages with <Alert Message> if values go out of normal range

The CAN Standard overview page displays the configuration slots; of note it includes whether the status is Enabled or Disabled, the CAN ID, and the Current Value. For descriptions of the remaining fields, see *Table 10-2*.

To configure a CAN Standard configuration slot:

1. Go to Services > CAN Bus. The global settings are displayed. Make sure that CAN Standard is selected as the protocol.
2. Click the CAN Standard tab.
3. Enter a name for the slot and click **Add**. The name can contain up to 64 characters (A-Z, a-z, 0-9, underscore- (_), no spaces or special characters). The new slot is displayed in the list.
4. Configure the slot you just created. Alternatively, to configure an existing slot, select the slot and click **Edit**. See *Table 10-2*.
5. Click **Save & Apply**.

Table 10-2 CAN Standard Configuration

Field	Description
Enabled	Select to enable the configuration slot. Clear the box to disable the configuration slot.
CAN Identifier	Enter the unique CAN identifier value in hexadecimal value format. For example: 0x12. The CAN identifier establishes the priority of the message. Lower values have higher priority. The identifier type can be “standard” 11-bit or “extended” 29-bit.

Field	Description
Start byte / Stop byte	The start and stop byte and start and stop bits are used to identify the length of the data message in the data frame. The configured data can be up to 32 bits, or 4 bytes. To configure, select the start byte and the stop byte. For example: For the maximum 32 bits, enter 0 as the start byte and 3 as the stop byte.
Start bit / Stop bit	The start and stop byte and start and stop bits are used to identify the length of the data message in the data frame. The configured data can be up to 32 bits, or 4 bytes. To configure, select the start bit and stop bit, from 0 to 7.
Byte Order	Select the byte order of the data. ◆ LSB - for little-endian ordering. The least significant byte is placed first. ◆ MSB - for big-endian ordering. The most significant byte is placed first.
Minimum Value	The minimum and maximum values are used to define the range to compare against the data broadcast on the bus. ◆ If the data falls outside the range of the minimum and maximum values, alert messages are generated. ◆ If the data falls inside the range of the minimum and maximum values, a normal message is generated. Enter the minimum value to set the bottom of the normal range.
Maximum Value	Enter the maximum value to set the top of the normal range.
Alert	Select the configured alert. For details on how to create an alert, see *Alerts* ***Note:*** *Alerts can be enabled or disabled on the Alerts page.*
Normal Message	Enter the notification message to be displayed when the received data is inside the range of the minimum and maximum values. The message may contain up to 64 characters and may include the following directives: %d System hostname %c Current value
Normal Reminder Interval (in minutes)	Enter the time to wait before sending the normal message again. The valid range is between 1 and 1440 minutes. A zero value means that the reminder message will be sent only once.
Alarm Message	Enter the notification message to be displayed when the received data is outside the range of the minimum and maximum values. The message may contain up to 64 characters and may include the following directives: %d System hostname %c Current value
Alarm Reminder Interval (in minutes)	Enter the time to wait before sending the alarm message again. The valid range is between 1 and 1440 minutes. A zero value means that the reminder message will be sent only once.

OBDII - Current Data

OBDII is used for continuous polling data for the Parameter IDs (PID). The Bus will be in Read/Write mode so the PID value is written as a request and read from response. Monitoring happens in polling mode every 5 seconds. A Custom PID section is also available to make it possible to access the byte based on the need.

The device polls the data and sends either an alert or an event message based on the data.

- an event message with <Normal Message> if values fall under normal range
- alert messages with <Alert Message> if values go out of normal range

The OBDII - Current Data overview page displays the status, current value, and configuration of the configuration slots. For descriptions of the configuration settings, see *Table 10-3*.

To configure an OBDII - Current Data configuration slot:

1. Go to Services > CAN Bus. The global settings are displayed. Make sure that OBDII - Current Data is selected as the protocol.
2. Click the OBDII - Current Data tab.
3. Enter a name for the slot and click **Add**. The name can contain up to 64 characters (A-Z, a-z, 0-9, underscore- (_), no spaces or special characters). The new slot is displayed in the list.
4. Configure the slot you just created. Alternatively, to configure an existing slot, select the slot and click **Edit**. See *Table 10-3*.
5. Click **Save & Apply**.

Table 10-3 OBDII- Current Data Configuration

Field	Description
Enabled	Select to enable the configuration slot. Clear the box to disable the configuration slot.
CAN Identifier	Enter the unique CAN identifier value in hexadecimal value format. For example: 0x12. The CAN identifier establishes the priority of the message. Lower values have higher priority. The identifier type can be “standard” 11-bit or “extended” 29-bit.
Is PID custom	If using a custom Parameter ID (PID), select this box and then enter the following information: ◆ CAN PID ◆ Return bytes (optional) ◆ Byte number ◆ Is Single Bit - check box. If selected, enter the Bit Number.

Field	Description
PID	Select the Parameter ID (PID) from the list of options. The following PIDs are available: ◆ Calculated Engine load(0x04) ◆ Engine Coolant Temperature(0x05) ◆ Short term Fuel Trim- Bank 1(0x06) ◆ Long term Fuel Trim- Bank 1(0x07) ◆ Short term Fuel Trim- Bank 2(0x08) ◆ Long term Fuel Trim- Bank 2(0x09) ◆ Fuel pressure(0x0A) ◆ Intake Manifold Absolute Pressure(0x0B) ◆ Engine RPM(0x0C) ◆ Vehicle Speed(0x0D) ◆ Timing Advance(0x0E) ◆ Intake Air Temperature(0x0F) ◆ Air flow rate(0x10) ◆ Throttle Position(0x11) ◆ Commanded secondary air status(0x12) ◆ Runtime equivalence ratio(0x44) ◆ Engine fuel rate(0x5E)
Minimum Value	The minimum and maximum values are used to define the range to compare against the data broadcast on the bus. ◆ If the data falls outside the range of the minimum and maximum values, alert messages are generated. ◆ If the data falls inside the range of the minimum and maximum values, a normal message is generated. Enter the minimum value to set the bottom of the normal range.
Maximum Value	Enter the maximum value to set the top of the normal range.
Alert	Select the configured alert. For details on how to create an alert, see *Alerts*. ***Note:*** *Alerts can be enabled or disabled on the Alerts page.*
Normal Message	Enter the notification message to be displayed when the received data is inside the range of the minimum and maximum values. The message may contain up to 64 characters and may include the following directives: %d System hostname %c Current value
Normal Reminder Interval (in minutes)	Enter the time to wait before sending the normal message again. The valid range is between 1 and 1440 minutes. A zero value means that the reminder message will be sent only once.
Alarm Message	Enter the notification message to be displayed when the received data is outside the range of the minimum and maximum values. The message may contain up to 64 characters and may include the following directives: %d System hostname %c Current value
Alarm Reminder Interval (in minutes)	Enter the time to wait before sending the alarm message again. The valid range is between 1 and 1440 minutes. A zero value means that the reminder message will be sent only once.

OBDII - Diagnostics

The OBDII - Diagnostics page provides the following diagnostic checks:

- **Check PID** tests whether a specified PID is supported or not by the end device.
- **Diagnostic Trouble code (DTC)** test displays the vehicle fault code.

To run OBDII - Diagnostics commands:

1. Go to Services > CAN Bus. The global settings are displayed. Make sure that OBDII - Diagnostics is selected as the protocol.
2. Click the OBDII - Diagnostics tab.
3. To check PID support, enter the PID and click **Check PID**.
4. To view diagnostic trouble code, click **Test** under Diagnostic Trouble Code (DTC).
5. The results for the selected test are displayed on the page.

CANOpen - Gateway

CANopen is a CAN-based communication system, standardized by CAN in Automation (CiA®). CANopen is specified by CiA 301 (or by EN 50325-4) standard. For more information, see https://www.can-cia.org/canopen/.

The CANOpen - Gateway Status indicates whether the CANopen gateway is running on the configured device.

To configure the CANopen gateway:

1. Go to Services > CAN Bus. The global settings are displayed.
2. On the Global Settings page, verify that CANOpen - Gateway is selected as the protocol, otherwise select it and click **Save & Apply**.
3. From the Services > CAN Bus page, click the CANOpen - Gateway tab.
4. Configure the CANopen gateway parameters. See *Table 10-4*.
5. Click **Save & Apply**.

Table 10-4 CANOpen Gateway Configuration

Field	Description
Enable	Enable or disable the CANopen interface
Node ID	The Node ID of the configured device. Node ID valid range is a digit between 1 and 127.
SDO Timeout (in milliseconds)	Wait time for the Service Data Object (SDO) request of the configured Node ID. This field sets the timeout abort error used by the gateway's SDO client. Valid range is 500 to 10000.
Enable Block Transfer	Select to enable block transfer of the CANopen gateway device.

CANOpen - Commands

The CANOpen - Commands page supports uploading and downloading SDO commands based on the standard and performing operational commands on a specified node in the gateway.

CANopen Command Syntax

[[net] node] <command> <parameter>

Parameter	Description
net	Specifies the CANopen network for the command
node	Specifies the CANopen node for the command
<command>	CANopen gateway command
<parameter>	One or more parameters of the command

Upload SDO

Function	Read SDO data from CANopen device
Syntax	[[net] node] r[ead] <multiplexor> <datatype>
Parameter	<multiplexor>: <index> <subindex> <datatype>: b|i8|i16|i32|u8|u16|u32|r32|vs|os|us|t|td|d|i24|r64|i40|i48|i56|i64|u24|u40|u48|u56|u64
Example	4 r 0x1017 0 u16

Download SDO

Function	Write SDO data to CANopen device
Syntax	[[net] node] w[rite] <multiplexor> <datatype> <data>
Parameter	<multiplexor>: <index> <subindex> <datatype>: b|i8|i16|i32|u8|u16|u32|r32|vs|os|us|t|td|d|i24|r64|i40|i48|i56|i64|u24|u40|u48|u56|u64
Example	4 w 0x1017 0 u16 1000

To upload or download SDO data:

1. Go to Services > CAN Bus. The global settings are displayed.
2. On the Global Settings page, verify that CANOpen - Gateway is selected as the protocol, otherwise select it and click **Save & Apply**.
3. From the Services > CAN Bus page, click the CANOpen - Commands tab.
4. Enter the Upload SDO or Download SDO command and click **Execute**.
5. The result appears in the Command Section at the top of the page.

Command specified node in the Gateway

Sends a specified CANopen command to the specified node in the gateway.

To send the CANopen command:

1. Go to Services > CAN Bus. The global settings are displayed.
2. On the Global Settings page, verify that CANOpen - Gateway is selected as the protocol,

otherwise select it and click **Save & Apply**.

3. From the Services > CAN Bus page, click the CANOpen - Commands tab.
4. Enter the Node ID and then click the desired action.

Command	Description
Start	Start the specified CANopen node
Stop	Stop the specified CANopen node
Reset node	Reset the specified CANopen node
Pre-OP	Set the specified CANopen node to pre-operational mode
Reset Communication	Reset communication of the specified CANopen node

5. The result appears in the Command Section at the top of the page.

DOTA

DOTA (download over the air) allows you to remotely update the gateway's firmware using the Lantronix server or your custom server.

Lantronix Server

Services > Dota > Lantronix Server

This page allows you to update the gateway's firmware using the Lantronix DOTA server.

To upgrade the firmware:

1. Go to Services > DOTA > Lantronix Server.
2. Select the channel and click **Check for update** to find available updates. See *Table 10-5*.

   The results of the update check are displayed in the area below the action bar. If an update is available, the firmware file is displayed under Available Firmwares.
3. To update the device, select the firmware file under Available Firmwares and click **Update now**.

   Do not power off the device during the update. After the firmware is updated, the device will reboot.

Table 10-5 DOTA using Lantronix Server

Parameters	Description
Channel	Select the channel on which to look for the firmware update files. The options are Development, Beta, and Released. The default channel option is Released.
Check for update	Click to check for available updates.
Available Firmware	Displays a list of firmware that is available on the server. Select the firmware from this list and click **Update now** to upgrade or downgrade the firmware.
Force Upgrade	Check this box for forceful upgrade or downgrade of the firmware version.

Parameters	Description
Update now	Click **Update now** to download the firmware selected in the Available Firmware list.

Custom Server

Services > Dota > Custom Server

This page allows you to update the gateway's firmware using a custom DOTA server.

To update firmware using a custom server:

1. Go to Services > DOTA > Custom Server.
2. Enter the server details. See *Table 10-6*.
3. Click **Update now**.

Table 10-6 DOTA Custom Server Configuration

Parameters	Description
Update now	After setting the Custom Server parameters, click **Update now** to download the firmware pointed to by the URL and the filename below.
Custom Server Settings	
Note: If the custom server is not configured, DOTA service will configure the Lantronix server.	
Protocol	Select HTTP or HTTPS as the protocol of the custom server. Enter the configuration depending on the protocol you selected.
URL/IP	Enter the URL or the IP address of the custom DOTA server. The URL, if provided, must include http or https.
Filename	Enter the firmware file name to be accessed for the update.
Username	This field is displayed if the selected protocol was HTTP. Enter the server login username.
Password	This field is displayed if the selected protocol was HTTP. Enter the server login password.
Cert-type	This field is displayed if the selected protocol was HTTPS. Choose the type of certificate file. The options are PEM, DER, or ENG.
Cert	This field is displayed if the selected protocol was HTTPS. Click the **Select file...** button to browse to the SSL certificate file to be uploaded.
Key	This field is displayed if the selected protocol was HTTPS. Click the **Select file...** button to browse to the key file to be uploaded.
Timeout in Minutes	Enter the period of time to wait for the download to complete. The download process will be aborted after the timeout period expires. The default value is 10 minutes.
Retries	Enter the number of retry attempts allowed to check and download the latest firmware file from the server. The default number of retries is 3.

Note: *DOTA update can also be triggered using SMS by sending the SMS AT+DOTA command after setting the custom server configuration from the Web UI (shown above) or*

by sending the AT+DOTASETTINGS command using SMS from a registered mobile number. For command syntax, see Table 10-23 SMS AT Command Syntax.

Dynamic DNS

Services > Dynamic DNS

Dynamic Domain Name System (Dynamic DNS or DDNS) offers a method of keeping a static domain/host name linked to a dynamically assigned public IP address allowing your server to be more easily accessible from various locations on the Internet.

The DDNS page lets you configure your DDNS service so that the gateway automatically updates its public IP to your DDNS provider. Before starting this configuration, you should already have registered a DNS name with a compatible DDNS service provider. For a list of compatible DDNS providers, visit: https://openwrt.org/docs/guide-user/services/ddns/client.

To add a DDNS configuration:

1. Go to Services > Dynamic DNS.
2. At the bottom of the Overview section, type the DDNS configuration name and click **Add**.

To edit a DDNS configuration:

1. Go to Services > Dynamic DNS.
2. In the Overview section, select the DDNS configuration that you want to edit and click **Edit**.
3. Edit the configuration settings. See *Table 10-7*.
4. Click **Save & Apply**.

Table 10-7 Dynamic DNS Client Configuration

Parameters	Description
Basic Settings	
Enabled	Select to enable Dynamic DNS. Clear to disable Dynamic DNS. Dynamic DNS allows the gateway to be reached with a fixed hostname while having a dynamically changing IP Address.
Lookup Hostname	Name to identify the host that you want to use on DDNS server. This is the domain name that you registered with your DDNS service provider. The hostname is received from the dynamic DNS service provider.
IP address version	Select the IP address version – IPv4 or IPv6.
DDNS Service Provider [IPv4/ IPv6]	Select the DDNS service provider from the drop down list.
Domain	The domain that you want to update. Usually the same as the lookup hostname.
Username	Username of DDNS account. The username is received from the DDNS service provider.

Parameters	Description
Password	Password of DDNS account. The password is received from DDNS service provider.
Use HTTP Secure	Select to use HTTPS with the DDNS provider. Otherwise, leave it unchecked.
Path to CA-certificate	This field is visible if HTTPS is selected. Enter the directory or file path of the ssl certs. To run HTTPS without verification of server certificates (insecure), enter IGNORE.
Advanced Settings	
IP address source [IPv4/IPv6]	Select the IP Address source: Network, Interface, URL, or Script and enter the appropriate configuration details. Network ◆ Network (IPv4) – Select the software interface to read systems IPv4 address from. Interface ◆ Interface – Select the physical network interface from the options URL ◆ URL to detect – Enter the URL to read systems IP address from. The source IP Address by default is URL. ◆ Event Network (IPv4) – network on which the ddns-updater scripts will be run ◆ Bind Network – leave as “default” or select the network to use for communication. Note that casual users should not change this setting. Script ◆ Script – Enter the script path and file name. ◆ Event Network (IPv4) – network on which the ddns-updater scripts will be run
Force IP Version	Select if you want to force the usage of either IPv4 or IPv6 only. This field is optional.
DNS-Server	Enter DNS server domain name or IP address if you want to override the default DNS server to detect the registered IP. Enter IP address or FQDN.
PROXY-Server	Enter the proxy server to use for detection and updates. Format: [user:password@]proxyhost:port IPv6 address must be given in square brackets: [2001:db8::1]:8080
Log to syslog	Select log level to write log messages to syslog. Critical errors are always logged to syslog. Available options include No logging, Info, Notice, Warning, Error. The default setting is Notice.
Log to file	Select to allow the detailed messages to be written to log files. Log files store up to 250 lines and then are automatically truncated.
Timer Settings	
Check Interval	Specify the time interval to check if the local IP has changed. Values less than 5 minutes (300 seconds) are not supported. Default is 10 minutes.

Parameters	Description
Force Interval	Specify the time interval after which the DDNS server should force update the IP address of your server even if no IP change was detected. The force interval should be greater than the check interval. Enter 0 to force the script to only run once. Default is 72 hours.
Error Retry Counter	The number of retries to attempt before the script stops execution. Default setting is 0 which indicates infinite retries.
Error Retry Interval	If an error occurs on detecting, sending or updating, the script will retry the relevant action according to the specified time interval. Default is 60 seconds.
Log File Viewer	
Read/Reread log file	Click to display the DDNS log file.

Events

Services > Events

The Event Management page allows you to map actions to events respective to the digital and versatile I/Os, and network interfaces.

G520 series gateways are equipped with two digital inputs/outputs (I/O). Digital inputs range from 3V to 24V and the same input pins are also available to be used as open collector digital output with maximum 200mA @ 24V.

To add an event:

1. Go to Services > Events.
2. In the Event Management page, select **Enable**.
3. In the Events section, click **Add**.
4. Enter the event parameters (see *Table 10-8*) and click **Save**.
5. Click **Save & Apply** to finish. The new event displays in the Events section.

Table 10-8 Events Configuration

Parameters	Description
Event	Select the event from the options. DIO by default are pulled up to high voltage level. ◆ Digital Input # 1 has voltage ◆ Digital Input # 1 is grounded ◆ Digital Input # 2 has voltage ◆ Digital Input # 2 is grounded ◆ Versatile Analog Input # 1 has voltage greater than or equal to <Threshold Voltage> ◆ Versatile Analog Input # 1 has voltage less than or equal to <Threshold Voltage> ◆ Versatile Analog Input # 2 has voltage greater than or equal to <Threshold Voltage> ◆ Versatile Analog Input # 2 has voltage less than or equal to <Threshold Voltage> ◆ WAN Down <Delay in seconds> ◆ WWAN Down <Delay in seconds> ◆ Cellular Down <Delay in seconds> ◆ WAN UP <Delay in seconds> ◆ WWAN UP <Delay in seconds> ◆ Cellular UP <Delay in seconds>
Action	Select the action from the options. The actions available are based on the event that you have selected. ◆ Close digital Output # 1 - to close the digital pin ◆ Open digital Output # 1 - to open the digital pin ◆ Close digital Output # 2 - to close the digital pin ◆ Open digital Output # 2 - to open the digital pin ◆ Close Versatile Digital Output # 1 - to close the versatile pin ◆ Open Versatile Digital Output # 1 - to open the versatile pin ◆ Close Versatile Digital Output # 2 - to close the versatile pin ◆ Open Versatile Digital Output # 2 - to open the versatile pin ◆ Start VPN – to start VPN ◆ Stop VPN – to stop VPN ◆ SMS – to send the event details using the SMS ◆ Reboot – to reboot the gateway. Use this option with caution. It may cause continuous reboot if the DI events are not properly configured. ◆ POWER_SAVEMODE_ON - to enable power save mode ◆ POWER_SAVEMODE_OFF - to disable power save mode
Mobile Number/Text	If SMS is selected as Action, enter: ◆ Mobile Number - The mobile number format is <countrycode><phonenumber> ◆ Text - Enter the text message to be sent to the configured mobile number in case the event occurs.
VPN Type/ VPN Name	If start VPN or Stop VPN is selected as Action, enter: ◆ VPN Type - enter the type of the VPN such as L2TP, PPTP, IPSEC, OPENVPN, and GRE. ◆ VPN Name - enter the VPN instance name for the type of VPN selected.

External Filesystems

Services > External Filesystems

The G520 series gateway supports an SD(HC)/MMC card or external USB flash drive for external file storage. This page configures the mount settings for the external filesystem.

To configure the external filesystem:

1. Insert the SD card in the SD card slot or the USB flash drive in the USB slot on the gateway.
2. Go to Services > External Filesystems.
3. Configure the external device settings. See *Table 10-9*.
4. Click **Save & Apply**.

Table 10-9 External Filesystems Configuration

Parameters	Description
External device	Select the external device.
Mount point	Enter the mount point directory to the file system, relative to the top level directory. Example: /tmp/usbdevice
Auto mount	Select to mount the device automatically when the gateway boots. If unselected, the device must be mounted manually.
Options	Enter the Linux mount options to be run when the device is mounted. Separate each of the options with a comma. Default mount option: rw, sync

GPS

Services > GPS

The built-in GPS receiver receives GPS data from GPS satellites for synchronizing the GPS time and position data.

Enable GPS

To enable GPS receiver:

1. Go to Services > GPS.
2. Select GPS Enable.
3. Click **Save & Apply**.

The data will be displayed on the page (see *Table 10-10*). It may take some time (about a minute) to receive and display the data.

Send GPS Data to an External Server

The GPS data can be sent in NMEA data format to an external TCP server on a real-time basis. You can also configure the GPS data to be sent to a backup server.

To send the GPS data to an external server:

1. Go to Services > GPS.
2. Select **Enable Data Send** and enter the server settings (see *Table 10-10*).
3. Click **Save & Apply**.

Table 10-10 GPS Service Configuration

Parameters	Description
GPS Parameters	
GPS Enable	Select GPS Enable check box to display current GPS data.
Time (GMT)	Time in hh:mm:ss
Latitude (degree.mmsss)	Latitude in ddmm.mmmm
N/S-Indicator	N = North or S = South
Longitude (degree.mmsss)	Longitude in ddmm.mmmm
E/W-Indicator	E = East or W=West
Position-Fix-Indicator	Indicates the type of signal or technique used by the GPS receiver to determine its location. ◆ **0 –** Fix not available or invalid ◆ **1 –** GPS SPS Mode, fix valid ◆ **2 –** Differential GPS, SPS Mode, fix valid ◆ **3 to 5 –** Not supported ◆ **6 –** Dead Reckoning Mode, fix valid
Number of Satellites Used	Number of satellites used to receive GPS signals. The range for the number of satellite used is 0 to 12.
HDOP	Horizontal Dilution of Precision (HDOP) indicates the relative accuracy of the horizontal position
Altitude (in meters)	Altitude above mean sea level

Parameters	Description
Status	Displays the status. A = Data valid V = Data not valid
Speed	Speed over ground in knots
Course of Ground	Track, or intended direction of travel
Protocol	
Enable Data Send	Select **Enable Data Send** check box to send data to the selected server. It sends the GPS information in NMEA format.
Protocol	Select the TCP protocol only.
IP1/URL1	Enter the primary IP address.
Port1	Enter the port number.
Backup	Click to use a backup server, in case sending the data fails using primary IP address. ◆ IP2/URL2 – Enter the backup IP address. ◆ Port2 – Enter the backup port number.
Polling Interval (in seconds)	The period of time between the end of the timeout period or the completion of the network request and the next request for data on the network.
Send Interval (in seconds)	The period of time to wait between attempts to send GPS data using the primary IP address or backup IP.

Description of NMEA Messages

The G520 series device receives NMEA sentences every second, depending on the configuration. The identifiers for the NMEA messages are listed below. All messages are based on the NMEA standard messages.

GPGGA	GPS Fix Data
GPRMC	Recommended Minimum Specific GPS Data
GPGSV	GPS Satellites in View
GPGSA	GPS DOP and Active Satellites
GPVTG	Course Over Ground and Ground Speed

A full description and definition of the listed messages above is provided in the next sections.

GPGGA Format

The $GPGGA message includes time, position, GPS quality and number of satellites in use.

Example: $GPGGA,120133.0,1907.469671,N,07250.544473,E,1,05,1.0,43.1,M,-64.0,M,*42

Table 10-11 GGA Data Format

Parameters	Description
MID GGA Parameters	
MID	GGA Protocol Header Example – $GPGGA
UTC Time	Time in hhmms.sss Example – 120133.0
Latitude	Latitude in ddmm.mmmm Example – 1907.469671
N/S-Indicator	N = North or S = South Example – N
Longitude	Longitude in ddmm.mmmm Example – 07250.544473
E/W-Indicator	E = East or W = West Example – E
Position-Fix-Indicator	Indicates ◆ 0 – Fix not available or invalid ◆ 1 – GPS SPS Mode, fix valid ◆ 2 – Differential GPS, SPS Mode, fix valid ◆ 3 to 5 – Not supported ◆ 6 – Dead Reckoning Mode, fix valid Example – 1
Satellite-Used	Number of satellite used to receive GPS signals. The range for the number of satellite used is 0 to 12. Example – 05
HDOP	Horizontal Dilution of Precision Example – 1.0
MSL Altitude	Altitude in meters. Example – 43.1 meters
Units	Example – M meters
Geoid Seperation	Geoid-to-ellipsoid separation. Ellipsoid altitude = MSL Altitude + Geoid Separation Example: -64.0 meters
Units	Example: M meters
Age of Diff.Corr.	Null fields when DGPS is not used.4 The units is sec.
Diff. Ref.Station ID	–
Checksum	*42
<CR><LF>	End of message termination

GPRMC Format

The $GPRMC message includes time, date, position, course, and speed datea.

Example: $GPRMC,120133.0,A,1907.469671,N,07250.544473,E,0.0,0.0,150915,0.3,W,A*1E

Table 10-12 RMC Data Format

Parameters	Description
MID RMC Parameters	
MID	RMC Protocol Header Example – $GPRMC
UTC Time	Time in hhmmss.sss Example – 120133.0
Status(1)	A = Data valid V = Data not valid Example – A
Latitude	Time in ddmm.mmmm Example – 1907.469671
N/S-Indicator	N = North or S = South Example – N
Longitude	Longitude in ddmm.mmmm Example – 07250.544473
E/W-Indicator	E = East or W = West Example – E
Speed Over Ground	Measured in knots. Example – 0.0
Course Over Ground	True. Measured in degrees Example – 0.0
Date	Date in ddmmyy Example – 150915
Magnetic Variation(2)	E = East or W = West Measured in degrees Example – 0.3
East/West Indicator(2)	W = West Example – W
Mode	Indicates ◆ **A –** Autonomous ◆ **D –** DGPS ◆ **E –** DR ◆ **N –** Output Data Not Valid ◆ **R –** Course Position(3) (4) (5) ◆ **S –** Simulator Example **–** A
Checksum	*1E

Parameters	Description
<CR><LF>	End of message termination

(1) A valid status is derived from all the parameters set in the software. This includes the minimum number of satellites required, any DOP mask setting, presence of DGPS corrections, etc. If the default or current software setting requires that a factor is met, and then if that factor is not met the solution will be marked as invalid.

(2) CSR Technology Inc. does not support magnetic declination. All courses over ground data are geodetic WGS84 directions relative to true North.

(3) Position was calculated based on one or more of the SVs having their states derived from almanac parameters, as opposed to ephemerides.

(4) This feature is supported in the GSD4e product only.

(5) This feature is supported in the GSD4e product, version 1.1.0 and later.

GPGSV Format

The $GPGSV includes the number of satellites in view, satellite ID numbers and their evaluation, azimuth and signal-to-noise ratio.

Example: $GPGSV,4,1,16,21,50,358,38,22,28,272,37,29,53,164,36,18,51,319,31,*71E

IMEI number is added at the start of every frame.

Table 10-13 GPGSV Data Format

Parameters	Description
MID GSV Parameters	
MID	GSV Protocol Header Example – $GPGSV
Number of Messages(1)	Total number of GSV messages to be sent in this group Example – 4
Message Number(1)	Message number in this group of GSV messages Example – 1
Satellites in View(1)	16
Satellite ID	Channel (Range 1 – 32) Example – 21
Elevation	Channel 1 (Maximum 90) Example – 50 degrees
Azimuth	Channel (True, Range 0 – 359) Example – 358 degrees
SNR (C/N0)	Range 0 – 99, null when not tracking Example – 38dBHz
….	(Satellite ID, elevation, azimuth, and SNR repeated for each satellite in view)
Satellite ID	Channel 4 (Range 1 – 32) Example – 18

Parameters	Description
Elevation	Channel 4 (Maximum 90) Example – 51 degrees
Azimuth	Channel 4 (True, Range 0 - 359) Example – 319 degrees
SNR (C/N0)	Range 0 – 99, null when not tracking Example – 31 dBHz
Checksum	*71
<CR><LF>	End of message termination

(1)Depending on the number of satellites tracked, multiple messages of GSV data may be required. In some software versions, the maximum number of satellites reported as visible is limited to 12, even though more may be visible.

GPGSA Format

The $GPGSA message includes the list of satellites being used.

Example: $GPGSA,A,3,18,20,21,22,29,,,,,,,2.4,1.0,2.2*36

Table 10-14 GSA Data Format

Parameters	Description
MID GSA Parameters	
MID	GSA Protocol Header Example – $GPGSA
Mode1	**M – Manual:** Forced to operate in 2D or 3D mode **A – 2D Automatic:** Allowed to automatically switch 2D/3D Example – A
Mode2	1 – Fix not available 2 – 2D (<4 SVs used) 3 – 3D (>3 SVs used) Example – 3
Satellite Used(1)	SV on Channel 1 Example – 18
Satellite Used(1)	SV on Channel 2 Example – 20
….	….
Satellite Used	SV on Channel 12
PDOP(2)	Position Dilution of Precision Example: 2.4
HDOP(2)	Horizontal Dilution of Precision Example: 1.0
VDOP(2)	Vertical Dilution of Precision Example: 2.2

Parameters	Description
Checksum	*33
<CR><LF>	End of message termination

(1) Satellite used in solution.

(2) Maximum DOP value reported is 50. When 50 is reported, the actual DOP may be much larger.

GPVTG Format

The $GPVTG message includes course over ground and ground speed.

Example: $GPVTG,0.0,T,0.3,M,0.0,N,0.0,K,A*20

Table 10-15 VTG Data Format

Parameters	Description
MID VTG Parameters	
MID	VTG Protocol Header Example – $GPVTG
Course	Measured heading Example – 0.0 degrees
Reference	True Example – T
Course	Measured heading Example – 0.3 degrees
Reference	Magnetic(1) Example – M
Speed	Measured horizontal speed Example – 0.0 knots
Units	Knots Example – N
Speed	Measured horizontal speed Example – 0.0 km/hr
Units	Kilometers per hour Example – K
Mode	Indicates ◆ **A –** Autonomous ◆ **D –** DGPS ◆ **E –** DR ◆ **N –** Output Data Not Valid ◆ **R –** Course Position(2) (3) (4) ◆ **S –** Simulator Example **–** A
Checksum	*20

Parameters	Description
<CR><LF>	End of message termination

(1) CSR does not support magnetic declination. All “course over ground” data are geodetic WGS84 directions.

(2) Position was calculated based on one or more of the SVs having their states derived from almanac parameters, as opposed to ephemerides.

(3) This feature is supported in the GSD4e product only.

(4) This feature is supported in the GSD4e product, version 1.1.0 and later.

Keepalived

Services > Keepalived

The Keepalived service provides frameworks for load balancing and high availability of the servers connected to the gateway. Keepalived uses Virtual Router Redundancy Protocol (VRRP) to check the health of load balanced routers and elect a router on the network that will serve a particular IP.

In a typical configuration, VRRP groups two or more routers into a virtual router, where one router is the master (active) server and the other is the backup node. The master server has a higher priority than the backup server. The master server transmits multicast VRRP advertisement packets at regular intervals, and the backup servers listen for these advertisement packets. If the backup servers fail to receive three consecutive VRRP advertisements, the backup router with the highest priority becomes the new master router so that the system remains functional.

The configuration for the backup server will be similar to that of the master server, with the exception of the values for priority, state, and interface, depending on the system hardware configuration.

Keepalived Configuration

The Keepalived configuration on the web interface includes the following sections:

- **General** – Keepalived log settings
- **Global** – Keepalived global settings
- **Tracking Scripts** – create tracking script blocks that Keepalived will run to determine the health of the host and increase or decrease the priority of the router by the value of the weight.
- **Tracking Interfaces** – configure which interfaces Keepalived will monitor. If a monitored interface fails, Keepalived will adjust the priority of the host according to the configured weight of the tracking interface.
- **Tracking Processes** – create tracking process blocks that Keepalived can use to monitor the health of the router. If the monitored process stops running, Keepalived will adjust the priority of the host according to the weight of the tracking process. After adding a process, you must restart the Keepalived service.
- **Virtual IP** – configure the Virtual IP address for the VRRP instance.
- **VRRP Instances** – add VRRP instances to be run on interfaces that Keepalived is monitoring. The VRRP instance is defined in the General and Advanced settings. The User Notify settings allow Keepalived to run specified scripts when the router transitions between backup and master states.

To configure Keepalived settings:

1. Go to Services > Keepalived.
2. Edit the configuration settings. See *Table 10-16*.
3. Click **Save & Apply** when you are finished.

Table 10-16 Keepalived Configuration

Parameters	Description
General	
Detailed Log	Select to enable detailed keepalived general/common logs.
Syslog level	Set the log level from 0-4, with 4 being the most detailed.
Keepalived Global	
Vrrp startup delay	Enter the time in seconds to delay before starting VRRP.
Global Router Id/name	Enter the global router ID/name. A default name is provided, but you can modify it if you want. It doesn't have to be the hostname, but it must be unique for each device in a pool.
Keepalived config file	Select the Keepalived configuration file. Settings in the configuration file will supersede settings configured on the Keepalived UI pages except for all scripts loaded in Tracking Scripts, and the User Notify settings in VRRP Instances. The name of the script should match the ones in the configuration file settings.
Remove configuration for Keepalived	Unlink the uploaded keepalived configuration so as to fill the configurations manually.
User	The user for script execution.
Enable Script Security	Select to prevent running any scripts that were configured to be run as root if any part of the path is writable by a non-root user.
Enable dynamic interfaces	Select to enable dynamic interfaces. Once enabled, next to Dynamic interfaces, select Allow or None
Tracking Scripts	
Name of trackscript block	Enter the tracking script block name.
Script	Select the tracking script file to upload it to the router. The file is uploaded to the /usr/sbin/ folder. The script name should start with "keepalived_" and end with ".sh".
Remove script	Click to remove the tracking script.
TrackScript interval	Enter the time interval between script invocations in seconds. Default is 1 second
Weight	Enter the weight to adjust the priority if the tracking script fails. Range is -253 to 253. Positive value will increase the priority. Negative value will decrease the priority. Setting it to zero (0) will ignore the weight, which means that any VRRP instance monitoring the script will transition to the fault state after the fail count number of consecutive failures of the script. A script returning 0 (zero) is success and everything else is fail.
TrackScript pass count	Enter the required number of successes for OK transition.
TrackScript fail count	Enter the required number of fails for NOK transition.
Tracking Interfaces	
Name of interface block	Enter the name of the tracking interface block
Interfaces	Select the interface to monitor for changing the state of the router or decreasing the weight.

Parameters	Description
Weight	Enter the weight to adjust the priority if the interface is present or absent. Range is -253 to 253. Positive value will increase the priority. Negative value will decrease the priority. Default is 0 (zero), which means that the router will fail in case of the interface not running.
Tracking Processes	
Name of process block	Enter the name of the process block.
Process	Enter the name of the process to monitor for running state.
Weight	Enter the weight to adjust the priority if the process is not running. Range is -253 to 253. Positive value will increase the priority. Negative value will decrease the priority. Default is 0 (zero), which means that the router will fail in case of the interface not running.
Virtual IP	
Name of address block	Enter the name of the address block.
Virtual ipaddress	Enter the Virtual IP address and netmask that will be used by the virtual router.
Physical device	Select the device used for the virtual IP.
Scope of the virtual ip	Select the scope. Options include: **global**, site, link, host, nowhere.
VRRP Instances	
VRRP Instances > General Settings	
Enable	Click to enable the VRRP instance. The VRRP instance defines and configures VRRP behavior to run on a specific interface.
Name of Instance	Enter a name for the VRRP instance.
Virtual Router ID	Enter the router ID. This number should be the same for all routers on the virtual router. Unique number from 1 to 155.
Interface to look for	Select the interface that needs to be monitored for switching.
Virtual Router Priority	Enter the priority. The router with the highest priority will be the master.
Delay	Enter the interval in seconds that VRRP will wait between sending advertisement packets. Default is 1 second.
Debug	Enter the debug level, from 1 to 4. ***Note:*** *Debug level is not implemented yet by Keepalived.*
Initial Virtual Router State	Select the initial virtual router state as MASTER or BACKUP. This is for initial state only. As soon as the other routers in the virtual router group come up, an election will be held and the router with the highest priority will become MASTER.
Enable Authentication	Select to enable authentication. Authentication type can be PASS (suggested) or AH – IPsec (not recommended). PASS is a simple text password. This should be the same value on all machines in the virtual router. Only the first eight (8) characters are used. ***Note:*** *Authentication was removed from the VRRPv2 specification, and use of the option is non-compliant and can cause problems.*

Parameters	Description
VRRP Instances > Advanced Settings	
Virtual IPs	Enter the Virtual IP block. The router will assume this IP when it becomes Master and release it when it changes to Backup. Add blocks configured in Virtual IP.
Track Process	Enter the track process block that the VRRP instance will monitor. Add blocks configured in Tracking Process.
Track interface	Enter the track interface block that the VRRP instance will monitor. Add blocks configured in Tracking Interfaces.
Track Script	Enter the tracking script block that the VRRP instance will monitor. Add blocks configured in Tracking Scripts.
VRRP Instances > User Notify Settings	
Notify master Script	Select the notify master script which will be run when the router becomes Master.
Remove master script	Remove the notify master script.
Notify backup Script	Select the notify backup script which will be run when the router becomes Backup.
Remove backup script	Remove the notify backup script.

Last Gasp

Services > Last Gasp

Last gasp transmits a text message to a specified mobile phone number when the gateway loses power. To use this function, the last gasp switch must be in the ON position. The battery is charged while the device is connected to an external power input.

To configure last gasp:

1. Go to Services > Last Gasp.
2. Select **Enable**.
3. Enter the configuration settings (see *Table 10-17*).
4. Click **Save & Apply**.

Table 10-17 Last Gasp Message Configuration

Field	Description
Enable	Select to enable or clear to disable the last gasp message. It is disabled by default.
Mobile Number	Enter the mobile number with country code
Power restore text	Enter the message to send to the mobile number in case the power to the gateway is restored.
Power failure text	Enter the message to send to the mobile number in case the power is lost.

Logs Information

Services > Logs Information

Logs Information page lets you view the system log file and download them to the local computer. The current log file and up to 3 historical log files may be saved.

The logs configuration is read from the system logging. In order to display and download the log file, the system logging must be configured to write system log to file (see *System > System > Logging*).

To display or download logs:

1. Go to Services > Logs Information. The Logs page appears.
2. Select the log file. The file is displayed on the page.
3. Click **Download**. The log file is downloaded to the local computer.

Reporting Agent

Services > Reporting Agent

The reporting agent captures current device and interface information from the gateway on a periodic basis and sends it to a generic device management server using TCP/UDP/HTTP/HTTPS protocol.

To configure the reporting agent:

1. Go to Services > Reporting Agent.
2. Select **Enable All** to enable collection data on all settings for all interfaces.
3. Select the settings to report for each of the network interfaces (LAN, WAN, Cellular, Wi-Fi, GPS). See *Table 10-18*.
4. Configure and enable the device info, reporting agent, and data send settings. See *Table 10-19*.
5. Click **Save & Apply**.

Table 10-18 Reporting Agent Configuration

Parameters	Description
Enable All	Select check box to enable all settings for all interfaces.
Disable All	Select check box to disable all settings for all interfaces.
LAN Parameters	
LAN	Select to enable reporting of individual LAN settings. ◆ Status ◆ Uptime ◆ IP ◆ Data usage
WAN Parameters	

Parameters	Description
	Select to enable individual WAN settings. ◆ Status ◆ Uptime ◆ IP ◆ Gateway ◆ DNS ◆ Data usage
Cellular Parameters	
	Select to enable individual Cellular settings. ◆ Status ◆ Uptime ◆ IP ◆ Gateway ◆ DNS ◆ Data usage ◆ RSSI ◆ Roaming Status ◆ Operator Name ◆ Network Status ◆ IMSI
Wi-Fi Parameters	
	Select to enable individual Wi-Fi settings. ◆ Status ◆ Uptime ◆ IP ◆ Gateway ◆ DNS ◆ Data usage ◆ Wifi Client Info
GPS Parameters	
	Select to enable individual GPS settings. ◆ Time ◆ Latitude ◆ Longitude ◆ Altitude
Vehicle	Select to enable individual Vehicle tracking settings. ◆ Ignition ◆ Routes ◆ Parking

Sending Data

Table 10-19 Reporting Agent Data Send Configuration

Parameters	Description
Device Info	Select to allow reporting agent to retrieve device IMEI information.
Reporting Agents	Select the reporting agent. Generic agent is the default selection.
Enable Data Send	Select to enable data send.

Parameters	Description
Protocol	Select the protocol used in the data transmission. Options are TCP, UDP, HTTP, or HTTPS. Depending on the protocol that you selected, the server fields will vary.
Starting string of the frame	When TCP is selected, a start of frame sequence can be used to indicate the first frame of the data sent by the reporting agent. This string must be less than 20 characters in length.
Ending string of the frame	When TCP is selected, a start of frame sequence can be used to indicate the first frame of the data sent by the reporting agent. This string must be less than 20 characters in length.
IP1/URL1	Enter the IP address or the URL of the destination server.
Port1	Enter the port number (for TCP and UDP).
TCP Timeout	Enter the timeout in seconds to switch between primary and backup IP in case of connectivity failure. TCP user timeout value should be between 10 and 900 seconds.
Backup	This option is available when TCP protocol is selected. Select Backup check box to configure the backup TCP server. ◆ IP2/URL2 ◆ Port2 The backup IP will be used after 3 failed attempts to send data to primary server. Reporting agent will continue to send data to backup server until the backup server fails or the device reboots.
Send Interval in Second	The period of time between two data transmissions.

Data Format

Figure 10-1 shows a portion of the reporting agent data format for a case where all settings were selected.

Figure 10-1 Reporting Agent Data Format (excerpt)

```
@IMEI=352948070039411,Lan Status=Connected,Lan
IP(IPv4)=192.168.1.1,Lan Uptime(Seconds)=329501,Lan TX
bytes=572260469,Lan RX bytes=117212098,Wan Status=Connected,Wan
IP(IPv4)=192.169.1.110,Wan Uptime(Seconds)=329389,Wan
gateway=192.169.1.1,Wan DNS=27.109.1.2 27.109.1.3,Wan TX
bytes=75455301,Wan RX bytes=344481735,Cellular
Status=Enabled,Cellular IP(IPv4)=,Cellular
uptime(Seconds)=,Cellular gateway=,Cellular DNS=,Cellular TX
bytes=208,Cellular RX bytes=0,RSSI(ASU)=99,Roaming Status=N/
A,Operator Name=N/A,Network Status=Not Registered,IMSI=ERROR,Wifi
Status=Enabled,Wifi IP(IPv4)=192.169.2.116,Wifi
Uptime(Seconds)=383,Wifi gateway=192.169.2.1,Wifi
DNS=192.169.2.1,Wifi TX bytes=14135074,Wifi RX bytes=34397774,Wifi
Client
```

SCEP Client

Services > SCEP Client

The Simple Certificate Enrollment Protocol (SCEP) client is used to enroll the certificate from the SCEP server by providing server URL and password.

The SCEP Client page displays the SCEP certificates, their details, and allows you to add a certificate and perform certain functions related to the certificates.

Table 10-20 SCEP Client page Overview

Parameters	Description
Name	Name of the certificate
Valid from	Certificate validity start date
Valid till	Certificate validity end date
Status	Status of the certificate
Manage	Provides the following functions: ◆ **Edit** - Click to edit the certificate ◆ **Delete** - Click to delete the certificate
Action	Provides the following functions: ◆ **Enroll** - Click to enroll the newly created certificate ◆ **Renew** - Click to renew the expired certificate
Add Certificate	Click to add a new certificate

To add a new certificate:

1. Click **Add Certificate**.
2. Enter the Certificate Details (see *Table 10-21*).
3. Click **Save & Apply**.
4. The new certificate displays on the SCEP Client page. Click **Enroll** to make the certificate active.

Table 10-21 SCEP Certificate Details

Parameters	Description
Name	Enter a name for the certificate.
Key Type	Select key type. Default value is RSA.
Key Length	Select key length. ◆ 768 ◆ 1024 (default) ◆ 2048 ◆ 3072
Subject Name	
Country	Enter country name (should consist only 2 characters, e.g., IN, US, UK etc.).
State	Enter state name.
Locality	Enter locality name.

Parameters	Description
Organization	Enter organization name.
Organization Unit	Enter organization unit name.
Common Name	Enter common name.
Subject Alternative	
Alternate Name	Select alternate name. ◆ Cert IP ◆ Cert DNS ◆ Cert Email ◆ None (default)
SCEP Server Credentials	
SCEP Sever URL	Enter the URL for SCEP server.
Password	Enter password for SCEP server.
Issuer Subject Name	Certificate issuer ID (optional)

Service Actions

Services > Service Actions

This page displays a list of the available services and allows you to manage the system resources. You can start, stop, reload, or restart the service; and enable or disable automatic startup of the service when the device is rebooted.

Note: *Use caution when changing the state of services as it may cause loss of network connectivity and data. Some features may stop working and the device may become unstable.*

Figure 10-2 Service Actions

SMS

Services > SMS

The SMS feature lets you send SMS messages to the gateway to request diagnostics information, configure gateway settings, or initiate certain actions such as DOTA upgrade or starting and stopping the VPN.

SMS Configuration

Services > SMS > SMS Configuration

You can configure up to four administrator mobile numbers to receive SMS messages containing gateway diagnostics information after a command is sent by SMS. The mobile number format is as follows: +<countrycode><phonenumber>

You should include the preceding special character “plus (+)”. Example: +9198xxxxxxxx

Table 10-22 SMS Service Configuration

Parameters	Description
SMS Configuration	
Enable	Enable remote SMS configuration.
AT Enable	Enable remote AT commands using SMS
PDU Enable	Enable to send messages in PDU mode
SMS Administrator	Displays up to four Administrators configured to receive the diagnostics via SMS after an SMS command is sent. ***Note:*** *If no number is configured then the gateway will accept SMS from any number.* For each administrator to be configured, enter the mobile number with country code. The format of mobile number must be: +<countrycode><phonenumber> with a preceding special character “plus (+)”. Example: +9198xxxxxxxx

SMS AT Commands

Table 10-23 describes the SMS AT commands in alphabetical order.

Table 10-23 SMS AT Command Syntax

Name	Command Syntax
AT Command	AT#ATCMD='<AT command string>',<Timeout> Description: The command passed in the AT command string will be sent directly to the internal GSM module. Parameters: ◆ AT command string – AT command such as AT+CSQ (signal quality) or AT+CREG? (to check the registration status of GSM module). ◆ Timeout – The timeout value should be an integer in seconds. If the timeout value is set to 0, don't wait for a response. Issue the command and leave it. Example: AT#ATCMD=AT+CSQ,5 – check signal strength
Cell Diagnostics	AT+CELLDIAG? Description: Get cellular diagnostics
CELL Ping	AT+CELLPING=<IPA> Description: Pings the cellular IP address Parameter: ◆ IPA – IP address of the WAN interface to ping.
DOTA Action	AT+DOTA=<C/M>,<update/check>[,<released/beta/development>,<filename>] Description: Update firmware on gateway or check for available firmware updates from configured server Parameters: ◆ C/M – C for custom server, M for Lantronix server ◆ update/check – whether to update the gateway with the specified filename or to check for available updates ◆ released/beta/development – the release channel on the Lantronix download server ◆ filename – filename of the package to use for the update
DOTA Custom Settings	AT+DOTASETTINGS=<HTTP/HTTPS>,<Server URL>,<File name>,<Username>,<Password>,<Timeout>,<Retry> Description: Update firmware on gateway from a custom server Parameters: ◆ HTTP/HTTPS – protocol of the custom server ◆ Server URL – server URL, must include http: or https: ◆ File name – the name of the file to be accessed for the update ◆ Username – server username ◆ Password – server password ◆ Timeout – period of time to wait for the download to complete (minutes) ◆ Retry Parameters – number of retry attempts for the download
Hardware Information	AT+HWI? Description: Get hardware information

Name	Command Syntax
Cellular Settings	AT+IPGPRS=<1/2>,<Apn>,<Username>,<Password>,<Auth-Type>,<Data-Roam> Description: Configure cellular SIM settings Parameters: ◆ 1/2 – SIM slot number ◆ Apn – access point name provided by the cellular network provider ◆ Username – username if auth type is pap, chap, or pap/chap ◆ Password – password if auth type is pap, chap, or pap/chap ◆ Auth-type – none, pap, pap/chap, or chap (auth-type parameter is case sensitive, must be all lowercase) ◆ Data-Roam – 0 for disabled or 1 for enabled
Install / Update / Remove / Autoremove IPK	AT+IPKDOTA=<Name of IPK file>,<install/upgrade/remove/autoremove>,<For install/upgrade: 0-both default URL and custom URL, 1-default URL, 2-custom URL> Description: Install, update, remove or auto remove packages Parameters: ◆ Name of IPK file – IPK file name that OPKG will install, upgrade, or remove. ◆ install/upgrade/remove/autoremove – action that OPKG will run. ◆ location to check for the package for install or upgrade. This argument is not required for remove or autoremove. ➢ 0 – Both default server URL & custom URL. Both servers should be running, otherwise it will return a failed response. ➢ 1 – default server URL ➢ 2 – custom server URL
Lan Settings	AT+IPLAN=<IPv4 address>,<SubnetMask> Description: Configure LAN IPv4 settings Parameters: ◆ IPv4 address – The IP address of the LAN interface ◆ Subnet mask – Subnet mask of the LAN IP address
LAN Diagnostics	AT+LANDIAG? Description: Get LAN diagnostics
LAN Ping	AT+LANPING=<IPA> Description: Ping LAN IP address Parameter: ◆ IPA – IP address of the LAN interface to ping
OPKG Configuration Settings	AT+OPKGSETTINGS=<Server URL> Description: Set OPKG server Parameter: ◆ Server URL – URL of the package server
Manage Digital Output	AT#OUT=<GPO1/GPO2>,<OPEN/CLOSE> Description: Pull high or push low GPIO pins Parameters: ◆ GPO1/GPO2 – the pin to be configured ◆ OPEN/CLOSE – Set OPEN for low, or CLOSE for high.
Reboot	AT+REBOOT=1 Description: Reboot the gateway

Name	Command Syntax
Enable Remote Access	AT+REMACC=<1/0> Description: remote access Parameter: ◆ 1/0 – Set 1 to enable, set 0 to disable remote access
Software Information	AT+SWI? Description: Get software information
WAN Diagnostics	AT+WANDIAG? Description: Get WAN diagnostics
WAN Ping	AT+WANPING=<IPA> Description: Ping WAN interface Parameter: ◆ IPA – IP address of the WAN interface to ping.
WWAN Ping	AT+WWANPING=<IPA> Description: Ping WWAN interface Parameter: ◆ IPA– IP address of the WAN interface to ping.
Start/Stop VPN	AT+VPN=<VPN Type>,<VPN Name>,<start/stop> Description: Start or stop the VPN instance Parameters: ◆ VPN type – pptp, l2tp, ipsec, openvpn ◆ VPN name – VPN instance name ◆ Start/stop – action to start or stop the VPN Examples: ◆ AT+VPN=ipsec,IPSEC1,start ◆ AT+VPN=ipsec,IPSEC1,stop

Ethernet SMS

Services > SMS > Ethernet SMS

This service enables the device connected on LAN to initiate an SMS using Ethernet port.

Table 10-24 Ethernet SMS Configuration

Parameters	Description
Enable	Check to enable the Ethernet SMS.
Port	Enter the port number. The port number range is from 0 to 65535.

To send an SMS you need to open a TCP client connection on the LAN IP and configured port. Once the connection is created, issue the following commands:

To send an SMS

```
AT#SENDSMS=+<Mobile Number with Country Code><Message end with CTRL+D>
```

To read an incoming SMS

```
AT#READSMS=<ALL/SMS ID><Enter>
```

To delete an SMS

```
AT#DELSMS=<ALL/SMS ID><Enter>
```

The internal SMS buffer is 10 messages – meaning, 11th incoming SMS will be over written on the 1st SMS.

Live Message

Services > SMS > Live Message

Sends SMS from the web interface.

Notes:

- *To activate the Live Message feature, you must first enable the Ethernet SMS feature.*
- *To send SMS, add a # symbol preceding the phone number instead of the + symbol.*

To send SMS from the web interface:

1. Go to Services > SMS > Live Message.
2. Under Send SMS:, type #<mobile number with country code>.
3. Under Message Area: type the message. It can be update 159 characters.
4. Click **SendSMS**.

To read SMS:

On the Live Message page, select the message number (from 1-10 or All) and click **ReadSms**.

To delete an SMS:

On the Live Message page, select the message number (from 1-10 or All) and click **DeleteSms**.

SNMPD

Services > SNMPD

The G520 series gateway uses Net-SNMP to implement SNMP v1, v2c, and v3 using both IPv4 and IPv6 to remotely manage and monitor network components and systems. The implementation includes an SNMP agent for responding to SNMP requests or actions from the SNMP manager, an SNMP-TRAP application for receiving and processing SNMP notifications (or traps), and support for a number of applications to retrieve information from an SNMP capable device (snmpget, snmpgetnext, snmpwalk), retrieve statistics (snmpstatus) or write configuration on the device (snmpset).

The configuration of the SNMP agent and SNMP-TRAP application configuration files (mainly snmpd.conf and snmptrapd.conf) are done using the web interface. Likewise, operations such as enabling or disabling the agent and trap receiver are done using the web interface. Most management operations and monitoring, however, will be done through the SNMP manager.

Prerequisites to use this feature include having knowledge of SNMP and having a network management system (NMS) with which to monitor the network.

For more information about Net-SNMP or SNMP in general, please refer to the Net-SNMP web site.

For information about using SNMP management systems, see the appropriate documentation for your NMS application.

SNMP Architecture

A typical SNMP implementation includes the following components:

- Network management system (NMS) – a combination of hardware devices and software (SNMP manager) used to monitor and administer a network. The manager polls the devices on the network for information about network connectivity, activity, and events.
- Managed device – any device on the network that is managed by the NMS.
- SNMP agent – the SNMP process that resides on the managed device and communicates with the SNMP manager. It responds to requests for information or actions from the manager and generates SNMP notifications (traps). The agent also controls access to the agent's MIB.
- Management Information Base (MIB) – collection of objects that specify the information that the agent provides to the SNMP manager.

SNMP Versions

The G520 series software supports the following versions of SNMP: SNMPv1, SNMPv2c and SNMPv3/USM.

- SNMPv1 – Simple Network Management Protocol, defined in RFC 1157. Security is based on community strings.
- SNMPv2c – The community string-based Administrative Framework for SNMPv2. SNMPv2c is defined in RFCs 1901, 1905, and 1906. Security is based on community strings.
- SNMPv3/USM – SNMPv3 is defined in RFCs 3413-3415. It provides secure access to devices by authenticating and encrypting packets over the network. SNMPv3 provides message integrity, authentication, and encryption security features.

Table 10-25 SNMP Security Models and Levels

SNMP Model	Level	Authentication	Encryption
v1	noAuthNoPriv	Community String	No
v2c	noAuthNoPriv	Community String	No
v3	noAuthNoPriv	Username	No
v3	authNoPriv	MD5 or SHA	No
v3	authPriv	MD5 or SHA	DES or AES

SNMP Configuration

The SNMP agent must be configured to use the version of SNMP that is supported by the management station. An agent can communicate with multiple managers. You can configure the SNMP agent to support communication with one management station using SNMPv1, one using SNMPv2c, and one using SNMPv3.

The web interface allows you to configure the SNMP settings. The configuration specifies directives in the following areas:

- agent behavior
- access control to the agent (VACM)
- system information and monitoring
- active monitoring of the local system

Agent Behavior

The following directives control the behavior of SNMP network service.

- agent address – the listening address on which to receive incoming SNMP requests. The default behavior is to listen on UDP port 161 on all IPv4 interfaces
- EngineID – SNMPv3 only. SNMPv3 requires an SNMP agent to define a unique engine ID to respond to SNMP requests.

For configuration details, see *Table 10-26 on page 145*.

View-based Access Control Model (VACM)

SNMP v1/v2c/v3-USM follow the VACM model. VACM determines whether to allow access to a managed object in a local MIB by a remote principal. VACM makes use of a MIB that defines the access control policy for the agent and makes it possible to use remote configuration.

The SNMP service uses four keywords to set up VACM:

- **Com2sec** – maps a v1 and v2c community string and a source IP or network to a security name.
- **Group** – maps a security name/security model pair to a group name.
- **View** – maps an OID subtree family and bitstring value (mask-optional), or MIB view, to a view name.
- **Access** – maps a group name to a minimum access level (noauth, auth, or priv) and read/write/notify scope for a specified security model (v1, v2c, v3/usm, or any).

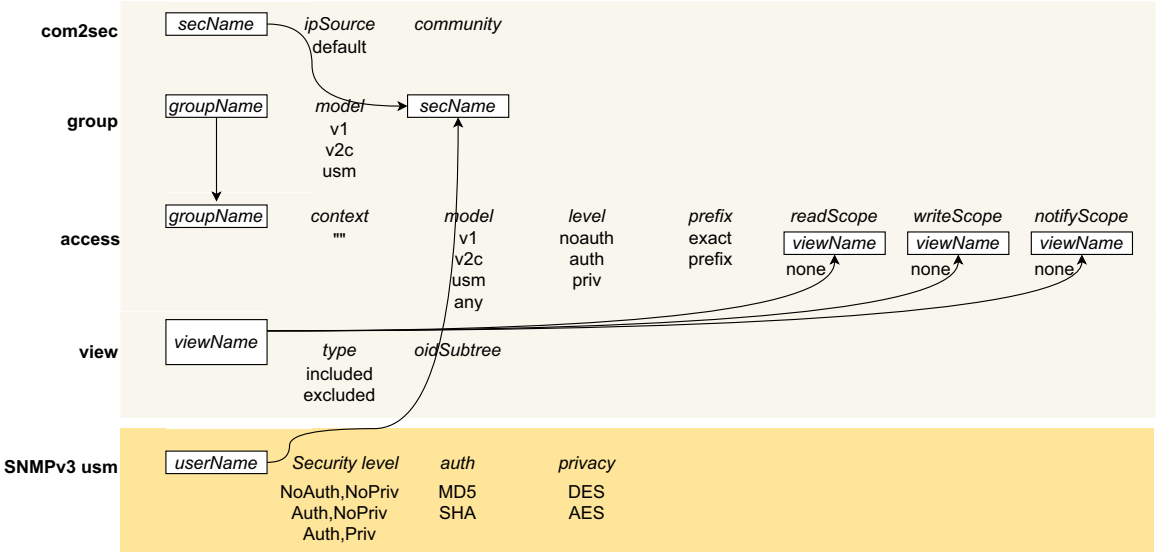
In summary:

- The Access and View keywords determine what access is being controlled.

- The Group and com2sec keywords determine who has this access.

Figure 10-3 shows how the fields map in the VACM configuration model.

Figure 10-3 VACM Configuration Model



For SNMP v1/v2c/USM VACM configuration details, see *Table 10-27 on page 147*.

SNMPv3 with User-based Security Model (USM)

SNMPv3 with USM contains a private list of users and keys specific to the SNMPv3 protocol. To use this model, the SNMPv3 USM users must be created and added to the VACM group table (as security name).

For SNMPv3 with USM user configuration details, see *Table 10-29 on page 150*.

System Information and Monitoring

System information includes system group information and monitoring information, which is described below. The system group information, such as name, location, contact, and description, are retrieved from the underlying network management system.

The agent is built with support for monitoring the local system. The following directives can be specified:

- Process monitoring – provides information about individual processes running on the local system
- Disk usage monitoring – provides information about disk usage for specified disks or all disks
- System load monitoring – provides information about system load average and swap space
- Log file monitoring – monitors the file size of specified log files

For system information and monitoring configuration details, see *Table 10-26 on page 145*.

Active Monitoring

The agent can be configured to generate trap notifications based on the following directives:

- Authentication failure trap – generate authentication failure traps

- Default monitors – configure the Event MIB tables to monitor various UCD-SNMP-MIB tables for problems
- Link up/link down notifications – monitor for network interfaces being taken up or down and triggering a linkUp or linkDown notification as appropriate
- Where to send the trap notifications – determine where to send the notifications such as to the localhost or to the SNMP manager.

For Trap sender configuration, see *Table 10-30 on page 150*.

Configure SNMPv1 or SNMPv2

To configure SNMPv1 or SNMPv2c:

1. Go to Services > SNMPD.
2. Enter the configuration settings as required according to the SNMP version (v1/v2c/v3-USM) you have chosen. Click **Save** before moving between tabs on the SNMP page.
3. To configure SNMP general settings including agent behavior and system information/ monitoring, select the General Settings tab. See *Table 10-26*.
4. To configure VACM access control settings, select the VACM tab. See *Table 10-27*.

   Note: *You do not need to configure the EngineID or SNMPv3 with USM settings.*

5. To configure SNMP agent trap sender, select the Trap Settings tab. See *Table 10-30*.

   Note: *To configure SNMP-TRAP application, see SNMPTRAPD on page 152.*

6. On the General Settings tab, select **Enable** if it is not already selected.
7. Click **Save & Apply**.

Configure SNMPv3 with USM

To configure SNMPv3 with USM:

1. Go to Services > SNMPD.
2. Enter the configuration settings as required according to the SNMP version (v1/v2c/v3-USM) you have chosen. Click **Save** before moving between tabs on the SNMP page.
3. To configure SNMP general settings including agent behavior and system information/ monitoring, select the General Settings tab. See *Table 10-26*.
4. To configure VACM access control settings, select the VACM tab. See *Table 10-27*.
5. To configure Engine ID settings for SNMPv3, select the VACM tab. See *Table 10-28*.
6. To create users for SNMPv3 with USM, select the VACM tab. See *Table 10-29*.
7. To configure SNMP agent trap sender, select the Trap Settings tab. See *Table 10-30*.

   Note: *To configure SNMP-TRAP application, see SNMPTRAPD on page 152.*

8. On the General Settings tab, select **Enable** if it is not already selected.
9. Click **Save & Apply**.

Table 10-26 SNMP General Settings Configuration

Parameters	Description
Enable	Select to enable the SNMPD application.
EngineID	Displays the SNMP engine ID, which is required to respond to SNMPv3 requests. This value is auto-generated when the agent is first started.
agentaddress	Defines a list of listening addresses on which to receive incoming SNMP requests. The default agent behavior is listening on all interfaces on UDP port 161. This is equivalent to the following directive: agentaddress udp:161 or simply agentaddress 161 To configure this field, specify one or more listening addresses using the format: [<transport-specifier>:]<transport-address> Examples: ◆ UDP:161, UDP6:161 – accept requests on all IPv4 and IPv6 interfaces on UDP port 161 ◆ localhost:161 – accept requests on the local loopback interface on UDP port 161 ◆ 127.0.0.1 – accept requests on the local loopback interface (UDP is implied) ◆ UDP:161, UDP6:161, TCP:161, TCP6:161 – accept requests on all IPv4 and IPv6 interfaces on UDP port 161 and TCP port 161 Other combinations are also valid.
System Information	Displays the system group information. System name, contact and location can be set through the SNMP Manager. ◆ sysName – default is Lantronix ◆ sysContact – default is root@localhost ◆ sysLocation – default is Unknown ◆ sysDescription – default 'uname -s -n -r -v -m' command output is not writable using a set request.
Process Monitoring	
Process Monitoring	Monitors the processes running on the local system and registers a command that can be run to fix errors. This table displays the processes that are being monitored and provides options to add, edit or delete items from the monitoring table. ◆ Click **Add** to add an entry to the process monitoring table. Enter the process name and other details as shown below. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table.
Process Name	Name of the process that is being counted.
Max Process	Maximum number of processes that should be running. Generates an error flag if the number of processes detected is greater than the maximum specified.
Min Process	Minimum number of processes that should be running. Generates an error flag if the number is less than the minimum.
Enable Fix Action	Tells the agent to attempt to fix the problem by calling the operation specified in the fix action. The command will not be invoked automatically.
Program Name (Procfix action)	The command that gets run when the error is detected and the fix action field is enabled.
Arguments	Arguments that support the command.

Parameters	Description
Disk Usage Monitoring	
Disk Usage Monitoring	Monitors the minimum threshold specified in KB or as a percentage of the total disk space and registers an error if the available disk space is less than the minimum required space configured for it. Disk usage monitoring section also allows for monitoring of all disks found on the system according to a specified percentage threshold. (See Include all disks.) This table displays the disks being monitored for disk usage and provides options to add, edit, or delete items from the monitoring table. ◆ Click **Add** to add an entry to the disk usage monitoring table. Enter the partition and space details as shown below. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table.
Partition	Path where the disk is mounted.
Minimum Space	Minimum space or minimum percentage must be configured. ◆ Minimum space required on the disk in KB before the errors are triggered. ◆ Minimum space required on the disk as a percentage of the total disk space before the errors are triggered.
Include All disks	Enables monitoring of all disks found on the system.
Minimum Percent	Minimum space required as a percentage of total disk space of all disks before the errors are triggered. ***Note:*** *The threshold for individual disks can be configured using the partition directives above.*
System Load Monitoring	
Load Monitoring	Displays the system load monitoring details if configured. Monitors the load average of the local system.
Enable Load Monitoring	Enables monitoring of system load averages
1 - Minute Max. Load	The one-minute maximum load average before errors are triggered.
5 - Minute Max. Load	The five-minute maximum load average before errors are triggered.
15 - Minute Max. Load	The fifteen-minute maximum load average before errors are triggered.
Swap Space Threshold (in KB)	Amount of swap space (in KB) available on the local system. The default threshold is 16 MB and it is enabled by default. If the available swap space is less than 16 KB if not user-configured, or less than the configured value, and if Default Monitoring is enabled, it will generate a notification to SNMP traps.
Log File Monitoring	
Log File Monitoring	Monitors the size of the log files and registers an error if the size exceeds the maximum size configured for it. Limit: Up to 20 files can be monitored. This table displays log files being monitored for file size limits and provides options to add, edit or delete items from the monitoring table. ◆ Click **Add** to add an entry to the log file monitoring table. Enter the details as shown below. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table.
File Path	File path and name of the file to be monitored.

Parameters	Description
Maximum Size	Maximum file size in KB before errors are triggered.

Table 10-27 SNMP v1/v2/USM VACM Settings

Parameters	Description
Com2Sec Configuration	
Com2Sec Configuration	The com2sec directive maps a v1/v2c community string and a source IP or network address to a security name (username). This table displays com2Sec entries and provides options to add, edit, or delete items from the table. ◆ Click **Add** to add an entry to the com2sec table. Enter the details as shown below. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table.
Security Name	Username specifies the security name to which this source and community string are to be mapped. Security name can contain alphanumeric characters, dash, underscore, or period. No spaces or other special characters allowed.
Source	Source can be one of the following: ◆ restricted source – a specific hostname or address ◆ subnet – represented as IP/Mask (10.10.10.10/255.255.255.0) or IP in CIDR notation (10.10.10.10/8) or the IPv6 equivalents ◆ global – use “default” ◆ localhost – use “localhost” or 127.0.0.1
Community	Specifies the community (user credential) to use for SNMP requests. The same community string can be specified in separate com2sec directives.
Group Configuration	
Group Configuration	The group directive maps a security name in the specified security model (see *Table 10-25 on page 142*) into a named group. This table displays groups and provides options to add, edit, or delete items from the table. ◆ Click **Add** to add an entry to the group table. Enter the details as shown below. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table. ***Note:*** ➢ Several group directives can specify the same group name, allowing a single access setting to apply to several users and/or community strings. ➢ All members of one group have the same access rights. ➢ A user cannot belong to more than one group for each of the security models. ➢ Groups must be set up for the community-based models separately. You would typically create two group directives for a single com2sec directive, one for v1 and one for v2c.
Group Name	Group name can contain alphanumeric characters, dash, underscore, or period. No spaces or other special characters allowed.

Parameters	Description
Version	◆ v1 ◆ v2c ◆ usm
Security Name	Security name should be one of the security names defined in the com2sec configuration.
Access Configuration	
Access Configuration	The access directive maps a group name to an access level (noauth, auth, or priv) and read/write/notify scope for a specified security model (v1, v2c, v3/usm, or any). The table displays access entries and provides options to add, edit, or delete items from the table. ◆ Click **Add** to add an entry to the access table. Enter the details as shown below. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table.
Group Name	Group name should be one of the group names defined in Group configuration.
Context	Default context is the empty string “”, which equates to “none”. For v1 or v2c, context will be empty (“none”).
Version	◆ v1 ◆ v2c ◆ usm ◆ any This value should match the SNMP version of clients that will connect to this agent.
Level	◆ noauth ◆ auth – (authNoPriv) use strong authentication ◆ priv – (authPriv) use strong authentication and encryption For v1 or v2c, set the level to noauth. For usm, set the level to at least the minimum level required. The SNMPv3–USM security level must be configured to this level or higher.
Match	Specifies how the context should be matched against the context of the incoming request. ◆ exact – context name must match exactly (default) ◆ prefix – only the first part of the context name must match
Read	Specifies the view to be used for GET requests. ◆ unspecified – if left unspecified, it will be treated as none - no access ◆ none – no access ◆ custom – name of the view from the view table
Write	Specifies the view to be used for SET requests. ◆ unspecified – if left unspecified, it will be treated as none - no access ◆ none – no access ◆ custom – name of the view from the view table
Notify	Specifies the view to be used for TRAP/INFORM requests. ◆ unspecified – if left unspecified, it will be treated as none - no access ◆ none – no access ◆ custom – name of the view from the view table
View	

Parameters	Description
View	Creates a named view, which determines what part of the MIB the access control is applied to. The table displays view entries and provides options to add, edit, or delete items from the table. ◆ Click **Add** to add an entry to the view table. Enter the details as shown below. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table.
View Name	View name can contain alphanumeric characters, dash, underscore, or period. No spaces or other special characters allowed.
Type	Specifies whether to include or exclude the elements of the subtree from the MIB view. ◆ included – the MIB view includes all the elements of the subtree ◆ excluded – the MIB view excludes all the elements of the subtree
OID	The OID defining the root of the subtree to include or exclude from the named view.
Mask (optional)	List of hex octets optionally separated by '.' or ':' with the set bits indicating which subidentifiers in the view OID to match against. Recommended to ignore this field.

Table 10-28 SNMP VACM Settings Engine ID Configuration

Parameters	Description
Engine ID Configuration	EngineID is required to respond to SNMPv3 requests. This ID is determined automatically, but can be configured manually. The string must be consistent through time and should not change or conflict with another agent's engineID. For this reason, it is recommended that you use the default values unless you know what you are doing.
Enable	Enables the engineID.
engineID	Specifies that the engineID should be built from the given text string. Default: lantronix
engineIDType	Specifies that the engineID should be built from given type. Type 1 – IPv4 address Type 2 – IPv6 address Type 3 – MAC address (default)
engineIDNic	Specifies that the engineID should use the following interface when determining the MAC address. Only required if engineIDType 3 is specified. Default: eth0

Table 10-29 SNMP VACM Settings SNMPv3-USM

Parameters	Description
SNMPv3 with USM Configuration	Create one or more SNMPv3 users. The table displays SNMPv3 with USM users and provides options to add, edit, or delete items from the table. ◆ Click **Add** to add an entry to the table. Enter the details as shown below. ◆ Click **Edit** to modify an entry. ◆ Click **Delete** to delete an entry from the table.
User Name	Map the security name from the VACM com2sec table here.
Security Level	Security level can be: ◆ NoAuth,NoPriv – no authentication or privacy protocol ◆ Auth,NoPriv – has authentication (MD5|SHA), no privacy protocol ◆ Auth,Priv – has authentication (MD5|SHA), and has privacy protocol (DES|AES).
Auth Protocol	Select the authentication protocol. ◆ MD5 ◆ SHA SHA authentication requires SSL.
Auth Password	Enter the MD5 or SHA passphrase to use for authentication. The passphrase must be at least 8 characters.
Priv Protocol	Select the privacy protocol. ◆ DES ◆ AES DES and AES require SSL.
Priv Password	Enter the privacy protocol passphrase. The passphrase must be at least 8 characters.

Table 10-30 SNMP Trap Settings Configuration

Parameters	Description
Enable	
Authentication Failure Trap Enable	If enabled, generates authentication failure traps. This is disabled by default.
Enable Default Monitors	Monitors the UCD-SNMP-MIB tables for problems. The monitored events (process, load, disk usage, log file) should first be configured on the General Settings page. By default, the agent will check the default monitors once on startup and then every 10 minutes.
Enable Link Up/Down Notification	Monitors the ifTable for changes in network interfaces link status and generates linkUp or linkDown notifications as appropriate.
Trap Configuration	
Version	Specifies the SNMP version. Can be v1, v2c, or v3. ◆ For v1, community and host are required. ◆ For v2c, type, community, and host are required. ◆ For v3, type, username, security level, and host are required.

Parameters	Description
Type	Select the type as trap or inform. For information about SNMPv3 notification behavior and the difference between traps and informs, see the following tutorial: http://www.net-snmp.org/tutorial/tutorial-5/commands/snmptrap-v3.html To use type inform, the SNMP manager must also support inform messages.
User Name	Username is the SNMP v3 security name, as defined in VACM settings.
Security Level	Security level can be: ◆ NoAuth,NoPriv – no authentication or privacy protocol ◆ Auth,NoPriv – has authentication (MD5|SHA), no privacy protocol ◆ Auth,Priv – has authentication (MD5|SHA), and has privacy protocol (DES|AES). If Auth,NoPriv or Auth,Priv are selected, additionals fields will be displayed. Enter the authentication and privacy protocol details as needed.
Community	Defines the v1 or v2c community string to be used when sending traps.
Host	Defines the IP address and port that the trap should be sent to. Typically, this could be localhost:162 or the IP and port of the SNMP manager. The well known SNMP Trap port is port 162.

SNMPTRAPD

Services > SNMPD TRAPD

The SNMP-TRAP application listens for incoming SNMP notifications. When it receives a notification, it can log the notification, pass the details to a handler program, or forward the trap to another notification receiver.

SNMP-TRAP Configuration

To configure SNMP-TRAP settings:

1. Go to Services > SNMPTRAPD.
2. Enter the configuration settings. See *Table 10-31*.
   - Logging – Notifications can be written to the syslog or to a file path on the gateway.
   - Notification processing – notifications can sent to a notification handler or to a notifications receiver.
3. Under General, select **Enable** if it is not already selected.
4. Click **Save & Apply**.

Table 10-31 SNMP-Trap Receiver Configuration

Parameters	Description
General	
Enable	Enables the SNMPTRAP application.
Ignore Authorization Failure	Select to ignore authentication failure traps.
SNMP-TRAP daemon configuration	
Version	Specifies the SNMP version. Can be v1, v2c, or v3. ◆ For v1, community and host are required. ◆ For v2c, type, community, and host are required. ◆ For v3, type, username, security level, and host are required.
Community	Specifies the community used for v1 and v2c authorization. Notifications using the specified community will be allowed to be processed per the notification handling configuration.
User Name	Enter the SNMP v3 username, as defined in VACM settings.
Type	Select the type as trap or inform. For information about SNMPv3 notification behavior and the difference between traps (unacknowledged) and informs (acknowledged), see the following tutorial: http://www.net-snmp.org/tutorial/tutorial-5/commands/snmptrap-v3.html
EngineID	Specifies the EngineID value. For use only with SNMPv3 traps.

Parameters	Description
Security Level	Security level can be: ◆ NoAuth,NoPriv – no authentication or privacy protocol ◆ Auth,NoPriv – has authentication (MD5|SHA), no privacy protocol ◆ Auth,Priv – has authentication (MD5|SHA), and has privacy protocol (DES|AES). Enter the authentication and privacy protocol type and passphrase as appropriate for the selection.
Source	Used for v1 and v2c authorization. The source field specifies that the configuration should only apply to notifications received from the listed sources.
OID	Specifies the OID defining the root of the subtree to add to or exclude from the named view.
Logging Configuration	
Log	Enables log.
Logging Location	Specifies where to log the notifications, either to a local file on the gateway or to the syslog. Select one: ◆ Specific file – enter the file path. ◆ syslog
Format1	Specify the format used to display SNMPv1 traps. If no format is defined, the default Net-SNMP format will be provided. For information about the format specification, see http://www.net-snmp.org/docs/man/snmptrapd.html.
Format2	Specify the format used to display SNMPv2c and SNMPv3 traps. SNMP v2c and v3 use the same PDU format. If no format is defined, the default Net-SNMP format will be provided. For information about the format specification, see http://www.net-snmp.org/docs/man/snmptrapd.html.
Notifications Handling	
Execute	Pass the details of the trap to a specified handler program.
Execute OID	Invokes the specified program with the given arguments whenever a notification is received that matches the OID token. For SNMPv2c and SNMPv3 notifications, this token will be compared against the snmpTrapOID value taken from the notification. For SNMPv1 traps, the generic and specific trap values and the enterprise OID will be converted to the equivalent OID per RFC 2576. If the OID field is the token default then the program will be invoked for any notification not matching another OID-specific traphandle entry.
Program	Program name with path specified followed by a space separated arguments if any. For example, /usr/bin/xyz 1 2 3
Net	Forward the trap to another notification receiver ***Note:*** *Do not use this directive for SNMPv3.*
Net OID	See description for Execute OID above.
Destination	Forwards notifications that match the specified OID to another receiver.

uHTTPd

Services > uHTTPd

uHTTPd is the web server that runs the web interface. It supports multiple instances such as multiple listening ports each with its own document root directory, TLS (SSL), and other web server features.

Web Server Configuration

The web server configuration has two sections, one for server settings and the other for default values for SSL certificates. The uHTTPd Main instance is provided by default and is used for configuring the gateway.

To configure the HTTP/S server:

1. Go to Services > uhttpd.
2. Edit the configuration settings for the gateway. See *Table 10-32*.
3. If you upload a new X.509 certificate and private key in the general web server settings, you will need to configure the uHTTPd Self-signed Certificate Parameters section. See *Table 10-33*.
4. Click **Save & Apply**.

Note: *If you want to create a new server instance, go to the bottom of the Main instance (on the General Settings tab), enter a name and click **Add**. For configuration details, see Table 10-32.*

Table 10-32 uHTTPd Server Configuration

Parameters	Description
General Settings	
HTTP listeners (address:port)	Either HTTP listener or HTTPS listener is required. Enter the ports and addresses to listen on for HTTP access. Use 0.0.0.0/[::] to bind to all devices present. Enter a specific IP address to restrict binding to a specific interface.
HTTPS listener (address: port)	Either HTTP listener or HTTPS listener is required. Enter the ports and addresses to listen on for HTTPS access. Use 0.0.0.0/[::] to bind to all devices present. Enter a specific IP address to restrict binding to a specific interface.
Redirect all HTTP to HTTPS	Select this option to redirect all HTTP to HTTPS.
Ignore private IPs on public interface	Select to ignore requests from private IP addresses (RFC1918) directed to the server's public IPs. The default setting is to ignore the requests from private IPs.
HTTPS Certificate (DER Encoded)	Upload the HTTPS cert file. Click the icon to expand the directory structure (from root).
HTTPS Private Key (DER Encoded)	Upload the HTTPS private key file. Click the icon to expand the directory structure (from root).
Remove old certificate and key	Click to remove old certificate and key files
Remove configuration for certificate and key	Click to remove the cert, key, and configuration information.

Parameters	Description
Full Web Server Settings	
Index page(s)	Enter the index file to use for directories. Usually index.html or index.php.
CGI filetype handler	Enter the interpreter to associate with file endings in the cgi scripts directory.
Do not follow symlinks outside document root	If selected, the HTTP/HTTPS server will not follow symbolic links outside the document root.
Do not generate directory listings	If selected, the HTTP/HTTPS server will not generate directory listings.
Aliases	Maps URL to filesystem locations outside the document root. The format should be /old/path=/new/path
Realm for Basic Auth	Enter the realm for basic authentication when prompting the client for credentials. The default is "Lantronix", which is the local hostname.
Config file (e.g. for credentials for Basic Auth)	Enter the path of the configuration file for credentials for basic authentication and additional settings. The server will not use HTTP authentication if this field is blank.
404 Error	Enter the virtual URL of file or CGI script to handle 404 (file not found) request. It must begin with a forward slash '/'.
Advanced Settings	
Document root	Enter the directory path to the server document root. By default the document root is /www.
Path prefix for CGI scripts	Enter the prefix for CGI scripts, relative to the document root. Leave it blank to disable CGI support.
Virtual path prefix for Lua scripts	Enter the prefix for sending requests to the embedded Lua interpreter, relative to the document root. Leave it blank to disable Lua support.
Full real path to handler for Lua scripts	Enter the full path to the Lua handler script to initialize Lua runtime on server start. This field is required if Lua prefix is given, otherwise it's optional.
Virtual path prefix for ubus via JSON-RPC integration	Enter the URL prefix for ubus via JSON-RPC handler, relative to the document root. Leave it blank to disable UBUS.
Override path for ubus socket	Enter the override ubus socket path
Enable JSON-RPC Cross-Origin Resource Support	Select to enable CORS HTTP headers on JSON-RPC API. By default, this setting is disabled.
Disable JSON-RPC authorization via ubus session API	If selected, do not authenticate JSON-RPC requests against the UBUS session API. By default the requests are authenticated.
Maximum wait time for Lua, CGI, or ubus execution	Enter the maximum wait time for CGI, Lua or ubus requests in seconds. If no output is generated within the timeout period, the requested executables are terminated. Default is 60 seconds.
Maximum wait time for network activity	Enter the maximum wait time for network activity. If no network activity occurs within the timeout period, the requested executables are terminated and the connection is shut down. Default is 30 seconds.
Connection reuse	Sets the time limit for connection reuse.

Parameters	Description
TCP Keepalive	Number of unanswered keep alive requests allowed. Default: 1
Maximum number of connections	Enter the maximum number of concurrent connections allowed. If the limit is reached, further TCP connection attempts are queued until the number of connections is below the limit. Default: 100
Maximum number of script requests	Enter the maximum number of concurrent requests. If the limit is reached, further requests are queued until the number of requests drops below the limit. Default: 6
Maximum wait time for rpc timeout in seconds per requests	Enter the maximum wait time for RPC timeout in seconds. Default: 55

Self-Signed SSL Certificate Parameters

uHTTPd requires an X.509 certificate and private key. This has been configured for the Main instance. You only need to configure this section if you choose to upload a new certificate and private key.

Table 10-33 uHTTPd Self-signed Certificate Configuration

Parameters	Description
uHTTPd Self-signed Certificate Parameters	
Valid for # of Days	Enter the validity time (number of days) of the generated certificate. Default: 730 days
Length of key in bits	Enter the length of the generated RSA key in bits Default: 2048
Server hostname	Enter the server hostname covered by the certificate. Default: Lantronix
Country	Country of the certificate issuer
State	State of the certificate issuer
Location	Location/city of the certificate issuer

Versatile IOs

Services > Versatile IOs

The Versatile Input/Output (V IO)

The device provides two Versatile IOs (Versatile #1 and Versatile #2) that can function as analog input or digital output. These map to the two hardware IOs, labeled as Digital IO and Versatile IO. Each IO has a common ground, with 3-pin COMBICON header and plug. Each I/O is independently user-configurable as analog input (user can supply 0V to 3.3V DC) or digital output.

To configure the versatile IOs:

1. Go to Services > Versatile IOs. Versatile #1 is selected.
2. Select the IO pin to be configured, Versatile #1 or Versatile #2.
3. Edit the configuration settings. See *Table 10-34*.
4. Click **Save & Apply**.

Table 10-34 Versatile IOs Configuration

Parameters	Description
Mode	Select the mode. Analog - for analog input. When 0V to 3V voltage is applied, the status is updated. Digital - for digital output.
State	If Digital mode is selected, ON - close OFF - open

11: Industrial Protocols

The G526RP Transportation pack gateways support a range of industrial protocols used in process automation systems and other automation purposes.

The gateways support the following industrial protocols:

- DLMS client
- EtherCAT
- DNP3
- IEC 101
- IEC 104
- Modbus Master

Industrial Protocol Converters

The gateways support the following protocol conversion:

- Modbus RTU to Modbus TCP
- Modbus RTU to DNP3
- Modbus to DNP3
- IEC 101 to IEC 104
- IEC 104 to IEC 104 Multimaster

Data Send Applications

The gateways support the following data send applications:

- Modbus Master to FTP
- Modbus Master to HTTP
- Modbus Master to Cumulocity
- Modbus Master to MQTT
- Modbus Master to MQTTS
- Modbus Master to Azure
- DLMS to FTP
- IEC 104 to MQTT

DLMS Client

Services > DLMS Client

The gateway acts as a DLMS client that communicates with the DLMS meter. The DLMS client is the master and the smart meter is the slave device. The DLMS client has the following functionality:

- DLMS client queries information from DLMS meter. The queried information includes instantaneous, load, billing, and event profile data. The data collected is based on the COSEM specification and the device capability of the meter.
- DLMS client stores queried information in a file in CSV format.
- DLMS client sends the CSV file to FTP.
- DLMS is available on both RS-232 and RS-485 serial interfaces.

To configure the DLMS client:

1. Go to Services > DLMS Client.
2. Click **Enable** to enable the DLMS client on the gateway.
3. Under DLMS Configuration, enter the configuration information. See *Table 11-1*.

Table 11-1 DLMS Client Configuration

Parameters	Description
Enable	Click to enable the DLMS client.
DLMS meter make	Secure Meters option is selected. The Secure meter default password is used by the back end. The option Others may be available. If selected, enter the meter password.
Client address	Enter the DLMS client address. The length is 8 bits.
Server address	Enter the DLMS server address.
Instantaneous profile read time	Enter the time interval in minutes that the instantaneous profile data will be read
Billing profile read time	Enter the time interval in minutes that the billing profile data will be read.
Load profile recording period 1 read time	Enter the time interval in minutes that the load profile for recording period 1 will be read.
Duration for load profile recording period 1	Select the duration in months of the load profile recording period.
Load profile recording period 2 read time	Enter the time interval in minutes that the load profile for recording period 2 will be read.
Event profile read time	Enter the time interval in minutes that the event profile data will be read.

4. Under Data Send Configuration, enter the FTP server settings where the client will send the information. See *Table 11-2*.

Table 11-2 DLMS Data Send Configuration

Parameters	Description
Protocol	FTP

Parameters	Description
IP/URL	IP address or URL of the FTP server
Port	21
Username	Username of the FTP server
Password	Password of the FTP server
Path	File path of the FTP server where the CSV file will be saved
File name	File name of the CSV file

5. Click **Save & Apply**.
6. Configure the Serial 1 (RS-232) or Serial 2 (RS-485) line mode to DLMS client.
7. Click **Save & Apply**.

EtherCAT

Services > EtherCAT

The gateway can act as an EtherCAT master for bidirectional communication with an EtherCAT slave device.

Note: *The EtherCAT application is not included with the default firmware. To use it, create it as a custom package (.ipk) using the SDK. The package can be included in a custom firmware image build or installed as a software package. For details on how to create a software package using the SDK, please refer to the G520 Series SDK Application Note.*

Note: *The EtherCAT protocol and master application will run on the Ethernet WAN interface.*

To configure the EtherCAT master application:

1. Go to Services > EtherCAT.
2. Under Status, view the status of the EtherCAT master application.
3. Under Configuration, select the checkbox next to Enable to enable EtherCAT master application, or clear it to disable EtherCAT.
4. Click **Save & Apply**.

IEC 104 to MQTT

Services > IEC 104 MQTT

The gateway supports the IEC 104 protocol to monitor remote devices. The IEC 104 master reads the data from the IEC 104 slave device over Ethernet. The data is then communicated via MQTT protocol to the MQTT subscriber.

IEC 104 MQTT Configuration

To configure IEC 104 MQTT:

1. Go to Services > IEC 104 MQTT. The Configuration page displays.
2. Select **Enable** to enable IEC 104 MQTT.
3. Enter a location for **Database Path**. This location stores the data collected by IEC 104 master from IEC 104 slave. The default location is /tmp.

Note: *The data stored in /tmp will be lost during device reboot.*

4. Upload the IEC 104 MQTT configuration file (CSV formatted file) to /etc/luci-uploads folder on the gateway. Click **Select file** and then click **Upload file**. Browse and select the required file. Click **Upload file** to start upload. Once the file is uploaded click the file to select it.
5. Click **Save & Apply** to save the configuration and start the service.

To view the IEC 104 MQTT configuration file currently in use:

1. Click **Download** tab, the Download page displays
2. Click **Submit**, the configuration file begins to download.

IEC 104 to IEC 104 Multimaster

Services > IEC 104 MQTT

The gateway supports the IEC 104 protocol to monitor remote devices. The IEC 104 master reads the data from the IEC 104 slave device over Ethernet. The data is then communicated to multiple IEC 104 masters.

IEC 104 Multimaster Configuration

To configure IEC 104 Multimster:

1. Go to Services > IEC 104 MQTT. The Configuration page displays.
2. Select **Enable** to enable IEC 104 Multimaster.
3. Enter a location for **Database Path**. This location stores the data collected by IEC 104 master from IEC 104 slave. The default location is /tmp.

Note: *The data stored in /tmp will be lost during device reboot.*

4. Upload the IEC 104 Multimaster configuration file (CSV formatted file) to /etc/luci-uploads folder on the gateway. Click **Select file** and then click **Upload file**. Browse and select the required file. Click **Upload file** to start upload. Once the file is uploaded click the file to select it.
5. Click **Save & Apply** to save the configuration and start the service.

To view the IEC 104 Multimaster configuration file currently in use:

1. Click **Download** tab, the Download page displays
2. Click **Submit**, the configuration file begins to download.

IEC 101 to 104

Services > IEC 101 to 104

The gateway supports protocol conversion from IEC 60870-5-101 (IEC 101) to IEC 60870-5-104 (IEC 104). IEC 101 master is available on both RS232 and RS485 interfaces.

To use this feature, configure both IEC 101 to 104 service and serial interface (RS232 or RS485).

To configure IEC-101 to 104:

1. Go to Services > IEC 101 to 104.
2. Select **Enable** to enable the IEC 101 to 104 service.
3. Under IEC 101 Slave Configuration, enter the information for the IEC 101 slave device. See *Table 11-3*.

Table 11-3 IEC 101 Slave Configuration

Parameters	Description
ASDU Address	Enter the ASDU address. The Application Service Data Unit (ASDU) is the data structure that holds application layer information to exchange between a control center and a remote terminal unit. If Unbalanced mode is selected, enter addresses separated by a comma.
Link Address	Enter the address of the end device. If Unbalanced mode (polling is used) is selected, enter addresses separated by a comma. All connected devices on the line receive the telegram and the addressed device responds using its own address as the link address.
ASDU Address size	Enter the address size as one or two octets (bytes)
COT size	Enter the Cause of Transmission (COT) size as one or two octets.
IOA address size	Enter the Information object address (IOA) size as one, two or three octets.
Link Address size	Enter the link address size as one or two octets or not present.
Link Transmission Procedure	Defines the control information for IEC 101. Select one of the following options: ◆ Balanced mode for point-to-point operation ◆ Unbalanced mode for polling operations to multiple targets

4. Under IEC 104 Master Configuration, enter the information for the IEC 104 master (control center). See *Table 11-4*.

Table 11-4 IEC-104 Master Configuration

Parameters	Description
ASDU Address	Enter the ASDU address.
COT size	Enter the COT size as one or two octets.
Time out T1	Enter the timeout for T1 in milliseconds
Time out T2	Enter the timeout for T2 in milliseconds
Time out T3	Enter the timeout for T3 in milliseconds

Parameters	Description
Type	Select the interface that the IEC 104 master listens on. Internal – listens on LAN. Select IP and enter port. External – listens on WAN/WiFi/Cellular with automatic fallback
IP	IP address of the IEC 104 master (control center). Select the LAN IP address of the gateway or enter a custom IP address.
Port	Enter the TCP port number of the IEC 104 master device. The default IEC 104 TCP port is 2404.

5. Click **Save & Apply**.

To configure the serial interface:

1. Go to Serial > Serial 1 (RS232) or Serial 2 (RS485).
2. Configure the serial communication settings to match the serial configuration of the IEC 101 slave.
3. Select the mode as **IEC 101 to 104**.
4. Click **Save & Apply**.

Modbus Master

Services > Modbus Master

Modbus Master configures the gateway as a master device that connects to slave devices. It supports Modbus RTU through a serial line or Modbus TCP through a TCP/IP network.

Modbus RTU based serial slave devices can also be connected via Ethernet through an existing Modbus TCP/IP network. Any device having access to a given Modbus implementation will be able to perform the full range of operations that the implementation supports.

The gateway can be configured to communicate through a tunnel using Modbus RTU to Modbus TCP conversion mode. For details, please see *Tunnel Modbus RTU to Modbus TCP*.

Serial Transmission Mode

The gateway can be configured to communicate on Modbus networks using RTU. *Table 11-5* shows the standard Modbus RTU packet data structure. Modbus RTU can use either the RS232 or the RS485 interface.

To use Modbus on the serial line, configure the Modbus master settings, the Serial port communication parameters, and the mode for the desired serial interface.

Table 11-5 Modbus RTU Packet Data Structure

Section	Description
Slave Address	8 bits (0 to 247 decimal, 0 is used for broadcast)
Function Code	8 bits (1 to 255, 0 is not valid)
Data	N X 8 bits (N=0 to 252 bytes)

CRC Check	16 bits

Ethernet Transmission Mode

The gateway can be set up to communicate on Modbus networks using TCP/IP. *Table 11-6* shows the structure of the Modbus application protocol header. This header is added to the start of each Modbus message and the slave address and CRC are removed. Modbus TCP uses a TCP port of 502 and includes a single byte function code (1=255) preceded by a 6 byte header:

To use Modbus using TCP/IP, configure the Modbus master settings on the gateway. Separately, configure the Modbus slave settings on the Modbus TCP device.

Table 11-6 Modbus Application Protocol Byte Header

Section	Size	Description
Transaction ID	2 bytes	Identification of request/response transaction – copied by slave
Protocol ID	2 bytes	0 – Modbus protocol
Length	2 bytes	Number of following bytes includes the unit identifier
Address	1 byte	Identification of remote slave

Modbus Master Configuration

Configure the Modbus master settings, enable or disable the Modbus master, and view the status of active Modbus connections. When a connection is active, the remote client information is displayed as well as the number of protocol data units (PDUs) that have been sent and received.

Note: *Generate the Modbus Master configuration file using the Modbus Configuration Utility at: https://modbus.d2sphere.com. The configuration file includes: target server where the data will be reported, FTP, HTTP, Cumulocity, MQTT, MQTTS, and Azure; Modbus logger details; up to 6 polling groups, and up to 5 upload groups.*

To configure Modbus master:

1. Go to Services > Modbus Master.
2. Click the Configuration tab.
3. Enter the configuration settings. See *Table 11-7*.
4. Click **Save & Apply**.

Table 11-7 Modbus Master Configuration

Field	Description
Enable	Click to enable Modbus Master on the selected interface.
Interface	Select the interface that Modbus will communicate over. ◆ Serial 1/TCP – Modbus RTU on RS232 interface ◆ Serial 2/TCP – Modbus RTU on RS485 interface ◆ TCP – Modbus TCP on TCP/IP interface. LAN recommended.

Field	Description
Upload Configuration File	Upload and select the Modbus configuration file (CSV formatted file). This file contains all the configuration for the Modbus server. Generate the Modbus configuration file using the Modbus Configuration Utility. Click **Select file...** to select the Modbus configuration file. Then click **Upload file** to upload the file to the /etc folder on the gateway. Then select the file from the file list. After it's selected, it will appear next to the field "Upload Configuration File".

Data Window

This page shows data by polling group. The polling groups are defined in the Modbus configuration file.

1. Click **Enable Data Window** to allow data to be read from the data window. This enables data logging for 5 minutes.
2. Select the polling group number and click **Show Data** to display the data for the specified polling group.

Modbus Download

This page allows you to download the Modbus configuration file from the file system.

Click **Download** to download the Modbus configuration file. The file is downloaded, or a message is displayed if there is no Modbus configuration file found.

Modbus RTU to DNP3

Services > Modbus RTU to DNP3

The gateway acts as a DNP3 outstation. DNP3 is an open standard communication protocol used in many SCADA environments. On the gateway, DNP3 has the following functionality:

- DNP3 serial to DNP3 over TCP by tunneling. DNP3 master communicates with DNP3 outstation using tunnel over RS-232 or RS-485. For configuration, see *Serial Line Configuration on page 230*.
- Modbus RTU to DNP3 conversion. The gateway facilitates the DNP3 master (DNP3 SCADA) to connect and monitor the Modbus RTU device connected over RS-232 or RS-485.

Configure DNP3 Outstation for Modbus RTU to DNP3 conversion

To use this feature, configure the DNP3 outstation, then configure the serial interface (RS-232 or RS-485). The Modbus configuration file must be configured with the DNP3 parameters. For details about modifying the configuration file, see *Modbus Configuration File for DNP3 Outstation*.

To configure the DNP3 outstation:

1. Go to Services > Modbus RTU to DNP3.
2. Select **Enable** to enable DNP3.
3. Under DNP3 Outstation Configuration, enter the DNP3 outstation server and link layer configuration settings. See *Table 11-8*.
4. Under Modbus Master Configuration, upload the Modbus configuration file with DNP3

parameters to the /etc folder. See *Table 11-8*.

5. Click **Save & Apply**.

Table 11-8 DNP3 Outstation and Modbus Master Configuration

Parameters	Description
DNP3 Outstation Configuration	
Protocol	TCP is the selected protocol
Type	Select the interface that the DNP3 server listens on. Internal – listens on LAN. Select IP and enter port. External – listens on WAN/WiFi/Cellular with automatic fallback.
IP	IP address of LAN interface (required if Internal type is selected)
Port	Server listen port
Local DNP3 Address	DNP3 master address ***Note:*** *Ensure that the link-layer local/remote addresses are configured correctly to avoid communication problems. There is no standard default address.*
Remote DNP3 Address	DNP3 remote outstation address
Poll Interval	Enter the poll interval, in seconds.
Modbus Master Configuration	
Upload Configuration File	Upload and select the Modbus configuration file (CSV formatted file). This file contains all the configuration for the Modbus server. Generate the Modbus configuration file using the Modbus Configuration Utility. Click **Select file...** to select the Modbus configuration file. Then click **Upload file** to upload the file to the /etc folder on the gateway. Then select the file from the file list. After it's selected, it will appear next to the field "Upload Configuration File".

To configure the serial interface:

1. Go to Serial > Serial 1 (RS-232) or Serial 2 (RS-485).
2. Configure the serial communication settings.
3. Select the mode as DNP3.
4. Click **Save & Apply**.

Modbus Configuration File for DNP3 Outstation

To configure the Modbus configuration file with DNP3 parameters:

1. Go to Services > Modbus Master.
2. Generate the Modbus Master configuration file using the Modbus Configuration Utility at: https://modbus.d2sphere.com.
3. Open the Modbus configuration file in a text editor, and add the DNP3 parameters to the configuration. For a sample, see the section below,*4. Save the configuration file in CSV format. Sample CSV with DNP3 Parameters*.
4. Save the configuration file in CSV format. Sample CSV with DNP3 Parameters

DNP3 parameters are displayed in blue text.

```
ConfigurationStart,,,,,,,,,,,
ModbusExtraInfoStart,,,,,,,,,,,
NULL,1000,1000,1,12345,,,,,,,
ModbusExtraInfoEnd,,,,,,,,,,,
PollingGroupStart,,,,,,,,,,,
Group1Start,,,,,,,,,,,
Group1,10,1,1,0,0,0,0,,,,
QueryStart,,,,,,,,,,,
Query1,1,3,100,2,NULL,NULL,,,,,
Tag1,0,8,7,1,0,4,NULL,NULL,NULL,0,0,0
Tag2,8,8,7,1,0,4,NULL,NULL,NULL,0,0,0
QueryEnd,,,,,,,,,,,
QueryStart,,,,,,,,,,,
Query2,2,1,100,1,NULL,NULL,,,,,
Tag1,0,1,1,1,0,4,NULL,NULL,NULL,0,0,0
QueryEnd,,,,,,,,,,,
QueryStart,,,,,,,,,,,
Query3,3,3,100,1,NULL,NULL,,,,,
Tag1,0,4,4,1,0,4,NULL,NULL,NULL,0,0,0
QueryEnd,,,,,,,,,,,
Group1End,,,,,,,,,,,
PollingGroupEnd,,,,,,,,,,,
DNP3_MappStart,,,,,,,,,,,
NodeStart,,,,,,,,,,,
5,3,1,12345,0,,,,,,,
Tag1,1,Query1,,,,,,,,,
Tag2,1,Query1,,,,,,,,,
NodeEnd,,,,,,,,,,,
NodeStart,,,,,,,,,,,
2,1,2,12345,0,,,,,,,
Tag1,1,Query2,,,,,,,,,
NodeEnd,,,,,,,,,,,
NodeStart,,,,,,,,,,,
4,1,3,12345,0,,,,,,,
Tag1,1,Query3,,,,,,,,,
NodeEnd,,,,,,,,,,,
DNP3_MappEnd,,,,,,,,,,,
```

Modbus to DNP3

Services > Modbus to DNP3

The gateway acts as a DNP3 outstation. DNP3 is an open standard communication protocol used in many SCADA environments. On the gateway, DNP3 has the following functionality:

- DNP3 serial to DNP3 over TCP by tunneling. DNP3 master communicates with DNP3 outstation using tunnel over RS-232 or RS-485. For configuration, see *Serial Line Configuration on page 230*.
- Modbus to DNP3 conversion. The gateway facilitates the DNP3 master (DNP3 SCADA) to connect and monitor the Modbus RTU/TCP slave device connected via serial or TCP interface.

Configure DNP3 for Modbus to DNP3 conversion

To use this feature, configure the DNP3 outstation, then configure the serial interface (RS-232 or RS-485). The Modbus configuration file must be configured with the DNP3 parameters. For details about modifying the configuration file, see *Modbus Configuration File for DNP3 Outstation*.

To configure the DNP3 outstation:

1. Go to Services > Modbus to DNP3. The DNP3 Configuration page displays.
2. Configure the DNP3 Configuration settings. See *Table 11-9*.
3. Click **Save & Apply**.

Table 11-9 DNP3 Configuration

Parameters	Description
Enable	Select to enable DNP3
Port	Server listen port
Local DNP3 Address	DNP3 master address ***Note:*** *Ensure that the link-layer local/remote addresses are configured correctly to avoid communication problems. There is no standard default address.*
Remote DNP3 Address	DNP3 remote outstation address
Poll Interval	Enter the poll interval, in seconds.

To configure the serial interface:

1. Go to Serial > Serial 1 (RS-232) or Serial 2 (RS-485).
2. Configure the serial communication settings.
3. Select the mode as DNP3.
4. Click **Save & Apply**.

The Modbus configuration file must be configured with the DNP3 parameters. For details about Modbus configuration see *Modbus Master Configuration* and for details about modifying the configuration file, see *Modbus Configuration File for DNP3 Outstation*.

12: Network

This chapter describes the network configuration settings. It contains the following sections:

- *Interfaces*
- *Wireless*
- *DHCP and DNS*
- *Hostnames*
- *Static Routes*
- *Diagnostics*
- *Firewall*
- *PoE*
- *QoS*
- *Load Balancing*

Interfaces

Network > Interfaces

The Interfaces section provides the overview and status of the network interfaces for LAN, WAN, Cellular, and WWAN. It also provides the configuration parameters for each of these interfaces, which allow you to configure or update the interface according to your requirements.

Additionally, you can add new virtual interfaces, such as GRE, L2TP, PPP, or PPtP VPN instances.

The Network Interfaces section contains the following pre-configured interfaces:

- *CELLULAR Interface*
- *LAN Interface*
- *WAN and WAN6 Interface*
- *WWAN and WWAN6 Interface*

Interfaces Overview

Network > Interfaces

Figure 12-1 shows a summary view of the network interfaces and interface status.

Figure 12-1 Interfaces Overview (partial view)

Table 12-1 Network Interfaces Overview

Parameters	Description
Interfaces Overview	
Network	Displays the network name and image representing the interface. *Note: When Wi-Fi is configured as Client, the WWAN interface will become active.*
Status	Displays the status of the interface. See *Interface Status*.
Actions	Select the action to be taken for the interface. ◆ **Restart** – Connects the interface or reconnects the already started interface. ◆ **Stop** – Stops the interface. ◆ **Edit** – Allows you to edit the interface settings. ◆ **Delete** – Deletes the interface. *Note: Default interfaces have predefined configurations and should not be deleted.*
Add new interface	Click **Add new interface** to add a virtual interface. See *Add Virtual Interface*.
Global Network Options	
IPv6 ULA-Prefix	Displays the IPv6 Unique Local Address (ULA)-Prefix

Parameters	Description
Network Watchdog	
Enable	Select this box to enable or clear the box to disable the network watchdog. The network watchdog monitors the connectivity of all WAN (external network) interfaces. In the absence of connectivity resulting in Network down, the gateway resets itself. By default, the network watchdog is in enabled mode.
Time	If the network watchdog is enabled, enter the watchdog timeout in minutes.
Wan as Lan	
Enable	Select the box to enable the WAN port to act as a LAN interface. This will provide two LAN interfaces on the gateway.

Interface Status

Figure 12-2 WAN Interface Status

Table 12-2 Wireless Overview and Associated Stations

Parameters	Description
Protocol	Protocol assigned to the interface
Uptime	Amount of time that the interface has been active since the last reconnection.
MAC Address	MAC address of the physical interface. ***Note:*** *MAC address is displayed for LAN, WAN, WWAN, and OpenVPN interfaces.*
RX	Number of received bytes over the interface for the current session.
TX	Number of transmitted bytes over the interface for the current session.
IPv4	IPv4 address
IPv6	IPv6 address

Interface Protocols

The protocol assigned to each interface defines rules for exchanging information on the interface. *Table 12-3* shows the available protocol options for each of the interfaces. When configuring an interface, please make sure that the protocol selection is appropriate for the interface.

Legend: ✓ = protocol can be assigned ✗ = protocol should not be assigned

Table 12-3 Network Interface Protocols

Interface Protocols	LAN	WAN	WWAN	Cellular
Static Address	✓	✓	✓	✗
DHCP client	✗	✓	✓	✗
DHCPv6 client	✗	✓	✓	✗
GRE	✗	✗	✗	✗
L2TP	✗	✗	✗	✗
WireGuard VPN	✗	✗	✗	✗
Unmanaged	✓	✓	✓	✗
PPP	✗	✗	✗	✗
PPPoE	✗	✓	✗	✗
PPtP	✗	✗	✗	✗
Cellular	✗	✗	✗	✓
QMI Cellular	✗	✗	✗	✓
Relay Bridge	✗	✗	✗	✗
464XLAT (CLAT)	✗	✗	✗	✓

The interface configuration involves selection or configuration of other settings such as default gateway, gateway metric, DHCP server, and firewall zone to name a few. These settings may or may not be used by the interface; the interface configuration depends on both the protocol selected as well as the network requirements. For descriptions of the protocols used with the LAN, WAN, WWAN, and Cellular interfaces, see the next section, *Protocol Descriptions*.

Many other protocols listed in *Table 12-3* are used for VPN connections. This includes GRE, L2TP, WireGuard VPN, and PPtP. For details about VPN protocol configuration, see *Add Virtual Interface*.

The interfaces can be set to Unmanaged, if no protocol is desired. This setting may be used to enumerate an interface for firewall purposes.

Protocol Descriptions

Static Address

Table 12-4 describes the Static Address protocol settings.

Table 12-4 Static Address Protocol Settings

Parameters	Description
General Settings	
Protocol	Static Address – Static configuration with fixed address and netmask
Bring up on boot	Allows the interface to be live after every reboot. Bring up on boot is checked by default.
IPv4 Address	Enter the IPv4 Address. This IP Address must be used to access the gateway. The default LAN IP Address is 198.162.1.1.
IPv4 Netmask	Select the IPv4 Netmask.
IPv4 Gateway	Enter the IPv4 address for gateway.
IPv4 broadcast	Enter the IPv4 address for broadcast.
Use Custom DNS servers	Enter the IP address of the custom DNS server. Click the + button to add more DNS servers.
IPv6 assignment length	Select the IPv6 assignment length. Available Options ◆ 64 or 60 – Assign a part of the given length of public IPv6-prefix to this interface. ◆ disabled – do not assign part of the prefix to this interface ◆ --custom-- – Assign a part of the given length of public IPv6-prefix to this interface. IPv6 assignment length is disabled by default. If assignment length is disabled, enter the following: ◆ IPv6 address – Enter the IPv6 Address. ◆ IPv6 gateway – Enter the IPv6 Address for Gateway. ◆ IPv6 routed prefix – Enter the public prefix to direct the client distribution to the gateway. If assignment length is 60, 64, or custom, enter the following: ◆ IPv6 assignment hint –Enter hexacimal subprefix ID for this instance to assign prefix parts. ◆ IPv6 suffix – Enter the IPv6 suffix.
Advanced Settings	
Use builtin IPv6 -management	Allows to use the built in IPv6 management configuration.
Force link	Select this option to assign interface properties regardless of the link being active or not. If not selected, items are assigned only after the link has become active. Default is not selected.
Override MAC address	Click to override the default MAC Address for the WAN Interface. On factory reset, it will be set to default MAC address.

Parameters	Description
Override MTU	Enter the number of bytes indicating the largest physical packet size that the network can transmit. The default MTU size is 1500 bytes. Blank value represents auto MTU size
Use gateway metric	Enter the gateway metric. It ensures a separate routing entry for the respective interface in the main routing table. The default metric is 5.
Physical Settings	
Bridge Interfaces	Click to enable creating a bridge over multiple interfaces. ◆ Enable STP – Check to enable the Spanning Tree Protocol over the bridge. ◆ Enable IGMP snooping – Check to enable IGMP snooping on the bridge.
Interface	Select the interface to be configured. Select more than one interface, if parameter creating a bridge over multiple interfaces is enabled.
Firewall Settings	
Create/Assign firewall -zone	Select the firewall zone to be assigned to the interface. Select unspecified – or – create to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box and click Save & Apply button.
DHCP > General Setup **DHCP Server - DHCP Server is used only for LAN interfaces**	
Ignore Interface	Check to disable the DHCP interface. ***Note:*** *If DHCP server is disabled for the interface, all the LAN devices connected to the gateway should have a static LAN IP configured.*
Start	Lowest leased address as offset from the network address. ***Note:*** *If your LAN IP address is 192.168.1.1 and the parameter Start is configured as 100, then the starting IP Address of the leased IP Address range is 192.168.1.100*
Limit	Maximum number of leased addresses that can be configured. Example ◆ If your LAN IP Address is 192.168.1.1, the parameter Start is configured as 100, and parameter Limit is configured as 150, then a total of 150 devices are configured. Thus the leased IP Address range is 192.168.1.100 to 192.168.1.249.
Lease time	Remaining time until the device can use the DHCP server leased IP Address. ***Note:*** *IP address allocated by the gateway will disappear from the Wi-Fi / Overview / Associated stations list only after individual lease time for each IP expires.*
DHCP > Advanced Settings	
Dynamic DHCP	Check to allocate DHCP IP addresses dynamically to the clients. When unchecked, service will be provided only to the clients having the static IP Address.

Parameters	Description
Force	Check to override the current configured Server and use DHCP server.
IPv4-Netmask	Enter the IPv4 netmask. This netmask will override the netmask used by the clients. In normal scenario netmask is calculated from the subnet.
DHCP-Options	Define additional DHCP options Example: ◆ “6,192.168.2.1, 192.168.2.2" which advertises different DNS servers to clients.
DHCP > IPv6 Settings	
Router Advertisement-Service	Select the Router Advertisement-Service mode; disabled, server mode, relay mode, hybrid mode.
DHCPv6-Service	Select the DHCPv6-Service mode; disabled, server mode, relay mode, hybrid mode.
NDP-Proxy	Select the NDP mode; disabled, server mode, relay mode, hybrid mode.
DHCPv6-Mode	Select the DHCPv6-Service mode: ◆ Stateless ◆ Stateful ◆ Stateless + Stateful ◆ Stateful only
Always announce default router	Select to Announce as default router even if no public prefix is available.
Announced DNS servers	Add the DNS servers
Announced DNS domains	Add the DNS domains.

DHCP Client

Table 12-5 describes the DHCP Client protocol settings.

Table 12-5 DHCP Client Protocol Settings

Parameters	Description
General Settings	
Protocol	DHCP client – Address and netmask are assigned by DHCP.
Bring up on boot	Allows the interface to be live after every reboot. Bring up on boot is checked by default.
Hostname to send when requesting DHCP	Hostname of the gateway
Advanced Settings	
Use builtin IPv6 -management	Allows to use the built in IPv6 management configuration.
Force link	Select this option to assign interface properties regardless of the link being active or not. If not selected, items are assigned only after the link has become active. Default is not selected.

Parameters	Description
Use broadcast flag	Check to use the broadcast flag. This flag is generally used by the ISP's.
Use default gateway	Click to configure a default gateway route. None of the gateway routes are configured by default.
Use DNS server advertised by peer	Allows advertising the DNS server address. Use DNS server advertised by peer for WAN interface is checked by default. If unchecked, the advertised DNS server addresses are ignored.
Use gateway metric	Enter the gateway metric. The Load Balancer uses these Metric values to determine priority of a WAN. The default metric is 4.
Client ID to send when requesting DHCP	Enter the Client ID that shall be sent when requesting DHCP.
Vendor Class to send when requesting DHCP	To allocate DHCP IP Addresses based on Vendor Class.
Override MAC address	Click to override the default MAC Address for the WAN Interface. On factory reset, it will be set to default MAC address.
Override MTU	Enter the number of bytes indicating the largest physical packet size that the network can transmit. The default MTU size is 1500 bytes. Blank value represents auto MTU size
Physical Settings	
Bridge Interfaces	Click to enable creating a bridge over multiple interfaces. Enable STP – Check to enable the Spanning Tree Protocol over the bridge. Enable IGMP snooping – Check to enable IGMP snooping on the bridge.
Interface	Select the interface to be configured. Select more than one interface if parameter creating a bridge over multiple interfaces is enabled.
Firewall Settings	
Create/Assign firewall -zone	Select the firewall zone to be assigned to the interface. Select unspecified – or – create to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box and click Save & Apply button.

DHCPv6 Client

Table 12-6 describes the DHCPv6 Client protocol settings.

Table 12-6 DHCPv6 Client Protocol Settings

Parameters	Description
General Settings	
Protocol	DHCPv6 Client – Address and netmask are assigned by DHCP
Bring up on boot	Allows the interface to be live after every reboot. Bring up on boot is checked by default.
Request IPv6-address	Enter the behavior for requesting addresses. Options are try (default), force, and disabled
Request IPv6-prefix of length	Enter the IPv6 address prefix length in bits. Options are: ◆ Unspecified ◆ Automatic (default) ◆ disabled – use if you want single IPv6 address for the AP without a subnet for routing ◆ 48, 52, 56, 60, 64 –hinted prefix length ◆ custom – enter custom prefix length
Advanced Settings	
Use builtin IPv6 -management	Allows to use the built in IPv6 management configuration.
Force link	Select this option to assign interface properties regardless of the link being active or not. If not selected, items are assigned only after the link has become active. Default is not selected.
Use default gateway	Click to configure a default gateway route. None of the gateway routes are configured by default.
Custom delegated IPv6 prefix	Enter the custom IPv6 prefix to be used.
Use DNS server advertised by peer	Allows advertising the DNS server address. Use DNS server advertised by peer for WAN interface is checked by default. If unchecked, the advertised DNS server addresses are ignored.
Client ID to send when requesting DHCP	Enter the Client ID that shall be sent when requesting DHCP.
Override MAC address	Click to override the default MAC Address for the WAN Interface. On factory reset, it will be set to default MAC address.
Override MTU	Enter the number of bytes indicating the largest physical packet size that the network can transmit. The default MTU size is 1500 bytes. Blank value means auto MTU size
Physical Settings	
Bridge Interfaces	Click to enable creating a bridge over multiple interfaces. ◆ Enable STP – Check to enable the Spanning Tree Protocol over the bridge. ◆ Enable IGMP snooping – Check to enable IGMP snooping on the bridge.

Parameters	Description
Interface	Select the interface to be configured. Select more than one interface, if parameter creating a bridge over multiple interfaces is enabled.
Firewall Settings	
Create/Assign firewall -zone	Select the firewall zone to be assigned to the interface. Select unspecified – or – create to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box and click Save & Apply button.

PPPoE

Table 12-7 describes the PPPoE protocol settings.

Table 12-7 PPPoE Protocol Settings

Parameters	
General Settings	
Protocol	PPPoE – Point to Point Protocol over Ethernet
Bring up on boot	Allows the interface to be live after every reboot. Bring up on boot is checked by default.
PAP/CHAP username	Enter the PAP/CHAP username. The default password is admin.
PAP/CHAP password	Enter the PAP/CHAP password.
Access Concentrator	Enter the access concentrator name.
Service Name	Enter the service name. ***Note:*** *Access Concentrator name and Service Name gets auto populated from the PPPoE Access Point router if they are not explicitly provided*
Advanced Settings	
Use builtin IPv6 management	Allows to use the built in IPv6 management configuration
Force link	Select this option to assign interface properties regardless of the link being active or not. If not selected, items are assigned only after the link has become active. This is the default.
Obtain IPv6-Address	Allow IPv6 negotiation on the PPP link
Use default gateway	Select to use the default gateway. If unselected, no default route will be configured.
Use DNS servers advertised by peer	Select to use DNS servers advertised by peer, otherwise ignore advertised DNS servers.
Use gateway metric	Enter gateway metric.
LCP echo failure threshold	Enter the number of LCP echo request failures allowed before considering the peer dead. Set to zero (0) to ignore failures.
LCP echo interval	The LCP echo interval in seconds. LCP echo failure threshold must be set, otherwise this value is ignored.
Host-Uniq tag content	Enter the custom Host-Uniq tag to be used.

Parameters	
Inactivity timeout	Enter the inactivity timeout in seconds, Close the connection if the timeout is reached or enter zero (0) to ignore inactivity timeout.
Override MTU	Enter MTU size in bytes. The default is 1500 bytes.
Physical Settings	
Bridge Interfaces	Click to enable creating a bridge over multiple interfaces. ◆ Enable STP – Check to enable the Spanning Tree Protocol over the bridge. ◆ Enable IGMP snooping – Check to enable IGMP snooping on the bridge.
Interface	Select the interface to be configured. Select more than one interface, if parameter creating a bridge over multiple interfaces is enabled.
Firewall Settings	
Create/Assign firewall -zone	Select the firewall zone to be assigned to the interface. Select unspecified – or – create to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box and click Save & Apply button.

QMI Cellular

Table 12-8 describes the QMI Cellular protocol settings.

Table 12-8 QMI Cellular Protocol Settings

Parameters	Description
General Settings	
Protocol	QMI Cellular – USB modems using QMI protocol
Bring up on boot	Allows the interface to be live after every reboot. Bring up on boot is checked by default.
Enable IP Passthrough	Enables the device connected to its WAN interface, to receive IP address from the cellular network.
Cellular Module	Displays the cellular module name
Modem device	Displays the modem device
PDP Type	Enter the IP stack mode as IPv4, IPv6, or IPv4/IPv6 (dual stack)
Primary SIM	Indicates which SIM is the primary SIM. SIM1 or SIM2
Firmware selection	Allows you to select the firmware that works best with SIM/Network carrier. ◆ Generic - Compatible with most carriers ◆ Automatic - Selects the firmware based on SIM/Network carrier used
Retries	Enter the number of retry attempts to make on the primary SIM before switching to the secondary SIM in case of data connection failures. Default: 5

Parameters	Description
Period after which the router will try and return to primary SIM	Enter the number of minutes after failover to the secondary SIM that the router should wait before attempting to switch back to the primary SIM. Default: 60
Routine switch to secondary SIM	Enter the number of minutes after which the interface should switch from primary to secondary SIM.
Advanced Settings	
Use builtin IPv6 -management	Allows to use the built in IPv6 management configuration.
Force link	Select this option to assign interface properties regardless of the link being active or not. If not selected, items are assigned only after the link has become active. Default is not selected.
Enable IPv6 negotiation	Click to enable IPv6 negotiation on PPP link.
Modem init timeout	Enter the maximum wait time in seconds for the modem to become ready. The default modem initiation timeout 20 seconds.
Default gateway	Click to configure a default gateway route. If unchecked, no default route is configured.
Use gateway metric	Enter the gateway metric. Default is 5
Override MTU	Enter the number of bytes indicating the largest physical packet size that the network can transmit. The default MTU size is 1500 bytes, which is the maximum size. A blank value means use auto MTU size.
Use DNS servers advertised by peer	Click to use DNS servers advertised by peer. If unchecked, the advertised DNS server addresses are ignored.
Firewall Settings	
Create/Assign firewall -zone	Select the firewall zone to be assigned to the interface. Select unspecified – or – custom to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box.
SIM1/SIM2 Settings	
PDP Type	IP stack mode ◆ IP (for IPv4) ◆ IPv6 (for IPv6) ◆ IPv4v6 (for dual-stack)
Service Type	◆ Automatic ◆ NR5G-NSA ◆ NR5G-SA ◆ LTE Only ◆ 3G only

Parameters	Description
Band Selection	◆ Auto - Enables all the supported bands for the cellular module ◆ Manual - Displays all the available bands and allows you to select the required bands. Enables only the selected bands for the cellular module. If you know the band the cellular provider is operating on, selecting that band may help in faster connection.
Use Custom APN	Select to allow gateway to use custom APN.
APN	Enter the APN used for the cellular connection.
PIN	Enter the PIN code to unlock the SIM card
PUK	Enter the PUK (personal unblocking key) used to unblock the SIM card if the PIN code has been repeatedly entered incorrectly
Authentication Type	Enter the authentication method used for the cellular connection. ◆ PAP (requires username and password) ◆ CHAP (requires username and password) ◆ None
Enable roaming	Enable data roaming on the cellular interface
Advanced Configuration	Allows you to view and edit the SIM configuration file. Click to display the SIM configuration file.When switching SIMs or carriers, the CID configuration may get out of sync. For example, if you are using a SIM from carrier 1 but the CID configuration is still set for carrier 2, you can manually update the CID configuration to restore network connectivity.

464XLAT (CLAT)

464XLAT is a simple and scalable technique that allows an IPv4 client with a private address to connect to an IPv4 host over an IPv6 network. This approach is useful for cellular providers that operate with an IPv6-only uplink. The 464XLAT protocol is implemented directly on the device and requires no user interaction or GUI configuration

CELLULAR Interface

Network > Interfaces > CELLULAR

This page allows you to configure the Cellular interface parameters. When the Cellular interface is first enabled or when the gateway is factory reset, the gateway detects the GSM module and assigns the appropriate protocol.

For descriptions of the protocol settings, see *QMI Cellular*.

To edit the interface:

1. Go to Network > Interfaces, select CELLULAR and click **Edit**.

Figure 12-3 Cellular Interface Configuration

2. Configure the interface settings.

Note:

- *General Settings – Protocol should not be changed for the cellular interface.*
- *Firewall Settings – Firewall zone should be set as WAN zone.*
- *SIM1 / SIM2 Settings – Configure the SIM settings according to the SIM slot.*

3. Click **Save**.
4. Click **Save & Apply** to save the configuration on the gateway.

LAN Interface

Network > Interface > LAN

This page allows you to configure the LAN interface. The LAN interface should use Static Address. Gateway may be used but is not required. DHCP server may be used to dynamically assign an IP address to clients connecting to the LAN. If DHCP server is disabled for the interface, all the LAN devices connected to the gateway should have a static LAN IP configured.

DHCP Server

The G520 series gateway can act as the DHCP server and assign IP addresses to devices connecting to the LAN network. The DHCP server maintains a database of available IP addresses and configuration information. When it receives a request from a client, the DHCP server determines the network to which the DHCP client is connected, allocates an IP address or prefix appropriate for the client, and sends configuration information appropriate for that client.

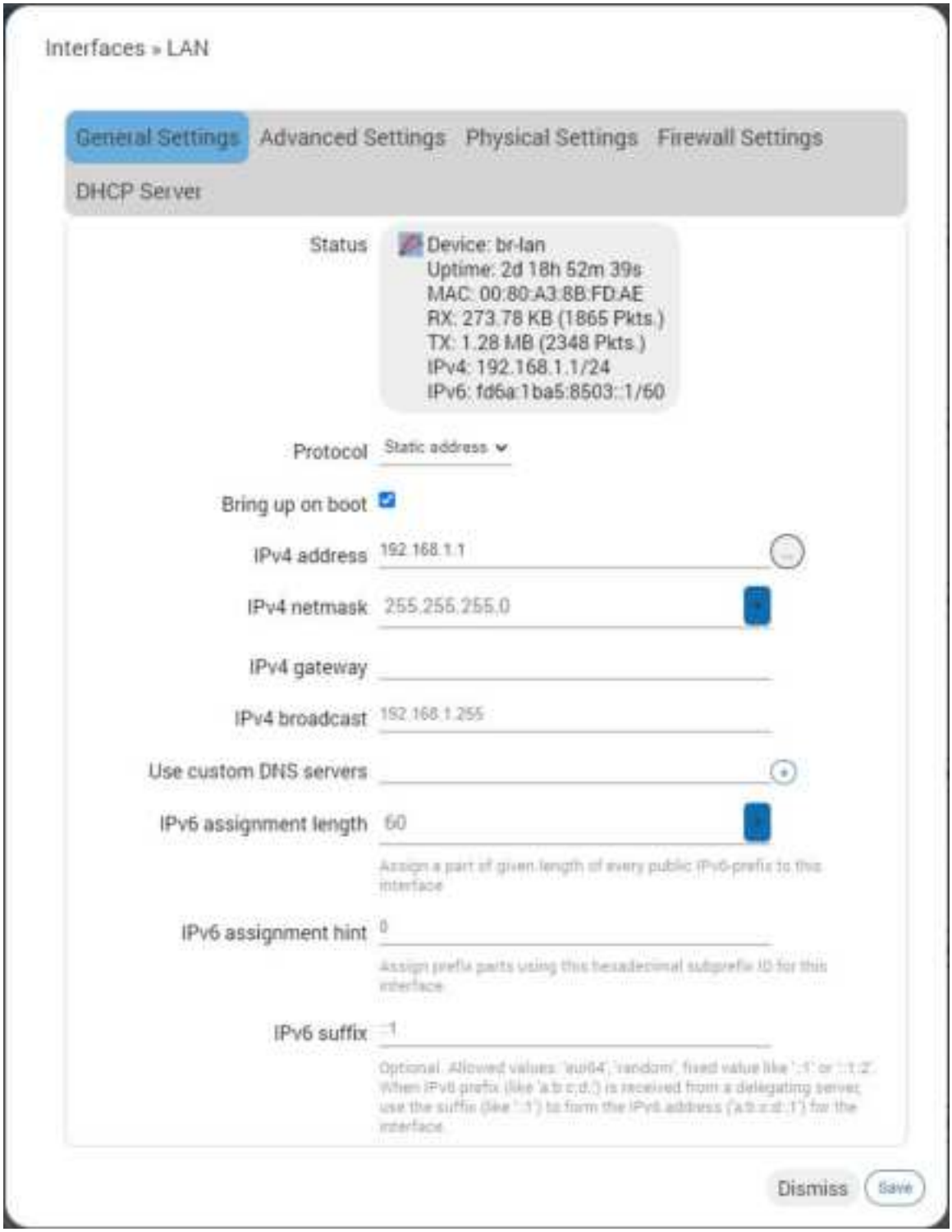
DHCP servers typically grant IP addresses to clients for a limited interval called a lease. DHCP clients are responsible for renewing their IP address before that interval has expired, and must stop using the address once the interval has expired, if they have not been able to renew it. DHCP is used for IPv4 and IPv6. While both versions serve the same purpose, the details of the protocol for IPv4 and IPv6 are sufficiently different that they should be considered separate protocols.

Interface configuration settings are determined mainly by the protocol selection. For a description of the protocol settings, see *Static Address.*

To edit the interface:

1. Go to Network > Interfaces, select LAN and click **Edit**.

Figure 12-4 LAN Interface (Static Address) Configuration



2. Configure the interface settings respective to the gateway model number.
   - For protocol settings, see *Static Address*.

     Note:

- *General Settings – Protocol should be Static Address for the LAN interface. Gateway is not required.*
- *Physical Settings – By default, the LAN interface bridges the eth0.1 and wlan0 physical interfaces.*
- *Firewall Settings – Firewall zone should be set as LAN zone.*
- *DHCP Server – DHCP server can be used to assign IP address to clients connecting to the LAN. To enable the DHCP server, make sure that the check box "Ignore Interface" is not selected, and configure the other DHCP settings.*

3. Click **Save**.
4. Click **Save & Apply** to save the configuration.

WAN and WAN6 Interface

Network > Interface > WAN or WAN6

The WAN and WAN6 pages allow you to configure the WAN and WAN6 interfaces, respectively. The WAN interface supports IPv4 or dual mode IPv4/IPv6 and the WAN6 interface supports IPv6 mode. Otherwise, the WAN and WAN6 interfaces are similar and are configured in a similar manner.

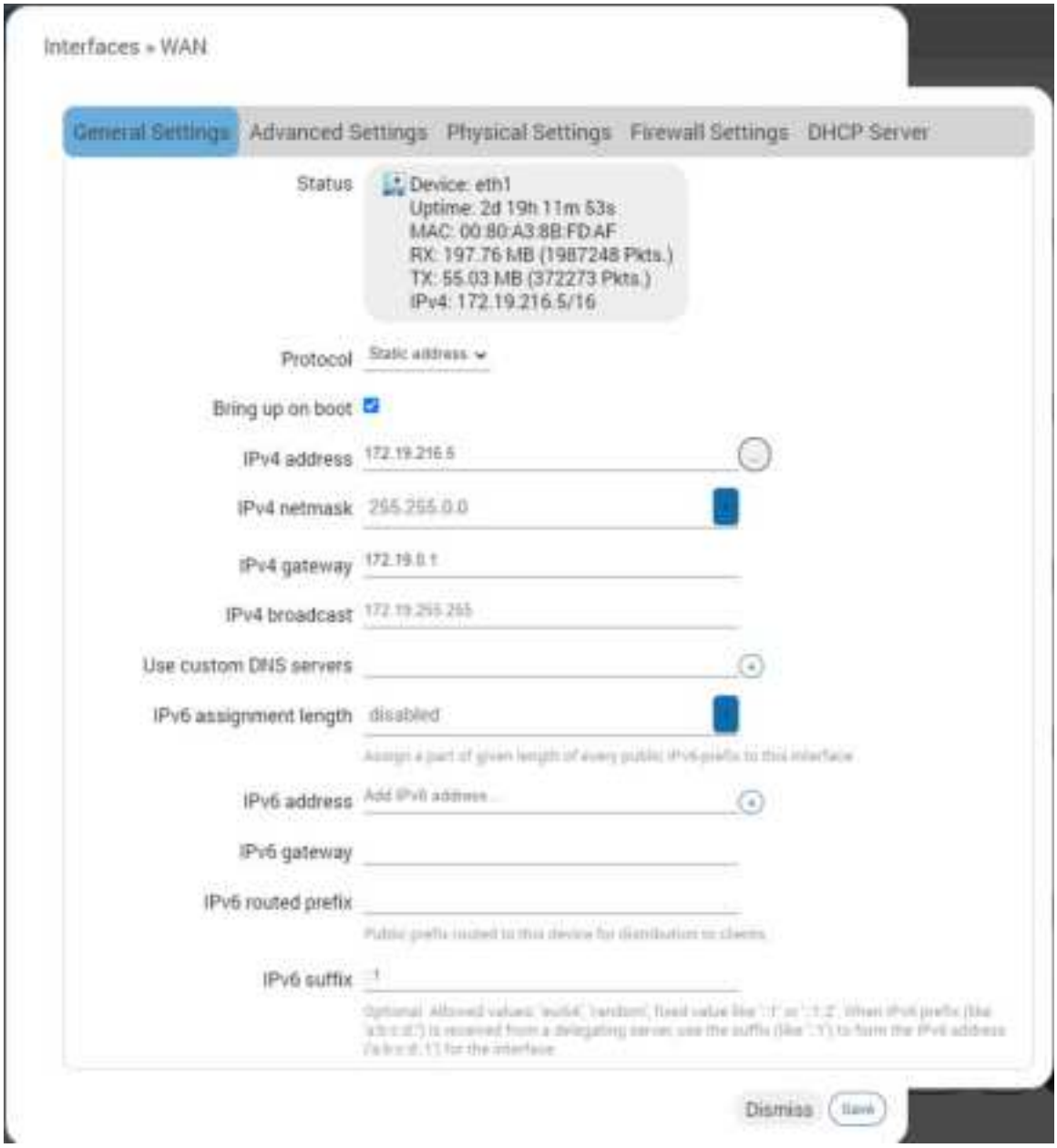
The WAN or WAN6 interface should use Static Address, DHCP client, DHCPv6 client, or PPPoE protocol. If you assign Static Address as the protocol, the IPv4 gateway is required for the external interface, but should not be used for internal use. DHCP server should be disabled.

The interface configuration parameters will depend on the assigned protocol. For descriptions of the protocol settings, see *Static Address*, *DHCP Client*, *DHCPv6 Client*, or *PPPoE*.

To edit the interface:

1. Go to Network > Interfaces, select WAN and click **Edit**.

Figure 12-5 WAN Interface (Static Address) Configuration



2. Configure the interface settings respective to the gateway.
   - For protocol settings, see *Static Address*, *DHCP Client*, or *PPPoE*.
   - General Settings – To change the WAN protocol, select the protocol and click the **Switch Protocol** button.
   - Firewall Settings – Firewall zone should be set as WAN zone.
   - DHCP Server – DHCP server should be disabled. Make sure to select "Ignore Interface."
3. Click **Save**.
4. Click **Save & Apply** to save the configuration.

WWAN and WWAN6 Interface

Network > Interface > WWAN or WWAN6

This page allows you to configure the WWAN and WWAN6 interface parameters. The WWAN interface becomes active when the wireless interface is configured as lient. The wireless interface is configured on the Network > Wireless page.

The WWAN interface supports IPv4 or dual mode IPv4/IPv6. WWAN6 interface supports IPv6 mode. Otherwise, the WWAN and WWAN6 interfaces provide similar functionality and are configured in a similar manner.

The WWAN or WWAN6 interface will use either Static Address, DHCP client, or DHCPv6 client protocol. On the WWAN interface, if you assign Static Address as the protocol, IPv4 gateway is required for external interface, but should not be used for internal use. DHCP server should be disabled.

Interface configuration settings will vary depending on the assigned protocol. For descriptions of the protocol settings, see *Static Address*, *DHCP Client*, or *DHCPv6 Client*.

To edit the interface:

1. Go to Network > Interfaces, select WWAN and click **Edit**.

Figure 12-6 WWAN Interface (DHCP client) Configuration

2. Configure the interface settings respective to the gateway.
   - For protocol settings, see *Static Address* or *DHCP Client*.
   - General Settings – To change the WWAN protocol, select the protocol and click the **Switch Protocol** button. If Static IP address protocol is selected, IPv4 gateway is required for external interface, but should not be used for internal use.

- Advanced Settings – Similar to WAN DHCP settings, except the metric is fixed by default for other features to work as per requirement.
- Firewall Settings – Firewall zone should be set as WAN zone.
- DHCP Server – DHCP server should be disabled.

3. Click **Save**.
4. Click **Save & Apply** to save the configuration.

Add Virtual Interface

The virtual network interface allows you to configure a new interface such as a VPN tunnel that encapsulates data inside a transport protocol. The supported tunneling protocols include GRE, L2TP, WireGuard VPN, PPP, and PPtP.

The virtual interface can be created for other reasons, such as to configure a relay bridge to extend the wireless network.

Note: *Adding a virtual interface may require modifications to the load balancer configuration. For load balancer configuration, see Load Balancing. For additional support and knowledge base articles, please visit Lantronix Support.*

To add a new interface:

1. Go to Network > Interfaces, scroll to the bottom of the list of interfaces and click **Add new interface.**

Figure 12-7 Network Add New Interface

2. Enter the interface name. The name must include only alpha numeric characters and special character underscore (_).
3. Select the protocol to assign to the interface.
4. Click **Create interface**.
5. Configure the interface settings relative to the selected protocol.
   - The first field below the protocol selection is Bring up on boot. This is enabled by default and will start the interface when the gateway is booted.
   - For the remaining configuration details, see *Table 12-9*.
6. Click **Save** to save the new interface.
7. Click **Save & Apply** to apply the configuration to the gateway.

Table 12-9 VPN Tunnel Protocols

Protocol	Description
GRE	
GRE General Settings	◆ Bring up on boot – Start the interface when the device is booted. Selected by default. ◆ Enable GRE tunnel – Enable the interface. ◆ GRE Server Address – Enter the WAN IP address or domain name of the remote GRE server. ◆ Local Address – Enter the WAN IP address of the gateway ◆ Local Tunnel Address – Enter the local IP address of the gateway on the GRE tunnel ◆ Remote Tunnel Address – Enter the remote IP address on the GRE tunnel ◆ Keepalive Interval (in minutes) – The amount of time before sending a keepalive probe packet to check the connection ◆ Keepalive Retries – The number of unanswered echo requests before considering the peer dead ◆ Interface – Enter the interface to bind to GRE. GRE cannot move from one interface to another. It must be bound to a particular interface.
GRE Advanced Settings	◆ Use builtin IPv6 management – Allows to use the built in IPv6 management configuration ◆ Force link – Select this option to assign interface properties regardless of the link being active or not. If not selected, items are assigned only after the link has become active. This is the default.
GRE Firewall Settings	Select the WAN zone as the firewall zone.
L2TP	
L2TP General Settings	◆ Bring up on boot – Start the interface when the device is booted. Selected by default. ◆ L2TP Server – Enter the public IP address of the VPN server for L2TP connection ◆ PAP/CHAP username – Enter the PAP/CHAP username. The default password is admin. ◆ PAP/CHAP password – Enter the PAP/CHAP password.
L2TP Advanced Settings	Advanced settings are similar to those of PPPoE with a few exceptions as noted below. For configuration details, see *QMI Cellular*. ◆ Keepalive Requests is similar to LCP echo failure threshold. ◆ Checkup Interval is similar to Inactivity timeout. ◆ L2TP does not include fields for LCP echo interval or Host-Uniq tag content.
L2TP Firewall Settings	Select the WAN zone as the firewall zone.
PPP	
PPP General Settings	◆ Modem device – Select the modem device from the list. ◆ PAP/CHAP username – Enter the PAP/CHAP username. The default password is admin. ◆ PAP/CHAP password – Enter the PAP/CHAP password.
PPP Advanced Settings	Advanced settings are similar to those of PPPoE. For configuration details, see *QMI Cellular*.
PPP Firewall Settings	Select the WAN zone as the firewall zone.
PPtP	

Protocol	Description
PPtP General Settings	*Note: Enabling PPtP will also enable a 20 mins PPtP watchdog which will reboot the gateway in absence of an active PPtP connection for a period of 20 mins.* ◆ VPN Server – Enter the public IP Address or DNS name of the remote VPN Server for the PPTP connection. ◆ PAP/CHAP username – Enter the PAP/CHAP username. ◆ PAP/CHAP password – Enter the PAP/CHAP password. The default password is admin. ◆ Interface – Select the interface that the device will use to initiate the PPtP connection. ◆ Unspecified – use the active interface to make the connection.
PPtP Advanced Settings	Advanced settings are similar to those of PPPoE. For configuration details, see *QMI Cellular*. One additional setting is described below: ◆ Use mppe – Select to enable encryption if this setting is enabled on the remote server.
PPtP Firewall Settings	◆ Select the WAN zone as the firewall zone.
WireGuard VPN	
WireGuard VPN General Settings	For details on how to configure a VPN connection using WireGuard VPN, see *WireGuard VPN on page 102*. ◆ Bring up on boot – Start the interface when the device is booted. Selected by default. ◆ Private Key – Enter the private key of the device. ◆ Listen Port – Optional. By default WireGuard uses UDP port 51820. ◆ IP Addresses – Recommended. Enter the IP addresses of the WireGuard interface.
WireGuard VPN Advanced Settings	◆ Use builtin IPv6 management – Allows to use the built in IPv6 management configuration ◆ Force link – Select this option to assign interface properties regardless of the link being active or not. If not selected, items are assigned only after the link has become active. This is the default. ◆ Metric – Optional. Metric of the interface ◆ MTU – Optional. Maximum Transmission Unit of the tunnel interface ◆ Firewall Mark – Optional. Enter 32-bit mark for outgoing encrypted packets. Enter value in hex, starting with 0x.
WireGuard VPN Firewall Settings	Select the firewall zone.
WireGuard VPN Peers	◆ This page lets you add a WireGuard peer. For information about WireGuard interfaces and peers, visit https://www.wireguard.com.

Relay Bridge

The Relay Bridge protocol provides an option to implement bridge behavior (on IPv4 only) to extend the wireless network. The virtual interface must have a local IPv4 address to access the bridge connection and relay between two networks.

Wireless

Network > Wireless

The Wireless interface on the gateway can operate in two modes:

- Client mode – The gateway will act as a Wi-Fi client to existing wireless networks. The gateway will accept Internet access through wireless access provided by another service provider and then distribute the access to the machines connected to the gateway on its LAN interface.
- Access point (Master) mode – The gateway will act as a wireless access point to provide a wireless LAN network that wireless clients may join.

The gateway can act as Wi-Fi master and client at the same time provided that the gateway's Wi-Fi client is connected to any AP.

Figure 12-8 and *Table 12-10* describe the Wireless Overview and Associated Stations.

Figure 12-8 Wireless Overview

Table 12-10 Wireless Overview and Associated Stations

Parameters	Description
Wireless Overview	Displays status and details about the wireless radio and wireless instances. The gateway provides the following interaction with the wireless radio: ◆ **Restart** – restart the radio ◆ **Scan** – scan for available wireless connections and join a network. This also adds a new client instance. ◆ **Add** – add a new instance The gateway provides the following interaction on the wireless interface instances: ◆ **Disable/Enable** – disable or enable the instance ◆ **Edit** – edit the instance configuration settings ◆ **Remove** – delete the instance

Parameters	Description
Associated Stations	Displays details about associated wireless stations such as network, MAC address, host, signal and Rx/Tx (rate).

Wireless Network Configuration

Note: *When Wi-Fi is configured as Client, the WWAN interface will become active.*

Wi-Fi Client

To join a wireless network in client mode:

1. Go to Network > Wireless.
2. Click **Scan** to find available wireless networks. The scan results will display a list of networks.
3. Select the network that you want to connect to and click **Join Network**.
4. On the wireless configuration window, enter the settings to join the network based on the network's encryption method (WPA, WPA2, WPA3 SAE, mixed WPA/WPA2). The assigned firewall zone should be WAN. If you select Replace wireless configuration, all existing networks will be deleted from the radio. Click **Submit**.
5. Configure the wireless network client. For details, see *Table 12-11* and *Table 12-12*.
6. Click **Save**.

   The client instance is created and the access point to which it is associated appears under Associated Stations.
7. Click **Save & Apply**.

Wireless Access Point

To configure the wireless instance as an access point:

1. Go to Network > Wireless.
2. If an access point exists and you want to edit it, click **Edit**.
3. If no access point exists, click **Add** to create an instance.
4. Configure the device and interface settings, selecting Access point as the Wi-Fi interface mode. For configuration details, see *Table 12-11* and *Table 12-12*.
5. Click **Save**.
6. The access point instance is created or modified.
7. Click **Save & Apply**.

Table 12-11 Wireless Device Configuration

Parameters	Description
General Setup	
Status	Displays the following details: ◆ Mode – Master (access point) or Client ◆ SSID – Service Set Identifier (SSID) is a public identifier up to 32 characters that uniquely names a Wi-Fi connection. ◆ BSSID – Basic Service Set Identification (BSSID); 24 bit MAC Address of Wireless Access Point ◆ Encryption – data encryption method ◆ Channel – wireless channel and frequency band ◆ Tx-Power – transmit power in dBm ◆ Signal/Bitrate – signal strength in dBm and bitrate in Mbit/sec ◆ Country – country code
Wireless network is enabled/ disabled	The field label displays the state of the wireless network as either enabled or disabled. Click **Enable** or **Disable** to update the network operation state.
Operating Band	By default, 'auto' lets the wireless device select the operating band to use. Alternatively, choose the band and channel. Channels are defined in 5 MHz increments and are 20 MHz wide. It's recommended to select 'auto' or to select channels that don't overlap with channels used by other access points in the immediate area of the access point that you are configuring.
Roaming	
Roaming State	Enable or disable the roaming state, which allows the wireless client to make roaming choices of which AP to associate to.
Level	Select preconfigured roaming settings or select Custom to configure custom settings for the client.
Time interval for consecutive scans	The interval in seconds between scans.
RSSI Delta for 2.4G	The RSSI delta for 2.4G represents the roaming threshold at which the client will roam to the target AP.
RSSI Delta for 5G	The RSSI delta for 5G represents the roaming threshold at which the client will roam to the target AP.
Scan Threshold for 2.4G	The 2.4G scanning threshold in dbm, after which the client will scan for potential target APs.
Scan Threshold for 5G	The 5G scanning threshold in dbm, after which the client will scan for potential target APs.

Table 12-12 Wireless Interface Configuration

Parameters	Description
General Setup	
Mode	Select the Wi-Fi Interface mode. Available Options ◆ Access Point – gateway will act as an access point (master mode) ◆ Client – gateway will act as a wireless client The default mode is Access Point.

Parameters	Description
ESSID	Displays the device name assigned to the gateway. The default name is Lantronix G52X
Priority	Displayed for Client only. The order of preference in which the gateway will attempt to join the configured wireless networks. The range is from 1 to 8 with 1 being the highest priority and 8 being the lowest priority.
BSSID	This field is displayed for Client only. Basic Service Set Identifier (BSSID) – 48-bit MAC address for the access point of the BSS. This can be left blank.
Isolate Clients	Displayed for Access Point only. Enable to prevent communication between clients connected to the access point.
Network	Select LAN for the Access Point or WWAN for Client Mode to configure the gateway as LAN or WWAN respectively.
Hide ESSID	Select Hide ESSID, to hide ESSID when client machines scan for available Wi-Fi networks.
Wireless Security	
Encryption	Select the Encryption mode for Wi-Fi network. Available Options: ◆ Open (no security) ◆ WPA3 SAE (strong security) ◆ WPA-PSK/WPA2-PSK Mixed mode (medium security)! ◆ WPA2-PSK/WPA3-SAE Mixed mode (strong security) ◆ WPA2-PSK (strong security) ◆ WPA-PSK (medium security) ◆ WPA3 Transition Mode (strong security) ◆ WPA2-EAP (strong security) ◆ WPA-EAP (medium security) The default encryption mode for access point configuration is WPA-PSK/WPA2-PSK Mixed mode. ***Note:*** *The encryption modes WPA3 SAE, WPA2-PSK/WPA3-SAE, WPA3 Transition Mode, WPA2-EAP, and WPA-EAP apply only to STA (client) interface. Some of these modes, when selected, display additional fields to enter certificate details.*
Cipher	For all encryption modes except No Encryption. Select the cipher suitable to the gateway. Options: ◆ Auto ◆ Force CCMP (AES) ◆ Force TKIP ◆ Force TKIP and CCMP (AES) The default cipher is auto mode.
Key	Enter the key respective to cipher type

Parameters	Description
802.11w Management Frame Protection	Improves WLAN security by encrypting the frames used to manage the connections between client (STA) devices and access points. Options: ◆ Disabled ◆ Optional ◆ Required In Access Point mode, if you select Optional or Required, the following fields display: ◆ 802.11w maximum timeout (ms) - Enter a value between 1 to 1000 ◆ 802.11w retry timeout (ms) - Enter a value between 1 to 201 ***Note:*** *For client (STA) interface select the same option that you have selected in Access Point mode.*
MAC-Address Filter	
MAC-Address Filter	Allows or blocks certain client MAC Addresses. Default is disabled. This setting applies only to Access point mode. Options: ◆ Disable ◆ Allow listed only – If this option is selected, choose the client MAC Addresses to allow. ◆ Allow all except listed – If this option is selected, choose the client MAC Addresses to block.

Default Wireless Client Profile

The G520 series device includes a default WLAN client profile configured for AP with SSID “Lantronix_Initial_Default_Infra” and “Open” security. The default profile is designed for provisioning gateways connected to a Wi-Fi hotspot set as “Lantronix_Initial_Default_Intra” to allow initial configuration of multiple gateways via Lantronix Provisioning Manager (LPM) using each device’s WAN interface.

Once the device connects to this SSID, it will automatically open the following firewall rules for LPM to discover and configure the device:

- AcceptDiscoveryWan
- AcceptSSHWan
- AcceptWeb
- AccessWanPS
- AcceptWebAccessWanP

Configure the devices using LPM and then disconnect them from this SSID. When the device disconnects from this SSID, it will automatically close the above firewall rules. Only the rules which were automatically opened are closed. No change is made if they were already opened by the user.

It is the responsibility of the user to disable or delete the profile after the initial configuration.

DHCP and DNS

Network > DHCP and DNS

Dynamic Host Configuration Protocol (DHCP) is a network protocol that is used to configure network devices to communicate on an IP network. A DHCP client uses the DHCP protocol to acquire configuration information, such as an IP address, a default route, and one or more DNS server addresses from a DHCP server. The DHCP client then uses this information to configure its host. Once the configuration process is complete, the host is able to communicate on the network.

For details about basic setup of DHCP server on the LAN side see *DHCP Server*.

The DHCP and DNS page allows you to configure advanced options such as custom DNS servers, custom lease files, advanced TFTP settings and MAC Address-based IP Address allocation.

To configure:

1. Go to Network > DHCP and DNS.
2. Enter the configuration settings. See *Table 12-13* to *Table 12-17*.
3. Click **Save & Apply**.

General Settings

Network > DHCP and DNS > General Settings

Table 12-13 General Configuration of DHCP Server and DNS-Forwarder

Parameters	Description
Server Settings	
Domain required	Check to allow forwarding of DNS request only if they have domain name.
Authoritative	Check to authorize the DHCP in the local network.
Local server	Enter the local server domain specification. These domain names are only resolved using DHCP or host files.
Local domain	Enter the local domain suffix appended to DHCP names and host file entries.
Log queries	Log the DNS request received in the syslog server.
DNS forwardings	Enter the DNS Server names to forward the received DNS requests.
Rebind protection	Check to discard upstream RFC1918 responses
Allow localhost	Check to allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services
Domain whitelist	Enter the list of domain name to allow RFC1918 responses.
Local Service Only	Select to accept DNS queries only from hosts whose address is on a local subnet.
Non-wildcard	Select to bind only configured interface addresses, instead of the wildcard address.
Listen Interfaces	Restrict listening to the specified interfaces.
Exclude Interfaces	Prevent listening on the specified interfaces.
Active DHCP Leases	

Parameters	Description
Hostname	Name of the device that is connected to the gateway and has been leased an IP Address by DHCP server.
IPv4-Address	IPv4 Address assigned to the device connected to the gateway.
MAC-Address	MAC address of the device connected to the gateway.
Leasetime remaining	Remaining time until which the device can use the DHCP server leased IP Address.
Active DHCPv6 Leases	
Hostname	Name of the device that is connected to the gateway and has been leased an IPv6 Address by DHCPv6 server.
IPv6-Address	IPv6 Address assigned to the device connected to the gateway.
DUID	DUID (Device Unique Identifier) of the device connected to the gateway
Leasetime remaining	Remaining time until which the device can use the DHCPv6 sever leased IPv6 Address.
Static Leases	
Hostname	Name of the device that is connected to the gateway and has been assigned a static IP Address.
MAC-Address	MAC address of the device connected to the gateway.
IPv4-Address	IPv4 Address to be assigned to the device connected to the gateway.
IPv6-Suffix (hex)	IPv6 Address to be assigned to the device connected to the gateway.

Resolv and Host Files

Network > DHCP and DNS > Resolv and Host File

Table 12-14 Resolv and Host File Configuration for DHCP and DNS

Parameters	Description
Use /etc/ethers	Check to use /etc/ethers for configuring the DHCP-Server.
Leasefile	Enter the directory path name where given DHCP-leases will be stored.
Ignore resolve file	Check to ignore the resolved file.
Resolve file	Enter the local DNS file.
Ignore /etc/hosts	Check to ignore the hosts file.
Additional Hosts file	Enter the additional host files.

TFTP Settings

Network > DHCP and DNS > TFTP Settings

This page provides settings to configure the gateway as a Trivial File Transfer Protocol (TFTP) server, which can be used to serve files for download to a remote TFTP client.

Table 12-15 TFTP Configuration for DHCP and DNS

Parameters	Description
Server Settings	

Parameters	Description
Enable TFTP server	Check to enable TFTP server. By default, the TFTP server is in disabled. ◆ TFTP server root – Enter the Root directory for the files served using TFTP. ◆ Network boot image – Enter the Filename of the boot image which is advertised to the clients.

Advanced Settings

Network > DHCP and DNS > Advanced Settings

Table 12-16 Advanced Configuration for DHCP and DNS

Parameters	Description
Server Settings	
Suppress logging	Suppress logging of the routine operation of DHCP. Errors and problems will still be logged.
Allocate IP Sequentially	Force DHCP server to allocate IP addresses sequentially, starting from the lowest available address. In this mode, clients that allow a lease to expire are more likely to move IP address.
Filter private	Check to deny the reverse lookups for local networks.
Filter useless	Check to deny the requests that cannot be answered by public name servers. By default the request are forwarded.
Localize queries	Check to localize hostname depending on the requesting subnet if multiple IP Addresses are available.
Expand hosts	Check to add local domain suffix to names served from hosts files.
No negative cache	Check to deny caching the negative replies, e.g. for non-existing domains.
Additional Servers file	List of DNS servers to forward requests to.
Strict order	DNS servers will be queried in the order of the resolve file.
All Servers	Select to query all upstream DNS servers.
Bogus NX Domain Override	Enter the hostname that supply bogus NX domain results.
DNS server port	Enter the listening port for inbound DNS queries. The default DNS server port is 53.
DNS query port	Enter the fixed source port number for outbound DNS queries. The default DNS query port is “any”
Max. DHCP leases	Enter the maximum number of allowed DHCP leases that are active. By default unlimited DHCP leases are allowed.
Max. EDNS0 packet size	Enter the maximum allowed size of EDNS.0 UDP packets. The default EDNS.0 UDP packet size is 1280.
Max. concurrent queries	Enter the maximum number of concurrent DNS queries allowed. By default 150 concurrent DNS queries are allowed.

Parameters	Description
Size of DNS query cache	Enter the maximum number of cached DNS entries. By default, 150 DNS entries are cached. Maximum is 10000. A value of zero (0) means no caching.

Static Leases

Network > DHCP and DNS > Static leases

Table 12-17 DHCP and DNS Static Leases

Parameters	Description
Add	Click to add a static lease.
Active DHCP Leases	
Hostname	Name of the device that is connected to the gateway and has been leased an IP Address by DHCP server.
IPv4-Address	IPv4 Address assigned to the device connected to the gateway.
MAC-Address	MAC address of the device connected to the gateway.
Leasetime remaining	Remaining time until which the device can use the DHCP server leased IP Address.
Active DHCP6 Leases	
Hostname	Name of the device that is connected to the gateway and has been leased an IPv6 Address by DHCPv6 server.
IPv6-Address	IPv6 Address assigned to the device connected to the gateway.
DUID	DUID (Device Unique Identifier) of the device connected to the gateway
Leasetime remaining	Remaining time until which the device can use the DHCPv6 sever leased IPv6 Address.
Static Leases	
Hostname	Name of the device that is connected to the gateway and has been assigned a static IP Address.
MAC-Address	MAC address of the device connected to the gateway.
IPv4-Address	IPv4 Address to be assigned to the device connected to the gateway.
IPv6-Suffix (hex)	IPv6 Address to be assigned to the device connected to the gateway.

Hostnames

Network > Hostnames

Allows you to enter host names for the devices on the LAN.

To add a host name:

1. Go to Networks > Hostnames.
2. Click **Add**.
3. Enter the hostname and the IP address of the host. See *Table 12-18*.
4. Click **Save**.
5. Click **Save & Apply**.

Table 12-18 Hostnames Configuration

Parameters	Description
Hostname	Enter the Hostname. The hostname can contain any combination of alphabetic characters, numbers, dashes, and underscores. No other special characters are allowed.
IP address	Enter the IP Address of the host.

Static Routes

Network > Static Routes

Configure static routes to define the explicit path between two different networks located in two different domains. Static routes must be manually reconfigured when network changes occur.

To configure static routes:

1. Go to Networks > Static Routes.
2. Select IPv4 or IPv6 tab.
3. Click **Add**.
4. Enter the configuration settings. For IPv4 static routes, see *Table 12-19* and for IPv6 static routes, see *Table 12-20*.
5. Click **Save**.
6. Click **Save & Apply**.

Static IPv4 Routes

Table 12-19 Static IPv4 Routes Configuration

Parameters	Description
General Settings	
Interface	Select the interface name of the parent interface this route belongs to.
Target	Enter the target host IPv4 Address or Network address if the target is a network.

Parameters	Description
IPv4-Netmask	Enter the IPv4 Netmask of the static route.
IPv4-Gateway	Enter the IPv4 gateway. If gateway is not entered, the gateway from the parent interface is used.
Advanced Settings	
Metric	Enter the metric of the static route.
MTU	Enter the number of bytes indicating the largest physical packet size that the network can transmit. The default MTU size is 1500 bytes. A blank value represents auto MTU size.
Route type	Select the route type. Available options: ◆ unicast – route entry describes real paths to the destinations covered by the route prefix. ◆ local – destinations are assigned by this host. Packets are looped back and delivered locally. ◆ broadcast – destinations are broadcast addresses. Packets are sent as link broadcasts. ◆ multicast – special type used for multicast routing. ◆ unreachable – these destinations are unreachable ◆ prohibit – these destinations are unreachable. ◆ blackhole – these destinations are unreachable. Packets are discarded silently. Local senders get an ENVAL error. ◆ anycast – these destinations are anycast addresses assigned to this host.
Route table	Define the table ID to use for the route. The table ID can be either a numeric table index ranging from 0 to 65535 or a symbolic alias declared in /etc/iproute2/rt_tables. The following special aliases are also recognized: local (255), main (254), default (253).
Source Address	Specify the preferred source address when sending to destinations covered by the target.
On-Link route	If enabled, the gateway is on link even if the gateway doesn't match any interface prefix.

Static IPv6 Routes

Table 12-20 Static IPv6 Routes Configuration

Parameters	Description
General Settings	
Interface	Select the interface name of the parent interface this route belongs to.
Target	Enter the target host IPv6 Address or Network CIDR if the target is a network.
IPv6-Gateway	Enter the IPv6 gateway for the static route. If gateway is not entered, the gateway from the parent interface is used.
Advanced Settings	
Metric	Enter the metric of the static route.

Parameters	Description
MTU	Enter the number of bytes indicating the largest physical packet size that the network can transmit. The default MTU size is 1500 bytes. Blank value represents auto MTU size
Route type	Select the route type. Available options: ◆ unicast – route entry describes real paths to the destinations covered by the route prefix. ◆ local – destinations are assigned by this host. Packets are looped back and delivered locally. ◆ broadcast – destinations are broadcast addresses. Packets are sent as link broadcasts. ◆ multicast – special type used for multicast routing. ◆ unreachable – these destinations are unreachable ◆ prohibit – these destinations are unreachable. ◆ blackhole – these destinations are unreachable. Packets are discarded silently. Local senders get an ENVAL error. ◆ anycast – these destinations are anycast addresses assigned to this host.
Route table	Define the table ID to use for the route.
Source Address	Specify the preferred source address when sending to destinations covered by the target.
On-Link route	If enabled, the gateway is on link even if the gateway doesn't match any interface prefix.

Diagnostics

Network > Diagnostics

The diagnostics feature allows you to run network utilities and cable diagnostics commands from the web interface.

Table 12-21 describes each of the network utilities.

Table 12-22 describes the cable diagnostics status messages.

Note: *The cable diagnostics command will bring down the Ethernet port link, which will take more time to complete the test. Cable diagnostics is only accurate for cable lengths of 7 - 120 meters.*

Table 12-21 Diagnostics - Network Utilities

Network Utility	Description
Ping	IP Address or fully qualified domain name to be pinged. Ping determines network connection between gateway and host on the network. The output shows if the response was received, packets transmitted and received, and packet loss if any.
Traceroute	IP Address or fully qualified domain name Traceroute displays all the routers present between the destination IP address and the gateway. The output shows all the gateways through which data packets pass on way to the destination system from the source system, maximum hops and total time taken by the packet to return measured in milliseconds.
Nslookup	IP Address or fully qualified domain name that needs to be resolved. Name lookup is used to query the Domain Name Service for information about domain names and IP addresses. It sends a domain name query packet to a configured domain name system (DNS) server. If you enter a domain name, you get back the IP address to which it corresponds. If you enter an IP address, you get back the domain name to which it corresponds. A message stating “Unknown Host” indicates that the Internet Name does not exist.

Table 12-22 Cable Diagnostics Status Messages

Status message	Description
<interface name:> No cable faults detected	The cable link is good.
<interface name:> Open circuit detected in cable	There is no cable.
<interface name:> Open circuit detected in cable Distance to cable fault is ~<disance> meter(s).	Open ended cable.
<interface name:> Short circuit detected in cable. Distance to cable fault is ~<distance> meter(s).	There is an issue with the cable.

Status message	Description
<interface name:> Short cable (less than 10 meters) detected.	Short cable detected.
<interface name:> Cable diagnostic test failed	The cable has failed the diagnostic test. Possible failure reasons include: interface is busy, link partner is not configured for auto-negotiation, or link partner is busy establishing the link.

Firewall

Network > Firewall

The firewall policy helps secure the network. The G520 series gateways follow a zone based firewall concept. Every interface of the gateway, whether physical or virtual, needs to be assigned to a firewall zone, and all traffic routed through that interface is bound by the assigned policy. At a minimum, there are two firewall zones, the LAN zone and WAN zone, with one or more interfaces assigned to each zone.

By default, there is a minimal firewall configuration predefined in the gateway. The minimal configuration consists of global firewall settings, and two zones, the LAN zone and WAN zone which serve as a source or destination for port forwarding, rules, and redirects. This configuration may be sufficient for your needs with little modification. Otherwise, you can use the web interface to modify the firewall configuration.

This section assumes that the reader has knowledge of implementing firewall policies or will consult their network administrator to set up the firewall policies.

Note: *Create a backup of the firewall configuration before making any changes.*

General Settings

The General settings page consists of the global settings and zones. The global firewall settings are default firewall settings that do not belong to any zone.

Firewall Global Settings

To configure firewall global settings:

1. Go to Network > Firewall.
2. In the top section of the General Settings page, if desired, modify global firewall settings. See *Table 12-23*.
3. Click **Save & Apply** to save the changes and reload the firewall.

Table 12-23 Firewall Global Settings

Parameters	Description
General Settings	
Enable SYN-flood protection	Check to enable SYN-flood protection. SYN-flood protection will enable spamming detection and block whenever there is a spam attack.
Drop invalid packet	Check to drop the invalid packets that are not matching any active connection.

Parameters	Description
Input	Select to accept or reject the inbound traffic to all the interfaces.
Output	Select to accept or reject the outbound traffic from all the interfaces.
Forward	Select to accept or reject the forwarded traffic from all the interfaces.

Firewall Zones

Two firewall zones, the LAN zone and WAN zone, are predefined in the gateway. All traffic from LAN to WAN has no restrictions but all incoming traffic from WAN source is blocked unless a port forwarding rule is set or unless a particular port is opened.

A zone section groups one or more interfaces and serves as source or destination for forwarding, rules, and redirects. A zone is defined by the following rules:

- Masquerade (NAT) of outgoing traffic (WAN) is controlled on a per zone basis on the outgoing interface.
- INPUT rules describe what happens to traffic trying to reach the gateway through an interface in that zone.
- OUTPUT rules zone describe what happens to traffic originating from the gateway going through an interface in that zone.
- FORWARD rules describe what happens to traffic passing between different interfaces in that zone.

Packet filtering actions

- ACCEPT – traffic is allowed to pass as if there is no firewall in place. If the port at the destination is closed, a response will be returned as if a Reject rule is in place.
- DROP – the firewall discards the packet and sends no response back to the source host that sent the packet. The source host will wait for a response until a timeout occurs and may attempt to retry the connection after timeout occurs.
- REJECT – the firewall discards the packet and sends a response back to the source host that the port is closed. Doing so can hint to the source that packet filtering firewall is in place.

In general, use REJECT to deny traffic from trusted hosts by gracefully informing them that traffic is not allowed to pass. Use DROP to deny traffic from untrusted hosts or when you don't want expose information about the destination host.

To configure firewall zones:

1. Go to Network > Firewall.
2. To add and configure a new firewall zone, click **Add**.
3. To modify settings for an existing firewall zone, click **Edit**.
4. Enter or modify the firewall zone settings. See *Table 12-24*.
5. Click **Save**.
6. Click **Save & Apply**.

Table 12-24 Firewall Zones Configuration (LAN)

Parameters	Description
General Settings	

Parameters	Description
Name	Enter the name of the zone.
Input	Select to accept, reject or drop the inbound traffic to all the configured zones.
Output	Select to accept, reject or drop the outbound traffic from all the configured zones.
Forward	Select to accept, reject or drop the forwarded traffic from all the configured zones.
Masquerading	Check to allow IP Masquerading (NAT).
MSS clamping	Check to allow MSS clamping.
Covered networks	Select the network interfaces that must be included in the zone configuration.
General Settings / Inter-Zone Forwarding	
Allow forward to destination zones	Select to allow or deny forwarding traffic to the configured destination zone.
Allowed forward from source zones	Select to allow or deny forwarding traffic from the configured source zone.
Advanced Settings	
Covered devices	List of raw network device names attached to this zone
Covered subnets	List of IP subnets attached to this zone.
Restrict to address family	Select IP Address family for configuring firewall for LAN zone from available options. Available Options ◆ IPv4 ◆ IPv6 ◆ IPv4 and IPv6
Restrict Masquerading to given source subnets	Enter the source subnet to which the masquerading must be restricted.
Restricts Masquerading to given destination subnets	Enter the destination subnet to which the masquerading must be restricted.
Enable logging on this zone	Check to enable logging of all the activities on the Zone.
Conntrack Settings	
Allow "invalid" traffic	Select to allow invalid traffic. More specifically, when selected, no rules can be installed that reject forwarded traffic with conntrack state equal to invalid. Disabled by default.
Automatic helper assignment	Automatically assign conntrack helpers for the zone.
Conntrack Settings	
Extra source arguments	Extra arguments passed directly to iptables for source classification rules.
Extra destination arguments	Extra arguments passed directly to iptables for destination classification rules

Port Forwards

Network > Firewall > Port Forwards

Port forwarding allows remote computers to connect to a specific host within the LAN by opening the WAN port and redirecting the connection (and data) on that port to an internal LAN IP and port. By default, all WAN side ports are closed.

To view port forwarding entries, go to Firewall > Port Forwards. See *Table 12-25* for a description. You can also edit, reorder or delete the entries from this view.

Table 12-25 Firewall Port Forwards

Parameters	Description
Match	Displays the WAN TCP/UDP ports for matching the conditions before forwarding it to LAN device.
Forward to	Displays the destination IP Address to which the traffic must be forwarded.
Enable	Check to enable the Port Forwarding rule.

Add Port Forwarding Rule

To add a port forwarding rule:

1. Go to Network > Firewall > Port Forwards.
2. At the bottom of the Port Forwards table, click **Add**.
3. Enter the configuration settings. See *Table 12-26*.
4. Click **Save**.
5. Click **Save & Apply**.

Table 12-26 Port Forwarding Configuration for Firewall Zone

Parameters	Description
Port Forwards General Settings	
Name	Enter the name of the Port Forwarding rule.
Protocol	Select the protocol. Available options: ◆ TCP ◆ TCP + UDP ◆ UDP ◆ ICMP ◆ unspecified ◆ custom
Source Zone	Specify the traffic source zone. This must refer to one of the firewall zones, usually WAN.
External Port	Enter the WAN port of the external network.
Destination zone	Specify the traffic destination zone. This must refer to one of the firewall zones, usually LAN.
Internal IP address	Enter the LAN IP address of the internal network.
Internal port	Enter the LAN port number of the internal network.
Port Forwards Advanced Settings	
Source MAC Address	The rule will match incoming traffic from the specified source mac address.

Parameters	Description
Source IP Address	The rule will match incoming traffic from the specified source IP address.
Source port	The rule will match incoming traffic from the specified source port number.
External IP Address	Enter the external IP address of the gateway.
Enable NAT Loopback	Enable NAT loopback to allow one machine on the LAN network to access another machine on the LAN through the external IP address of the gateway
Extra arguments	Passes additional arguments to iptables. Should be used with care.

Traffic Rules

Network > Firewall > Traffic Rules

Traffic rules are security policies that allow or restrict access to specific ports or hosts. Rule actions can be configured to accept, drop, or reject traffic.

The following describes good practices for configuring traffic rules.

- Block all traffic by default and explicitly enable specific traffic to known services.
- Allow specific traffic, using the principle of least privilege.
- Specify source IP address. It's okay to specify "any" if the service should be accessible to everyone on the Internet, otherwise, specify the source address.
- Specify the destination IP address.
- Specify the destination port. The value of the destination port should never be "any".

Rule and zone matching

The source and destination zones are tied to the target action.

- If source and destination are given, the rule matches forwarded traffic.
- If only source is given, the rule matches incoming traffic.
- If only destination is given, the rule matches outgoing traffic.
- If neither source nor destination are given, the rule defaults to an outgoing traffic rule.

To view traffic rules, go to Network > Firewall > Traffic Rules. See *Table 12-27* for a description. You can also enable or disable the traffic rule from this page view.

Table 12-27 Firewall Zone Traffic Rules

Parameters	Description
Name	Displays the name of the traffic rule.
Match	Displays the details of the traffic rule configuration and the conditions in which the rule is applicable.
Action	Action to be taken on the traffic when the rule conditions are satisfied. Indicates whether the rule is for incoming, forwarded, or outgoing traffic.

Parameters	Description
Enable	Select the box to enable the traffic rule. If the rule is enabled, clear the box to disable the rule.
Edit	Click to edit the traffic rule settings.
Delete	Click to delete the traffic rule.
Add	Click to add a new traffic rule. This button appears at the bottom of the Traffic Rules page.

Add Traffic Rule

To add a traffic rule:

1. Go to Network > Firewall > Traffic Rules.
2. At the bottom of the Traffic Rules table, click **Add**.
3. Enter the configuration settings. See *Table 12-28*.
4. Click **Save**.
5. Click **Save & Apply**.

Table 12-28 Firewall Traffic Rule Configuration

Parameters	Description
General Settings	
Name	Enter the name of the traffic rule.
Protocol	Select the protocol from the available options. ◆ TCP – Allows only TCP traffic to the open port ◆ UDP – Allows only UDP traffic to the open port ◆ TCP+UDP – Allows both TCP and UDP traffic to the open port
Source zone	Select the traffic source zone. This is usually WAN zone.
Source address	Match incoming traffic from the specified source IP address
Source port	Match incoming traffic from the specified source port
Destination zone	Select the destination firewall zone. If specified the rule applies to forwarded traffic, otherwise it is treated as an input rule.
Destination address	Match incoming traffic directed to the specified destination IP address. If no destination zone is specified, the rule is treated as an input rule.
Destination port	Match incoming traffic directed to the specified destination port.
Action	Sets the target parameter to indicate the firewall action. Options include: ◆ Accept ◆ Reject ◆ Drop ◆ Don’t track
Advanced Settings	
Restrict to address family	Enter the protocol family to generate iptables rules for. Options include: ipv4, ipv6, or any.
Source MAC address	Match incoming traffic from the specified MAC address.

Parameters	Description
Extra arguments	Enter extra arguments to pass to iptables. This can be used to specify additional match options.
Time Restrictions	
Week Days	If specified, only match traffic during the given days of the week.
Month Days	If specified, only match traffic during the given days of the month.
Start Time (hh.mm.ss)	Specify a time to start matching traffic.
Stop Time (hh.mm.ss)	Specify a time to stop matching traffic.
Start Date (yyyy-mm-dd)	Specify a date to start matching traffic.
Stop Date (yyyy-mm-dd)	Specify a date to stop matching traffic.
Time in UTC	Select to interpret all time values as UTC time instead of local time.

Custom Rules

Network > Firewall > Custom Rules

The shell script allows you to add custom iptable commands that will be executed after the firewall is restarted, immediately after the default ruleset has been loaded.

To configure custom rules:

1. Go to Network > Firewall > Custom Rules.
2. Enter the custom iptable rule command after the commented lines. Each rule should be on a separate line.
3. Click **Save**.
4. Click **Save & Apply**.

PoE

Network > PoE

PoE (Power over Ethernet) feature is available only on G520 series models with Security pack.

PoE is used to transmit electrical power to remote devices over standard Ethernet cable. It can be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply. PoE Auto Power Reset allows you to specify the auto detection parameters to check the link status between the PoE port and the powered device (PD). When it detects a failed connection, the gateway will reboot the remote PD automatically.

To configure PoE port and PoE Auto Power Reset:

1. Go to Network > PoE.
2. Select the PoE port and configure the PoE auto power reset settings. See *Table 12-29*.
3. Click **Save & Apply**.

Table 12-29 PoE Configuration

Parameters	Description
Port	The logical port number used for PoE.
Ping IP Address	IP address of the powered device (PD). This IP address will be pinged.
Startup Time (seconds)	When a PD has been started, the switch will wait this amount of time to do PoE Auto Power Reset. The default is 60 seconds. The valid range is 30-600 seconds.
Interval Time (seconds)	Device will send checking message to PD each interval time. The default is 30 seconds. The valid range is 10-120 seconds.
Retry Times	When the PoE port can't ping the PD, it will try to send detection again. When the retry times is reached, it will trigger failure action. The default is 3 retries. The valid range is 1-5 retry attempts.
Failure Log	Failure loggings counter (error = x, total = y).
Failure Action	The action when the failure is detected. Nothing: Ping the remote PD but do nothing further. Reboot Remote PD: Cut off the power of the PoE port and reboot PD.
Reboot Time (seconds)	When the PD has been rebooted, the PoE port restored power after the specified time. The default is 15 seconds. The valid range is 3-120 seconds.
Max. Reboot Times	When Failure Action is set to Reboot Remote PD, this setting limits the number of times to reboot the PD. The default is 3 times. The valid range is 0-10 retries. Entering 0 means unlimited reboot attempts.

QoS

Network > QoS

QoS allows you to prioritize specific flows in network traffic to manage handling and allocation of network capacity. Assign traffic to target classes and allocate the amount of bandwidth that is given to those classes. QoS service provides the following functionality:

- Configure two to four predefined **classes** with rate, priority, and packet latency (delay) settings
- Configure one or more **interfaces** (WAN, WWAN, LAN, cellular, VPN) with global connection characteristics such as upload and download speed limits. Each interface can have its own buffer.
- Configure **classification rules** to allocate packets to the configured classes (targets). Traffic is differentiated by source and destination IP addresses, protocols, and ports.

You can configure up to four QoS classes, although you can achieve results by configuring as few as two classes. The predefined classes to limit traffic are Priority, Normal, Express, and Bulk, as well as classes to limit ingress traffic, which are appended with the _down suffix. If the classes to limit ingress traffic are configured, then the original classes will limit egress traffic only. Otherwise, if they are not configured, then Priority, Normal, Express, and Bulk will limit both ingress and egress traffic.

To enable QoS:

Enable QoS by interface. Go to Network > QoS > Interfaces.

To configure QoS:

1. Go to Network > QoS.
2. Enter the QoS configuration settings. See *Table 12-30*.
3. To enable QoS, go to the Interfaces tab and select **Enable** to apply QoS to the interface.
4. Click **Save & Apply**.

Table 12-30 QoS Configure Classes

Parameters	Description
Configure Classes	
Name	Class name. ◆ Priority ◆ Express ◆ Normal ◆ Bulk When configured, these classes will limit both egress (outgoing from the host) and ingress (incoming to the host) traffic. Classes to limit ingress traffic: ◆ Priority_down ◆ Normal_down ◆ Express_down ◆ Bulk_down If Priority_down or Normal_down are configured, then Priority or Normal will limit egress traffic only.
Packet Size	Maximum packet size in bytes, up to 1500 bytes.

Parameters	Description
Average Minimum Rate	Average rate for this class, expressed as the percentage of bandwidth
Priority	Priority of the class, expressed as percentage. The sum priority of all classes should not exceed 100.
Packet Delay in ms	The amount of time, in milliseconds, that the packet will wait in queue before it is transmitted.
Max Rate in percentage	Maximum rate, expressed as percentage of total bandwidth
Interfaces	
Name	Displays the name of the interface that QoS will be configured on. Click **Add** to add an interface to the list.
Enable	Select to enable or clear to disable QoS on the interface.
Classification Group	One classification group “Default” is defined.
Calculate Overhead	Select to enable or clear to disable. Decreases upload and download ratio to prevent link saturation.
Half-duplex	Limit the interface to half-duplex mode.
Download Speed (kbit/sec)	Enter the download limit for the interface.
Upload Speed (kbit/sec)	Enter the upload limit for the interface.
Classification Rules	
Target	Select the target class. There can be one rule set for each class. If a target is deleted and you want to configure it, click **Add**.
Source Host	Enter the source IP address or IP and mask (CIDR notation). All packets that match this source host value will be included in the QoS target class.
Destination Host	Enter the destination IP address or IP and mask (CIDR notation). All packets that match this destination host value will be included in the QoS target class.
Protocol	Packets matching this protocol will be included in the target class
Ports	Packets matching this port or range of ports will be included in the target class.
Number of bytes	Packets matching this will be included in the target class.
Comment	Description field.

Load Balancing

Network > Load Balancing

Load balancing is a mechanism that enables balancing traffic between various links. It distributes traffic among various links, optimizing utilization of all the links to accelerate performance and reduce operating costs. Interfaces are assigned a priority by means of a metric.

How it works

Load balancing is determined by the load metric, in other words, the weight. Each link is assigned a relative weight and the gateway distributes traffic across links in proportion to the ratio of weights assigned to each individual link. This weight determines how much traffic will pass through a particular link relative to the other links.

Weights can be selected based on:

- Link capacity (for links with different bandwidth)
- Link/Bandwidth cost (for links with varying cost)

Note: *The default configuration of the load balancer is in Failover Mode with the highest priority given to WAN, then WWAN and then Cellular.*

MWAN Concept

On G520 series gateways, one or more sources of Internet can be used at the same time. In failover mode, the gateway uses one source of Internet and fails over to another according to defined priorities. Once the source with a higher priority is online, the same will be used as a primary source of Internet.

Priority can be defined by setting the metric. The lower the metric, the higher the priority.

The decision of when to failover or rollback is dependent on which interfaces are online and which ones are offline. Online and offline interface status is based on the PING responses to a particular server at a particular time interval. You can speed up the failover by sending PING packets in a shorter interval and you can add reliability by adding multiple server candidates.

Load balancing is where two or more sources of Internet are used at the same time and the load is split between the multiple interfaces in the ratio of their assigned weights.

The gateway supports a feature called WAN affinity whereby a particular source IP, Destination IP or a data type can be bound to a particular interface. To accomplish this, you need to create members which correspond to physical interfaces, assign the members in a particular policy, create rules and assign a policy to the rules.

In summary:

- Members correspond to physical interfaces with an assigned metric and weight
- Policy consists of a member or group of members
- Rules specify which traffic will use a particular policy

Globals

Network > Load Balancing > Globals

To configure MWAN global settings:

1. Go to Network > Load Balancing > Globals.

2. Enter or modify the settings. See *Table 12-31*.
3. Click **Save & Apply**.

Table 12-31 MWAN Globals Configuration

Parameters	Description
Firewall mask	Enter the firewall mask value in hexadecimal, starting with 0x.
Logging	Select to enable global firewall logging and select the log level.
Update Interval	Enter the update interval for the interface routing table. Default is 5 seconds.
Routing table lookup	Enter an additional routing table to be scanned for connected networks

Interfaces

Network > Load Balancing > Interfaces

To view and add MWAN interfaces:

1. Go to Network > Load Balancing.
2. The MWAN Interfaces table is displayed. See *Table 12-32*.
3. Go to the bottom of the table, enter the interface name and click **Add**.
4. Enter the interface settings. See *Table 12-33*.
5. Click **Save & Apply**.

Note: *Configuring a large number of tracking IP addresses, a high ping count, or a low ping interval time will result in faster switchover but will consume more data.*

Table 12-32 MWAN Interface

Parameters	Description
MWAN Interfaces	Displays the interfaces and provides options to add, edit, or delete items from the table. ◆ Enter the interface name (must match an existing interface name) and click **Add** to add member. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table.
Name	Name of the available Interface.
Enabled	Displays the Interface status. Yes for enabled No for disabled
Tracking method	Displays the method used to track the interface.
Tracking source	Displays the tracking source as address or interface.
Tracking reliability	Displays the number of tracking IP addresses. The acknowledgment/ responses from these tracking IP addresses are considered to determine the interface as up or down.
Ping interval	Displays the time in seconds between sending two successive ping packets.

Parameters	Description
Interface down	Displays the number of consecutive failed attempts after which the interface is declared offline.
Interface up	Displays the number of consecutive successful pings after which the interface is declared online.
Metric	Metric assigned to the interface.

Edit MWAN Interface

To edit MWAN interface settings:

1. Go to Network > Load Balancing > Interfaces.
2. To modify an interface, select the interface and click **Edit**.
3. Modify the settings. see *Table 12-33*.
4. Click **Save & Apply**.

Table 12-33 MWAN Interface Configuration

Parameters	Description
Enabled	Enable the Interface. ◆ No – Interface do not participate in Load Balancing. ◆ Yes – Interface is enabled and can connect to Internet. Once enabled it can be tracked using ping configuration.
Initial State	Offline – traffic goes via this interface only if the load balancer has checked the connection first. Online – the interface is marked as online immediately. Default is Online
Internet Protocol	Displays the internet protocol of the interface as IPv4 or IPv6.
Tracking hostname or IP address	IP Address to which the ping requests are sent from the interface to determine if the interface is up or down. Leave the field blank to assume the interface is always online.
Tracking method	Select the tracking method in use. Default is ping.
Tracking source	Select the tracking source to use. Options are Interface or Address
Tracking reliability	Enter the number of responses that must be received from tracking IP Addresses to consider the Interface as up.
Ping count	Enter the number of ping packets that will be sent. The default ping count is 5.
Ping size	Size of the ping request in bytes. Default value is 56.
Max TTL	Displays the Max Time to Live (Max TTL) timer value to be included in the packets that tells the recipient how long to hold or use the packet before expiring or discarding the packet or data.
Check link quality	Select to check link quality otherwise leave box unselected.

Parameters	Description
Ping timeout	Enter the time to wait for a response to ping request sent before declaring the interface unreachable. The wait time is in seconds. The default value depends on the interface used. Cellular will have different values to reduce data consumption.
Ping interval	Specifies the time in seconds between sending ping packets. The default ping interval is 5 seconds.
Interface down	The number of consecutive failed attempts after which the interface is declared down. The default value depends on the interface used. Cellular will have different values to reduce data consumption.
Interface up	The number of consecutive successful attempts to determine the reliability of the network connection through the interface. The default value depends on the interface used. Cellular will have different values to reduce data consumption.
Metric	Displays the Interface Metric. The route with least metric is considered as best route. The default metric assigned to the interface is 1. For load balancing between two interfaces, both the interfaces must have the same metric value on the Member configuration page.

Members

Network > Load Balancing > Members

MWAN Members are profiles corresponding to individual interfaces where you can set metric and weight.

To view and add MWAN members:

1. Go to Network > Load Balancing > Members.
2. The MWAN Members table is displayed. See *Table 12-34*.
3. To add a member profile, at the bottom of the table enter the name and click **Add**.
4. Enter the settings. See *Table 12-35*.
5. Click **Save & Apply**.

Table 12-34 MWAN Members

Parameters	Description
MWAN Members	Displays the members and provides options to add, edit, or delete items from the table. ◆ Enter a name and click **Add** to add member. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table. ◆ The buttons to the left of the Edit button can be used to reorder the items in the list. This does not change the configuration.
Name	Displays the interface member notation number.
Interface	Displays the name of the interface associated with the member.

Parameters	Description
Metric	Displays the metric assigned to the interface. The interface with the lowest metric has the highest priority and all data is always routed through it. ***Note:*** *If two or more interfaces have same metric configured and that metric is lowest compared to other interfaces, then the data/load is balanced and data/load is distributed among the two interfaces in the ratio of the respective weight.*
Weight	Displays the weight assigned to the interface. Members with the same metric will distribute load based on the weight value.
Add	Enter the name of the new interface to be added.

Edit MWAN Member

To edit an MWAN member:

1. Go to Network > Load Balancing > Members.
2. Select the member and click **Edit**.
3. Modify the configuration settings. See *Table 12-35*.
4. Click **Save & Apply**.

Table 12-35 MWAN Members Configuration

Parameters	Description
Interface	Select the name of the interface.
Metric	Enter the interface metric. The route with lowest metric is considered as best route. For load balancing between two interfaces, both the interfaces must have the same metric value.
Weight	Enter the interface weight. The default weight assigned to the interface is 2. For load balancing between two interfaces, both the interfaces must have the same metric value. The route with higher weight carries more traffic. Also the connections will be distributed amongst the interfaces with the same weight and not the actual data traffic.

Policies

Network > Load Balancing > Policies

Policies define how traffic is routed through the different WAN interfaces. Policy consists of a member or group of members. If a policy has one member, traffic will only go out through that member. If a policy has more than one member, members within the policy with a lower metric have precedence and are used first. Members with the same metric will be load balanced based on the assigned weight values.

Policy can also be configured to use one member and then fail over to another.

To view and add MWAN policies:

1. Go to Network > Load Balancing > Policies.

2. The MWAN Policies table is displayed. See *Table 12-36*.
3. To add a policy, at the bottom of the table enter the name and click **Add**.
4. Enter the settings. See *Table 12-37*.
5. Click **Save & Apply**.

Table 12-36 MWAN Policy

Parameters	Description
MWAN Policies	Displays the policies and provides options to add, edit, or delete items from the table. ◆ Enter a name and click **Add** to add policy. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table.
Name	Name of the policy. The name must be 15 characters or less, and may contain characters A-Z, a-z, 0-9, _ and no spaces. Policies must not share the same name as configured interfaces, members or rules.
Members assigned	Interface members to which the policy is applied.
Last resort	Displays the failover routing behavior when all WAN policy members are offline.
Errors	Displays if an error has occurred during the Policy configuration. Error messages are displayed as warnings.

Edit MWAN Policy

To edit MWAN policy:

1. Go to Network > Load Balancing > Policies.
2. Select the policy and click **Edit**.
3. Modify the configuration settings. See *Table 12-37*.
4. Click **Save & Apply**.

Table 12-37 MWAN Policy Configuration

Parameters	Description
Member used	Select the interface to apply the policy on for traffic passing through the interface.
Last Resort	Select the failover routing behavior when all WAN policy members are offline. Available options: ◆ unreachable (reject) ◆ blackhole (drop) ◆ default (use main routing table)

Rules

Network > Load Balancing > Rules

A rule specifies what traffic to match and what policy to assign for that traffic.

The MWAN Rules page displays the rules and provides options to add, edit, or delete items from the table. The Rules page also lists key points to consider when configuring rules.

To add MWAN rules:

1. Go to Network > Load Balancing > Rules.
2. The MWAN Policies table is displayed. See *Table 12-38*.
3. At the bottom of the Rules table, add a rule name and click **Add**.
4. Modify the configuration settings. See *Table 12-39*.
5. Click **Save & Apply**.

Table 12-38 MWAN Rules

Parameters	Description
MWAN Rules	Displays the rules and provides options to add, edit, or delete items from the table. ◆ Enter a name and click **Add** to add rule. ◆ Click **Edit** to modify a table entry. ◆ Click **Delete** to delete an entry from the table.
Name	Displays the rule name.
Source address	Displays the Source IP address.
Source port	Displays the Source port number.
Destination address	Displays the Destination IP address.
Destination port	Displays the Destination port number.
Protocol	Displays the protocols on which the rule is applicable.
Policy assigned	Policy to be applied to the rule.
Errors	Displays if an error has occurred during the rule configuration. Error messages are displayed as warnings.

Edit MWAN Rule

To edit MWAN rules:

1. Go to Network > Load Balancing > Rules.
2. Select the rule name and click **Edit**.
3. Modify the configuration settings. See *Table 12-39*.
4. Click **Save & Apply**.

Table 12-39 MWAN Rules Configuration

Parameters	Description
Source address	Enter the Source IP Address.

Parameters	Description
Source Port	Enter the Source Port number.
Destination address	Enter the Destination IP Address.
Destination port	Enter the Destination Port number.
Protocol	Select the protocols on which the rule is applicable.
Sticky	Select Yes to allow traffic from the same source IP address within the timeout limit to use the same WAN interface as the previous session. Otherwise, select No.
Sticky timeout	Enter the stickiness timeout value in seconds. If no value is entered, this defaults to 600.
IPset	Enter the name of the IPset rule. IPset lets you route traffic over WAN interfaces based on a set of IP addresses. When the ipset option is configured, the rule will match traffic directed at the given destination IP address to the ipset set.
Logging	Select Yes to enable firewall logging. The global load balancing logging setting must also be enabled. Otherwise, select No.
Policy assigned	Policy to be applied to the rule.

Notification

Network > Load Balancing > Notification

MWAN Notification lets you write custom MWAN actions, to be executed with each netifd hotplug interface event on interfaces for which MWAN is enabled. The file is interpreted as a shell script, and is preserved during sysupgrade.

The script must start with the line “#!/bin/sh” (without quotation marks).

Commented lines (lines starting with #) will not be executed.

Three main environment variables are passed to the script. They are described below:

```
# $ACTION
#       <ifup>          Is called by netifd and mwan3track
#       <ifdown>        Is called by netifd and mwan3track
#       <connected>     Is only called by mwan3track if tracking was
                        successful
#      <disconnected> Is only called by mwan3track if tracking has failed

# $INTERFACE           Name of the interface which went up or down
                      (e.g. "wan" or "wwan")

# $DEVICE             Physical device name which interface went up or down
                      (e.g. "eth0" or "wwan0")
```

13: Bluetooth

The G520 series gateways support dual-mode Bluetooth BR/EDR (Classic Bluetooth) and BLE wireless connectivity. The Serial Port Profile (SPP) is included for Bluetooth BR/EDR. Bluetooth SPP allows two Bluetooth devices to connect and exchange serial data using the Bluetooth SPP profile for tunneling.

Bluetooth Settings

Bluetooth > Settings

The Bluetooth Settings page lets you configure Bluetooth settings and scan for and pair to Bluetooth devices.

Configure Bluetooth settings

To configure Bluetooth settings:

1. Go to Bluetooth > Settings.
2. Next to Bluetooth State, select or clear the box to enable or disable Bluetooth.
3. Enter the configuration settings. See *Table 13-1*.

Table 13-1 Bluetooth Settings Configuration

Parameters	Description
Bluetooth State	Select to enable or clear to disable Bluetooth.
Device name	Displays the Bluetooth device name. The name can be edited. ***Note:*** *Changing the device name will disconnect any existing Bluetooth SPP master or slave connections.*
Device Address	Displays the Bluetooth device address.
Allow Discovery	Select to allow the gateway to be visible to other Bluetooth devices during a scan. Clear the box if you do not want the gateway to be visible to other Bluetooth devices during a scan.
Scan	Click **Scan** to scan for nearby discoverable Bluetooth devices. A device must be discoverable in order to pair to it.
Paired devices	Displays the paired devices. Click **Unpair** to unpair the device.

4. Click **Save & Apply**.

Scan for and Pair a Device

To scan for and pair to nearby devices:

1. On the Bluetooth Settings page under Scan, click **Scan**. The scan will take a few seconds to complete.
2. The Bluetooth Scan Result page shows the discovered devices and contains the following details:

Table 13-2 Bluetooth Scan Results

Parameters	Description
Device Address	Displays the Bluetooth device address.
Device Name	Displays the Bluetooth device name.
Type	Displays the Bluetooth service type that the device advertises. BR/EDR – the device advertises Bluetooth BR/EDR service type and supports SPP. BLE (Public or Random) – the device advertises BLE service type.
RSSI	Displays the signal strength of the Bluetooth device.
Pair	Click **Pair** to pair the device. The device that initiates the pairing, in this case the G520 series gateway, acts as the master device, and the paired device acts as the slave device.
Scan Again	Click **Scan Again** to run the scan again.
Dismiss	Click **Dismiss** to close this page.

3. Click **Pair**.

   The paired device appears under Paired devices.

To unpair a device:

1. On the Bluetooth Settings page under Paired Devices, view the paired devices.
2. In the row containing the device to be unpaired, click **Unpair**.

Bluetooth SPP

Bluetooth > Bluetooth SPP

Bluetooth SPP page allows you to configure the Bluetooth SPP connection.

To use Bluetooth SPP, the Bluetooth device and the gateway must first be paired. The master device makes the RFCOMM connection. Once the Bluetooth connection is established, configure a tunnel on the Bluetooth SPP line to enable serial data transmission.

Either device in the Bluetooth connection can be the master or the slave, and either can be the tunnel server or client.

The following describes the Bluetooth SPP roles:

- Master – The master is the device that initiates the pairing with the other Bluetooth device. The master device can:
  - establish the RFCOMM connection with the paired device
  - disconnect the RFCOMM connection
  - be configured in tunnel accept (server) or tunnel connect (client) mode
- Slave – The slave is the device that is paired. The slave device can:
  - disconnect the RFCOMM connection
  - be configured in tunnel accept (server) or tunnel connect (client) mode

Configure Bluetooth SPP Connection

To configure the Bluetooth SPP connection:

1. Select the Master tab to configure the gateway as the Bluetooth master device, or select the Slave tab to configure the gateway as the Bluetooth slave device.
2. Enter the line configuration settings. See *Table 13-3*.
3. To establish the connection, click the **Connect** button. To end a connection, click the **Disconnect** button.

Table 13-3 Bluetooth SPP Line Configuration

Parameters	Description
Name	Displays the line name. The name can be edited.
State	Select to enable or clear to disable the line.
Protocol	Select the protocol. ◆ **Tunnel** – the line will use tunnel over Bluetooth SPP connection. Tunnel will use the settings configured under the Server or Client tab to select tunnel accept or tunnel connect mode. ◆ **None** – no protocol will be used.
Gap Timer	Set the number of milliseconds to delay from the last character received before the driver forwards the received serial bytes. By default, the delay is four character periods at the current baud rate (minimum 1 msec). Gap timer range is 1 to 5000 milliseconds (default value is 4000 msec).
Threshold	Enter the number of threshold bytes which need to be received in order for the driver to forward received characters. Default value is 56 bytes.
Discover Channel	Select to enable.The number of channels supported is 30. If enabled, the device will cycle through channels 1-30 when attempting to connect to the peer device. If disabled, you can enter a specific channel to connect to peer device. This may reduce connection time if the peer device is listening on a channel other than channel 1.
RFCOMM	If Master tab was selected, click **Connect** to establish the connection or **Disconnect** to end the connection. If Slave tab was selected, click **Disconnect** to end the connection.

Configure Tunnel SPP Slave

To configure the Tunnel SPP Slave:

1. Go to Tunnel > Tunnel SPP Slave.
2. Enter the Accept configuration if the connection attempt originates from the network (see *Table 19-2, "Tunnel Accept Mode Configuration," on page 252*), or enter the Connect configuration if the connection attempt originates from the gateway (*Table 19-3, "Tunnel Connect Mode Configuration," on page 255*)
3. Click **Save & Apply**.
4. On the remote device, configure the tunnel server or client settings appropriate for the connection.

Configure Tunnel SPP Master

To configure the Tunnel SPP Master:

1. Go to Tunnel > Tunnel SPP Master.
2. Enter the Accept configuration if the connection attempt originates from the network (see *Table 19-2, "Tunnel Accept Mode Configuration," on page 252*), or enter the Connect configuration if the connection attempt originates from the gateway (*Table 19-3, "Tunnel Connect Mode Configuration," on page 255*)
3. Click **Save & Apply**.
4. On the remote device, configure the tunnel server or client settings appropriate for the connection.

14: Percepxion

The G520 series gateways come integrated with Percepxion® cloud platform to allow for the remote management of devices. To set up the Percepxion client, you need to configure the following settings:

- Percepxion Client – to connect to the Percepxion cloud platform.
- Line 1 and Line 2 – to enable remote management and data access to your application or device attached on the serial line.

Client

Percepxion > Client

To configure the Percepxion client:

1. Go to Percepxion > Line 1 (or Line 2).

   This page displays the configuration and status for the Percepxion client.
2. Enter the client and connection configuration information. See *Table 14-1*.
3. Click **Save & Apply**.

Table 14-1 Percepxion Client Configuration

Percepxion Client	Description
Enable	Select to enable or clear to disable the Percepxion client.
Device ID	Read only. Displays the gateway's Device ID. Device ID may be provisioned through Lantronix Provisioning Manager. *Note: Device ID can only be provisioned once. It will persist across resets.*
Serial Number	Read only. Displays the serial number of the device.
Device Name	Enter the Percepxion Device Name.
Device Description	Enter the Percepxion Device Description.
Status Update Interval (in minutes)	Enter the frequency that the gateway updates the device status to Percepxion. The valid range is between 1 minute and 1440 minutes (1 day).
Send Dynamic Updates	If selected, device agent will send updates for RSSI and Temperature. The fields will be updated dynamically on Percepxion. This field is disabled by default.
Content Check Interval (in hours)	Enter the frequency that the gateway checks Percepxion for updates to configuration or firmware. The valid range is between 1 hour and 2160 hours (90 days).
Apply Firmware Updates	Select to allow firmware updates to be applied via Percepxion. Enabled by default.
Apply Configuration Updates	Select the option to indicate when to apply configuration updates. ◆ **Always**: always apply configuration updates. ◆ **Never**: never apply configuration updates.
Reboot After Update	Automatically reboot device after configuration update.

Percepxion Client	Description
Allow Remote Connections	Select to allow remote connections or clear to disable. Enabled by default.
Audit Log	If checked, client will send audit events such as user login, firmware update, configuration update, and CLI access to Percepxion server.
Remote Access Local Port	Local port for remote access connection
Active Connection	Select the connection instance to use when connecting to Percepxion. You can configure two connections. The configuration options for Connection 1 and Connection 2 are listed below.
Connection 1/Connection 2	
Connect to	Select Cloud or On-premise connection.
Host	Enter the host name or IP address of the Percepxion server, used to register the device.
Port	Enter the Percepxion port. Default: 443
Secure Port	Select to enable or clear to disable the Percepxion client secure port 443.
Validate Certificates	Select to enable or clear to disable the validation of the Percepxion server certificates. To validate certificates, both MQTT Security and Secure Port must be enabled.
Local Port	Local port for Percepxion MQTT client. When configured, a total of 32 consecutive ports will be reserved.
MQTT State	Select to enable or clear to disable MQTT.
MQTT Port	Enter the port number of the Percepxion MQTT server. When configured, a total of 32 consecutive ports will be reserved.
MQTT Security	Select to enable SSL for MQTT.
MQTT Local Port	Local port for Percepxion MQTT client. When configured, a total of 32 consecutive ports will be reserved.
Use Proxy	Select to enable the use of a proxy for this connection. If enabled, complete the proxy fields displayed under the Use Proxy field. Disabled by default.
Proxy Type	Proxy server type. The supported type is SOCKS5.
Proxy Host	Hostname or IP address of the proxy server to be used.
Proxy Port	Port of the proxy server to be used. Default port is **80**.
User Name	Username for the proxy server.
Password	Password for the proxy server.

Percepxion Line

Percepxion > Line 1 (or Line 2)

Configure Percepxion Line settings to enable remote management and data access to your application or device attached on the serial line. The gateway offers 2 lines for configuration.

To configure Percepxion Line settings:

1. Go to Percepxion > Line 1 (or Line 2).

   This page displays the configuration and status for Percepxion Line.

2. Enter the following information. See *Table 14-2*.
3. Click **Save & Apply**.

Note: *The Serial line mode should be configured as None or Tunnel.*

Table 14-2 Percepxion Line

Percepxion Line	Description
Enable	Select to enable or clear to disable the Percepxion line client.
Project Tag	Enter the Percepxion project tag string, as provided by the Percepxion project administrator.
Status Update Interval	Enter the frequency in minutes that the gateway updates the device status to Percepxion. The valid range is between 1 minute and 1440 minutes (1 day).
Content Check Interval	Enter the frequency in hours that the gateway checks Percepxion for updates to configuration or firmware. The valid range is between 1 hour and 2160 hours (90 days).
Command Delimiter	Enter the command delimiter for attached serial devices. ***Note:*** *Send delimiter before command and after response is received.*

15: Discovery

Query port service running on the device allows network discovery of devices using Lantronix Provisioning Manager. If enabled, the device responds to auto-discovery messages on port 0x77FE.

Query Port

Discovery > Query Port

The Statistics section displays the query port status as enabled or disabled. If the query port state is enabled, it displays statistics such as the number of queries made and replied to, number of errors and the last connection (IP address).

Query port is enabled by default.

To enable or disable network discovery:

1. Go to Discovery > Query Port.
2. Under Configuration, select or clear **Enable**.
3. Click **Save & Apply**.

16: Serial

The G520 series gateways offer two serial ports. Serial port 1 uses a standard RS-232 interface and Serial port 2 uses the RS-485 interface. All serial settings such as baud rate, parity, data bits, stop bits, and flow control apply to these lines.

For wiring configuration details for the RS-485 port in half-duplex mode, see Appendix *B: Power Cable Schematic.*

The default serial settings:

- Baud rate: 115200
- Parity: None
- Data bits: 8
- Stop bits: 1
- Flow control: None

Serial Line Statistics

Serial line statistics contain information on bytes, queued bytes, breaks, flow control, parity errors, framing errors, overrun errors, no Rx buffer errors, CTS input, RTS output, DSR input, and DTR output.

To view line statistics, go to Serial and select Serial 1 or Serial 2.

Serial Line Configuration

To configure Serial line settings:

1. Go to Serial > Serial 1 for RS-232 or Serial 2 for RS-485.
2. Enter the line configuration settings. See *Table 16-1*.
3. Click **Save & Apply**.

Table 16-1 Serial Line Configuration

Parameters	Description
Name	Descriptive name.
Enabled	Select to enable the line on the serial port.
Interface	The interface of the Serial Port. ◆ If Serial 1 is selected, the interface is RS232. ◆ If Serial 2 is selected, the interface options are RS485 Full-Duplex (default) or RS485 Half-Duplex.
Termination	Termination of the RS485 bus, if available.
Is baudrate custom	If using a custom baud rate, select the box and add a value between 2400 bps and 921600 bps.

Parameters	Description
Baud Rate	Select the desired baud rate from the drop-down list. Baud rate options: 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400, 460800, 921600
Parity	Select parity from the drop-down list: ◆ None ◆ Even ◆ Odd
Data Bits	Select data bits from the drop-down list: ◆ 7 ◆ 8
Stop Bits	Select the stop bits from the drop-down list: ◆ 1 ◆ 2
Flow Control	Select the flow control from the drop-down list: ◆ None ◆ Hardware ◆ Software
Gap Timer	Set the number of milliseconds to delay from the last character received before the driver forwards the received serial bytes. By default, the delay is four character periods at the current baud rate (minimum 1 msec). Gap timer range is 1 to 5000 milliseconds (default value is 4000 msec).
Threshold	Set the number of threshold bytes which need to be received in order for the driver to forward received characters. Default value is 56 bytes.
Mode	Select the mode of serial communication as determined by the protocols available on the gateway model. ◆ None – can be used if Percepxion line is configured ◆ Tunnel – (see *Chapter 19: Tunnel*) ◆ Tunnel/Modbus RTU to Modbus TCP – (see *Tunnel Modbus RTU to Modbus TCP*) ◆ Managed Device ◆ DLMS Client – (see *DLMS Client*) ◆ DNP3 – (see *Modbus RTU to DNP3*) ◆ Modbus Master – (see *Modbus Master*) ◆ IEC 101 to 104 – (see*2. Click Submit, the configuration file begins to download.*) ◆ Management Console - Provides authenticated shell access on the serial lines (default mode)

17: SSL

Secure Sockets Layer (SSL) is a protocol that creates an encrypted connection between devices. It also provides authentication and message integrity services. SSL is used widely for secure communication to a Web server, and for wireless authentication.

SSL certificates identify the G520 series gateway to peers and are used with some methods of wireless authentication. Provide a name at upload time to identify certificates on the G520 series gateway.

You can upload Certificate and Private key combinations, obtained from an external Certificate Authority (CA), to the G520 series gateway. The G520 series gateway can also generate self-signed certificates with associated private keys.

Credentials

SSL > Credentials

The G520 series gateway can generate self-signed certificates and their associated keys for RSA and DSA certificate formats. When you generate certificates, assign them a credential name to help identify them on the G520 series gateway. After you create your credentials, then configure them with the desired certificates.

To configure a new credential:

1. Go to SSL > Credentials.
2. Type the name for your credential in the Credential Name field.
3. Enter the fields under Upload Certificate (see *Table 17-1*) or Create New Self-Signed Certificate (see *Table 17-2*).
4. Click **Save & Apply**. The process to create a self-signed certificate may take up to 30 seconds, depending on the length of the key.

   The newly created credential is displayed at the top of the SSL Credentials page.

To view a credential:

1. Go to SSL > Credentials.
2. Under Current Credentials, click the name of the credential to view its details.

To delete a credential:

1. Go to SSL > Credentials.
2. Under Current Credentials, click the **Delete** button next to the name of the credential.

Table 17-1 SSL Credentials - Upload Certificate

Field	Description
SSL Certificate	Click the **Select file...** button to browse to the SSL certificate to be uploaded. RSA or DSA certificates are allowed.

Field	Description
Certificate Type	Select the certificate type to upload: ◆ PEM ◆ PKCS7 ◆ PKCS12 For PKCS certificates, enter a password. Ensure that the certificate is formatted properly with a valid open and close tag.
SSL Private Key	Click the **Select file...** button to browse to the SSL private key to be uploaded. The key must belong to the entered certificate. Ensure that the private key associated to the selected certificate and that it is formatted properly with a valid open and close tag.
Key Type	Select the key type being uploaded: ◆ PEM ◆ Encrypted PEM ◆ PKCS12 For encrypted PEM or PKCS12 key types, enter a password.

Table 17-2 SSL Credentials - Create Self-Signed Certificate

Field	Description
Country (2 Letter code)	Enter the 2 letter code for the country where the organization is located. This is a two-letter ISO code (e.g., “US” for the United States).
State/Province	Enter the state or province where the organization is located.
Locality (City)	Enter the city where the organization is located.
Organization	Enter the organization name to which the G520 series gateway belongs.
Organization Unit	Enter the organization unit which specifies the department or organization to which the G520 series gateway belongs.
Common Name	Enter a network name for the gateway when installed in the user’s network (usually the fully qualified domain name). It is identical to the name that is used to access the gateway with a web browser without the prefix `http://`. In case the name given here and the actual network name differ, the browser will pop up a security warning when the gateway is accessed using HTTPS.
Expires	Type the date that the self-signed certificate expires in **mm/dd/yyyy** format.
Type	Select **RSA**, **DSA**, or **ECDSA**.
Key length	Select the key length in bits.

Trusted Authorities

SSL > Trusted Authorities

One or more authority certificates are used to verify the identity of a peer. Authority certificates are used with some wireless authentication methods. These certificates do not require a private key.

To upload an authority certificate:

1. Go to SSL > Trusted Authorities.
2. Enter the Upload Certificate fields. See *Table 17-3*.
3. Click **Save & Apply**.

Table 17-3 SSL Trusted Authority

Field	Description
SSL Certificate	Click the **Select file...** button to browse to an existing SSL authority certificate. RSA or DSA certificates are allowed. The format of the authority certificate can be PEM or PKCS7. PEM files must start with "`-----BEGIN CERTIFICATE-----`" and end with "`-----END CERTIFICATE-----`". Some certificate authorities add comments before and/or after these lines. Those comments must be deleted before upload.
Certificate Type	Select the certificate type through the drop-down list. This field may automatically update, depending upon extension of the certificate entered.
Clear	Click to clear the fields.

To delete an existing certificate authority:

1. Go to SSL > Trusted Authorities.
2. Under Current Certificate Authorities, click the **Delete** button next to the name of the authority.

18: Vehicle

The vehicle tracking and management features are available on G526RP (Transport Pack) models only.

To use the vehicle tracking features, GPS must be enabled. See *Services > GPS*. Also, to send SMS alerts, Ethernet SMS must be enabled. See *Services > SMS*.

This chapter describes how to configure the following:

- *Information*
- *Ignition*
- *Routes*
- *Parking*
- *Alerts*

Information

Vehicle > Information

The Information page contains the following sections:

- Driving Behavior and Trip Report
- Driving Behavior Thresholds
- Configuration

Driving Behavior and Trip Report

This sections displays the following information:

Table 18-1 Driving Behavior and Trip Report Details

Field	Description
Ignition	Current state of the ignition
Start time	Time when ignition was switched on
Start location	Location at which ignition was switched on
Distance	Distance traveled since ignition was switched on
Current location	Current device location
X-axis acceleration (m/s^2)	Current X-axis acceleration from accelerometer
Y-axis acceleration (m/s^2)	Current Y-axis acceleration from accelerometer
Z-axis acceleration (m/s^2)	Current Z-axis acceleration from accelerometer
Harsh brakes	Number of harsh brakes since ignition was switched on. This is based on the threshold.
Acceleration	Number of rapid accelerations since ignition was switched on. This is based on the threshold.

Field	Description
Sharp turns	Number of sharp turns since ignition was switched on. This is based on the threshold.
Stop time	Time when ignition was switched off
Stop location	Location when ignition was switched off

Driving Thresholds

This section displays the following information:

Table 18-2 Driving Thresholds

Field	Description
Maximum speed (km/h)	The device will publish GPS/Speed information when speed exceeds this threshold.
Harsh brake	The device will publish GPS/Speed information when accelerometer reading exceeds this threshold. Harsh brake counter will be incremented.
Acceleration	The device will publish GPS/Speed information when accelerometer reading exceeds this threshold.Acceleration counter will be incremented.
Sharp turn	The device will publish GPS/Speed information when accelerometer reading exceeds this threshold. Sharp turns counter will be incremented.
Publish time (s)	Frequency at which device will publish GPS/Speed information. This or Publish distance (m), whichever occurs first.
Publish distance (m)	Distance at which device will publish GPS/Speed information. This or Publish time (s), whichever occurs first.

Configuration

This section allows you to load the Google Maps Javascript API key.

You will need to load a Google Maps API key to visualize the geofences, areas, and routes using an interactive map. You will need a valid API key and a Google Cloud project with billing enabled to access Google core product.

To create a Google Maps API key:

1. Go to the Google Cloud Console at https://console.cloud.google.com/.
2. Sign in to your Google account or create a new one if you don't have one already.
3. Create a new project by clicking the menu in the top navigation bar and selecting **New Project**. Give it a name and click **Create**.
4. Enable billing for your project by clicking the **Billing** button on the left navigation menu and following the instructions to set up billing.
5. Click the **APIs & Services** option on the left navigation menu, then select **Credentials**.
6. Click the **Create credentials** button and select **API key**.
7. Copy the API key that is generated for you.
8. It is recommended that you restrict the usage of your API key. You can set up restrictions

under the **API restrictions** section. Select to restrict the following APIs: Maps JavaScript API and Maps Static API.

To load the Google Maps API key:

1. Go to Vehicle > Information.
2. In the Configuration section paste the Google Maps API key into the **Google Maps Javascript API key** field.
3. Click **Save & Apply**.

To verify and view Google Maps, go to the Routes page and add a geofence. Select the geofence and click **Edit**. The interactive map will be displayed.

Ignition

Vehicle > Ignition

The Ignition feature monitors the vehicle's ignition and shuts off the G526RP device or the LAN interface when the ignition is Off and start the device when the ignition is On. Use this feature to manage battery usage on the G526RP device.

Warning: ***Enable this option only when the device's IGN-pin is connected to the ignition sense of your vehicle. The device can be configured to shut down when the Ignition is OFF and will start only when the Ignition is ON.***

To configure ignition monitoring:

1. Go to Vehicle > Ignition.
2. Configure the Ignition settings. See *Table 18-3*.
3. Click **Save & Apply**.

Table 18-3 Ignition Configuration

Field	Description
Enable Ignition Monitoring	Enable or disable the ignition monitoring. *Warning:* ***Enable this option only when the device IGN-pin is connected to the ignition sense of your vehicle.*** ***The device can be configured to shut down when Ignition is Off and will only start when Ignition is On.***
Shutdown LAN interface	When selected, the device will shut down the LAN interface when ignition Off is detected.
Shutoff Device	When selected, the device will shut off when ignition Off is detected.
Shutoff Delay (in minutes)	Enter the time in minutes to wait before shutting off the device. The default is 0.

Routes

Vehicle > Routes

Overview

The Routes feature supports up to 3000 geofences (circular/rectangular), 32 areas, 32 routes, and one parking area (see *Vehicle > Parking*).

A geofence describes virtual boundaries or perimeters around a physical location using GNSS/GPS or other location-based technologies. A vehicle fitted with a G526RP (transport pack) cellular gateway that enters or leaves the predefined geofenced area raises an entry or exit event, respectively, that may generate an alert notification according to the alert configuration.

The process of creating a geofence involves the following steps:

1. Define (plan) the boundaries of the location or area you want to create a boundary around. This can be done by using GPS coordinates or by drawing a shape on a map and recording the coordinates of the shape.
2. Once you have defined the boundaries, decide whether to use Google Maps platform or enter the geofence parameters manually. To use Google Maps platform, you will need to load your Google Maps API key on the *Vehicle > Information* page.
3. Set up the geofence parameters including the coordinates, size, and shape of the boundary.
4. Set up the alerts that will be activated when the vehicle fitted with the GNSS-equipped device enters or exits the user-defined geographic boundary.
5. Test and monitor the geofence to track the movement of the assets within and across the boundary of the geofenced area.

Figure 18-1 shows an example a rectangular geofence displayed on the map. Entry and exit events occur when the GNSS-equipped device enters or exits the geofence, respectively.

Figure 18-1 Rectangular Geofence

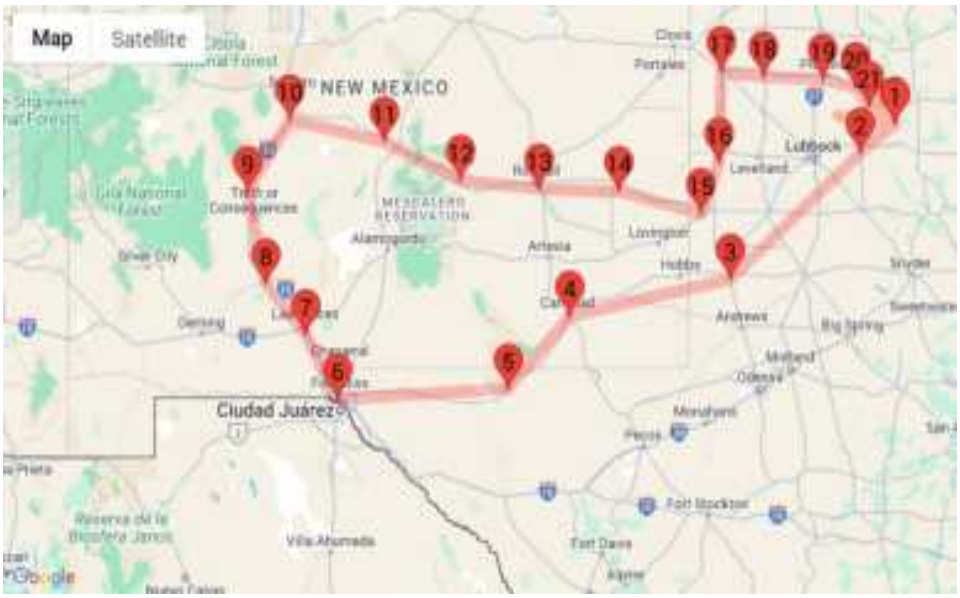
An *Area* is composed of up to 100 geofences. The geofences may be overlapping or not. *Figure 18-2* shows an example of a geographic area composed of overlapping rectangular geofences. Entry and exit events occur when the GNSS-equipped device enters or exits the area, respectively.

The area's boundary is automatically increased or decreased according to the set of the size of geofences. When the GNSS-equipped device enters or exits the predefined area, an inside or outside event occurs, respectively, and an alert notification is generated. If an area contains more than one overlapped geofence, then no area event occurs while the device is moving within the set of geofences within that area.

Figure 18-2 Geographic Area Composed of Overlapping Geofences

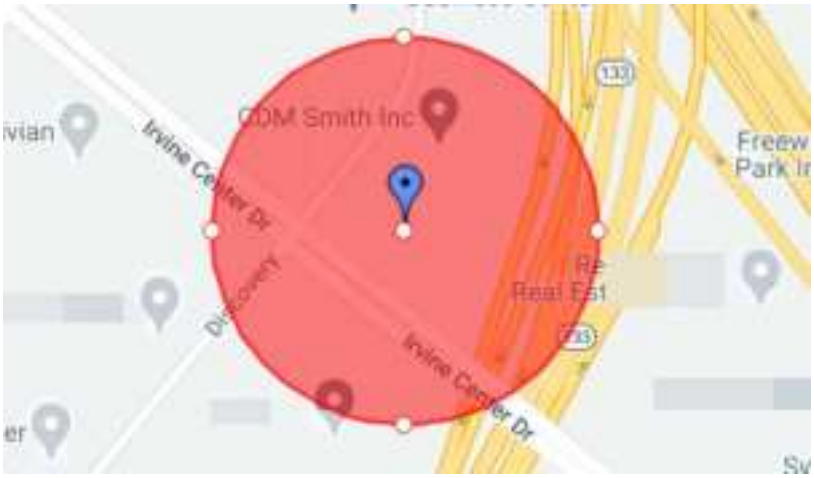
A *route* is a set of selected sequential points on the route to be followed by the vehicle. The highlighted *route* should follow the streets and intersections that the vehicle will go through along the route. Alerts are generated when the vehicle is on or off route. *Figure 18-3* shows the example of a *route*.

Figure 18-3 Route



A *parking area* is a circular geofence centered around the parked location of the vehicle fitted with the GNSS-equipped device. *Figure 18-4* shows an example of a parking area. The blue dot represents the GNSS-equipped device parked in the parking area. Events occur when parking is enabled and when the vehicle leaves the boundary of the parking area.

Figure 18-4 Parking Area



Geo-Fences Overview Page

The Geo-Fences Overview page displays the following information:

- Name - name of the geofence
- Enabled - (Yes/No) to indicate if the geofence is enabled or disabled.

- Parameters - to indicate the shape (rectangular/circular) and coordinates (latitude and longitude) of the geofence,
- Status - (In/Out) to indicate if the GPS device is inside or outside the boundaries of the geofence.

The Overview page includes the following actions:

Add button - to add a geofence

Edit button - to configure or modify the geofence configuration

Delete button - to delete a geofence

Note: *If you edit or delete a geofence, any areas using the geofence will also be affected.*

Add a Geofence

To add and configure a geofence:

1. Go to Vehicle > Routes. The Geo-Fences tab is highlighted.
2. Enter a unique geofence name and click **Add**. The name can contain up to 64 characters (A-Z, a-z, 0-9, underscore- (_), no spaces or special characters). The geofence is displayed in the list.
3. Select the geofence and click **Edit**. The map displays the geofence using its default settings (circular type, latitude and longitude at location of device, radius 200 meters).
4. Configure the type, location, and size of the geofence. You can modify the size and location by grabbing, dragging, and resizing the highlighted shape on the map or by modifying the type, latitude, longitude, and radius (for circular shape only) in the geofence configuration fields. For details, see *Table 18-4*.
5. Select the configured alert and enter the alert parameters. For details on how to create an alert, see *Alerts*.
6. Click **Save & Apply**.

Table 18-4 Geofence Configuration

Field	Description
Status	Indicates if the device is inside or outside the boundaries of the geofence. In - means that the device is located within the geofence boundary. Out - means that the device is located outside the geofence boundary.
Map	The interactive map displays the type (circular or rectangular), location and size of the geofence as a highlighted shape on the map, if the Google Maps API key has been configured (see *Information*). You can resize the geofence by clicking on the edge of the highlighted shape and dragging it to make it larger or smaller. You can move the location of the geofence by clicking inside the boundary of the highlighted shape and dragging it to the desired location on the map, or by editing the coordinates of the latitude and longitude.

Field	Description
Track current position	If this box is selected, the map displays the current position of the device and updates the displayed position when the device sends new location data. It is enabled by default.
Enable	Select to enable or clear disable the geofence. If enabled, alerts will be sent when the entry and exit events occur.
Type	Select the shape of the geofence. The options are: ◆ Rectangular ◆ Circular
Latitude (for rectangular shapes: Top Left Latitude and Bottom Right Latitude)	Displays the latitude of the selected shape in decimal degree format and allows you to configure the location and size of the geofence. ◆ For a rectangular shape, the top left latitude and bottom right latitude are required. ◆ For a circular shape, the latitude of the center of the circle is required. Enter the coordinates for the shape, in decimal degree format. ◆ When you edit the shape using the map, the latitude, longitude and radius (for circular shape) fields are automatically adjusted. Valid range: -90 to 90 ◆ Use 0 to 90 for positions north of the equator. ◆ Use 0 to -90 for positions south of the equator.
Longitude (for rectangular shapes: Top Left Longitude and Bottom Right Longitude)	Displays the longitude of the selected shape in decimal degrees format and allows you to configure the location and size of the geofence. ◆ For a rectangular shape, the top left longitude and bottom right longitude are required. ◆ For a circular shape, the longitude of the center of the circle is required. Enter the coordinates for the shape, in decimal degree format. ◆ When you edit the shape using the map, the latitude, longitude and radius (for circular shape) fields are automatically adjusted. Valid range: -180 to 180 ◆ Use 0 to 180 for positions east of the prime meridian. ◆ Use 0 to -180 for positions west of the prime meridian.
Radius	If Circular type is selected, this field displays the radius of the geofence in meters. The default radius is 200 meters. To edit the radius, enter the value in meters. Alternatively, on the map, grab and drag the outer edge of the highlighted circular shape.
Alert	Select the configured alert. For details on how to create an alert, see *Alerts*. ***Note:*** *Alerts can also be enabled or disabled on the Alerts page.*

Field	Description
Normal Message	Enter the notification message to be displayed when the device enters the geofence. The message may contain up to 64 characters and may include the following directives: %d System hostname %n Geofence name %x Current latitude %y Current longitude %z Current altitude
Normal Reminder Interval (in minutes)	Enter the time to wait before sending the normal message again. The valid range is between 1 and 1440 minutes. A zero value means that the reminder message will not be sent.
Alarm Message	Enter the notification message to be displayed when the device exits the geofence. The message may contain up to 64 characters and may include the following directives: %d System hostname %n Geofence name %x Current latitude %y Current longitude %z Current altitude
Alarm Reminder Interval (in minutes)	Enter the time to wait before sending the alarm message again. The valid range is between 1 and 1440 minutes. A zero value means that the reminder message will not be sent.

Areas Overview Page

The Areas Overview page displays information:

- Name - name of the area
- Enabled - (Yes/No) to indicate if the area is enabled or disabled.
- Geo-Fences - to indicate the geofences that compose the area,
- Status - (In/Out) to indicate if the GPS device is inside or outside the boundaries of the area.

The Overview page includes the following actions:

Add button - to add an area

Edit button - to configure or modify the area's configuration

Delete button - to delete an area

Add an Area

To add and configure an area:

1. Go to Vehicle > Routes. The Geo-Fences tab is highlighted.

2. Select the Areas tab.
3. Enter an area name and click **Add**. The name can contain up to 64 characters (A-Z, a-z, 0-9, underscore- (_), no spaces or special characters). The area is displayed in the list.
4. Select the area and click **Edit**. The Area Configuration page is displayed.
5. Configure the area and alert parameters. For details, see *Table 18-5*.
6. Click **Save & Apply**.

Table 18-5 Areas Configuration

Field	Description
Status	Indicates if the device is inside or outside the boundaries of the geofence. In - means that the device is located within the area boundary. Out - means that the device is located outside the area boundary.
Map	The interactive map displays the type (circular or rectangular), location and size of the area on the map, if the Google Maps API key has been configured (see *Information*). The area's boundary is drawn according to the set of geofences. To edit the area's shape, it is necessary to edit the shapes of the individual geofences that compose the area.
Track current position	If this box is selected, the map displays the current position of the device and updates the displayed position when the device sends new location data.
Enable	Select to enable or clear to disable the area. If enabled, alerts will be sent when the entry and exit events occur.
Fence settings	Choose the geofences that compose the sections of the area. The area may contain between 1 and 100 geofences. The --custom-- option is not currently supported.
Alert	Select the configured alert. For details on how to create an alert, see *Alerts*. ***Note:*** *Alerts can be enabled or disabled on the Alerts page.*
Normal Message	Enter the notification message to be displayed when the device enters the geofence or area. The message may contain up to 64 characters and may include the following directives: %d System hostname %n Geofence name %x Current latitude %y Current longitude %z Current altitude
Normal Reminder Interval (in minutes)	Enter the time to wait before sending the normal message again. The valid range is between 1 and 1440 minutes. A zero value means that the reminder message will not be sent.

Field	Description
Alarm Message	Enter the notification message to be displayed when the device exits the geofence or area. The message may contain up to 64 characters and may include the following directives: %d System hostname %n Geofence name %x Current latitude %y Current longitude %z Current altitude
Alarm Reminder Interval (in minutes)	Enter the time to wait before sending the alarm message again. The valid range is between 1 and 1440 minutes. A zero value means that the reminder message will not be sent.

Routes Overview Page

The Routes Overview page displays the following information:

- Name - name of the route
- Enabled - (Yes/No) to indicate if the area is enabled or disbaled
- Waypoints - The number of waypoints on the route. The are managed directly from Map view.
- Status - (In/Out) to indicate if the GPS device is inside or outside the boundaries of the route

The Overview page includes the following actions:

Add button - to add a route

Edit button - to configure or modify the route's configuration

Delete button - to delete a route

Add a Route

To add and configure a route:

1. Go to Vehicle > Routes. The Geo-Fences tab is highlighted.
2. Select the Routes tab.
3. Enter a route name and click **Add**. The name can contain up to 64 characters (A-Z, a-z, 0-9, underscore- (_), no spaces or special characters). The route is displayed in the list.
4. Select the route and click **Edit**. The Route Configuration page is displayed.
5. Configure the route and alert parameters. For details, see *Table 18-6*.

Click **Save & Apply**

Table 18-6 Route Configuration

Field	Description
Map	The interactive map displays the route on the map, if the Google Maps API key has been configured (see *Information*). The route is drawn according to the series of waypoints. Use the map to edit the waypoints. **Track Current Position** - If this box is selected, the map displays the current position of the device and updates the displayed position when the device sends new location data.
Enable	Select to enable or clear disable the route. If enabled, alerts will be sent when the entry and exit events occur.
Route radius (in m)	The default radius is 200 meters. To edit the radius, enter the value in meters.
Alert	Select the configured alert. For details on how to create an alert, see *Alerts*. ***Note:*** *Alerts can also be enabled or disabled on the Alerts page.*
Normal Message	Enter the notification message to be displayed when the device enters the route. The message may contain up to 64 characters and may include the following directives: %d System hostname %n Geofence name %x Current latitude %y Current longitude %z Current altitude
Normal Reminder Interval (in minutes)	Enter the time to wait before sending the normal message again. The valid range is between 1 and 1440 minutes. A zero value means that the reminder message will not be sent.
Alarm Message	Enter the notification message to be displayed when the device exits the route. The message may contain up to 64 characters and may include the following directives: %d System hostname %n Geofence name %x Current latitude %y Current longitude %z Current altitude
Alarm Reminder Interval (in minutes)	Enter the time to wait before sending the alarm message again. The valid range is between 1 and 1440 minutes. A zero value means that the reminder message will not be sent.

Parking

Vehicle > Parking

A Parking area is a circular area that contains the device placed inside the area, where the current position (including latitude and longitude) is the center of the circle and the user-specified parking radius value is the radius in meters of the circular area. The parking area raises events when the parking is enabled or when the GNSS-equipped device moves out of the parking area.

To configure a parking area:

To add a geofence:

1. Go to Vehicle > Parking.
2. Configure the parking area. You can do this by grabbing, dragging, and resizing the highlighted area on the map or by editing the configuration fields. For details, see *Table 18-7*.
3. Enter the alert parameters. For details on how to create an alert, see *Alerts*.
4. Click **Save & Apply**.

Table 18-7 Parking Configuration

Field	Description
State	Displays the state of the parking feature, enabled or disabled.
Parking location	Displays the latitude and longitude of the parking location.
Status	Indicates if the device is inside or outside the boundaries of the parking area. In - means that the device is located within the parking boundary. Out - means that the device is located outside the parking boundary.
Map	The interactive map displays the parking area (highlighted circle) with the device represented as a blue dot, if the Google Maps API key has been configured (see *Information*).
Track current position	If this box is selected, the map displays the current position (blue pin) of the device and periodically updates the displayed position when the device sends new location data.
Enable	Select to enable or clear to disable the parking area. If enabled, alerts will be sent when the entry and exit events occur.
Radius (meters)	Displays the radius of the parking area in meters. To edit the radius from the map, grab and drag the outer edge of the highlighted circular shape. Alternatively, to manually edit the radius, enter the new radius value in meters. The minimum radius is 200 meters. This is also the default radius.
Alert	Select the configured alert. For details on how to create an alert, see *Alerts*. ***Note:*** *Alerts can be enabled or disabled on the Alerts page.*

Field	Description
Normal Message	Enter the notification message to be displayed when the device enters the parking area. The message may contain up to 64 characters and may include the following directives: %d System hostname %n Geofence name %x Current latitude %y Current longitude %z Current altitude
Normal Reminder Interval (in minutes)	Enter the time to wait before sending the normal message again. The valid range is between 1 and 1440 minutes. A zero value means that the reminder message will not be sent.
Alarm Message	Enter the notification message to be displayed when the device exits the parking area. The message may contain up to 64 characters and may include the following directives: %d System hostname %n Geofence name %x Current latitude %y Current longitude %z Current altitude
Alarm Reminder Interval (in minutes)	Enter the time to wait before sending the alarm message again. The valid range is between 1 and 1440 minutes. A zero value means that the reminder message will not be sent.

Alerts

Vehicle > Alerts

The Alerts feature lets you configure the alert notification method or methods for the route, parking, and CAN Bus features. Alerts can be sent when when entry or exit events are raised with geofences, areas, and parking areas; or when broadcast messages are sent on the CAN bus.

To enable all alerts, select the **Alerts Enable** box on the Alerts Overview page. In this case, the enable setting on individual alerts will be ignored. When the **Alerts Enable** box is not checked (this is the default), the enable setting on individual alerts will be used.

The Overview section shows a list of the configured alerts. You can create up to 32 alerts.

Note: *If you edit or delete an alert, any geofences or areas using the alert will also be affected.*

To configure alerts:

1. Go to Vehicle > Alerts.
2. Enter a name and click **Add**. The name can contain up to 64 characters (A-Z, a-z, 0-9, underscore (_), no spaces or special characters). The alert is displayed in the list.
3. Select the alert and click **Edit**. Configure the alert. Note that one or more methods can be configured. For details, see *Table 18-8*.
4. Click **Save & Apply**.

Table 18-8 Alerts Configuration

Field	Description
Enable	Select to enable the individual alert. Clear to disable the alert. If set to disabled, this setting will be overridden when alerts are globally enabled on the Alerts Overview page (Alerts Enable box is selected).
SMS	This option is used to send SMS alerts. Enter up to 3 mobile numbers. The format is: +<mobile number with country code>. To send SMS alerts, Ethernet SMS must be enabled. See *Services > SMS*.
Serial Write	This option is used to send the alert notification on the serial line. Choose Serial 1 or Serial 2 to select the serial line.
LED	This option allows the alert to be displayed on one of two user LEDs. Choose the appropriate user LED from the options (G520-user1 or G520-user2). The LED behavior for Alarm On and Alarm Off is: Alarm On = LED On, when device is out of geofence or area, or when device receives a value for a CAN ID that is outside the defined minimum and maximum values Alarm Off = LED Off, when device is in geofence or area, or when device receives a value for a CAN ID that is inside the defined minimum and maximum values ***Note:*** *When the user LED is configured for an alert, it must not be configured elsewhere for any other applications.*

Field	Description
GPIO	This option is used to send alerts on the GPIO interface. Choose the appropriate Digital Output from the options (Digital Output 1 or Digital Output 2). The behavior is: Alert ON = GPIO High Alert OFF = GPIO Low

19: Tunnel

Tunneling allows serial devices to communicate over a network without being aware of the devices that establish the network connection between them. The Tunnel settings allow you to configure how the serial network tunneling operates. Tunneling is available on serial lines. The connections on one serial line are separate from those on another serial port.

Tunnel Statistics

Tunnel statistics contains data counters, error counters, connection time and connection information. Aggregate and individual connection statistics are displayed.

To view tunnel statistics, go to Tunnel and select Tunnel 1, Tunnel 2, Tunnel SPP Slave, or Tunnel SPP Master.

Tunnel Modbus RTU to Modbus TCP

The G520 series gateway acts as a converter between a Modbus RTU and a Modbus TCP device. Modbus RTU polls the data from the Modbus slave and sends it to the Modbus master using Modbus TCP.

To use this feature, configure the serial interface and TCP interface. You can use either the RS-232 or RS-485 interface.

To configure the serial interface:

1. Go to Serial and select Serial 1 (RS232) or Serial 2 (RS485).
2. Configure the serial port settings.
3. Select Mode as Tunnel/Modbus RTU to Modbus TCP.
4. Click **Save & Apply**.

To configure the TCP interface:

1. Go to Tunnel and select Tunnel 1 or Tunnel 2.
2. Under Modbus RTU to Modbus TCP, select **Enable** and then enter the configuration settings. See *Table 19-1*
3. Click **Save & Apply**.

Table 19-1 Tunnel for Modbus RTU to Modbus TCP

Field	Description
Enable	Select to enable and configure the Modbus RTU to Modbus TCP settings.
Protocol	TCP option is selected.

Field	Description
Mode	◆ **Server** - the gateway acts as a server and listens for the TCP connection from external Modbus master. TCP Port is required. ◆ **Client** - the gateway acts as a TCP client and sends the TCP connection request to the external Modbus master. IP address and TCP port of the Modbus master is required
IP	IP address of the external Modbus master on the LAN or WAN interface.
Port	Modbus TCP port number that the server is listening on. The default Modbus TCP port number is 502.
Backup Server Enable	Select to configure a backup Modbus master. Enter the IP address and port number.
Socket Timeout Enable	Select to configure socket timeout. Enter the Inactivity Timeout in seconds.

Tunnel Accept

In Tunnel Accept mode, the G520 series gateway listens (waits) for incoming connections from the network. Accept mode can be configured on Tunnel 1, Tunnel 2, Tunnel SPP Slave, or Tunnel SPP Master.

A remote node on the network initiates the connection. The configurable local port is the port the remote device connects to for this connection. There is no remote port or address. Supported serial lines and associated local port numbers progress sequentially in matching value. For instance, the default local ports are 10001 for serial line 1, 1002 for serial line 2, 10003 for Bluetooth SPP Slave, and 10004 for Bluetooth SPP Master. Serial data can still be received while waiting for a network connection, keeping in mind serial data buffer limitations.

To configure Accept mode:

1. Go to Tunnel > Tunnel 1, Tunnel 2, Tunnel SPP Slave, or Tunnel SPP Master.
2. Under Accept, enter the accept mode configuration settings. See *Table 19-2*.
3. Click **Save & Apply**.

Table 19-2 Tunnel Accept Mode Configuration

Field	Description
Mode	Set the method used to start the tunnel in Accept mode. Choices are: ◆ **Disable** - do not accept an incoming connection. ◆ **Always** - accept an incoming connection (*default*). ◆ **Any Character** - start waiting for an incoming connection when any character is read on the serial line. ◆ **Start Character** - start waiting for an incoming connection when the start character for the selected tunnel is read on the serial line.

Field	Description
Local Port	Set the port number for use as the network local port. The default local port number correlates with the tunnel instance: ◆ Tunnel 1: 10001 ◆ Tunnel 2: 10002 ◆ Tunnel SPP Slave: 10003 ◆ Tunnel SPP Master: 10004
Protocol	Select the desired security protocol: ◆ SSL ◆ TCP (*default protocol*) ◆ TCP AES ◆ Telnet Configure the protocol fields as determined by the protocol selection.
Secure Protocols	When using SSL, select the secure protocols and the SSL credential. Protocol options are: ◆ SSL3 ◆ TLS1.0 ◆ TLS1.1 (default selected) ◆ TLS1.2 (default selected) ◆ TLS1.3 (default selected)
TCP Keep Alive	The TCP keep alive time is the time in which probes are periodically sent to the other end of the connection to ensure the other side is still connected. Enter the TCP Keep Alive time in milliseconds. Set to 0 to disable TCP Keep Alive, and blank the field to restore the default.
TCP Keep Alive Interval	Enter the time, in milliseconds, to wait between Keep Alive probes in order to keep the TCP connection up during idle transfer periods. Blank the field to restore the default.
TCP Keep Alive Probes	Enter the number of TCP Keep Alive probes to send before closing the connection if no response is received. The probes are sent after the initial TCP Keep Alive probe is sent. Valid values are between 1 and 16. Blank the field to restore the default.
AES Encrypt Key	Enter the AES Encrypt Key. This configuration field becomes available when the TCP AES protocol is selected.
AES Encrypt Key Type	Select **Text** or **Hexadecimal** to indicate format. This configuration field becomes available when the TCP AES protocol is selected.
AES Decrypt Key	Enter the AES Decrypt Key. This configuration field becomes available when the TCP AES protocol is selected.
AES Decrypt Key Type	Select **Text** or **Hexadecimal** to indicate format. This configuration field becomes available when the TCP AES protocol is selected.

Field	Description
Initial Send	Enter the **Initial Send** data to be sent out the network upon connection establishment before any data from the Line. It may contain one or more **Directives** of the form `%<char>`. The Initial Send string can be entered in **Text** or **Binary** form. The Binary form allows square braces `[]` to enclose one or more character designations separated by commas. Use straight decimal numbers up to 255 or hexadecimal numbers prefixed with `0x` up to `0xFF` within the square braces. To specify an open brace in binary mode, use two in a row. Example The selection (in binary mode): `AB[255,0xFF]C[[D]` results in a string containing binary values where the dots appear: `AB...C[D]` **Directives** ◆ `%i` local IP address ◆ `%m` MAC address ◆ `%n` network interface name ◆ `%p` local port ◆ `%s` serial number ◆ `%%` %
Initial Send Type	The format of the initial send data. ◆ **Text** ◆ **Binary**
Flush Serial	Set whether the serial line data buffer is flushed upon a new network connection. Choices are: ◆ **Enabled** – serial data buffer is flushed on network connection ◆ **Disabled** – serial data buffer is not flushed on network connection (*default*)
Block Serial	Set whether Block Serial is enabled for debugging purposes. Choices are: ◆ **Enabled** – incoming characters from the serial line will not be forwarded to the network. Instead, they will be buffered and will eventually flow off the serial line if hardware or software flow control is configured. ◆ **Disabled** – this is the default setting; incoming characters from the serial line are sent to the network. Any buffered characters are sent first.
Block Network	Set whether Block Network is enabled for debugging purposes. Choices are: ◆ **Enabled** – incoming characters from the network will not be forwarded to the serial line. Instead, they will be buffered and will eventually flow off the network side. ◆ **Disabled** – this is the default setting; incoming characters from the network are sent to the serial line. Any buffered characters are sent first.
Password	The password can be up to 31 characters in length. Valid characters are alphanumeric characters and punctuation. When set, clients must send the correct password string to the device within 30 seconds from opening network connection in order to enable data transmission. The password sent to the device must be terminated with one of the following: ◆ 0A (Line Feed) ◆ 00 (Null) ◆ 0D 0A (Carriage Return/Line Feed) ◆ 0D 00 (Carriage Return/Null) If **Prompt for Password** is selected and a password is configured, the user will be prompted for the password upon connection.

Tunnel Connect

In Connect mode, the G520 series gateway continues to attempt an outgoing connection on the network until established. If the connection attempt fails or the connection drops, then it retries after a timeout. The remote node on the network must listen for the Connect mode's connection.

For Connect mode to function, it must be enabled, have a remote station (node) configured, and a remote port configured (TCP or UDP). When established, Connect mode is always on. Enter the remote station as an IPv4 or IPv6 address or DNS name. The gateway will not make a connection unless it can resolve the address. For Connect mode using UDP, the gateway accepts packets from any device on the network. It will send packets to the last device that sent it packets.

Note: *The port in Connect mode is not the same port as the one configured in Accept mode. The TCP keep alive time is the time in which probes are periodically sent to the other end of the connection. This ensures the other side is still connected.*

To configure Tunnel Connect mode:

1. Go to Tunnel > Tunnel 1, Tunnel 2, Tunnel SPP Slave, or Tunnel SPP Master.
2. Under Connect, enter the connect mode configuration settings. See *Table 19-3*.
3. Under Connect Host, configure 1 to 4 hosts. See *Table 19-4*.
4. Click **Save & Apply**.

Table 19-3 Tunnel Connect Mode Configuration

Field	Description
Connect Mode	Set the method to be used to attempt a connection to a remote host or device. Choices are: ◆ **Disable** – an outgoing connection is never attempted. (*default*) ◆ **Always** – a connection is attempted until one is made. If the connection gets disconnected, the gateway retries until it makes a connection. ◆ **Any Character** – a connection is attempted when any character is read on the serial line. ◆ **Start Character** – a connection is attempted when the start character for the selected tunnel is read on the serial line.
Host Mode	If more than one host is configured, set the method to be used to access multiple hosts. **Sequential –** A tunnel will connect to hosts in sequential order. Host 1 will be attempted first. If that fails, it will proceed in order to Host 2, 3, and then 4. When a connection drops, the cycle starts again with Host 1 and proceeds in order. (default setting) **Simultaneous –** A tunnel will connect to all hosts accepting a connection. Simultaneous connections occur at the same time to all listed hosts. The gateway supports a maximum of 4 host connections.
Local Port	Enter an alternative local port. The local port is set to <Random> by default but can be overridden. Blank the field to restore the default.
Reconnect Timer	Set the value of the reconnect timeout (in milliseconds) for outgoing connections established by the gateway. Valid range is 1 to 65535 milliseconds. Default is 15000.

Field (continued)	Description
Flush Serial	Set whether the serial line data buffer is flushed upon a new network connection. Choices are: ◆ **Enabled** – serial data buffer is flushed on network connection ◆ **Disabled** – serial data buffer is not flushed on network connection (*default*)
Block Serial	Set whether Block Serial is enabled for debugging purposes. Choices are: ◆ **Enabled** – If Enabled, incoming characters from the Serial Line will not be forwarded to the network. Instead, they will be buffered and will eventually flow off the serial line if hardware or software flow control is configured. ◆ **Disabled** – this is the default setting; incoming characters from the serial line are sent on into the network. Any buffered characters are sent first.
Block Network	Set whether Block Network is enabled for debugging purposes. Choices are: ◆ **Enabled** – If Enabled, incoming characters from the network will not be forwarded to the serial line. Instead, they will be buffered and will eventually flow off the network side. ◆ **Disabled** – this is the default setting; incoming characters from the network are sent on into the serial line. Any buffered characters are sent first.

Hosts

The Connect mode supports up to 4 hosts. Hosts may be accessed sequentially or simultaneously.

Notes:

Configure the keep alive timeout to be larger than the user timeout.

- *If the keep alive time expires, the user timeout is expired, and there are probes in flight, the connection will be reset. For this reason, it is recommended that if keep alive is used in conjunction with the user timeout, the keep alive timeouts be larger than the user timeout.*
- *If it is smaller, what will typically be seen is that the initial probe will be sent, then at the interval where the next probe would normally be sent, the connection will be reset, with no additional probes sent. Also note that in these cases: if the keep alive timer is significantly smaller than the user timeout, probes will continue to be sent for an unreachable host until the user timeout expires.*

The user timeout will not be an exact limit; in practice, it will always take somewhat longer for the connection to be closed.

- *If there is data in flight when the TCP retransmission timeout kicks in, the user timeout is checked as a limiting condition only when the timer expirations would normally be checked during RTO handling. The longer the user timeout is, the more likely it will expire between exponentially slower retransmissions, and the connection will not experience an error until the next retransmission timeout is checked.*
- *The user timeout expiration during retransmission returns an error to the application; it does not automatically reset the connection as happens with the keep alive timeout. It is up to the application (e.g., tunneling) to close the connection (this happens almost immediately with tunneling).*

Table 19-4 Host Configuration

Host Field	Description
Address	Enter the destination IP address or DNS address for the connection.
Port	Enter the TCP or UDP port number on the target host for the connection.
Protocol	Select the desired security protocol. ◆ SSL ◆ TCP ◆ TCP AES ◆ Telnet ◆ UDP ◆ UDP AES Configure the remaining protocol fields as determined by the protocol selection.
Secure Protocols	When using SSL, select the secure protocols and the SSL credential. Protocol options are: ◆ SSL3 ◆ TLS1.0 ◆ TLS1.1 (default selected) ◆ TLS1.2 (default selected) ◆ TLS1.3 (default selected)
TCP Keep Alive	Enter the time, in milliseconds, the gateway waits during a silent TCP connection before the first Keep Alive probe is sent to the remote host in order to keep the TCP connection up during idle transfer periods. Set to 0 to disable TCP Keep Alive, and blank the field to restore the default.
TCP Keep Alive Interval	Enter the time, in milliseconds, to wait between Keep Alive probes in order to keep the TCP connection up during idle transfer periods. Blank the display field to restore the default.
TCP Keep Alive Probes	Enter the number of TCP Keep Alive probes to send before closing the connection if no response is received. The probes are sent after the initial TCP Keep Alive probe is sent. Valid values are between 1 and 16. Blank the field to restore the default.
TCP User Timeout	Specify the amount of time the TCP segments will be retransmitted before the connection is closed.
AES Encrypt Key	Enter the AES Encrypt Key. This configuration field becomes available when the TCP AES or UDP AES protocol is selected.
AES Encrypt Key Type	Select **Text** or **Hexadecimal** to indicate format
AES Decrypt Key	Enter the AES Decrypt Key. This configuration field becomes available when the TCP AES or UDP AES protocol is selected.
AES Decrypt Key Type	Select **Text** or **Hexadecimal** to indicate format
Initial Send	Enter the Initial Send character to be sent out the network upon connection establishment before any data from the line. It may contain one or more **Directives** of the form `%<char>`. This configuration field becomes available when the TCP, UDP, or UDP AES protocol is selected.
Initial Send Type	Select **Text** or **Hexadecimal** to indicate format.
Credentials	If SSL is the selected protocol, select an existing credential from the drop-down list. Go to SSL > Credentials to create, view, or edit SSL credentials.
Validate Certificate	Select to enable validation of the SSL certificate on the server. This configuration field becomes available when the SSL protocol is selected.

Connecting Multiple Hosts

The Connect mode supports up to 4 hosts. Hosts may be accessed sequentially or simultaneously.

- **Sequential** – A tunnel will connect to hosts in sequential order. The host specified as Host 1 will be attempted first. If that fails, it will proceed to Host 2, 3, and 4. When a connection drops, the cycle starts again with Host 1 and proceeds in order. Sequential is the default Host mode.
- **Simultaneous** – A tunnel will connect to all hosts accepting a connection. Simultaneous connections occur at the same time to all listed hosts. The gateway can support a maximum of 4 connections.

Tunnel Disconnect

Disconnect specifies the optional conditions for disconnecting any tunnel connection that may be established. If any of these conditions are selected but do not occur and the network disconnects the tunnel, a Connect mode connection will attempt to reconnect. However, if none of these conditions are selected, a closure from the network is taken as a disconnected host.

To configure Disconnect settings:

1. Go to Tunnel > Tunnel 1, Tunnel 2, Tunnel SPP Slave, or Tunnel SPP Master.
2. Under Disconnect, enter the configuration settings.
3. Click **Save & Apply**.

Table 19-5 Tunnel Disconnect Configuration

Field	Description
Stop Character	Enter the Stop Character which, when received on the serial line, disconnects the tunnel. The Stop Character may be designated as a single printable character or as a control character. Control characters may be input in any of the following forms: `<control>J` or `0xA`(hexadecimal) or `\10` (decimal). To disable the Stop Character, blank the field, which sets it to `<None>`.
Flush Stop Character	Set whether to flush the stop character when the tunnel is disconnected. Options: ◆ **Enabled** ◆ **Disabled** (default)
Timeout	Enter the number of milliseconds a tunnel may be idle before disconnection. To disable the timeout, set the field to zero (0).
Flush Serial Data	Set whether to flush the serial line when the tunnel is disconnected. Choices are: ◆ **Enabled** ◆ **Disabled** (default)

Tunnel Serial

Tunnel Serial setting allows you to select the conditions in which Data Terminal ready (DTR) signal is asserted on the serial line.

To select Serial DTR option:

1. Go to Tunnel > Tunnel 1 or Tunnel 2
2. Under Serial, select the required DTR option.
   - **Asserted while connected** - The DTR is asserted whenever either a connect or an accept mode tunnel connection is active
   - **Continuously asserted**
   - **Unasserted**
   - **TruPort** - The DTR is asserted whenever either a connect or an accept mode tunnel connection is active with the Telnet Protocol RFC2217 saying that the remote DSR is asserted
3. Click **Save & Apply**.

A: Compliance Information

(According to ISO/IEC Guide and EN 45014)

Manufacturer's Name & Address:

Lantronix, Inc. 48 Discovery, Suite 250, Irvine, CA 92618 USA

Product Family:

G520 Series

Conforms to the following standards or other normative documents:

Table A-1 Regional Certifications

Country /	Specification
USA	FCC 47 CFR part 15 Subpart B FCC 47 CFR part 15 Subpart 22H, 22E, 27 & 90S FCC 47 CFR Part 15 Subpart E
Canada	ISED RSS-130 Issue 2 RSS-132 Issue 3 RSS-133 Issue 6 RSS 139 Issue 3 RSS195 Issue 2 RSS-199 RSS-247 Issue 2 RSS-GEN Issue 5
EU	EU Declaration of Conformity See *Figure A-1*.
Australia, New Zealand	AS/NZS CISPR 32:2015
Safety	UL/EN 60950-1 UL/EN 62368-1 CAN/CSA C22.2 62368-1-14 CAN/CSA C22.2 60950-1-07
Cellular Certification	PTCRB, AT&T

Table A-2 Country Transmitter IDs

Country	Specification
USA FCC ID	Cellular Module: N7NEM7455 Wi-Fi Module (pending): SQG-60SIPT
Canada IC ID	Cellular Module: 2417C-EM7455 Wi-Fi Module (pending): 3147A-602230C

FCC Statement

Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations are restricted to indoor usage only.

Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Antenna Installation

1) The antenna must be installed such that 20 cm is maintained between the antenna and users, and

2) The transmitter module may not be co-located with any other transmitter or antenna.

ISED Statement

This device complies with RSS-247 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-247 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

This device is intended only for use under the following conditions:

1) The antenna must be installed such that 20 cm is maintained between the antenna and users, and

2) The transmitter module may not be co-located with any other transmitter or antenna.

Cet appareil est conçu uniquement pour les intégrateurs OEM dans les conditions suivantes: (Pour utilisation de dispositive module)

1) L'antenne doit être installée de telle sorte qu'une distance de 20 cm est respectée entre l'antenne et les utilisateurs, et

2) Le module émetteur peut ne pas être coïmplanté avec un autre émetteur ou antenne.

EU Declaration of Conformity

Figure A-1 EU Declaration of Conformity

LANTRONIX®

CE

EU DECLARATION OF CONFORMITY

Manufacturer's Name: LANTRONIX, INC.
Manufacturer's Address: 7535 Irvine Center Drive, Suite 100, Irvine, CA. 92618. USA

Product Type: Gateway
Product Family: G520 Series
Model name: G526GP12S
Rated: 10.8-60 VDC
Intended use: Commercial installations, indoor use

Manufacturer's Quality System:

ISO 9001:2015 Certificate No. 74 300 4282 TUV Rheinland

Applicable EU Directives:

Low Voltage Directive (2014/35/EU)
- EN 62368-1:2020+A11:2020

EMC Directive (2014/30/EU)
- EN 301 489-1 V2.2.3 (2019-11)
- EN 301 489-17 V3.2.4 (2020-09)
- EN 301 489-19 V2.1.1 (2019-04)
- Draft EN 301 489-52 V1.1.2 (2020-12)
- EN 55032:2015+A11: 2020, Class B
- EN 61000-3-2:2019
- EN 61000-3-3:2013+A1:2019
- EN 55035:2017+A11:2020

RF Radio Directive (2014 / 53 / EU)
- EN 301 908-1 V13.1.1 (2019-11)
- EN 301 908-2 V13.0.1
- EN 301 908-13 V13.1.1
- EN 301 511 V12.5.1 (2017-03)
- EN 300 328 V2.2.2 (2019-07)
- EN 301 893 V2.1.1 (2017-05)
- EN 303 413 V1.2.1 (2021-04)

Healthy Directive (2014 / 53 / EU)
- EN 62311:2020

RoHS
1) 2011/65/EU Restriction of the use of Hazardous Substances in EEE (RoHS)
2) 2015/863/EU Change of Annex II from 2011/65/EU
3) Directive 2018/736/EU and 2018/741/EU
- EN 63000-2018

Statement of Conformity: The product specified above complies with applicable EU directive referenced, including the application of sound engineering practice.

Signature: _____ Date: April 6, 2022

Name: Fathi Hakam Title: VP of Engineering

CERT-00241 rev A

EU Statements

Table A-3 EU Statements

Code	Language	Statement
bg	Bulgarian	Lantronix, Inc., декларира, че този G520 Series отговаря на основните изисквания и други приложими разпоредби на Директива 2014/53 / ЕС. Пълният текст на декларацията на ЕС за съответствие е достъпен на следния интернет адрес: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Известие на ЕС за ограничения при употреба: Това устройство е ограничено само за вътрешна употреба. Може да не се работи на открито.
cs	Česky [Czech]	Lantronix, Inc. tímto prohlašuje, že tento G520 Series je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 2014/53/EU. Úplné znění ES prohlášení o shodě je k dispozici na této internetové adrese: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Oznámení EU o omezení používání: Toto zařízení je omezeno pouze na použití uvnitř. Nesmí být provozován venku.
da	Dansk [Danish]	Undertegnede Lantronix, Inc. erklærer herved, at følgende udstyr G520 Series overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU. Den fulde tekst til EU-overensstemmelseserklæringen er tilgængelig på følgende internetadresse: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads EU-meddelelse om begrænsninger i brug: Denne enhed er kun begrænset til indendørs brug. Det betjenes måske ikke udendørs.
de	Deutsch [German]	Hiermit erklärt Lantronix, Inc., dass sich das Gerät G520 Series in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 2014/53/EU befindet. Der vollständige Text der EU-Konformitätserklärung ist unter folgender Internetadresse abrufbar: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads EU-Hinweis zu Nutzungsbeschränkungen: Dieses Gerät darf nur in Innenräumen verwendet werden. Es darf nicht im Freien betrieben werden.

Code	Language	Statement
et	Eesti [Estonian]	Käesolevaga kinnitab Lantronix, Inc. seadme G520 Series vastavust direktiivi 2014/53/EU põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele. EL-i vastavusdeklaratsiooni täielik tekst on saadaval järgmisel Interneti-aadressil: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads EL-i teade kasutuspiirangute kohta: seda seadet saab kasutada ainult siseruumides. Seda ei tohi õues kasutada.
en	English	Hereby, Lantronix, Inc., declares that this G520 Series is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads EU Notice of Restrictions on Use: This device is limited to indoor use only. It may not be operated outdoors.
es	Español [Spanish]	Por medio de la presente Lantronix, Inc. declara que el G520 Series module cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/EU. El texto completo de la declaración de conformidad de la UE está disponible en la siguiente dirección de Internet: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Aviso de restricciones de uso de la UE: este dispositivo está limitado solo para uso en interiores. No puede ser operado al aire libre.
el	Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Lantronix, Inc. ΔΗΛΩΝΕΙ ΟΤΙ G520 Series ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU. Το πλήρες κείμενο της δήλωσης συμμόρφωσης της ΕΕ διατίθεται στην ακόλουθη διεύθυνση διαδικτύου: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Ειδοποίηση της ΕΕ για περιορισμούς χρήσης: Η συσκευή αυτή περιορίζεται μόνο σε εσωτερικούς χώρους χρήσης. Μπορεί να μην λειτουργεί σε εξωτερικούς χώρους.

Code	Language	Statement
fr	Français [French]	Par la présente Lantronix, Inc. déclare que l'appareil G520 Series est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/EU. Le texte complet de la déclaration de conformité UE est disponible à l'adresse Internet suivante : https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Avis de restrictions d'utilisation de l'UE: Cet appareil est limité à une utilisation en intérieur uniquement. Il ne doit pas être utilisé à l'extérieur.
is	Icelandic	Hér með lýsir Lantronix, Inc. því yfir að G520 Series sé í samræmi við grunnkröfur og önnur viðeigandi ákvæði tilskipunar 2014/53 / ESB. Í heildartexta ESB-samræmisyfirlýsingarinnar er að finna á eftirfarandi internetfangi: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Tilkynning ESB um takmarkanir á notkun: Þetta tæki er eingöngu takmarkað við notkun innanhúss. Það má ekki nota það úti.
it	Italiano [Italian]	Con la presente Lantronix, Inc. dichiara che questo G520 Series è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/EU. Il testo completo della dichiarazione di conformità UE è disponibile al seguente indirizzo Internet: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Avviso di restrizioni d'uso dell'UE: questo dispositivo è limitato esclusivamente all'uso in interni. Potrebbe non essere utilizzato all'aperto.
lv	Latviski [Latvian]	Ar šo Lantronix, Inc. deklarē, ka G520 Series atbilst Direktīvas 2014/53/EU būtiskajām prasībām un citiem ar to saistītajiem noteikumiem. Pilns ES atbilstības deklarācijas teksts ir pieejams šādā tīmekļa vietnē: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads ES paziņojums par lietošanas ierobežojumiem: šo ierīci var izmantot tikai iekštelpās. To nedrīkst darbināt ārpus telpām.
lt	Lietuvių [Lithuanian]	Šiuo Lantronix, Inc. deklaruoja, kad šis G520 Series atitinka esminius reikalavimus ir kitas 2014/53/EU Direktyvos nuostatas. Visą ES atitikties deklaracijos tekstą galite rasti šiuo interneto adresu: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads ES pranešimas apie naudojimo apribojimus: Šis prietaisas skirtas naudoti tik patalpose. Jo negalima naudoti lauke.

Code	Language	Statement
nl	Nederlands [Dutch]	Hierbij verklaart Lantronix, Inc. dat het toestel G520 Series overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU. De volledige tekst van de EU-conformiteitsverklaring is beschikbaar op het volgende internetadres: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads EU kennisgeving van gebruiksbeperkingen: dit apparaat is beperkt tot gebruik binnenshuis. Het mag niet buitenshuis worden gebruikt.
mt	Malti [Maltese]	Hawnhekk, Lantronix, Inc., jiddikjara li dan G520 Series jikkonforma malħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/EU. It-test sħiħ tad-dikjarazzjoni ta 'konformità tal-UE huwa disponibbli fl-indirizz tal-internet li ġej: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Avviż tal-UE dwar Restrizzjonijiet fuq l-Użu: Dan l-apparat huwa limitat għal użu ġewwa biss. Ma jistax jitħaddem barra.
hu	Magyar [Hungarian]	Alulírott, Lantronix, Inc. nyilatkozom, hogy a G520 Series megfelel a vonatkozó alapvetõ követelményeknek és az 2014/53/EU irányelv egyéb elõírásainak. Az EU-megfelelőségi nyilatkozat teljes szövege a következő internetes címen érhető el: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads EU értesítés a korlátozásokról: Ez az eszköz csak beltéri használatra korlátozódik. Lehet, hogy szabadban nem üzemeltethető.
no	Norwegian	Lantronix, Inc. erklærer herved at denne G520 Series er i samsvar med de grunnleggende kravene og andre relevante bestemmelser i direktiv 2014/53 / EU. Den fullstendige teksten til EU-samsvarserklæringen er tilgjengelig på følgende internettadresse: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads EUs merknad om bruksbegrensninger: Denne enheten er bare begrenset til innendørs bruk. Det kan hende at den ikke brukes utendørs.

Code	Language	Statement
pl	Polski [Polish]	Niniejszym Lantronix, Inc. oświadcza, że EMG 8500 jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 2014/53/EU. Pełny tekst deklaracji zgodności UE jest dostępny pod następującym adresem internetowym: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Zawiadomienie UE o ograniczeniach użytkowania: To urządzenie jest przeznaczone wyłącznie do użytku w pomieszczeniach. Nie można go obsługiwać na zewnątrz.
pt	Português [Portuguese]	Lantronix, Inc. declara que este G520 Series está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU. O texto completo da declaração UE de conformidade está disponível no seguinte endereço na Internet: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Aviso da UE de restrições de uso: Este dispositivo está limitado apenas ao uso interno. Não pode ser operado ao ar livre.
ro	Romanian	Prin prezenta, Lantronix, Inc., declară că acest G520 Series respectă cerințele esențiale și alte dispoziții relevante din Directiva 2014/53 / UE. Textul complet al declarației de conformitate a UE este disponibil la următoarea adresă de internet: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Notificarea UE privind restricțiile de utilizare: Acest dispozitiv este limitat numai la uz interior. Este posibil să nu funcționeze în aer liber.
sr	Serbian	Овиме, Лантроник, Инц., изјављује да је овај G520 Series у складу са суштинским захтевима и осталим релевантним одредбама Директиве 2014/53 / ЕУ. Комплетан текст ЕУ изјаве о усаглашености доступан је на следећој Интернет адреси: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Обавештење ЕУ о ограничењима употребе: Овај уређај је ограничен само на унутрашњу употребу. Можда се не користи на отвореном.
sl	Slovensko [Slovenian]	Lantronix, Inc. izjavlja, da je ta G520 Series v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 2014/53/EU. Celotno besedilo izjave EU o skladnosti je na voljo na naslednjem spletnem naslovu: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Obvestilo EU o omejitvah uporabe: Ta naprava je omejena samo na notranjo uporabo. Morda ga ne uporabljate na prostem.

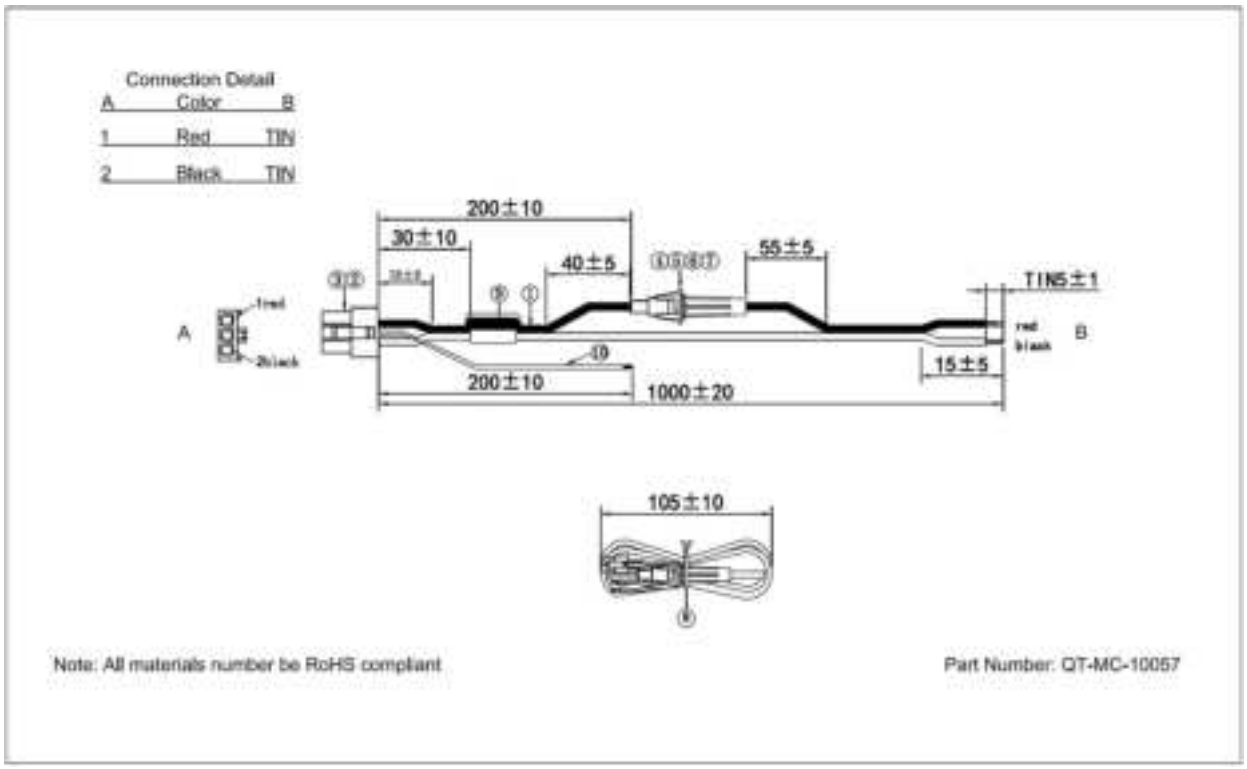
Code	Language	Statement
sk	Slovensky [Slovak]	Lantronix, Inc. týmto vyhlasuje, že G520 Series enterprise Wi-Fi IoT module spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 2014/53/EU. Úplné znenie EÚ vyhlásenia o zhode je k dispozícii na tejto internetovej adrese: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads Oznámenie EÚ o obmedzeniach pri používaní: Toto zariadenie je obmedzené iba na použitie v interiéri. Nesmie sa používať vonku.
fi	Suomi [Finnish]	Lantronix, Inc. vakuuttaa täten että G520 Series tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen. EU-vaatimustenmukaisuusvakuutuksen koko teksti on saatavana seuraavassa Internet-osoitteessa: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads EU: n ilmoitus käyttörajoituksista: Tämä laite on rajoitettu vain sisäkäyttöön. Sitä ei saa käyttää ulkona.
sv	Svenska [Swedish]	Härmed intygar Lantronix, Inc. att denna G520 Series står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU. Den fullständiga texten till EU-försäkran om överensstämmelse finns på följande internetadress: https://www.lantronix.com/products/lantronix-emg/#tab-docs-downloads EU-meddelande om begränsningar för användning: Den här enheten är endast begränsad till inomhusbruk. Det får inte användas utomhus.

B: Power Cable Schematic

Power Cable Schematic

3-pin power cable schematic

Figure B-1 3-pin Power Cable



C: List of Acronyms and Protocols

Acronym	Description
2G	2nd Generation
3G	3rd Generation
AES	Advanced Encryption Standard
AP	Access Point (or wireless access point) is a device that provides wireless service for clients within its coverage area.
APN	Access Point Name is the name of an access point for the cellular network data connection.
ASDU	Application Service Data Unit is the IEC-101/IEC-104 data structure that holds application layer information to exchange between a control center and a remote terminal unit.
CHAP	Challenge handshake protocol is used by PPP to authenticate users and can be used with many VPNs.
CSQ	Cellular Signal Strength (CSQ). It ranges from 0 to 32.
DHCP	Dynamic Host Configuration Protocol is a standardized networking protocol used by hosts to dynamically discover and lease an IP address, and learn the correct subnet mask, default gateway, and DNS server IP address.
DIO	Digital Input/Output
DLMS	Device Language Message Specification is a set of standards for electricity meter data exchange.
DMZ	Demilitarized Zone is a physical or logical sub network that contains and exposes an organization's external-facing services to a larger and un-trusted network, usually the Internet.
DNP3	Distributed Network Protocol version 3 is a protocol used for automation and remote control communication with serial and TCP/IP capabilities used in SCADA environments.
DNS	Domain Name System is an application layer protocol used throughout the Internet for translating hostnames into their associated IP addresses.
DynDNS, DDNS	Dynamic DNS is a method of automatically updating a name server in the Domain Name System (DNS), often in real time, with the active DNS configuration of its configured hostnames, addresses or other information.
EDGE	Enhanced Data rates for GSM Evolution (EDGE) is a backwards-compatible extension of GSM that provides higher data transmission rates than GSM
GPRS	General packet radio service is a packet oriented mobile data standard on the 2G and 3G cellular communication network's GSM
GPS	Global Positioning Satellite
GSM	Global system for mobile communications
HT Physical mode	High Throughput Physical Mode
IEC-101/IEC-104	IEC-101 (serial) and IEC-104 (TCP) are part of the IEC 60870-5 set of standards that define systems or methods used for telecontrol in electrical engineering and power system automation applications.

Acronym	Description
ICMP	Internet Control Message Protocol (ICMP) is a TCP/IP network layer protocol that reports errors and provides other information relevant to IP packet processing.
IGMP	Internet Group Management Protocol is a communications protocol used by hosts and adjacent gateways on IP networks to establish multicast group memberships
IKEv1 and IKEv2	Internet Key Exchange (version 1 or version 2) is an encryption key exchange mode used between two peers.
IPsec	Internet Protocol Security is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.
ISP	Internet service provider
L2TP	Layer Two Transport Protocol
LAN	Local Area Network
LED	Light emitting diode
M2M	Machine to machine
MAC address	Media Access Control address is a unique identifier (6 bytes) assigned to a network interface for use as a network address.
MD5	MD5 is a message digest algorithm used as a checksum to verify data integrity
Modbus	Modbus is a data communication protocol used for connecting industrial electronic devices.
MTU	Maximum transmission unit of a communications protocol of a layer is the size (in bytes) of the largest protocol data unit that the layer can pass onwards
MWAN	multiple WAN interface
NAT	Network Address Translation is a method of translating IP addresses that are not globally unique into public addresses in the globally routable address space.
NMS	Network Management System. Component in SNMP architecture that includes SNMP manager.
NTP	Network Time Protocol is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks
PAP	Password Authentication Protocol is a password based protocol used by PPP (point to point protocol) to authenticate users and can be used with many VPNs. PAP is considered less secure than CHAP or some other authentication protocols.
PDU	Protocol Data Unit
PoE	Power over Ethernet describes standards for passing electric power and data over Ethernet cabling between the Power Sourcing Equipment (PSE) and the Powered Device (PD).
PLC	Programmable Logic Controller
PPP	Point to Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol

Acronym	Description
PSK	Pre-shared key
QoS	Quality of Service
RF	Radio Frequency
RTU	Remote terminal unit
Rx	Reception
SCP	Secure Copy Protocol
SHA1/SHA2	Secure Hash Algorithm is an encryption cipher type
SIM	Subscriber identity module
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SPI	Serial Peripheral Interface
SSH	Secure Shell
SSID	Service Set Identifier
SSL/TLS	Secure Sockets Layer/Transport Layer Security are encryption-based security protocols designed to provide data security for Internet communications.
STP	Spanning Tree Protocol is a network protocol that prevents loops when switches or bridges are interconnected through multiple paths.
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
Tx	Transmission
UDP	User Datagram Protocol
VPN	Virtual private network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area network
WPA/WPA2/WPA3	Wi-Fi Protected Access® (WPA) family of technologies are security protocols for wireless networks.

D: Running Commands

Commands can be run on the G520 series gateway using the following methods:

- SSH (login as root using SSH)

  The user has full control and can run commands as described.

- System/Custom commands

  The user can run commands as described. It is not recommended to run a command or series of commands (in a series, commands are separated by semicolon) which take more than 60s to complete or require additional user interaction. For example: `vi`.

- Percepxion/CLI commands

  The user can run commands as described. It is not recommended to run a command or series of commands (commands separated by semicolon) which take more than 60s to complete or require additional user interaction. For example: `vi`.

Types of Commands

The following types of commands are available:

- Bash commands
- opkg commands
- UCI commands

Bash Commands

Bash shell is distributed with Busybox which provides a stripped down implementation of common Linux commands.

Usage

BusyBox is a multi-call binary. A multi-call binary is an executable program that performs the same job as more than one utility program. That means there is just a single BusyBox binary, but that single binary acts like a large number of utilities. This allows BusyBox to be smaller since all the built-in utility programs can share code for many common operations.

Please refer to https://www.busybox.net/downloads/BusyBox.html for usage of these commands.

Note: *Some configuration and commands may not be available on the gateway.*

Bash Command Examples

`ls`

List directory contents

Example

To show current directory contents:

```
# ls
bin        etc       lib          ltrx_user     overlay      rom
sbin       tmp       var
dev        http      ltrx_private  mnt          proc        root
sys        usr       www
```

ifconfig

Configure a network interface

Example

To show information for eth1 interface:

```
# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr A4:AE:9A:04:84:24
          inet addr:172.19.100.119  Bcast:172.19.255.255
Mask:255.255.0.0
          inet6 addr: 2001:db80:ac13:d91e:a6ae:9aff:fe04:8424/64
Scope:Global
          inet6 addr: fe80::a6ae:9aff:fe04:8424/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:102970 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8137 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6833857 (6.5 MiB)  TX bytes:1812823 (1.7 MiB)
          Interrupt:32
```

ip

Replaces the older and now deprecated ifconfig command. The ip command can display and administer the network configuration of a system. It is used to view, add, and delete network interfaces, routing table entries, and IP addresses.

Example

To show current routing table:

```
# ip route
default via 172.19.0.1 dev eth1 proto static src 172.19.100.119 metric
5
default via 172.19.0.1 dev wlan0 proto static src 172.19.100.136 metric
6
default via 63.42.182.202 dev wwan0 proto static src 63.42.182.201
metric 7
63.42.182.200/30 dev wwan0 proto static scope link metric 7
172.19.0.0/16 dev eth1 proto static scope link metric 5
172.19.0.0/16 dev wlan0 proto static scope link metric 6
192.168.13.0/24 dev br-lan proto kernel scope link src 192.168.13.1
```

cat

Displays the contents of a file

Example

To show contents of a file:

```
# cat /etc/sysupgrade.conf
## This file contains files and directories that should
## be preserved during an upgrade.

# /etc/example.conf
# /etc/openvpn/
/etc/confdone
/etc/sysupgrade.conf
/etc/hwinfo.json
/ltrx_private/cfg/
/etc/board.json
```

logread

Displays logs for diagnostics and troubleshooting

Example

To show syslogd diagnostic logs

```
# logread
Oct 11 20:00:16 Lantronix-G526RP-A4AE9A048423 user.info Eventsms:
TEMPERATURE : 40.00 °Celsius
Oct 11 20:00:16 Lantronix-G526RP-A4AE9A048423 user.info Eventsms:
CONF_BAND : LTE: [ B2 B4 B5 B13 B66 ]
Oct 11 20:00:16 Lantronix-G526RP-A4AE9A048423 user.info Eventsms:
REG_BAND : B4
Oct 11 20:00:16 Lantronix-G526RP-A4AE9A048423 user.info Eventsms:
Operator : 311480
Oct 11 20:00:16 Lantronix-G526RP-A4AE9A048423 user.info Eventsms:
Operator : Verizon
Oct 11 20:00:16 Lantronix-G526RP-A4AE9A048423 user.info Eventsms:
OperatorType : LTE
```

opkg Commands

The functionality of the system can be upgraded by downloading and installing pre-made packages from package repositories. The packages may be built using the SDK or hosted on the Lantronix package server (at update.lantronix.com).

opkg update

Update the packages list

opkg install

Install software package

opkg remove

Remove software package

Example

To update the packages list, install, and remove zerotier package:

```
# opkg update

# opkg install zerotier
Installing zerotier (1.4.6-1) to root...
Downloading http://update.lantronix.com/G526RP/ipks/main/
zerotier_1.4.6-1_arm_arm926ej-s.ipk
Installing libminiupnpc (2.1.20190408-2) to root...
Downloading http://update.lantronix.com/G526RP/ipks/main/
libminiupnpc_2.1.20190408-2_arm_arm926ej-s.ipk
Installing libnatpmp (20150609-1) to root...
Downloading http://update.lantronix.com/G526RP/ipks/main/
libnatpmp_20150609-1_arm_arm926ej-s.ipk
Configuring libminiupnpc.
Configuring libnatpmp.
Configuring zerotier.
disabled in config

# opkg remove zerotier
Removing package zerotier from root...
```

Please refer to: https://openwrt.org/docs/guide-user/additional-software/opkg for usage of the opkg command.

Note: *The System > Software menu on the Web GUI of the gateway provides methods to configure repositories and install software packages. See* *Software on page 79**.*

UCI Commands

Unified Configuration Interface (UCI) is a small utility written in C (a shell script-wrapper is available as well) and is intended to centralize the whole configuration of the router.

Example

To change Percepxion client status update interval:

```
# uci get percepxion.Basic.Status_Update_Interval
1
# uci set percepxion.Basic.Status_Update_Interval=5
# uci commit percepxion
# /etc/init.d/percepxion reload
Changed Status Update Interval to '5 minutes'.
```

Please refer to: https://openwrt.org/docs/guide-user/base-system/uci for usage of the UCI commands.

Note: *Some configuration and commands may not be available on the router.*

D: Lantronix Technical Support

Lantronix offers many resources to support our customers and products at http://www.lantronix.com/support.

For example, you can browse the knowledge base, open a support issue, find firmware downloads, view tutorials, and more. At this site you can also find FAQs, product bulletins, warranty information, extended support services, and product documentation.

To submit a support request, please use the Lantronix Technical Support portal at https://ltrxdev.atlassian.net/wiki/spaces/LTRXTS/overview (registration required).

To contact Lantronix Sales, look up your local office at https://www.lantronix.com/about-us/contact/.