ePACK User Manual
E210 and E220 Series Devices

Part Number PMD-00018
Revision E May 2024

Intellectual Property

© 2024 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/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.

Open Source Software

Some applications are Open Source software licensed under the Berkeley Software Distribution (BSD) license, the GNU General Public License (GPL) as published by the Free Software Foundation (FSF), or the Python Software Foundation (PSF) License Agreement for Python 2.7.3 (Python License). Lantronix grants you no right to receive source code to the Open Source software; however, in some cases, rights and access to source code for certain Open Source software may be available directly from Lantronix' licensors. Your use of each Open Source component or software is subject to the terms of the applicable license. The BSD license is available at http://opensource.org/licenses. The GNU General Public License is available at http://www.gnu.org/licenses/. The Python License is available at http://cmpt165.csil.sfu.ca/Python-Docs/license.html. Your use of each Open Source component or software is subject to the terms of the applicable license.

OPEN SOURCE SOFTWARE IS DISTRIBUTED WITHOUT ANY WARRANTY, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SEE THE APPLICABLE LICENSE AGREEMENT FOR ADDITIONAL INFORMATION.

You may request a list of the open source components and the licenses that apply to them. Contact your regional Lantronix sales associate. www.lantronix.com/about-us/contact/

Revision History

Date	Rev.	Comments
March 2017	2.2.0	—
February 2018	2.3	—
October 2019	A	Added Lantronix document part number, Lantronix logo, branding, contact information, and links.
January 2020	B	Renamed document to ePack User Manual. ePack firmware for E210 and E220 series devices, version 2.3
December 2020	C	Updated to ePack firmware release 3.7
April 2023	D	Updated to firmware release 3.8.1.0, which includes the following: • Added SNMP support for version v1, v2c, vs and SNMPTRAPD • Added Modbus Master • Added custom baudrate settings and FTP to Serial support • Added SDK support Updated to firmware release 3.9.17.0, which includes the following: • Added Modbus TCP Slave • Added GSM Update service for cellular module firmware upgrade • Added ConsoleFlow • Added SMS commands to send data to serial port, change SerialFTP prameters for Serial to FTP

		• Updated SMS command for Install/Update IPK • Removed Temperature display from status page Updated to firmware release 3.10.5.0, which includes the following: • Added SIM features PUK, PDP type, Service Type, and Cid • Added IEC 104 Multi-master Updated to firmware release 3.11.11.0, which includes the following: • Added Power Saving Mode ON/OFF feature via DI triggered events • Added SMS command to change SIM priority • Added IP passthrough setting for cellular interface • Added SMS command for cellular firmware upgrade Updated to firmware release 3.12.0.0, which includes the following: • Added Discovery tool • Removed D2sphere client Updated to firmware release 3.13.0.0, which includes the following: • Added DNP3 to IEC104 converter integration • Added SMS command to set Custom URL and firmware file name for cellular module firmware upgrade Updated to firmware release 3.14.0.0, which includes the following: • Added AT command mode option for Serial Configuration • Added On Premise and On Cloud options in ConsoleFlow Updated to firmware release 3.15.0.0 • Added SCEP client to IPSec
May 2024	E	Updated to firmware release 3.18.0.0, which includes the following: • Added PDU mode for SMS • Enabled use of special characters as arguments for Custom commands • Added SCEP Client service • Added Strict Cipher to IPSEC connection • Added Temperature field to System Status • Renamed ConsoleFlow to Percepxion • Added Audit Log and Send Dynamic Updates to Percepxion client settings Added Appendix D. Running Commands

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

Contents

1 About this Guide 10
1.1 Purpose and Audience 10
1.2 Summary of Chapters 10
1.3 Additional Documentation 11

2 Introduction 13
2.1 Product Features 14
2.1.1 E210 Series 14
2.1.2 E220 Series 15

3 Default Configuration 16
3.1 Web Admin Page 16
3.2 Wireless Access Point SSID 16
3.3 Default Interface Configuration 16

4 Web Administration Interface 18
4.1 Web Admin Interface 18
4.2 Logging In 19
4.3 Change Passwords After Initial Login 20
4.4 Logging Out 21

5 Quick Setup 22
5.1 Quick Setup 22

6 Status 25
6.1 Overview 25
6.1.1 Status 25
6.2 Firewall Status 37
6.2.1 IPv4 Firewall 37
6.2.2 IPv6 Firewall 38
6.3 Routes 39
6.4 System Log 41
6.5 Kernel Log 42
6.6 Processes 42
6.7 Realtime Graphs 43
6.7.1 Load 43
6.7.2 Traffic 44
6.7.3 Wireless 45
6.7.4 Connection 46

6.8 Load Balancing 48
6.8.1 Interface 48
6.8.2 Detail 48
6.8.3 Diagnostics 49
6.8.4 Troubleshooting 49

7 System 50
7.1 System 50
7.1.1 General Settings 50
7.1.2 Logging 52
7.1.3 Time Synchronization 54
7.1.4 Language and Style 54
7.2 Administration 56
7.2.1 Router Password 56
7.2.2 SSH Access 57
7.2.3 SSH-Keys 59
7.3 Software 60
7.3.1 Installed and Available Packages 60
7.3.2 OPKG Configuration 61
7.4 Startup 62
7.4.1 Initscripts 62
7.4.2 Local Startup 62
7.5 Scheduled Tasks 63
7.6 LED Configuration 63
7.6.1 Add/Edit LED Configuration 64
7.7 Backup / Flash Firmware 65
7.7.1 Actions 65
7.7.2 Configuration 67
7.8 Custom Commands 68
7.8.1 Dashboard 68
7.8.2 Configure 69
7.9 Reboot 70

8 VPN 71
8.1 IPSec (Internet Protocol Security) 71
8.1.1 Gateway to Gateway 72
8.2 OpenVPN 78
8.2.1 OpenVPN Instances 78
8.2.2 Edit OpenVPN Instance from Template 81
8.2.3 Edit OpenVPN Instance from Configuration File 84

9 Services 85

9.1 Dynamic DNS 86
9.1.1 Basic Settings 86
9.1.2 Advanced Settings 88
9.1.3 Timer Settings 89
9.1.4 Log File Viewer 90
9.2 Agents 92
9.3 SD(HC)/MMC Card 93
9.4 SNMPD 94
9.4.1 SNMP Architecture 94
9.4.2 SNMP Versions 94
9.4.3 SNMP Configuration 95
9.5 SNMPTRAPD 108
9.5.1 SNMP-TRAP Configuration 108
9.6 Modbus Master 112
9.6.1 Serial Transmission Mode 112
9.6.2 Ethernet Transmission Mode 112
9.6.3 Modbus Master Configuration 112
9.6.4 Data Window 113
9.6.5 Download 114
9.7 Modbus Slave 115
9.7.1 Modbus Slave Configuartion 115
9.8 DNP3 117
9.8.1 Configuring DNP3 Outstation for Modbus RTU to DNP3 conversion 117
9.8.2 Modbus Master configuration file for DNP3 Outstation 119
9.8.3 Sample CSV with DNP3 Parameters 119
9.8.4 DOTA 121
9.8.5 Lantronix Server 121
9.8.6 Custom Server 122
9.9 IEC 104 Multi-master 124
9.9.1 IEC 104 Multi-master Configuartion 124
9.10 DNP3 to IEC104 125
9.10.1 DNP3 To IEC104 Configuration 125
9.11 Page Selector 126
9.12 SMS 126
9.12.1 SMS Configuration 126
9.12.2 Ethernet SMS 132
9.12.3 Live Message 132
9.13 Reporting Agent 134
9.13.1 Sending Data 136
9.13.2 Data Format 137
9.14 GPS 139
9.14.1 Sample GPS Frames 142

9.15 Keepalived 150
9.15.1 General 150
9.15.2 Keepalived Global 151
9.15.3 Tracking Scripts 153
9.15.4 Tracking Interfaces 154
9.15.5 Tracking Processes 155
9.15.6 Virtual IP 156
9.15.7 VRRP Instances 158
9.16 Last Gasp 160
9.17 Serial 161
9.17.1 Serial Configuration 161
9.17.2 Serial Data Send Configuration 162
9.18 Service Actions 167
9.19 Events 168
9.19.1 Event Management 168
9.20 GSM Update 170
9.20.1 Lantronix Server 170
9.20.2 Custom Server 170
9.21 uHTTPd 172
9.21.1 General Settings 172
9.21.2 Full Web Server Settings 175
9.21.3 Advanced Settings 177
9.22 SCEP Client 180
9.22.1 Certificate Details 180

10 Network 183

10.1 Interfaces 183
10.1.1 Interfaces Overview 184
10.1.2 Interface Status 186
10.1.3 Interface Protocols 187
10.1.4 CELLULAR Interface 200
10.1.5 LAN Interface 202
10.1.6 WAN and WAN6 Interface 205
10.1.7 WWAN and WWAN6 Interface 208
10.1.8 Add Virtual Interface 210
10.2 Wireless 213
10.2.1 Wireless Network Configuration 215
10.3 Switch 225
10.4 DHCP and DNS 226
10.4.1 General Settings 227
10.4.2 Resolv and Host Files 229
10.4.3 TFTP Settings 230

10.4.4 Advanced Settings 231
10.4.5 Static Leases 233
10.5 Hostnames 234
10.6 Static Routes 235
10.6.1 Static IPv4 Routes 235
10.6.2 Static IPv6 Routes 236
10.7 Diagnostics 238
10.8 Firewall 239
10.8.1 General Settings 239
10.8.2 Port Forwards 246
10.8.3 Traffic Rules 249
10.8.4 Custom Rules 252
10.9 Load Balancing 253
10.9.1 How it works 253
10.9.2 Globals 254
10.9.3 Interfaces 255
10.9.4 Members 259
10.9.5 Policies 261
10.9.6 Rules 263
10.9.7 Notification 266

11 Percepxion 267
11.1 Percepxion Configuration 267

12 Discovery 271
12.1 Query Port 271

Appendix A. Wiring Diagrams 272

Appendix B. LED Behavior 273

Appendix C. List of Acronyms 277

Appendix D. Running Commands 280

1 About this Guide

1.1 Purpose and Audience

This guide provides the information needed to configure and use the Lantronix E210 series and E220 series cellular routers. The E210 and E220 series rugged cellular routers are designed for IoT professionals for M2M and enterprise IoT applications requiring faultless connectivity.

The information in this document assumes the reader has working knowledge of networking technology and routing concepts.

1.2 Summary of Chapters

The remaining chapters in this guide include:

Chapter	Description
2: Introduction	Describes the E210 and E220 series models.
3: Default Configuration	Provides the default credentials for web interface user access, the default wireless access point credentials, and describes the default interface configuration.
4: Web Administration Interface	Describes the web administration interface available for configuring the E2xx series routers. The configuration chapters (5-10) provide detailed instructions for using the web interface.
5: Quick Setup	Provides instructions for configuring the Quick Setup.
6: Status	Provides overview of the router status pages.
7: System	Provides instructions for configuring the clock and logging settings, enabling SSH access and keys, changing the router password, enabling startup scripts, defining and scheduling cron jobs, customizing LED behavior, and executing custom shell commands, Provides instructions for installing software packages, upgrading firmware, saving and restoring router configuration, rebooting the router.
8: VPN	Provides instructions for configuring and enabling OpenVPN and IPSec tunneling.
9: Services	Provides instructions for enabling and configuring Dynamic DNS, Lantronix (D2Sphere) and custom (DOTA) device management servers, and high availability (using Keepalived) settings. Provides instructions for enabling the MWAS agent, reporting agent, SMS with AT commands, GPS, and Last Gasp (E220 devices only), Provides instructions for configuring serial port settings, software-configurable DIOs, HTTP/HTTPS server, and for

Chapter	Description
	starting, stopping, restarting available services.
10: Network	Provides instructions for configuring the cellular, WAN, LAN, WWAN and wireless interfaces, routing, switch, DHCP and DNS, firewall, and load balancing settings. Provides instructions for enabling the VLAN functionality (switch), defining hostname, and running network diagnostic commands from the web interface.
11. Percepxion	Cloud platform which allows for the remote management of devices.
12. Discovery	Allows your computer to locate other computers and devices on the network. This setting also allows other computers to see your computer.
Appendix A. Wiring Diagrams	Provides RS-485 wiring diagrams and power over ethernet (POE) diagram.
Appendix B. LED Behavior	Provides information about the E210 and E220 series device LED indicators and brief descriptions.
Appendix C. List of Acronyms	Provides a glossary of acronyms of relevant protocols and terms.
Appendix D: Running Commands	Provides information about running commands on the E210 and E220 series gateways.

1.3 Additional Documentation

Visit the Lantronix web site at https://www.lantronix.com/support/documentation for the latest documentation and the following additional documentation for this product series.

Document	Description
E210 Series Cellular Router Quick Start Guide	Provides hardware installation instructions, directions to connect the E210 series router, and network IP configuration information.
E220 Series Cellular Router Quick Start Guide	Provides hardware installation instructions, directions to connect the E220 series router, and network IP configuration information.
E210 Series User Guide	Provides E210 series accessories and part number information, product features and hardware description, hardware installation instructions, compliance statements and notices.
E220 Series User Guide	Provides E220 series accessories and part number information, product features and

Document	Description
	hardware description, hardware installation instructions, compliance statements and notices.
E210 Series Product Brief	Provides E210 series router product overview information and specifications.
E220 Series Product Brief	Provides E220 series router product overview information and specifications.
Using the epack series SDK Application Note	Describes how to use the SDK to create custom packages and the Image Builder to build custom firmware images.

2 Introduction

With high-speed cellular (3G and beyond), WAN, LAN and Wi-Fi connectivity, the Lantronix e-series of routers are highly versatile, reliable and rugged routers designed for mission-critical M2M and enterprise applications requiring faultless connectivity. Cellular can be configured to be the primary connectivity mode or the WAN failover alternative to a wire line connection. They also support a wide range of advanced routing protocols and VPN configurations.

This manual covers the following products:

E210 Series*	E220 Series*
E213	E224
E214	E225
E214G	E225G Mk II
E215	E225 Lite
E218	E228
-	E228G Mk II

**Contact Lantronix Sales regarding additional models available subject to MOQ and other considerations*

2.1 Product Features

2.1.1 E210 Series

Model name	Geographical area(s) / Operator	Cellular type [1]	Bands [2]	Fallback mode(s) [1]	Bands [2]	Location services	Certifications [3] Completed | In progress | Under consideration		FCS [4]	Order code
E215	EMEA; South-East Asia; South Asia	3G[ζ1]	8/1	2G[λ1]	8/3	×	**EN300328** | *ETA, TEC*	MIL-STD-810H [9]	Aug. '18	E215F002S
E213	World	LTE-M1 [5]	12[a]/28/13/20/27/26[b]/8/3[c]/66[d]/25[e]/1	2G	5/8/3/2		-		*TBD*	E213F102S
E214	Australia & New Zealand; Thailand; Malaysia	LTE cat. 1	28/5/8/3	3G[ζ2]	5/8/1		**RCM**;		Aug. '18	E214F003S
	EMEA; Asia Pacific		28/20/8/3/1/7	3G[ζ3]; 2G[λ3]	8/1; 8/3	*Optional*	**CE** [7]		Dec. '18	E214F002S
	China; Thailand; Indonesia; India		5/8/3/1; TDD 40/41[f]				*ETA, TEC* | *SRRC, CTA; Postel*			E214F00CS
E214G	Verizon Wireless		13/4	×	N/A	✓	**FCC** [8], **Verizon Wireless**		Nov. '18	E214G001S
	The Americas – excl. Verizon Wireless		12/5/4/2	3G[ζ3]	5/4/2		**FCC** [8], **PTCRB**, **AT&T Wireless**; **ISED**			E214G000S
E218	Brazil; Australia & New Zealand; Thailand	LTE cat. 4	28/5/8/3/1/7	3G[ζ3]; 2G[λ3]	5/8/1; 8/3	*Optional*	**NBTC**		Mar. '19	E218F004S
	NTT docomo		19/21/1	×	N/A	×	-		May '19	E218F005S
E213	*450 MHz operators*	*LTE-M1* [6]	*87 TBC/88 TBC/73/72/31/ 12[a]/28/13/20/27/26[b]/8/3[c]/66[d]/25[e]/1*				*Postel*		*tbd*	*E213F10ES*
E214G	*USA & Canada*	*LTE cat. 1*	*71/12/13/14/26(5)/66(4)/25(2)*			✓	*FCC* [8], *PTCRB; ISED*		*tbd*	*E214G10AS*
	Japan; South Korea		*18/5(19)/8/21/3/1/7*				*JRF, JPA; KC*		*tbd*	*E214G107S*
E218	*EMEA; Asia Pacific*	*LTE cat. 4*	*28/20/8/3/1/7*	*3G[ζ3]; 2G[λ3]*	*8/1; 8/3*	*Optional*	*CE; RCM; NCC*		*tbd*	*E218F102S*

Please consult us regarding the models or features shown in grey italics, which are subject to MOQ and other considerations

1. *Uplink / Downlink maximum data rates*
   - *2G: [λ1] 85.6 / 236.8; or [λ2] 236.8 / 236.8; or [λ3] 236.8 / 296 kbps*
   - *3G: [ζ1] 5.76 / 7.2; or [ζ2] 5.76 / 10.1; or [ζ3] 5.76 / 42.2 Mbps*
   - *LTE-M1 [NB1]: 375 / 300 [62.5 / 27.2] kbps updated to LTE-M2 [NB2]: 1,000 / 600 [140 / 120] kbps*
   - *LTE cat. 1: 5 / 10 Mbps (FDD); 3.1 / 8.96 Mbps (TDD)*
   - *LTE cat. 4: 50 / 150 Mbps (FDD); 35 / 130 Mbps (TDD)*

2. *Ranked by increasing frequencies*
   - [a] *incl. North America's B17*
   - [b] *incl. KDDI's B18 as well as North America's B5, the latter*
   - [c] *incl. NTT docomo's B19, itself incl. Japan's B6 (3G) incl. Japan's B9*
   - [d] *incl. North America's B10, itself incl. North America's B4*
   - [e] *incl. North America's B2*
   - [f] *More precisely, B41's 2535 MHz ~ 2655 MHz subset, suited to China well*

3. *Please consult us, should any other certification be required*
4. *First customer shipment [date of]*
5. *23 dBm output power*
6. *26 dBm output power from 410 MHz to 467.5 MHz, 23 dBm otherwise*
7. *Based on compliance with RED; EN 60950-1; etc.*
8. *Also, Class I Division 2 for use in explosive atmospheres, as a factory option subject to MOQ and other considerations*
9. *by Switzerland's SGS*

2.1.2 E220 Series

Model name	Geographical area(s) or Operator	Cellular type [1]	Bands [2]	Fallback mode(s) [1]	Bands [2]	Location services	Certifications Completed | In progress | Under consideration	FCS [3]	Order code
E225 Lite	EMEA; South-East Asia; South Asia	3G[ζ1]	8/1	2G[λ1]	8/3	×	**CE** | ETA, TEC	Sep. '16	E225FLZ2S
E225G Mk II	World	3G[ζ1]	5/8/2/1		5/8/3/2	cf. footnote [5]	-	TBD	E225F00FS
E228G Mk II	EMEA; Asia Pacific	LTE cat. 4	28/20/8/3/1/7	3G[ζ3]; 2G[λ3]	8/1; 8/3	IZat™ gen. 8C gpsOne	**CE**	Nov. '18	E228G002S
	Brazil; Australia & New Zealand		28/5/8/3/1/7		5/8/1; 8/3		-		E228G004S
	China; Thailand; Indonesia; India		5/8/3/1; TDD 40/41[a]		8/1; 8/3		-		E228G00CS
E225	World	3G[ζ1]	5/8/2/1	2G[λ1]	5/8/3/2	cf. footnote [6]	-	Oct. '16	E225HPLFS
E224	EMEA	LTE cat. 1	20/8/3	2G[λ3]	8/3		**CE**	Apr. '17	E224HPL2S
	Australia & New Zealand		28/5/8/3	3G[ζ2]	5/8/1		**RCM**	Sep. '17	E224HPL3S
E228	Verizon Wireless [4]	LTE cat. 4	13/4/2	×	N/A		**FCC**, **Verizon Wireless**	TBD	E228HPL1S
	The Americas [4]		17/5/4/2	3G[ζ3]	5/2		**FCC**, **PTCRB**, **AT&T Wireless**; **ISED**	Nov. '16	E228HPLAS
	NTT docomo		19/21/1	×	N/A		**JRF**, **JPA**	May '17	E228HPL5S

Please consult us regarding the models or features shown in grey italics, which are subject to MOQ and other considerations

[1] *Uplink / Downlink maximum data rates*
- *2G: [λ1] 85.6 / 236.8; or 236.8 / [λ2] 236.8; or [λ3] 296 kbps*
- *3G: 5.76 / [ζ1] 7.2; or [ζ2] 10.1; or [ζ3] 42.2 Mbps*
- *LTE cat. 1: 5 / 10 Mbps (FDD); 3.1 / 8.96 Mbps (TDD)*
- *LTE cat. 4: 50 / 150 Mbps (FDD); 35 / 130 Mbps (TDD)*

[2] *Ranked by increasing frequencies*

[g] *More precisely, B41's 2535 MHz ~ 2655 MHz subset, suited to China well*

[3] *First customer shipment [date of]*

[4] *Each model is user-reconfigurable into the other model, i.e. E228HPL1S into E228HPLAS and vice versa*

[5] *SiRFstarV-based Concurrent GPS and GLONASS*

[6] *Concurrent GPS, Galileo and either GLONASS (factory setting) or Beidou*

Note

- ***Except when explicitly mentioned, all the screenshots in this user guide are taken from a Lantronix E228 unit.***

3 Default Configuration

All usernames and passwords are case sensitive.

3.1 Web Admin Page

If you are running ePack firmware release 2.4.4 and above, the default factory passwords are:

User	Default Password
admin	admin
root	L@ntr0n1x

Table 3.1-1: Default Web Admin Page Credentials

Note

- ***ePack firmware versions 2.4.4 and above require you to change the factory default passwords before any other router configuration can be done. Both the admin and root passwords must be changed.***

If you are running ePack firmware releases older than 2.4.4, the default factory passwords are:

User	Default Password
admin	admin
root	M@estroW1rele$$

Table 3.1-2: Default Web Admin Page Credentials

3.2 Wireless Access Point SSID

Parameter	Details
SSID	Lantronix E21X - for E210 series devices Lantronix E22X - for E220 series devices
WPA/WPA2 TKIP Key	W1rele$$

Table 3.2-1: Default Wi-Fi Credentials

3.3 Default 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

Interface	Details
Wireless (LAN)	Wi-Fi enabled as access point with SSID "Lantronix E21X" or "Lantronix E22X"

Table 3.3-1: Default Interface Configuration

4 Web Administration Interface

For installation and setup procedures, refer to the hardware manual for your device.

- *Lantronix E210 Series Cellular Router User Guide*
- *Lantronix E220 Series Cellular Router User Guide*

4.1 Web Admin Interface

The Web admin interface allows the administrator and other authorized users to configure and manage the Lantronix E210 and E220 cellular routers using most web browsers (Firefox, Internet Explorer or Safari web applications with the latest browser updates).

The following figure shows a typical web page:

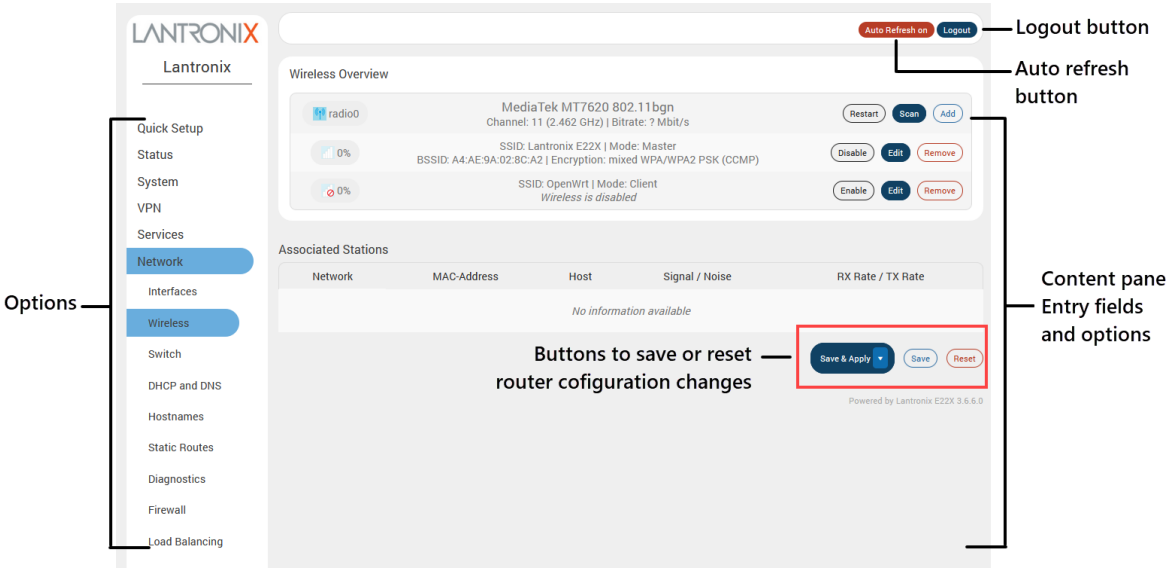


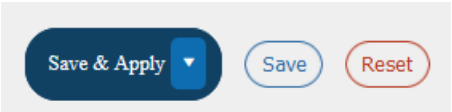
Figure 4.1-1: Web Admin Interface

The web page has the following components:

Options – Groups of router settings to configure.

Entry fields and options (content pane) – Main content pane fields and options allow you to enter data and select options for the settings.

Save/Apply/Reset Configuration



Save & Apply button – Applies the changes on the web page and saves them to the router so that they will be there when the router is rebooted.

Apply unchecked button– Use this if you are changing the interface parameters on which the session is active.

Save button – Saves the changes on the web page without committing the changes. All saved configuration will be lost when the router is rebooted if they are not saved and applied.

Reset button– Discards the unsaved changes on the form.

Auto refresh indicator – Allows you to switch on or off the browser auto-refresh setting. The auto-refresh value is configured in System > System > Language and Style settings.

Logout button – Log off from the web interface.

4.2 Logging In

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

If your router is new, please inspect and set up the router as shown in the Lantronix E210 or E220 Series Cellular Router User Guides.

Before logging in, make sure you have an active SIM card and a computer equipped with the following:

- Ethernet port or Wi-Fi connectivity and Internet service
- Web browser –Google Chrome, Mozilla Firefox, Internet Explorer or Microsoft Edge, Apple Safari (with the latest updates installed)
- DHCP client is enabled on the computer to obtain a valid IP Address from the router with LAN IP address 192.168.1.1. See below for help.

To enable DHCP in Windows 8 or 10:

1. Access the active network. Go to Start > Control Panel > Network and Internet > Network and Sharing Center. Click the active network connection. The Network Connection Status dialog box appears.
2. From the Network Connection Status dialog, click Properties, select Internet Protocol Version 4 (TCP/IPv4) and click Properties to display the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box.
3. On the General tab of the IPv4 Properties dialog, select the following options:
    - Obtain an IP address automatically
    - Obtain DNS server address automatically

To log into the web interface:

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

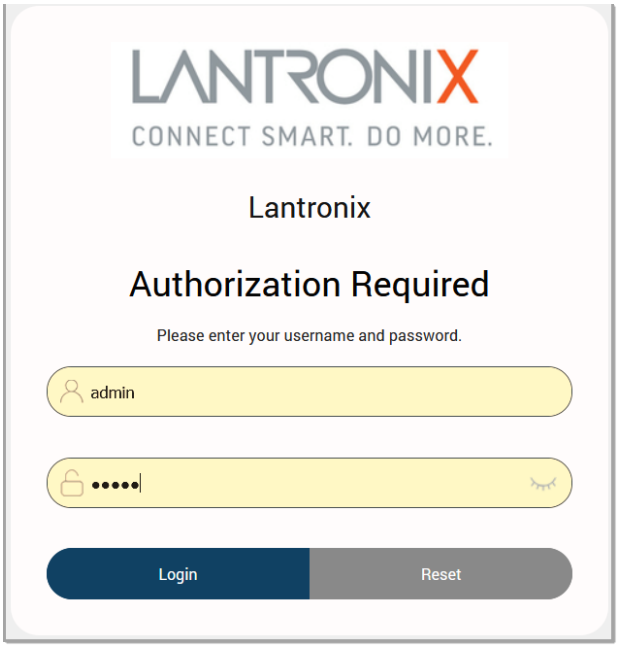


Figure 4.2-1: Web Admin Login Page

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

Note

- ***If you are running ePack firmware version 2.4.4 and above, you will be required to change the factory default passwords for both the admin and root users before you can do any other router configuration.***

4.3 Change Passwords After Initial Login

Upon first login, you are directed to change the factory default passwords for both the admin user and the root user.

Assuming that you logged in as "admin", you'll see the Change Initial Password page as shown below:

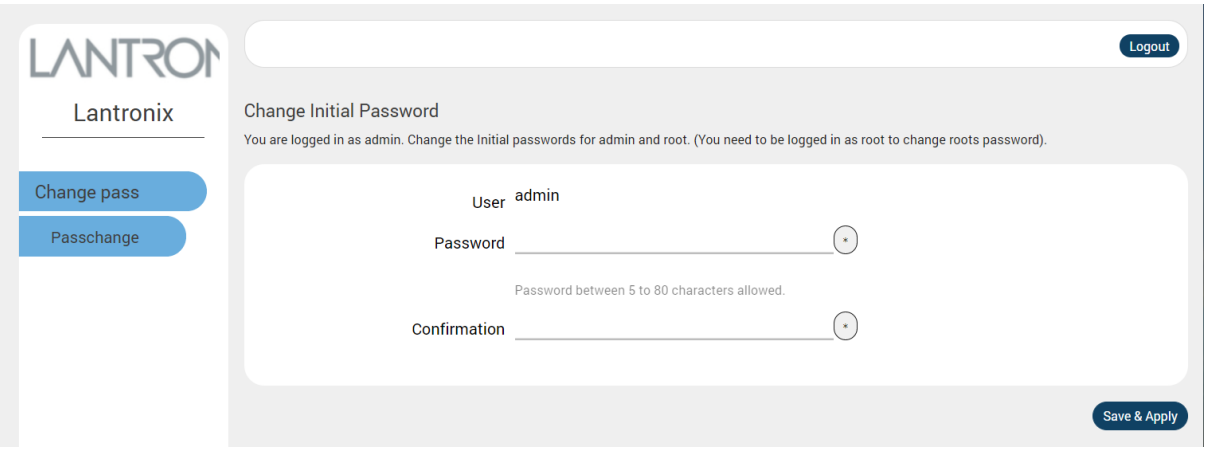


Figure 4.3-1: Change Initial Password

1. Enter the new password for "admin" user and then re-enter it to confirm it.
2. Click **Save & Apply**.
3. This will log you out and return to the login page automatically.
4. Log in as "root" user using the factory default password (hint: root/L@ntr0n1x).
5. The Change Initial Password page for the root user is displayed. As before, enter the new password and re-enter it to confirm it.
6. Click **Save & Apply**.

Note

- ***You can log in to root user and change both admin and root password at the same time.***

4.4 Logging Out

To log off the ePack web interface:

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

5 Quick Setup

Quick Setup helps get the IP network port up and running so that you can configure other router settings. To skip the Quick Setup and directly configure the network settings including advanced settings, go to the Network tab.

5.1 Quick Setup

On the Quick Setup page, click **Quick Setup**. The Quick Setup > Network Setup page is displayed. Basic network parameters for LAN, WAN, Cellular, and Wireless LAN can be configured from the Network Setup page.

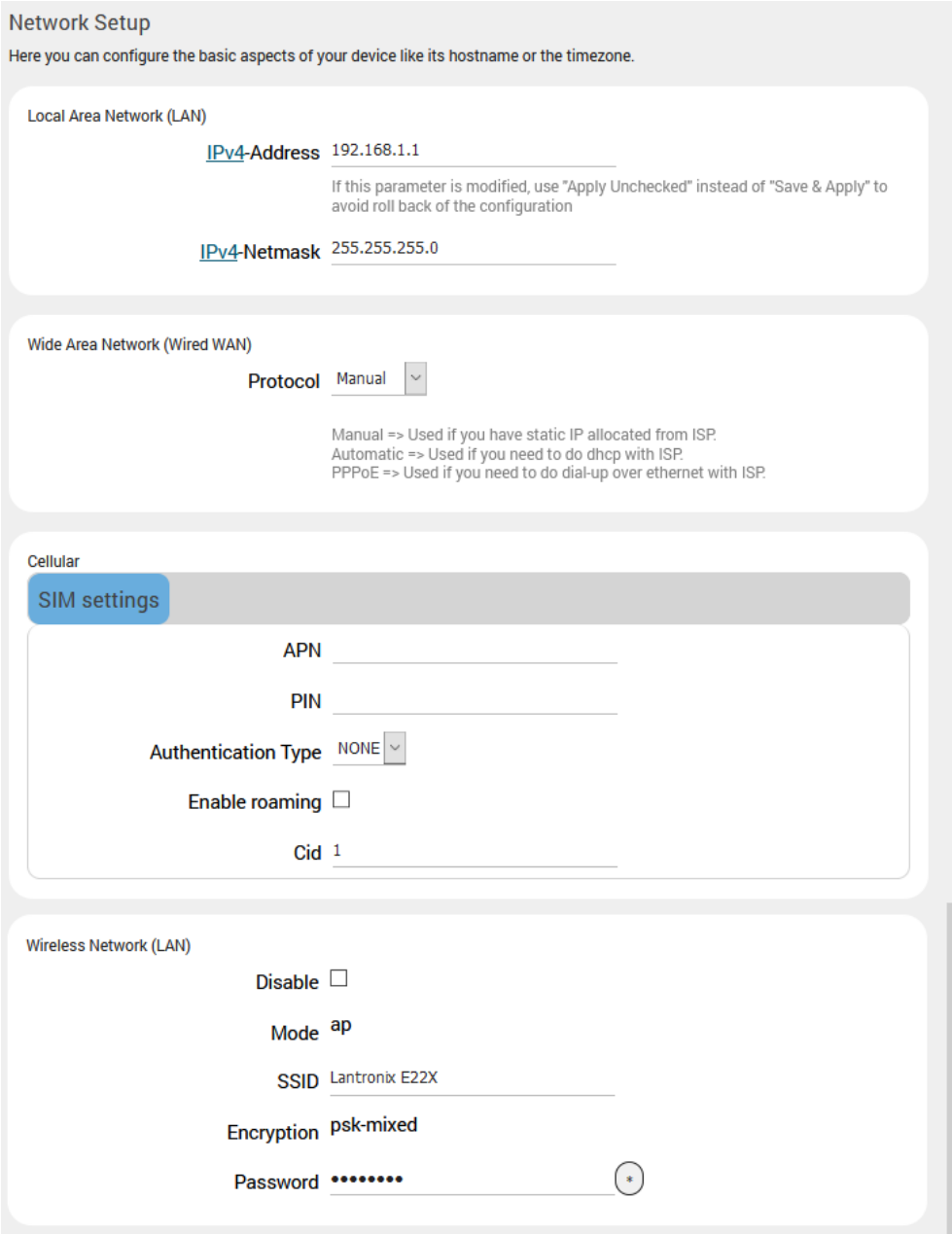


Figure 5.1-1 - Quick Setup > Network Setup page (E228 shown)

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 Router. The default LAN IPv4 Address is 192.168.1.1.
Ipv4-Netmask	Enter IPv4 Subnet Mask of the LAN interface. The default Netmask is 255.255.255.0
Wide Area Network (Wired WAN)	
Protocol	Select the WAN protocol from the available options: *Manual - to set a static IP address. If selected, enter the IPv4*

Parameters	Description
	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 user name and password.* The default WAN protocol is selected as Automatic.
Cellular	
SIM 1 settings/SIM2 settings	Cellular SIM card settings for one or two SIM card slots, depending on the router model number.
APN	Access Point Name (APN) is the name of an access point for the cellular network data connection. Generally, the wireless cellular network operator will provide the APN to their end users. Enter the APN provided by the cellular network operator.
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, then username and password must be entered.
Username	Enter the PAP/CHAP user name.
Password	Enter the PAP/CHAP password.
Enable Roaming	Select to enable data roaming on the cellular interface of the router.
Wireless Network (LAN)	
Disable	Select the check box to disable the Wireless interface. By default, the Wireless interface is enabled.
Mode	Displays the Wireless network (LAN) mode. Mode can be ap (access point) or client. To configure, go to Network > Wireless.
SSID	Enter the Service Set Identifier (SSID) name. Leave the field blank to use the default SSID value. The default SSID is **Lantronix E21x** for E210 series devices and **Lantronix E22x** for E220 series devices.
Encryption	Displays the type of encryption. To configure the encryption type, go to Network > Wireless.
Password	The default SSID password is **W1rele$$**.

Table 5.1-1: Quick Setup Network Configuration

6 Status

Status provides a summary view of the vital configurations of the router. It includes the following topics:

- Overview
- Firewall
- Routes
- System Logs
- Kernel Log
- Processes
- Real-Time Graphs
- Load Balancing

6.1 Overview

Status > Overview

Overview page provides a listing of the important parameters of the router.

6.1.1 Status

Status > Overview > Status

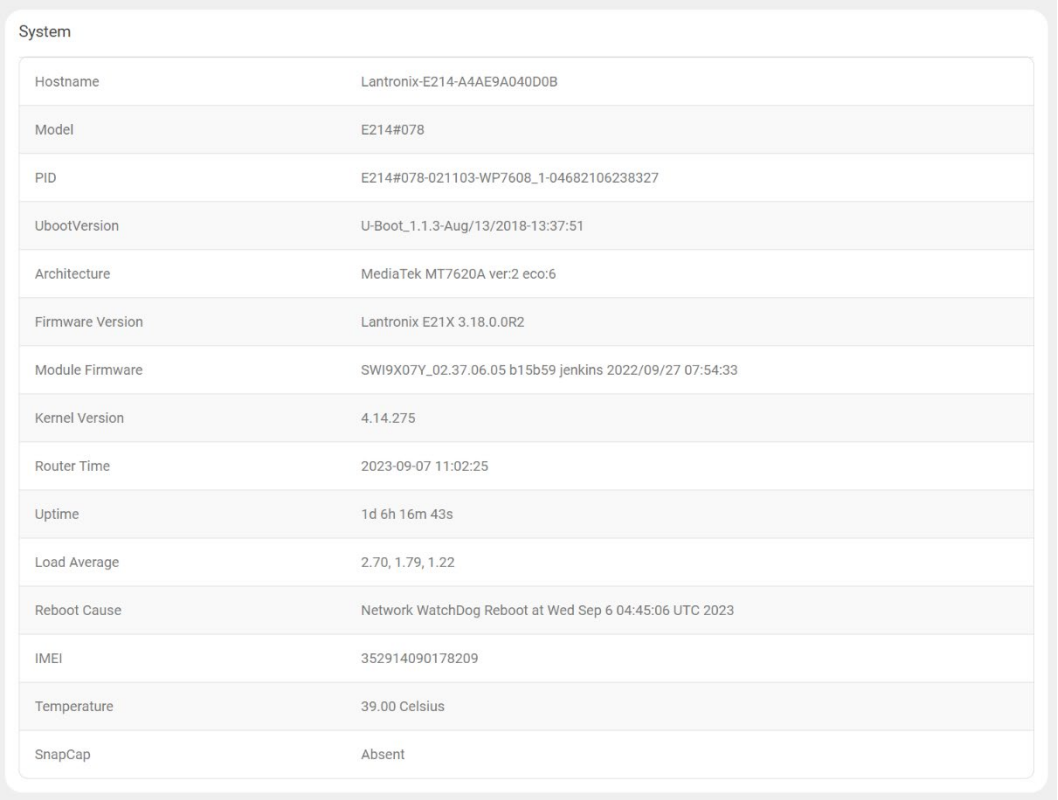
Status Overview page outlines the configuration settings for the basic sub-modules of the router. It includes the following information:

- System
- Percepxion
- Cellular
- Memory
- Network
- Active DHCP Leases
- Wireless
- Digital Input/Output
- Dynamic DNS
- MWAN Interfaces

6.1.1.1 System

Status > Overview > Status

The System group provides the router's model and software related information.



System

Hostname	Lantronix-E214-A4AE9A040D0B
Model	E214#078
PID	E214#078-021103-WP7608_1-04682106238327
UbootVersion	U-Boot_1.1.3-Aug/13/2018-13:37:51
Architecture	MediaTek MT7620A ver:2 eco:6
Firmware Version	Lantronix E21X 3.18.0.0R2
Module Firmware	SWI9X07Y_02.37.06.05 b15b59 jenkins 2022/09/27 07:54:33
Kernel Version	4.14.275
Router Time	2023-09-07 11:02:25
Uptime	1d 6h 16m 43s
Load Average	2.70, 1.79, 1.22
Reboot Cause	Network WatchDog Reboot at Wed Sep 6 04:45:06 UTC 2023
IMEI	352914090178209
Temperature	39.00 Celsius
SnapCap	Absent

Figure 6.1-1 System Status Overview

Parameters	Description
Hostname	Name assigned to the router for addressing purposes.
Model	Model number of the router that is deployed.
PID	Display 35 characters long, unique Product Identification number (PID). Consider an example of PID E225-071102-HL8548-xxxxxxxxxxxxxx. It is composed of: *4 characters SKU: E225* ***6 characters UID:*** *071102 (WAN, GNSS, Wi-Fi, 2x LAN, SIM)* *6 character Module Name: HL8548* *14 characters Serial Number:* *xxxxxxxxxxxxxx. Comprises of HW/PCB version (01 to 99), Lot number (01 to 99), Production date (YYMMDD), Unit number (4 digits).*
UbootVersion	U-Boot version number
Architecture	Architecture type
Firmware Version	Base Firmware Version number.
POE	Power Over Ethernet is available in E220 series where the router can be

Parameters	Description
	powered from a PSE-POE device over WAN port
Module Firmware	Modem firmware version
Kernel Version	The Linux Kernel version number on the router.
Local Time	Displays the day of the week, month, date, time and year configured on the router. The format is Day Month Date hh:mm:ss Year. The time is displayed in 24 hour clock format.
Up Time	Displays the time for which the router is up and running since last power ON. The format is hh:mm:ss. The time is displayed in 24 hour clock format.
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/MEID **(MEID is only available in CDMA / EVDO Routers)**	Displays 15 digit IMEI number or 14 digit MEID 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. A MEID number (Mobile Equipment Identifier) is used to identify a cell phone that utilizes the CDMA technology for wireless service. ***Note*** • ***We recommend you record the IMEI or MEID number and secure it so that it can be quickly accessed in the event of theft or loss of the router.***
Temperature	Temperature of the internal GSM module.
SnapCap	Indicates whether serial port is in use (Feature available only in E21X devices.).

Table 6.1-1: System Status Overview

6.1.1.2 Percepxion

System > Overview > Status

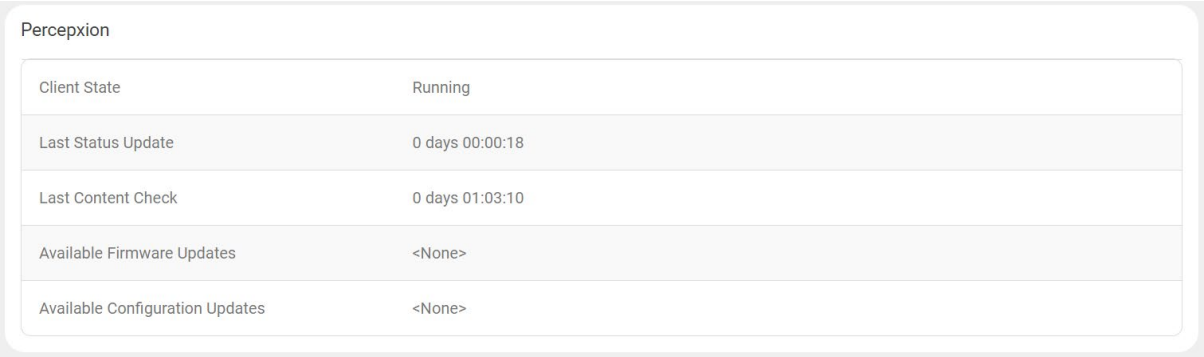


Figure 6.1-2: Percepxion Status Overview

Parameters	Description
Client State	Current state of Percepxion client.
Last Status Update	Time since last status update.
Last Content Check	Time since last content check.
Available Firmware Updates	Firmware updates available.
Available Configuration Updates	Configuration updates available.

Table 6.1-2: Percepxion Status Overview

6.1.1.3 Cellular

Status > Overview > Status

The Cellular group provides the status of the SIM card inserted in the router.

Cellular

Cellular Data	CONNECTED
Signal Strength	11
Network Status	Registered
Operator Name	Vi India Vi India
Operator Number	40407
Operator Type	2G
Roaming Status	HOME
SIM Status	READY
IMSI	404071748795495
Configure BAND	GSM:900, DCS:1800 UMTS:B1,B5,B8, LTE:B1,B3,B5,B7,B8,B28,
Registered BAND	DCS1800
ICCID	89910273103002322887

Figure 6.1-3: Cellular Status Overview

Parameters	Description
Cellular Data	Displays the status of the Cellular data. **Status** ***Connected*** *– Data 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* ***1*** *–111 dBm* ***2 to 30*** *–109 to –53 dBm* ***31*** *– 51dBm or greater* ***Note*** • ***Signal strength for a good cellular data connection must be 12 or above.***
Network Status	Displays the registration status of the router on the current cellular network. *Registered* *Not Registered*

Parameters	Description
Operator Name	Name of the current cellular operator in use.
Operator Number	Current cellular operator number
Operator Type	Operator type
Roaming Status	The roaming status of the router: *Home* *Roaming* *N/A*
SIM 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. Present only for E210 series routers that have dual SIM support.
IMSI	Displays the IMSI Number. In case of UMTS, it is read from the SIM card. An International Subscriber Identity (IMSI) is 15 digit unique Mobile number associated with 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	Temperature in degrees Celsius
Iccid	Integrated circuit card id (ICCID) unique serial number that identifies the SIM card

Table 6.1-3: Cellular Status Overview

6.1.1.4 Memory

Status > Overview > Status

The Memory group provides information about the Memory in KB available with the router.

Figure 6.1-4: Memory Status Overview

Parameters	Description
Total Available	Total available RAM memory. Total Memory is summation 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.

Table 6.1-4: Memory Status Overview

Model	RAM size	Flash size
E220LITE	64MB	32MB
E220	128MB	64MB
E210	128MB	32MB

Table 6.1-5: E210 and E220 Devices RAM and Flash Size

6.1.1.5 Network

Status > Overview > Status

The Network group provides the IPv4and IPv6 WAN status. The number of active connections is also displayed.

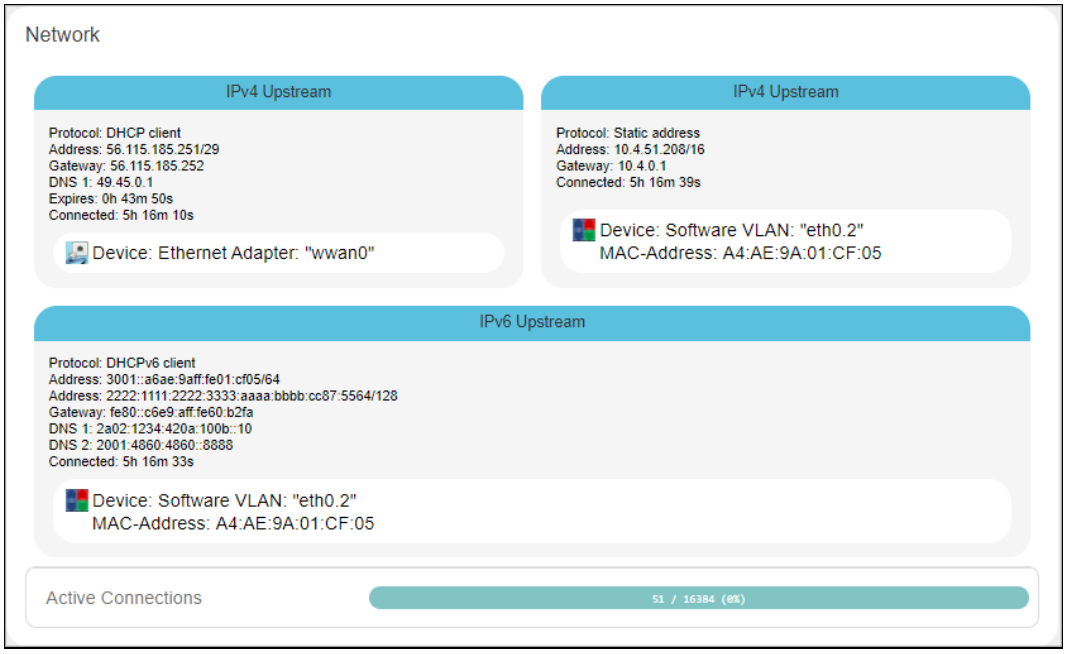


Figure 6.1-5: Network Status Overview

Parameters	Description
WAN	Displays status of fixed-line WAN connection with following details: ***IP*** *– IP Address of the WAN Interface.* ***Gateway*** *– IP Address of the WAN Interface Gateway.* ***DNS*** *– Two DNS IP Address; Primary DNS Server and Secondary DNS Server.* ***Note*** • ***In case of WAN Access Wi-Fi must be configured in client mode and connected to an Access Point.***
Cellular	Displays status of Cellular network data connection with following details: ***IP*** *– IP Address of the Cellular Interface.* ***Gateway*** *– IP Address of the Cellular Interface Gateway.* ***DNS*** *– Two DNS IP Address; Primary DNS Server and Secondary DNS Server.*
WWAN	Displays status of Wi-Fi WWAN connection with following details: ***IP*** *– IP Address of the WWAN Interface.* ***Gateway*** *– IP Address of the WWAN Interface Gateway.* ***DNS*** *– Two DNS IP Address; Primary DNS Server and Secondary DNS Server.*

Table 6.1-6: Network Status Overview

6.1.1.6 Active DHCP and DHCPv6 Leases

Status > Overview > Status

Displays the information about the machines connected to router using a DHCP lease. This includes IPv4 as well as IPv6 connections.

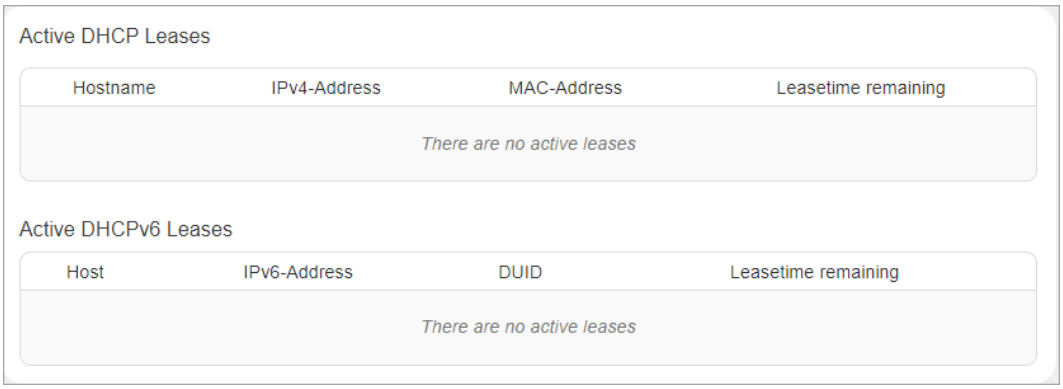


Figure 6.1-6: Active DHCP Leases Status Overview

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

Table 6.1-7: Active DHCP Leases Status Overview

6.1.1.7 Wireless

Status > Overview > Status

The Wireless Group describes the Wi-Fi network used by the router and the associated stations that are connected to the router over Wi-Fi.

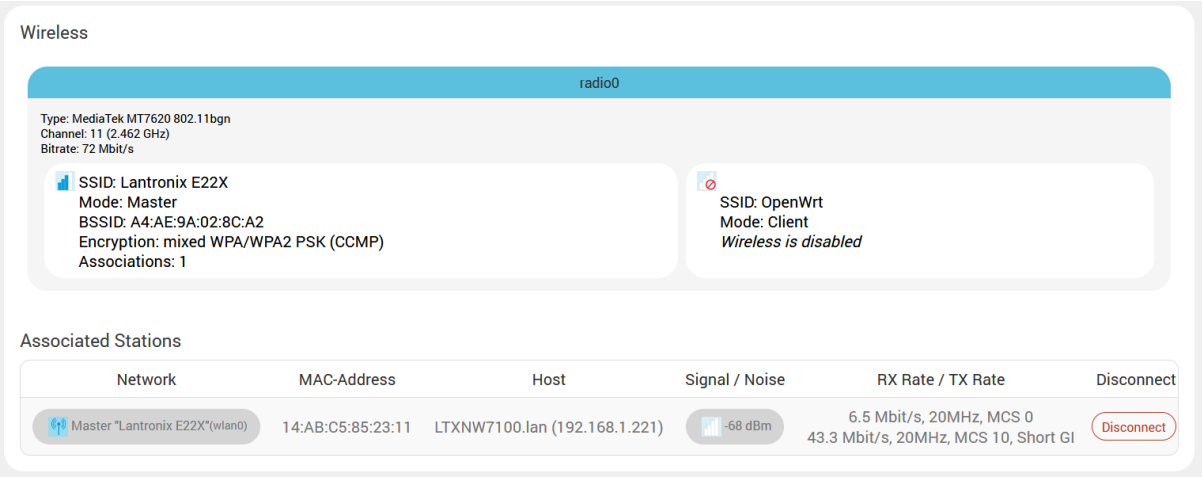


Figure 6.1-7: Wireless Status Overview

Parameters	Description
Connection Name	Displays the name of the connection and the details: ***Type*** *– The wireless radio chipset* ***Channel*** *– WiFi 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 this 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 this button to disconnect the associated station from the access point.

Table 6.1-8: Wireless Status Overview

6.1.1.8 Digital Input/Output

Status > Overview > Status

The Status Overview page shows the state of the two digital input/output pins on the router. When the pins are LOW/OPEN, the status is Red and when the pins are HIGH/CLOSED, the status is Green.

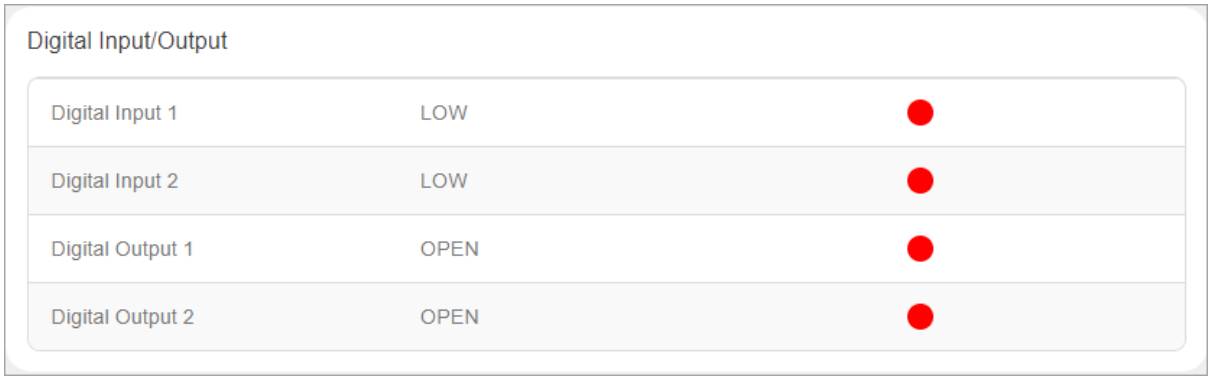


Figure 6.1-8: Status DIO Pins

6.1.1.9 Dynamic DNS

Status > Overview > Status

The status page displays the dynamic DNS IPv4 and IPv6 configuration.

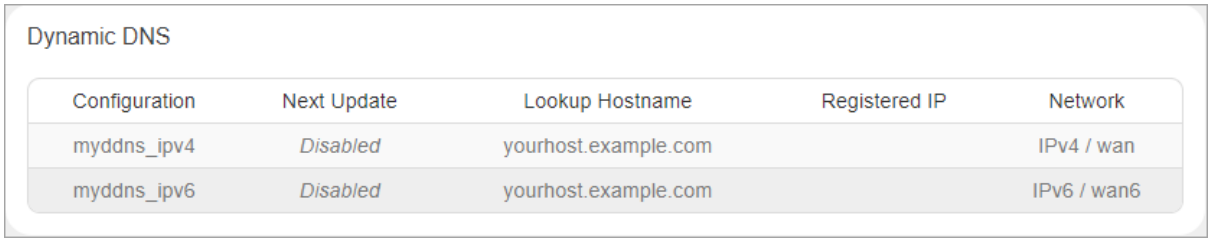


Figure 6.1-9: Status Dynamic DNS

6.1.1.10 MWAN Interface

Status > Overview > Status

Lantronix routers have multiple sources of internet and can switch seamlessly between them. The screenshot shows 3 sources of internet: WAN (Wired Ethernet), WWAN (Wi-Fi when used as a WAN instead of LAN) and Cellular.

The MWAN Interface status page provides a view of all the available and connected WAN options. In the figure below, the interfaces marked in green are live and connected while the ones in red are disabled.

For more information, refer to *Network > Load Balancing*.

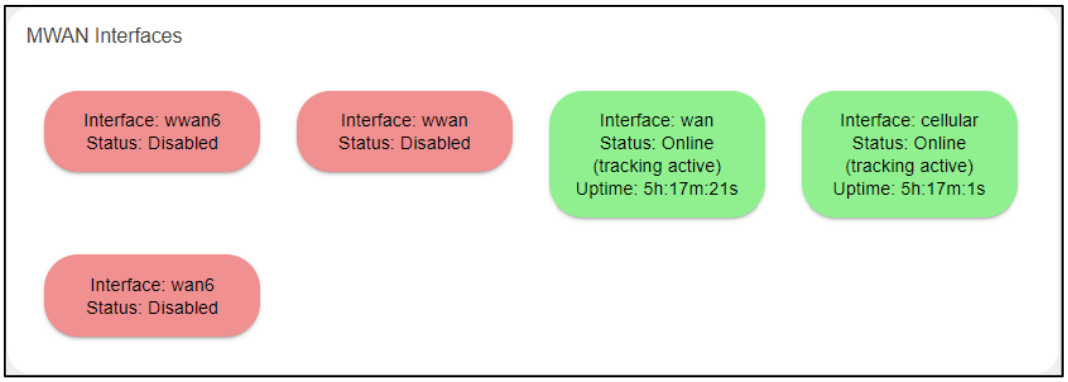


Figure 6.1-10: MWAN interfaces Status Overview

Parameters	Description
Interface	The type of interface. Can be wan, wwan, or cellular. Wan6 or wwan6 indicate IPv6 interfaces.
Status	Shows whether the interface is Online (green), Offline, or Disabled (red). If the status is Online, the following details are displayed: *tracking active – the interface is being tracked for internet availability by pinging the IP provided in its configuration section.* *tracking off – the interface is not being tracked for internet availability by pinging the IP provided in its configuration section but deemed active if the interface is up and has an IP address.* *Uptime – the duration in hours, minutes and seconds that the interface has been connected* If the status is Offline, the following is displayed: *Downtime – The time that the interface has been down since the last retry.* If the status is Disabled, no details are displayed.

Table 6.1-9: MWAN interfaces Status Overview

6.2 Firewall Status

Status > Firewall Status

6.2.1 IPv4 Firewall

Status > Firewall Status > IPv4 Firewall

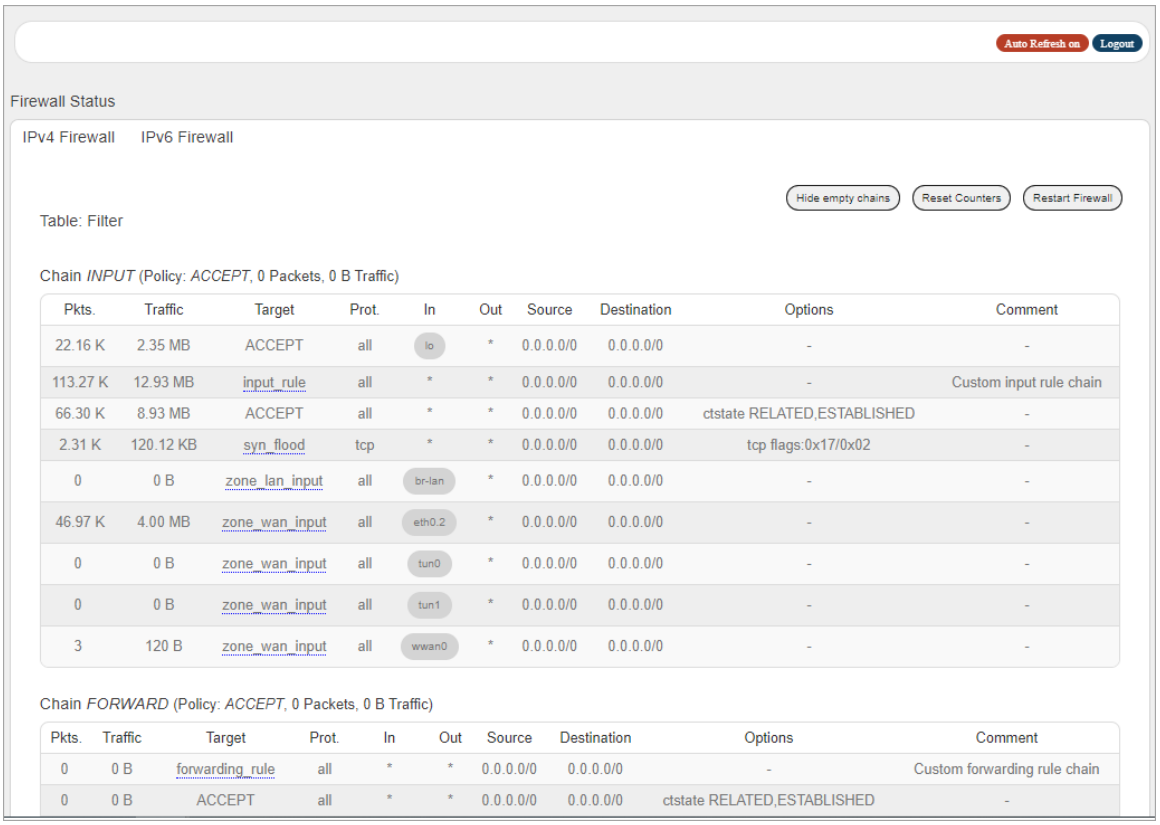


Figure 6.2-1: Ipv4 Firewall Status

Parameters	Description
Hide empty chains	Click to hide the chains that have no rules.
Reset Counters	Click to rest counters for Packets and Traffic.
Restart Firewall	Click to reload the existing Firewall configuration of every interface.
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.
Prot.	Displays the name of all the protocols configured in the Firewall Rule.
In	Input Interface

Parameters	Description
Out	Output Interface
Source	Displays the source IPv4 Address.
Destination	Displays the destination IPv4 Address.
Options	Displays option details
Comment	Displays comment details

Table 6.2-1: IPv4 Firewall Status

6.2.2 IPv6 Firewall

Status > Firewall Status > IPv6 Firewall

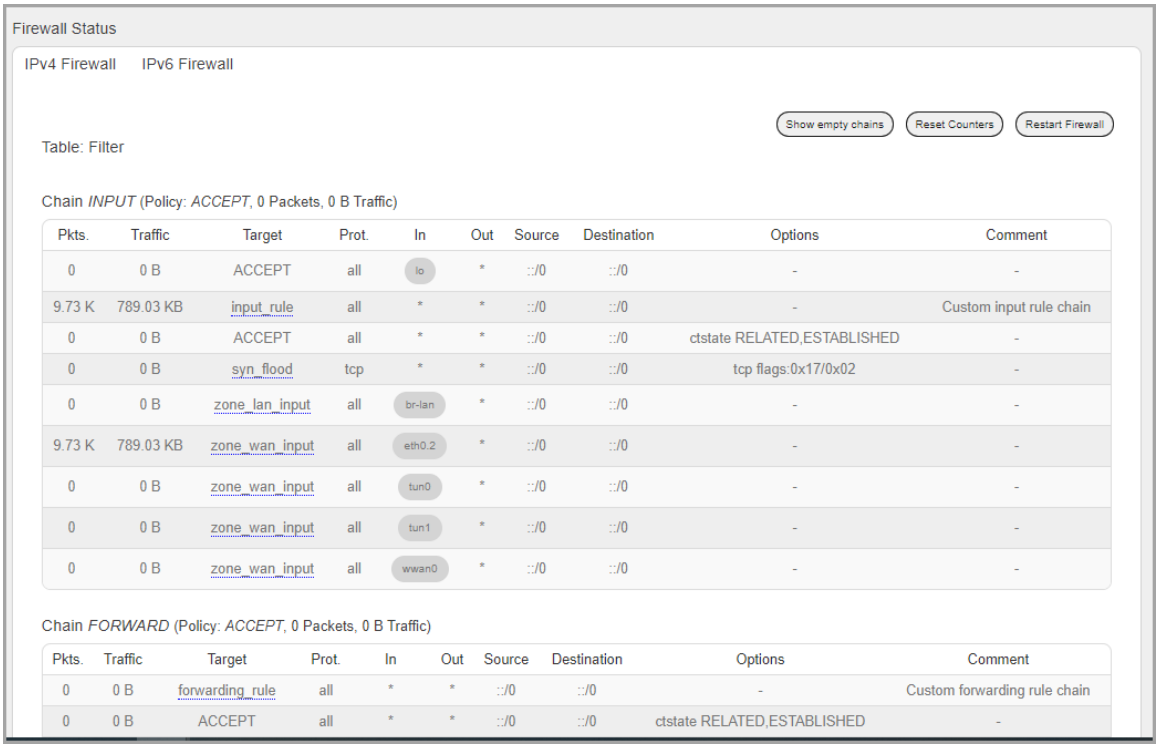


Figure 6.2-2: IPv6 Firewall Status

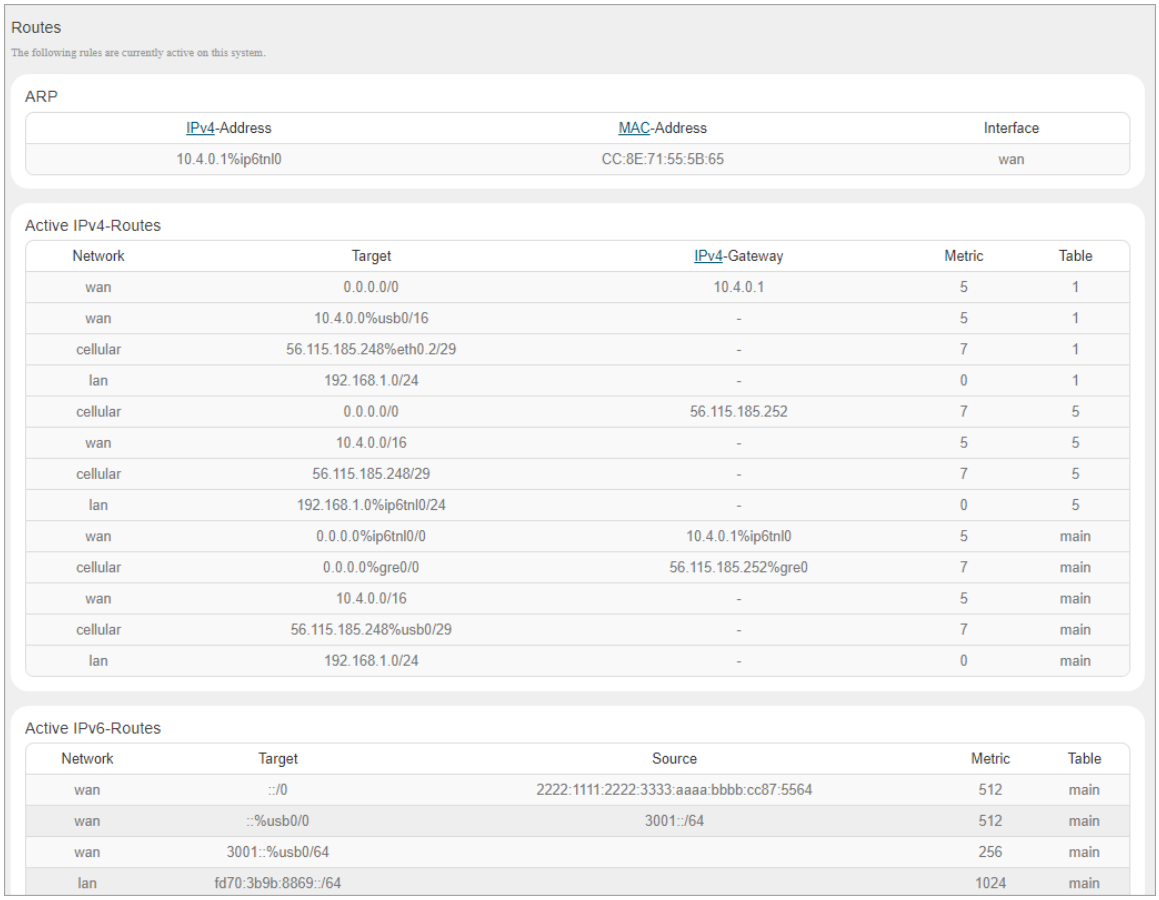
Parameters	Description
Hide empty chains	Click to hide the chains that have no rules.
Reset Counters	Click to rest counters Packets and Traffic.
Restart Firewall	Click to reload the existing Firewall configuration of every interface.
Pkts	Displays the number of accepted packets.
Traffic	Displays the amount of traffic captured by the filter.

Parameters	Description
Target	Displays the target.
Prot.	Displays the name of all the protocols configured in the Firewall Rule.
In	Input Interface
Out	Output Interface
Source	Displays the source IPv6 Address.
Destination	Displays the destination IPv6 Address.
Options	Displays option details
Comment	Displays comment details

Table 6.2-2: IPv6 Firewall Status

6.3 Routes

Status > Routes



Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	Interface
10.4.0.1%ip6tnl0	CC:8E:71:55:5B:65	wan

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric	Table
wan	0.0.0.0/0	10.4.0.1	5	1
wan	10.4.0.0%usb0/16	-	5	1
cellular	56.115.185.248%eth0.2/29	-	7	1
lan	192.168.1.0/24	-	0	1
cellular	0.0.0.0/0	56.115.185.252	7	5
wan	10.4.0.0/16	-	5	5
cellular	56.115.185.248/29	-	7	5
lan	192.168.1.0%ip6tnl0/24	-	0	5
wan	0.0.0.0%ip6tnl0/0	10.4.0.1%ip6tnl0	5	main
cellular	0.0.0.0%gre0/0	56.115.185.252%gre0	7	main
wan	10.4.0.0/16	-	5	main
cellular	56.115.185.248%usb0/29	-	7	main
lan	192.168.1.0/24	-	0	main

Active IPv6-Routes

Network	Target	Source	Metric	Table
wan	::/0	2222:1111:2222:3333:aaaa:bbbb:cc87:5564	512	main
wan	::%usb0/0	3001::/64	512	main
wan	3001::%usb0/64		256	main
lan	fd70:3b9b:8869::/64		1024	main

Figure 6.3-1: Routes Status

Parameters	Description
ARP – ARP table provides information about the peripherals connected on each interface	
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 – Displays the active IPv4 network route information.	
Network	Displays the network Type used by the active IPv4 routes.
Target	Displays the destination IPv4 Address.
IPv4 Gateway	Displays the IPv4 Address Gateway used for traffic routing.
Metric	Displays the metric assigned to the Interface.
Active IPv6 Routes – Displays the active IPv6 network route information.	
Network	Displays the network Type used by the active IPv4 routes.
Target	Displays the destination IPv6 Address.
IPv6 Gateway	Displays the IPv6 Address Gateway used for traffic routing.
Metric	Displays the metric assigned to Interface.

Table 6.3-1: Routes Status

6.4 System Log

Status > System Log

The E210 and E220 series routers provide extensive logging capabilities for traffic, system, and network protection functions. Detailed log information and reports provide historical as well as current analysis of network activity to help identify security issues and reduce network abuse.

The router can either store logs locally or send logs to external syslog UDP servers for storage and archival purposes.

The network activities and traffic logs include:

- Firewall logs
- Interface Activity logs
- Administrator logs
- User Authentication logs

The single syslog server allows for remote logging and can be configured from *System > System > Logging*.

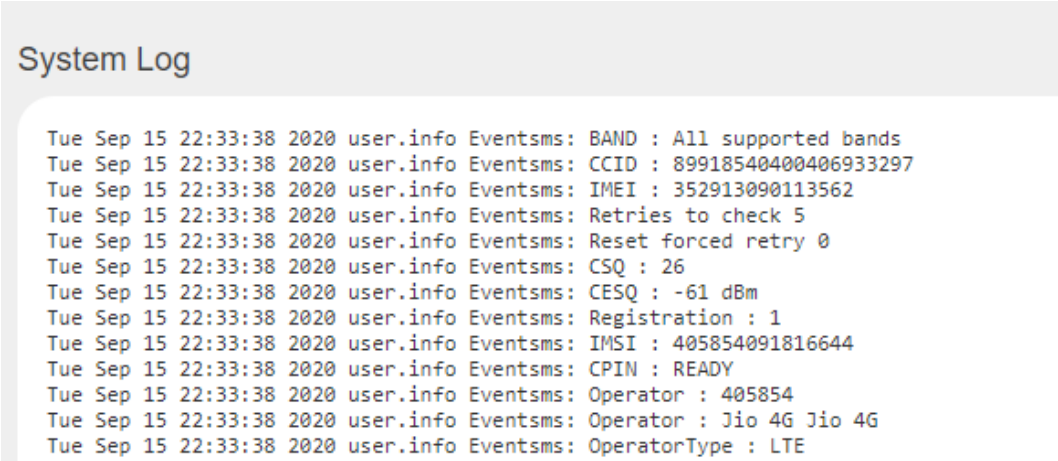


Figure 6.4-1: System Logs

6.5 Kernel Log

Status > Kernel log

This log displays the Linux kernel log events.

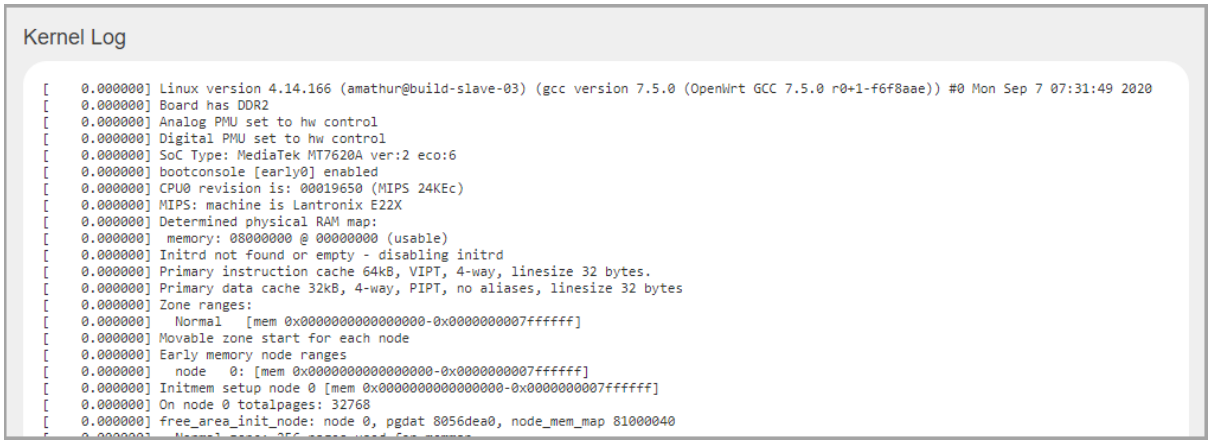


Figure 6.5-1: Kernel Log

6.6 Processes

Status > Processes

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

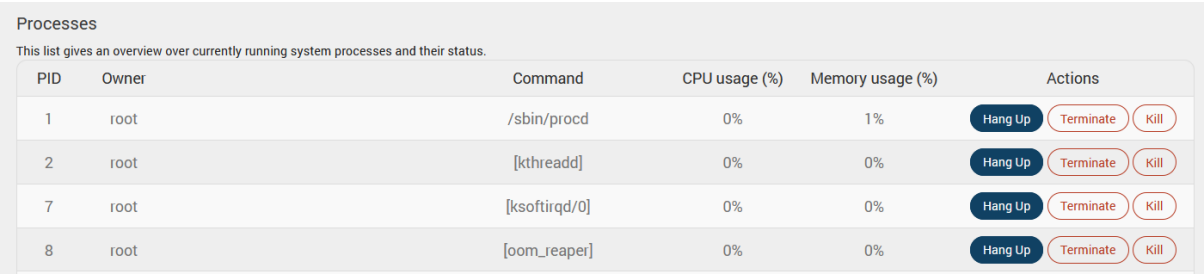


Figure 6.6-1: Processes Status

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

Parameters	Description
	displayed as a percentage.
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 and the process will not perform any cleanup operations.

Table 6.6-1: Processes Status

6.7 Realtime Graphs

Status > Realtime Graphs

The Realtime graphs display router activities over different time intervals. The following graphs are provided: load average, interface traffic information for LAN, WAN, Tunnel and Wi-Fi interfaces, wireless usage, and connection-detailed information.

6.7.1 Load

Status Realtime Graphs > Load

Graph shows past three minutes average CPU load and peak CPU load on the router.

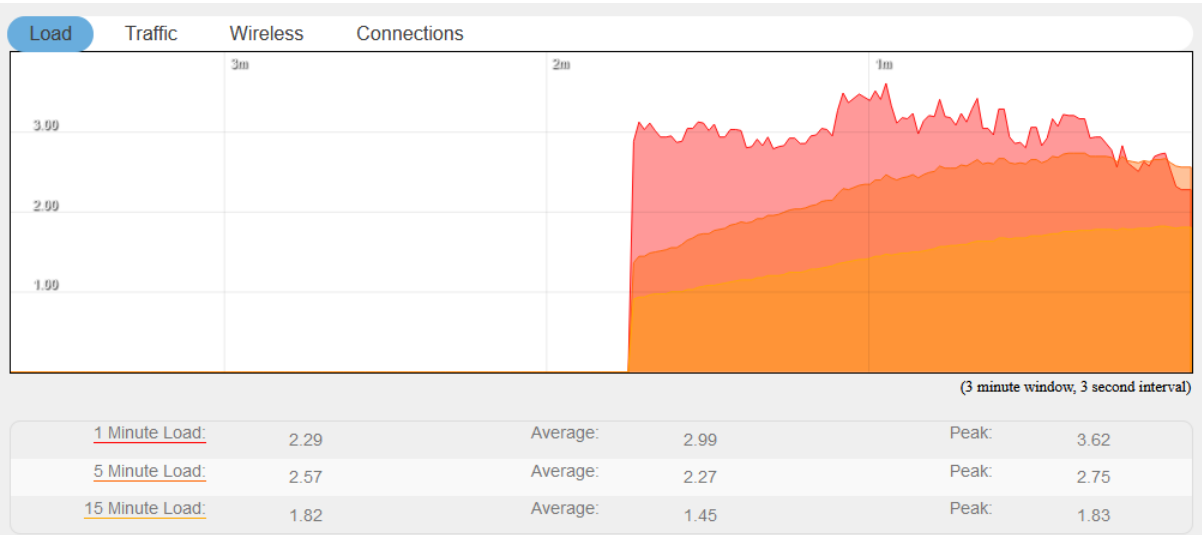


Figure 6.7-1: Real Time Load Graph

Parameters	Description
Load	Graph shows the periodic average CPU load on the Router.

Parameters	Description
	Details *X axis – Time Interval (1 minute)* *Y axis – CPU Load (Percentage)* **Legends** *Red – 1 Minute Load* *Orange – 5 Minute Load* *Yellow – 15 Minute Load*

Table 6.7-1: Real Time Load Graph

6.7.2 Traffic

Status > Realtime Graphs > Traffic

Traffic indicates the WAN side incoming and outgoing traffic on the router. The graphs display the average and peak data transfer for LAN, WAN, WLAN, WWAN, Tunnel and Cellular interfaces, color coded to indicate upload and download traffic.

The following figure shows the traffic graph for the eth0 interface:

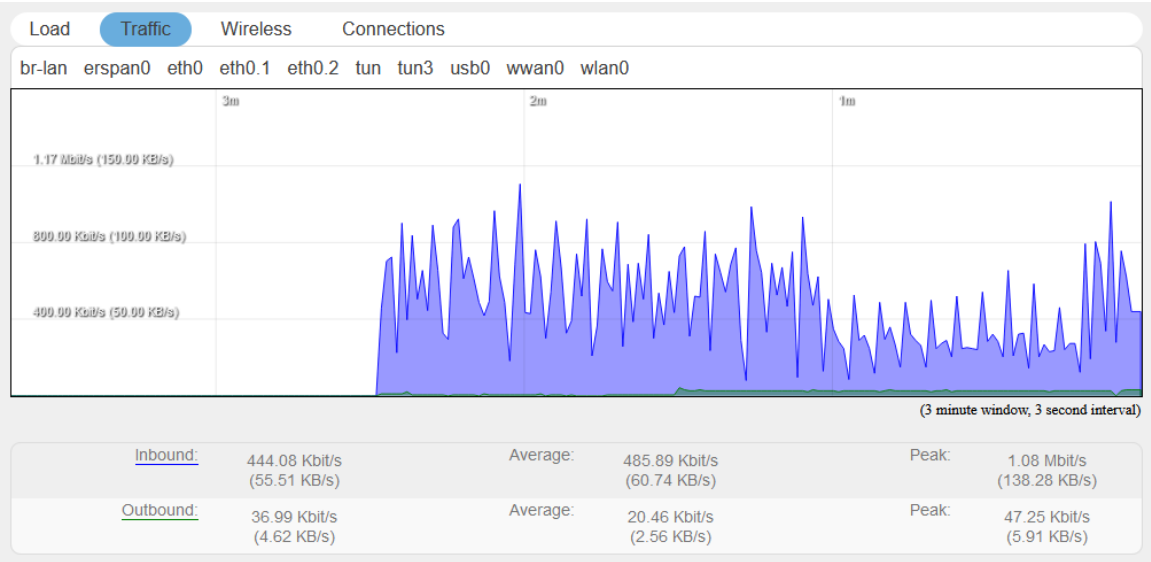


Figure 6.7-2: Status Realtime traffic for eth0

For each graph, the time interval (1 minute) is shown on the x-axis and the traffic (in kB/s) is shown on the y-axis. Blue represents inbound traffic while green represents outbound traffic.

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

6.7.3 Wireless

Status > Realtime Graphs > Wireless

Wireless indicates the traffic on Wi-Fi irrespective of Wi-Fi being used as an access point (LAN) or Client (WAN).

Wireless Graphs displays real time graph combined for Signal and Noise data transferred in real time. Colors differentiate Signal and Noise data rates. It also displays the Physical data transfer rate. In addition, it shows the average and peak Signal and Noise and Physical data rates individually.

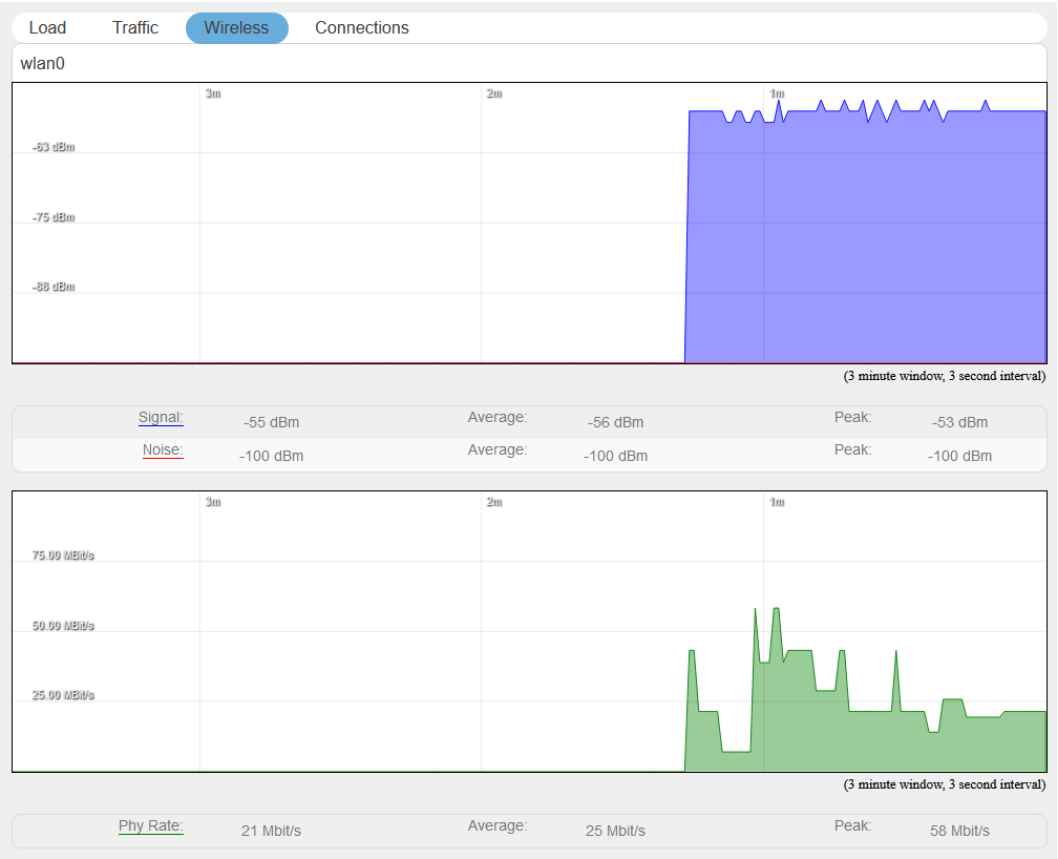


Figure 6.7-3: Real Time Wireless Traffic Graph

Parameters	Description
WLAN Interface	
Signal	Graph shows the periodic average of Signal and Noise on the Router. **Details** *X axis – Time Interval (1 minute)* *Y axis – Data Rate (Mbit/s)* **Legends** *Blue – Signal* *Red – Noise*

Parameters	Description
	Green – Physical Rate

Table 6.7-2: Real Time Wireless Traffic Graph

6.7.4 Connection

Status > Realtime Graphs > Connection

Connection graphs provide an overview of active network connections; those originating from the router and also those that are originating from LAN/WAN of the router.

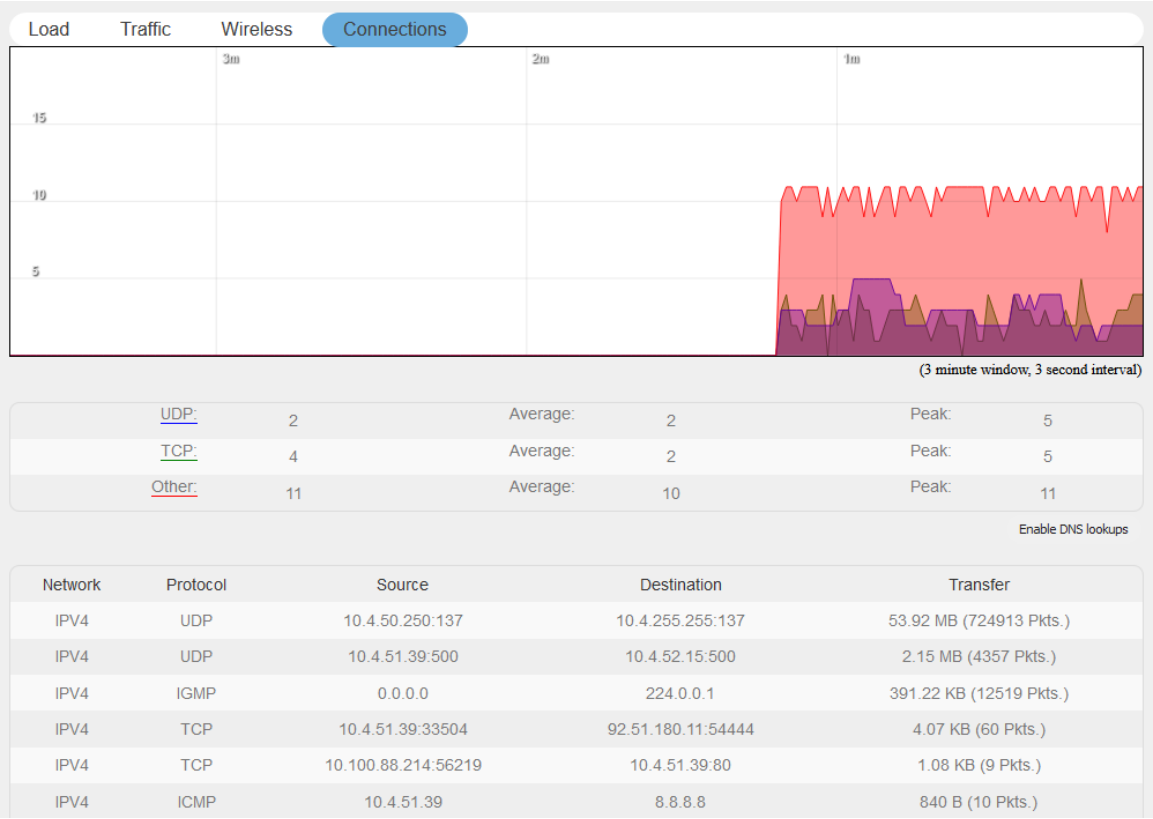


Figure 6.7-4: Real Time Connection Traffic Graph

Parameters	Description
Protocol	Graph shows the periodic average of data transfer using specific protocols on the Router using the active connections in real time. **Details** *X axis – Time Interval (1 minute)* *Y axis – Number of Active Connections*

Parameters	Description
	Legends *Blue – UDP* *Green – TCP* *Red – Other Protocols*
Network	Network connection type, IPv4 or IPv6.
Protocol	Name of the protocol used for routing data.
Source	Source IP Address and port number of an active connection.
Destination	Destination IP Address and port number of an active connection.
Transfer	Displays the total data transferred using the specific network connection.

Table 6.7-3: Real Time Connection Traffic Graph

6.8 Load Balancing

Status > Load Balancing

6.8.1 Interface

Status > Load Balancing > Interface

This status page shows the MWAN interfaces, where active interfaces are shown in green and disabled interfaces are shown in red.

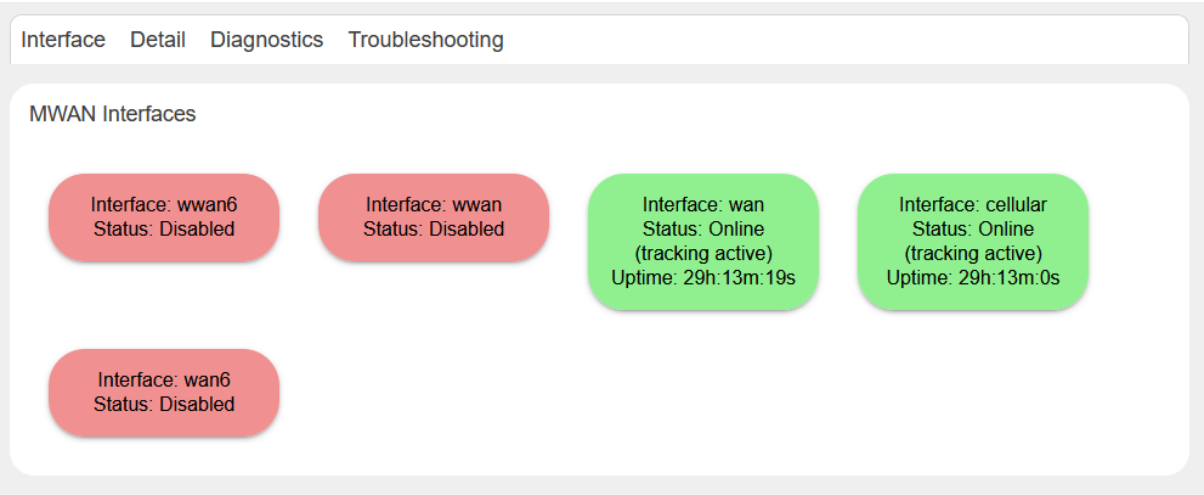


Figure 6.8-1: MWAN Interface Status

6.8.2 Detail

Status > Load Balancing > Detail

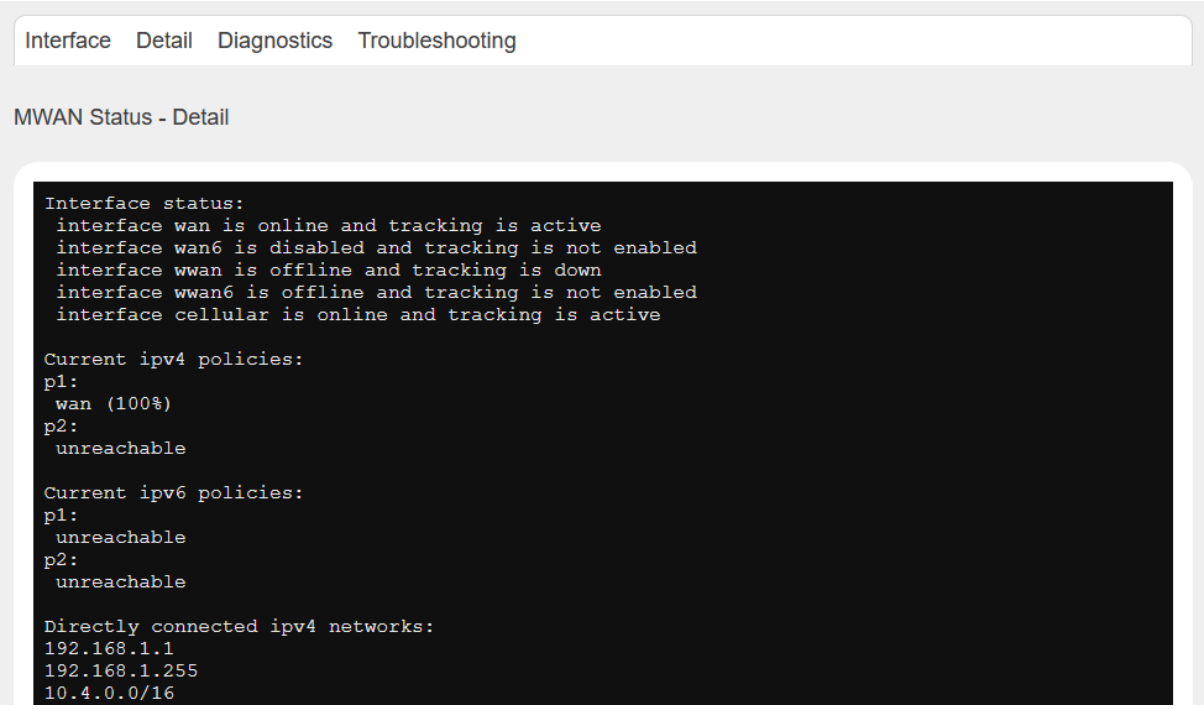


Figure 6.8-2: MWAN Status Detail

6.8.3 Diagnostics

Status > Load Balancing > Diagnostics

The MWAN Status – Diagnostics page shows all configured interfaces in MWAN3 and allows you to run diagnostics commands on the specified MWAN interface. The results of the diagnostics are displayed below the task.

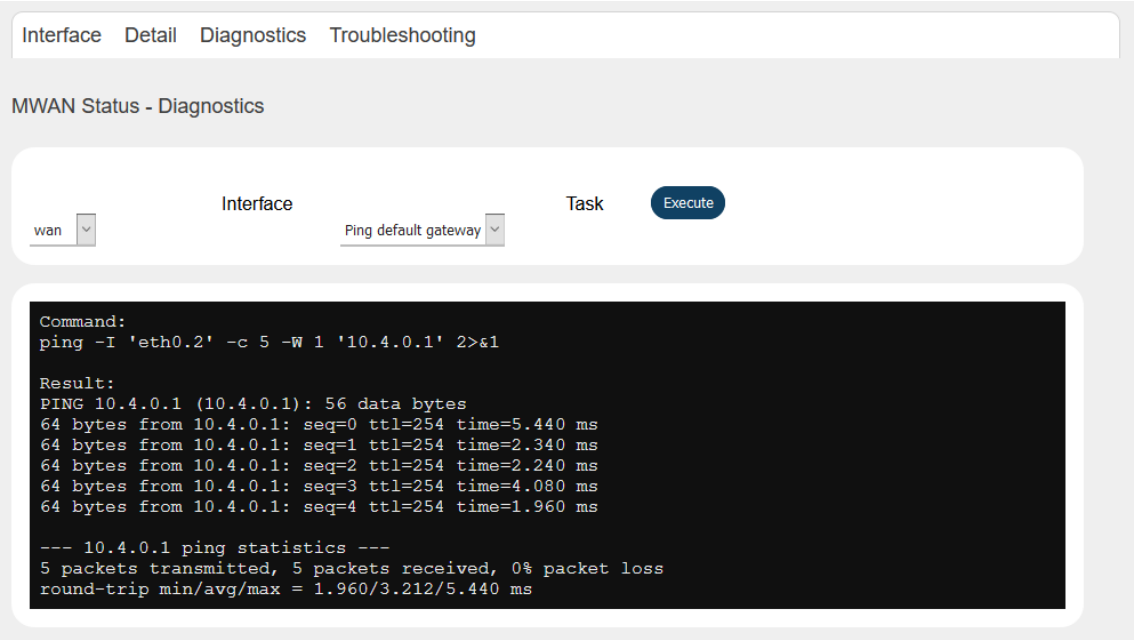


Figure 6.8-3: MWAN Status Diagnostics

6.8.4 Troubleshooting

Status > Load Balancing > Troubleshooting

Load balancing troubleshooting page shows the output of IP commands to use for troubleshooting purposes.

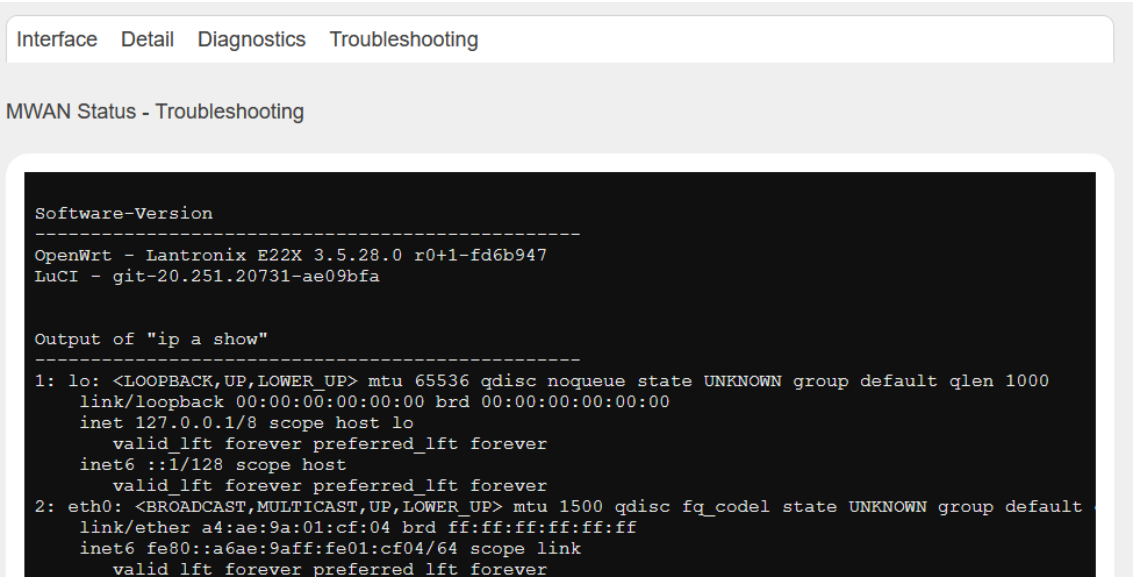


Figure 6.8-4: MWAN Status Troubleshooting

7 System

System allows configuration and administration of the router for secure local and remote management. Many system functions can be configured from the following menus:

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

7.1 System

System > System

This page provides basic system settings including time management, system log, synchronization, and UI theme settings.

7.1.1 General Settings

System > System > General Settings

The current date and time of the router's internal clock can be set locally to match the date/time of your computer's browser or the router can be configured to synchronize its internal clock with an NTP server so that logs show the precise time and router activities can happen at a precise time.

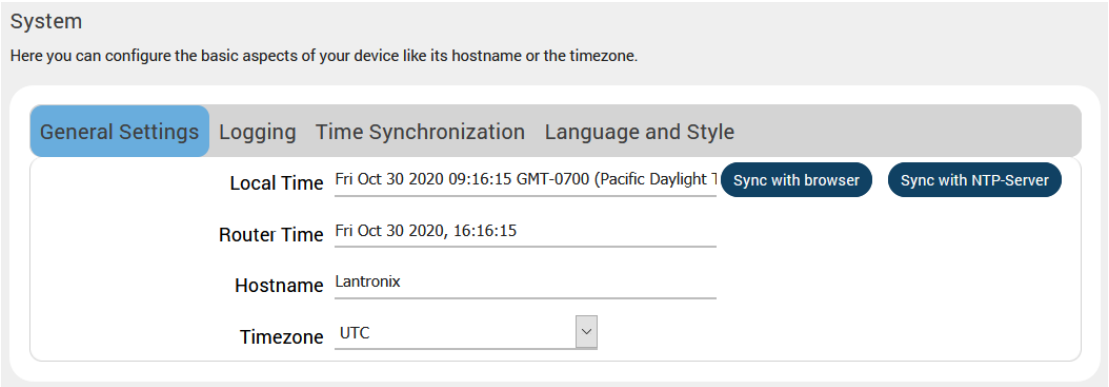


Figure 7.1-1: System General Settings

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 router clock with the local computer browser. Click **Sync with NTP-Server** to synchronize the router 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.
Hostname	Enter the Hostname for this router. Do not include period character "." in the hostname as only the string before the period will be used as the hostname. The configured Hostname appears on the **Status > Overview page**.
Timezone	Select time zone according to the geographical region in which router is deployed. The default time zone is UTC.

Table 7.1-1: System General Settings

7.1.2 Logging

System > System > Logging

The router can capture and log system activity including interface connection status, internal debugging messages, critical and emergency logs. It can either store the logs locally and/or send them to an external UDP syslog server for storage and archival purposes. The system log buffer uses First In First Out (FIFO) mechanism.

Note

- ***All the logs are lost on Router reboot.***

SYSLOG is an industry standard protocol/method for collecting and forwarding messages from devices to a server running a syslog daemon usually via UDP Port 514. The syslog server on a remote computer accepts the log messages and stores them in files or prints them. Logging to a central syslog server facility helps in the aggregation of associated logs and alerts and provides protected long term storage. This is useful for incident handling, routine troubleshooting, and historical analysis.

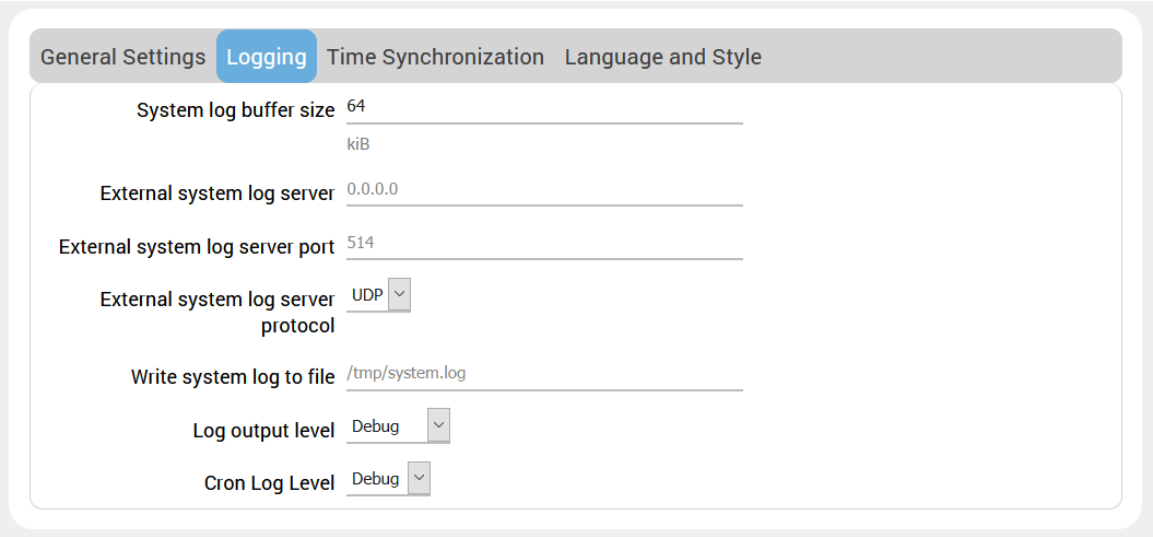


Figure 7.1-2: System Log Configuration

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.
External system log server	Enter the IP Address of an External server system. This server will be used to save all the real time logs. The default IP Address of external log server is 0.0.0.0 ***Note*** • ***Enabling Remote Log features requires a Router to be manually rebooted in all firmware versions below V2.2.0***
External system log server port	Enter the Port number of an External UDP server system.

Parameters	Description
	UDP server is used to store the system logs The default port is 514.
External system log server protocol	UDP or TCP
Log output level	Select the Log severity output level. Debug and Info levels are lower severity than Warning and Error levels and are more verbose. Selecting debug or info level will also include the higher severity messages. ***Debug –*** *Logs will be used by The E2xx series router software developer for debugging the router application. These logs are not useful during operations.* ***Info –*** *These logs provide 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 –*** *A warning messages is displayed 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 logs indicating an error condition.* ***Note*** • ***For help with log errors, please contact Lantronix Technical Support.*** ***Critical –*** *Indicates failure in secondary system and must be corrected immediately.* ***Alert –*** *Problems which should be corrected immediately.* ***Emergency –*** *System is Unusable.*
Cron log level	Select the minimum level for cron messages to be logged to syslog. ***Debug –*** *Helps you debug cron process which has failed during runtime.* ***Normal –*** *Normal informational messages* ***Warning –*** *Indicates some issues can happen or error could be generated in cron process.* ***Note*** • ***For help with Cron log warning messages, please contact Lantronix Technical Support.***

Table 7.1-2: Syslog Configurations

7.1.3 Time Synchronization

System > System > Time Synchronization

Select the method that the router uses to synchronize its internal clock.

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

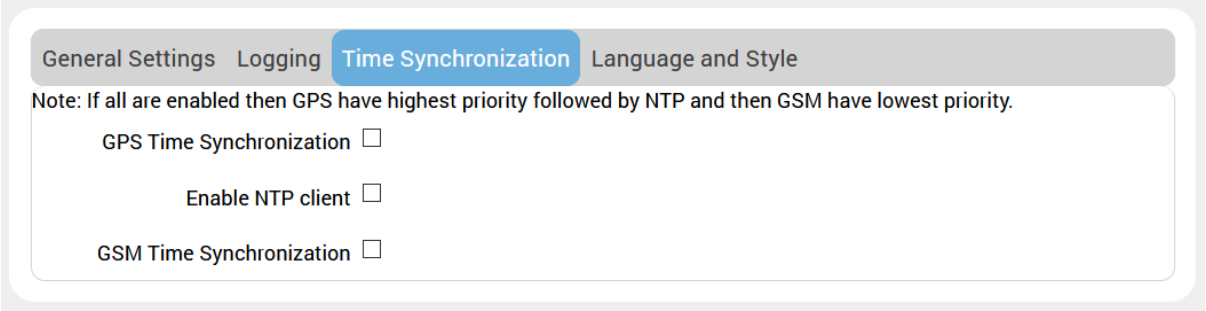


Figure 7.1-3: System Time Synchronization Configuration

Time Synchronization	
GPS Time Synchronization	For routers that support GPS. If enabled, the router will synchronize its internal clock using GPS. ***Note*** • ***GPS Antenna will be needed for GPS time sync***
Enable NTP client	If enabled, the router will synchronize its internal clock from an NTP server. ***Note*** • ***If NTP Server is activated, the Router will update time every 60 minutes from the NTP Servers.*** • ***Enabling NTP Client consumes data.***
GSM Time Synchronization	If enabled, the router will synchronize using GSM functionality.

Table 7.1-3: System Time Synchronization Configuration

7.1.4 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.

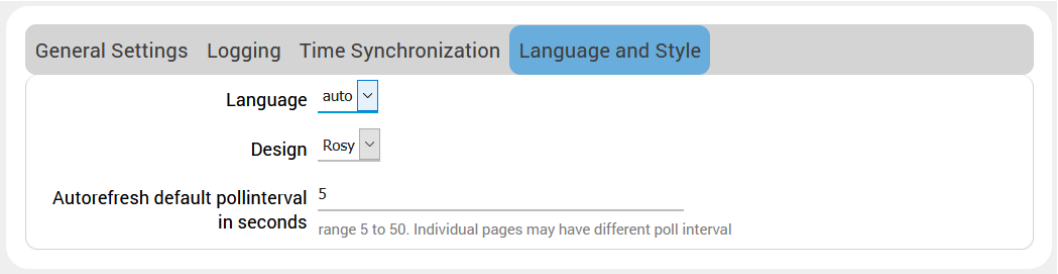


Figure 7.1-4: System Language and Style Configuration

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

Table 7.1-4: Language and Style Configurations

7.2 Administration

System > Administration

The Administration page allows configuration of general router settings including the router password and settings for SSH access. the router. Various ports and login security can be configured using Administration submenu.

7.2.1 Router Password

System > Administration > Router Password

This page allows you to change your login password at any time.

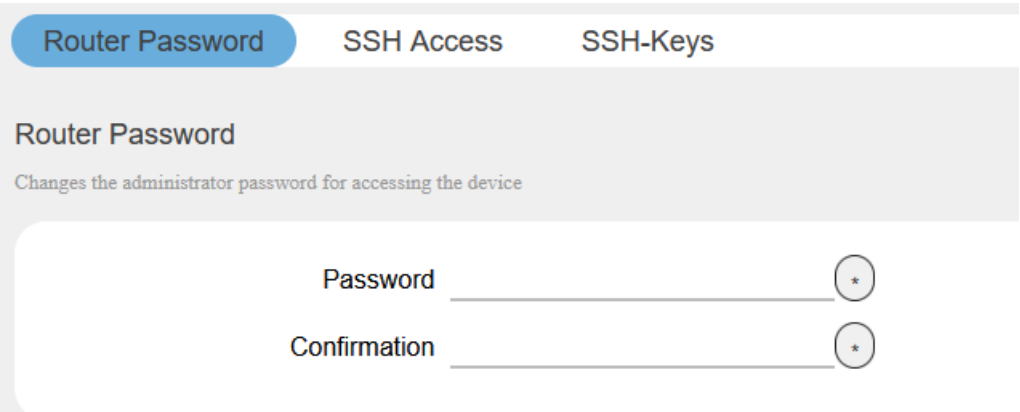


Figure 7.2-1: Change Router Password

Parameters	Description
Password	Specify the new password.
Confirmation	Confirm the new password.

Table 7.2-1: Router Password Configuration

7.2.2 SSH Access

System > Administration > SSH Access

The E2xx series routers integrate Dropbear which offers SSH network shell access and an integrated SCP (Secure Copy Protocol) server for file transfer.

You can also set parameters for Dropbear instance for SSH Access. On the SSH-Keys page you can add public SSH-Keys (one per line) for SSH public-key authentication.

By default, the remote SSH access over WAN is disabled. You can enable the remote SSH access from the web interface or alternately can send an SMS from a registered admin number to enable it. You are required to use the SSH keys displayed on the webpage for SSH access.

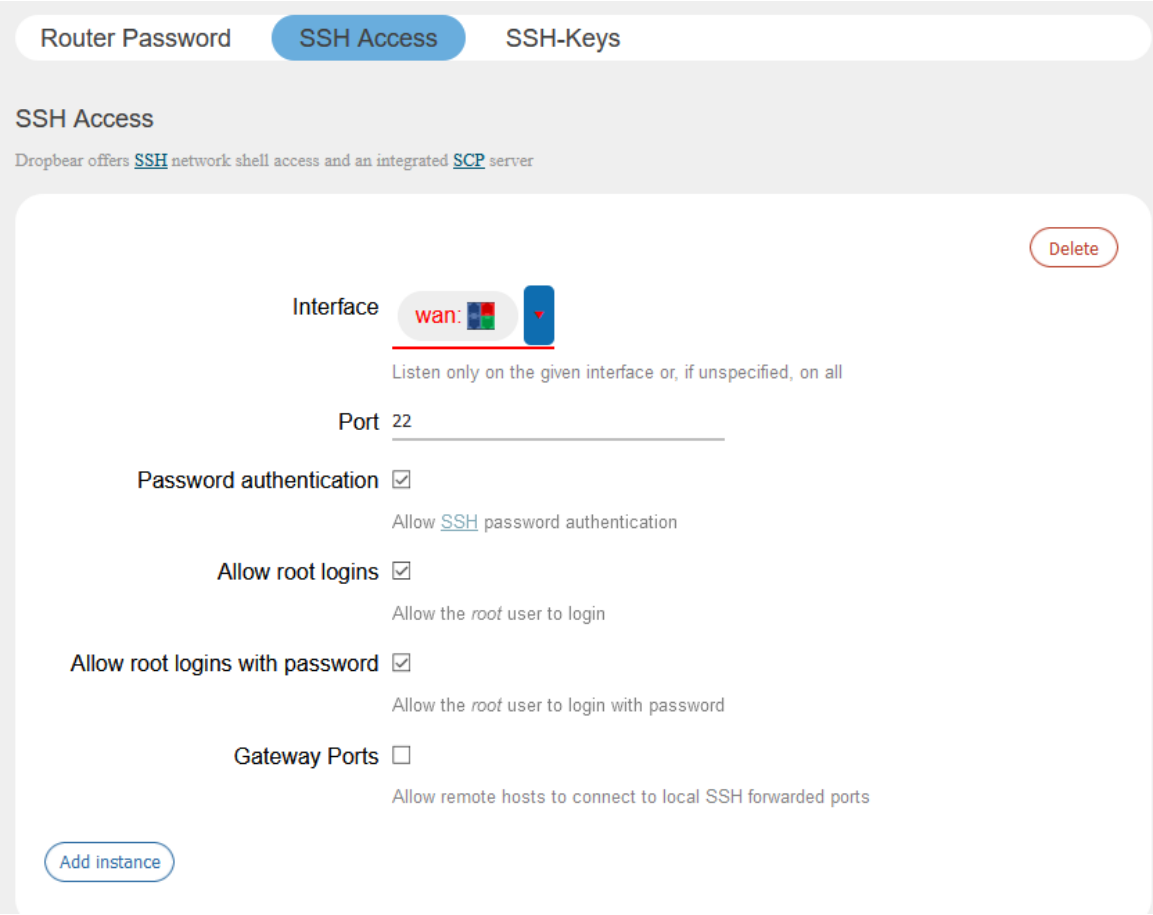


Figure 7.2-2: SSH Access Configuration

Parameters	Description
Dropbear Instance	
Interface	Select the interface. SSH listens only on the selected interface. *Unspecified – If this option is selected, SSH listens on all interfaces.*
Port	Provide listening port of the Dropbear instance. Default port is 22.
Password Authentication	Select to allow authentication using SSH password.

Parameters	Description
	The default option is disabled.
Allow root logins	Select to allow root user logins to the router.
Allow root logins with password	Select to allow root logins and require a password.
Gateway ports	Select to allow remote hosts to connect to local SSH forwarded ports.
Add Instance	Click to add another SSH instance with the specified configuration.
Delete	Click to delete the Interface.

Table 7.2-2: SSH Access Configurations

7.2.3 SSH-Keys

System > Admin > SSH-Key

Public SSH keys can be added one per line to authenticate with SSH public key authentication.

Public SSH keys are provided by default. They are configured on port 22. SSH from WAN network is disabled by default. To enable it, you must enable port 22 from the Network > Firewall page.

To add a new key, copy the public key from the Host system, paste it in the text box (see the figure below), and then click **Add key**.

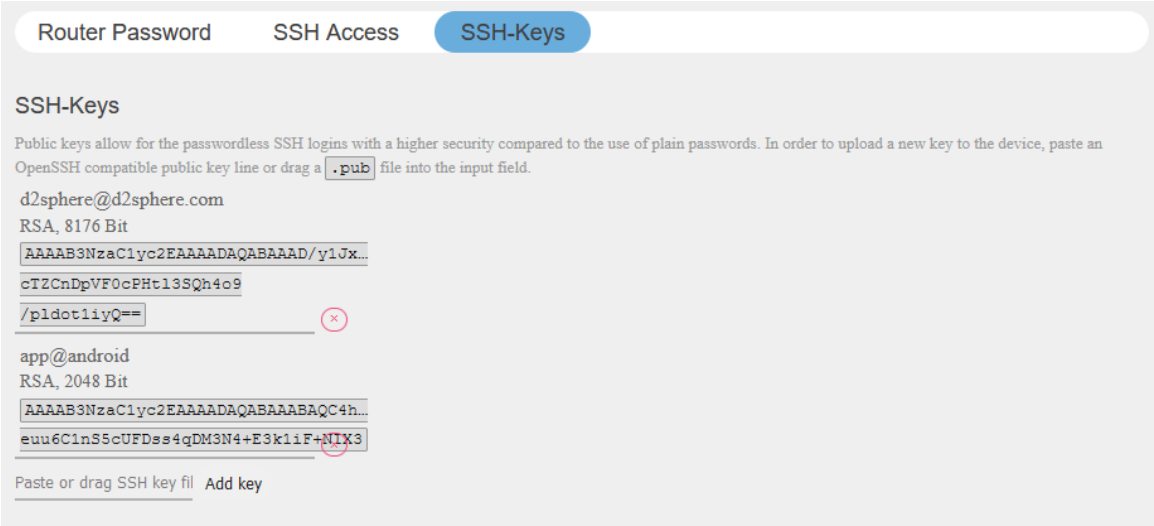


Figure 7.2-3: SSH Key Administration

7.3 Software

System > Software

The Software page gives you access to manage software packages in the router.

Lantronix has its own list of packages that can be downloaded from D2Sphere. For details on D2Sphere, please contact Lantronix Sales.

7.3.1 Installed and Available Packages

System > Software > Installed/Available/Updates

The Software page displays the available packages, installed packages, or updates, on the Available, Installed, and Updates tabs, respectively.

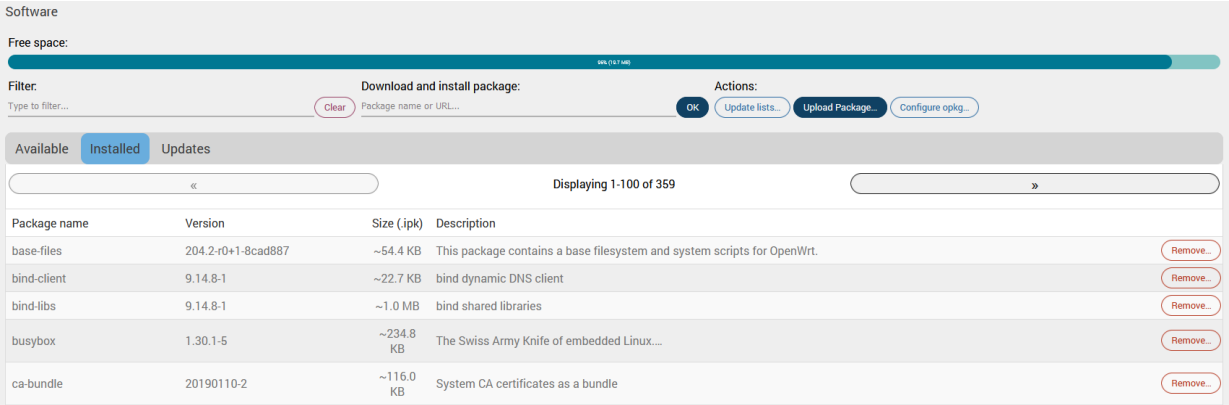


Figure 7.3-1: Installed Software Packages

Parameters	Description
Available Memory, Package Filter, and Actions	
Free space	Indicates the free and used space on the flash memory. The darker line represents the portion of free space.
Filter	Enter the **keyword** of the required package to search for it from package repository servers.
Download and install package	Enter the **exact name** or URL of the package to be downloaded from package repository servers and install it. Click OK initialize installation.
Update lists	Click to update the package list from the package repository servers.
Upload Package	Click to upload a package file from your local drive.
Configure opkg	Click to modify the OPKG package manager configuration files, which provide the path to tell the router where to fetch the packages from. See Section *7.3.2* for more information.
Status – Installed/Available/Update Package	
Package name	Displays the name of package.
Version	Displays the version of package.
Size	Displays the size of the installed package.

Parameters	Description
Description	Displays the package description, if one has been provided.
Remove	Click to remove the package. On the confirmation page, select or clear the option to automatically remove unused dependencies.

Table 7.3-1: Software Installation and Package Details

7.3.2 OPKG Configuration

System > Software

OPKG Configuration allows you to modify the following configuration files used by the OPKG package manager:

- opkg.conf – This is the main configuration file. It provides the path from where the router should fetch and update the packages.
- customfeeds.conf – This file is used to add your custom package repositories.
- distfeeds.conf – This file is used to set the feeds. By default, it provides the path to the Lantronix packages on the D2Sphere server. All Lantronix packages may be updated from D2Sphere.com, however, you can add your own HTTP servers where you wish to upload your packages.

To modify the OPKG configuration, go to the System > Software page and click the **Configure opkg** button.

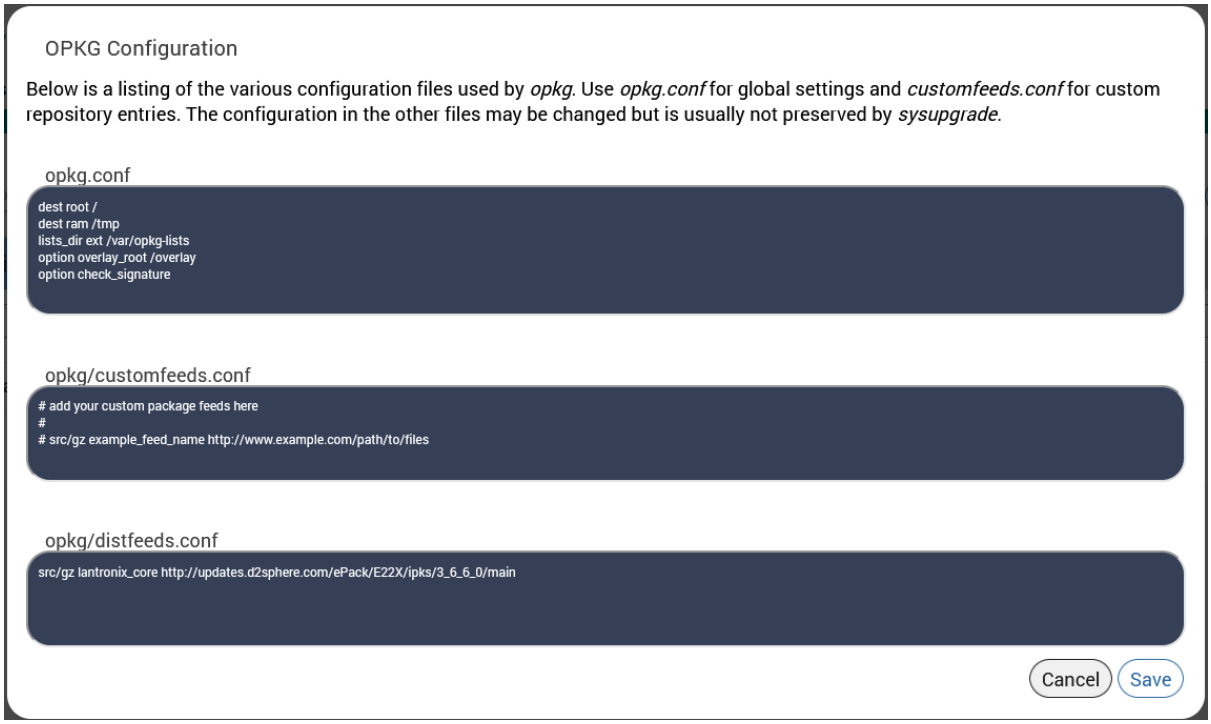


Figure 7.3-2: OPKG Configuration

7.4 Startup

System > Startup

7.4.1 Initscripts

System > Startup > Initscripts

Init scripts are run to start required processes during the boot process. Enable/Disable shows the current status and allows you to enable or disable the script. Newly enabled or disabled services take effect after the device reboots.

Start, Restart, and Stop will perform the specified action on the process immediately.

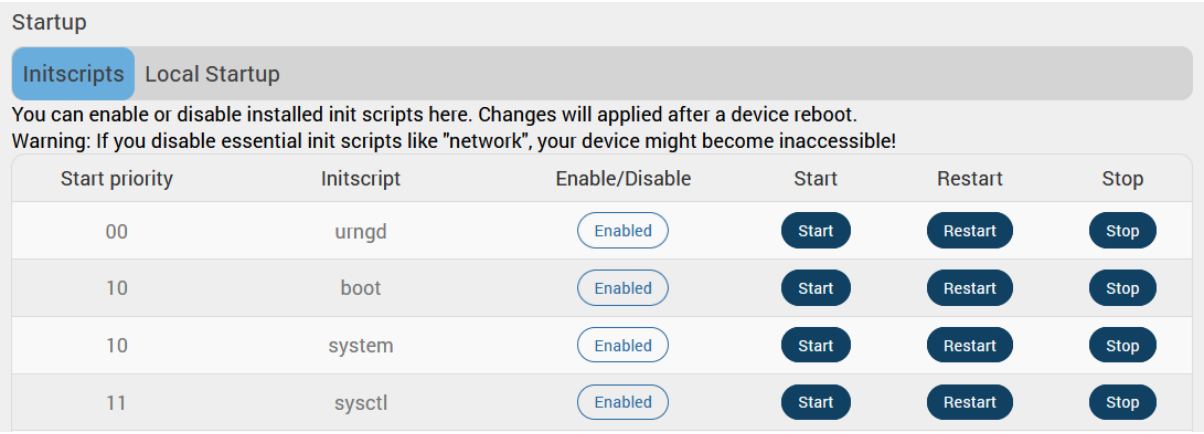


Figure 7.4-1: Startup Initscripts

7.4.2 Local Startup

System > Startup > Local Startup

The local startup file tells the router to run commands when the router boots, after the system init. It is empty by default and does nothing.

To configure the local startup file, add commands in the editor before the line "exit 0" and click **Save**. Changes will take effect on the next reboot.

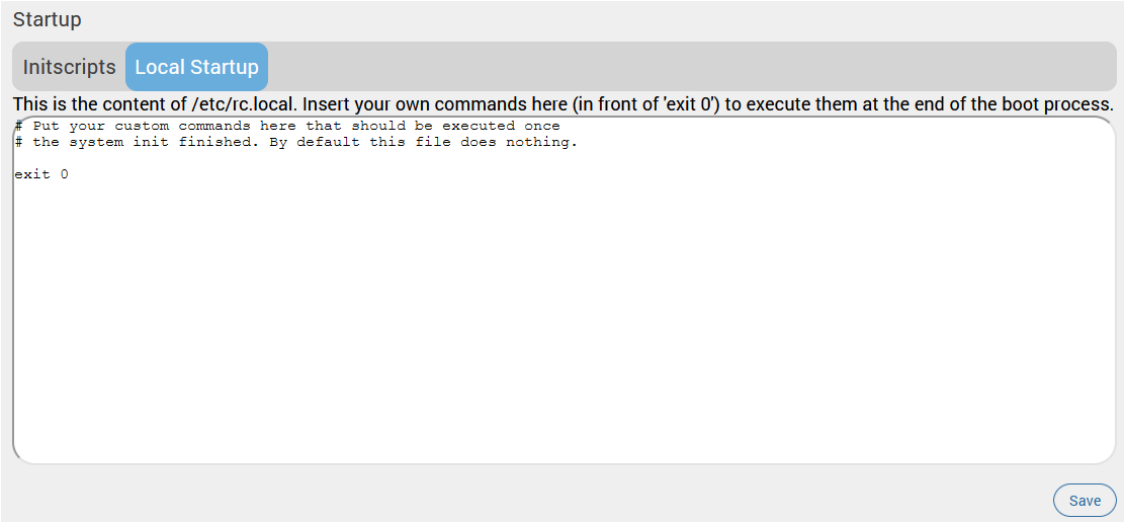


Figure 7.4-2: Local Startup Script

7.5 Scheduled Tasks

System > Scheduled Tasks

Use the system crontab to schedule tasks to run periodically at fixed times, dates, or intervals.

Each line in the script is a single task that includes the time (minute, hour, day of month, month, day of week) and the command to execute.

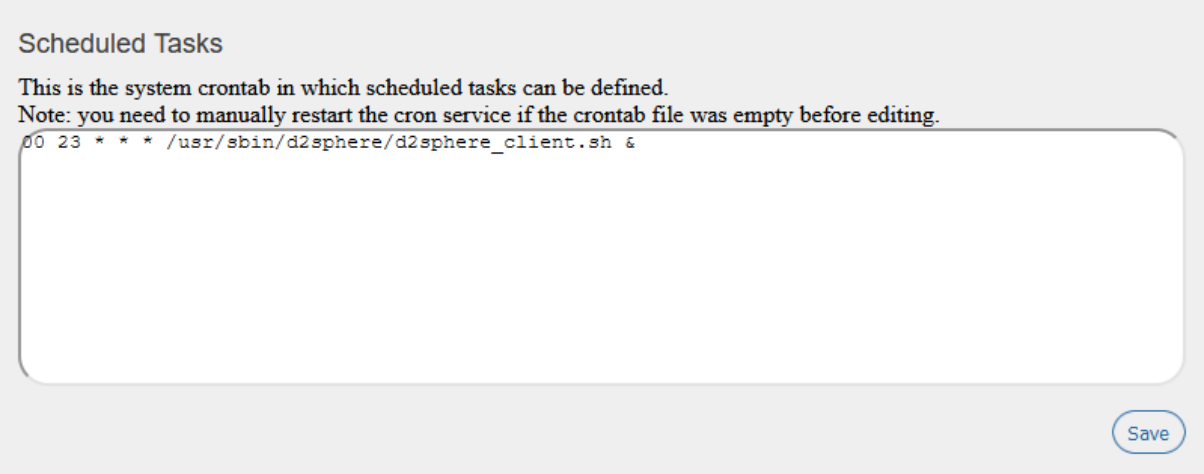


Figure 7.5-1: Scheduled Tasks Crontab

7.6 LED Configuration

System > LED Configuration

This section allows you to customize the behavior of the device LEDs. The LED Configuration page displays the LEDs that are present on the router, their default state, and the trigger event for the LED. LED entries are stored in the sys filesystem, more specifically the /sys/class/leds directory. The LED can be controlled by various system events, which is selected by the trigger option. To determine which triggers are available for an LED, refer to the trigger file of that LED.

For a description of the E210 and E220 LEDs, see *Appendix B. LED Behavior.*

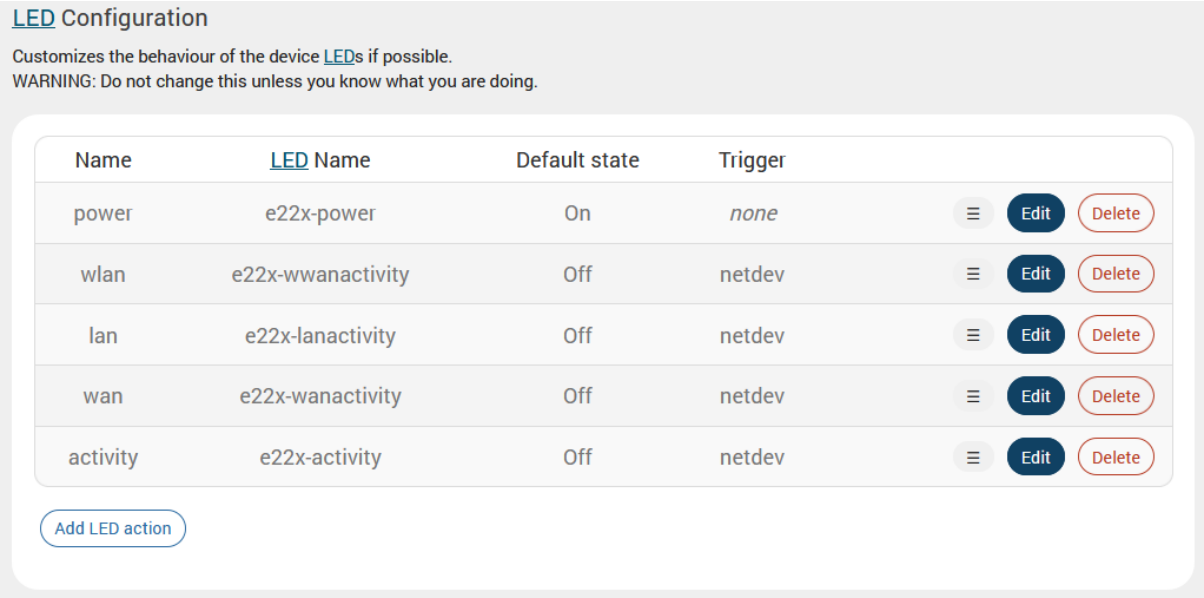


Figure 7.6-1: LED Configuration

7.6.1 Add/Edit LED Configuration

Edit the LED configurations with care.

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. *Default-on – defaulton. deprecated, use default = ON and trigger = None instead.* *Network Activity triggers – netdev. The LED flashes with link status and/or send and receive activity (trigger mode) on the configured interface (device).* *None – none. LED is always in default state (off). Can be used to set the LED to always On* *WiFi Activity triggers – Options with "phy" prefix. The LED flashes on events in the physical interface rather than in the software network interface.* *Switch – switch0. The LED is on if a link on one of the configured switch ports is established. If this option is selected, enter the Switch port mask and Switch speed mask (hexadecimal).* *Timer – timer. The LED blinks with the configured on/off frequency. If this option is selected, enter the On-State Delay and Off-State Delay in milliseconds to indicate how long the LED should be On or Off.* *USB Device – usbdevice or usbport. The LED turns On if USB device is connected. If this option is selected, choose the USB device name or USB port.*

Table 7.6-1: LED Configuration

7.7 Backup / Flash Firmware

System > Backup / Flash Firmware

Backups should be run to keep the working configuration data. The backup file can used to restore configuration on the router or to configure a new router with the same settings.

The backup consists of all policies and all other user related information. After generating the backup, you need to upload the file to restore the backup.

Note

- ***Configuration archive is not compatible between versions 2.x and 3.x.***

7.7.1 Actions

System > Backup / Flash Firmware > Flash Operations

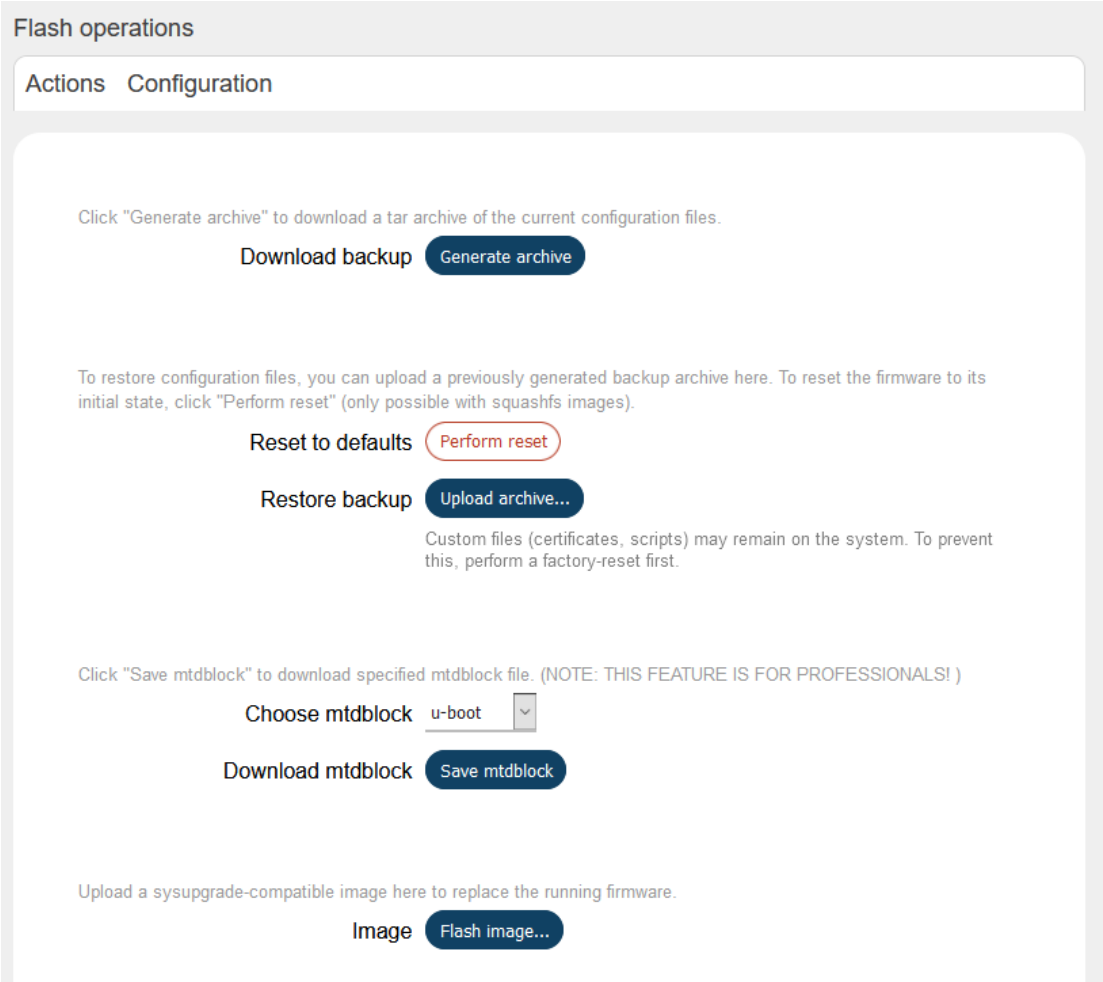


Figure 7.7-1: Backup Restore and Flash Firmware

Parameters	Description
Backup/Restore	
Download Backup	Click **Generate archive** button to download a .tar archive file of the current configuration files.
Reset to defaults	Click **Perform Reset** button to reset the firmware to its default configurations. This is valid only with squashfs images. ***Note*** ***The router can also be reset by pressing the reset button on the router.*** • ***Press and hold for more than 5 seconds for router to do a factory reset.*** • ***Press and hold for more than one second but less than 5 seconds for router to reboot.*** • ***For any pressed or released event to be detected the duration of the press/release event must be at least 200ms.***
Restore backup	Click **Upload archive** button to upload a previously generated backup archive.
Flash image	
Image	Click **Flash image** button to upload a sysupgrade compatible image for replacing the running firmware. When the binary image is loaded (.bin file), a file integrity check is done through the use of md5 algorithm. You should verify the md5 value with the one given along with the binary file. When uploading the binary image, the UI will prompt to "Keep settings and retain the current configuration." This is selected by default. If you deselect it, the device configuration will be reset to factory setting after updating to the new firmware. Avoid the "Keep settings" option when upgrading from version 2.x to 3.x or downgrading from 3.x to 2.x.

Table 7.7-1: Backup - Restore and Flash Operations

7.7.2 Configuration

System > Backup / Flash Firmware > Flash Operations

The custom files to be preserved during an upgrade should be added to the backup list text area, one per line.

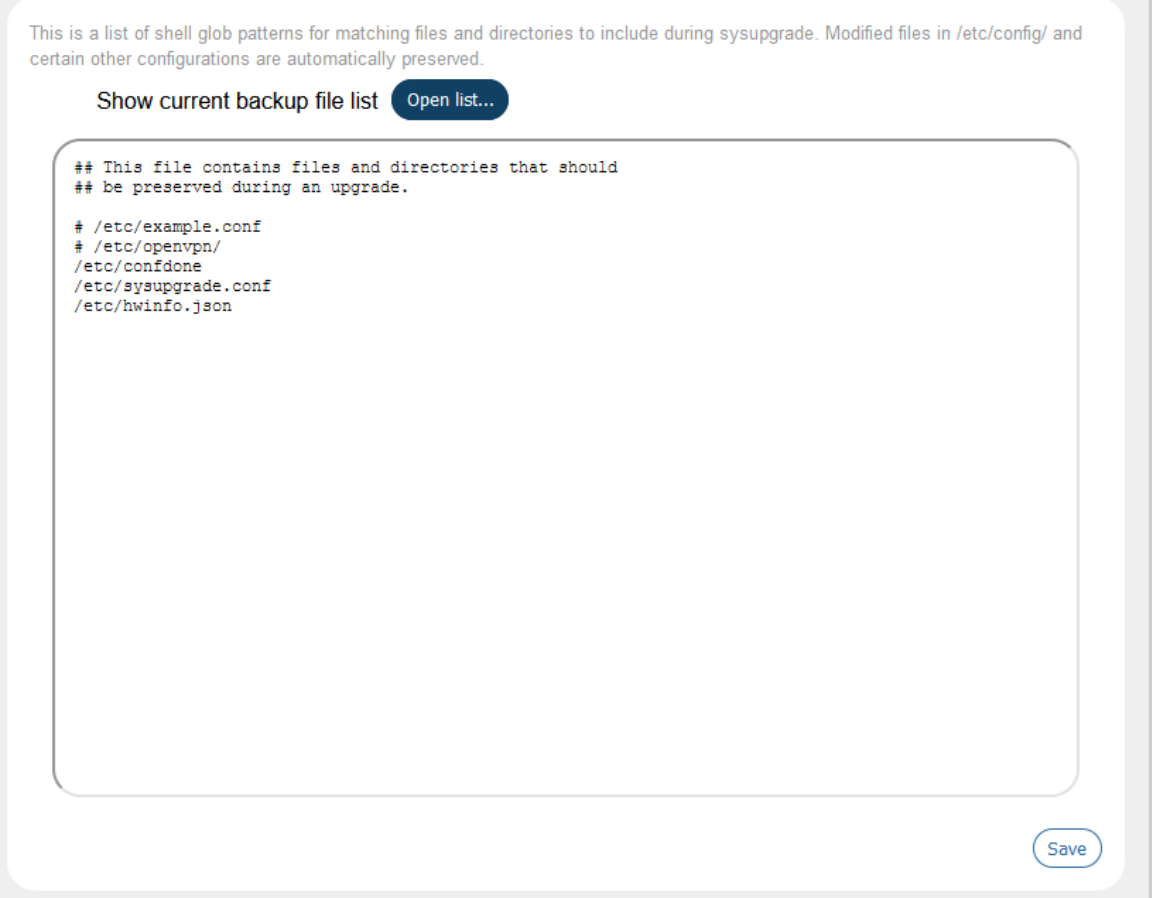


Figure 7.7-2: Backup File List Configuration

Parameters	Description
Open list	Click to open the list of default files and directories that should be preserved during an upgrade. Add the custom or additional files in the text area, one per line.

Table 7.7-2: Backup File Configurations

7.8 Custom Commands

System > Custom Commands

Write and execute custom shell commands from the web interface.

7.8.1 Dashboard

System > Custom Commands > Dashboard

View and run the custom commands from the dashboard. Custom commands support special characters as arguments.

Figure 7.8-1: Custom Command Dashboard

Parameter	Description
Run	Execute the command.

Table 7.8-1: Custom Command Dashboard

7.8.2 Configure

System > Custom Commands > Configure

Configure the custom commands that can be run on the dashboard.

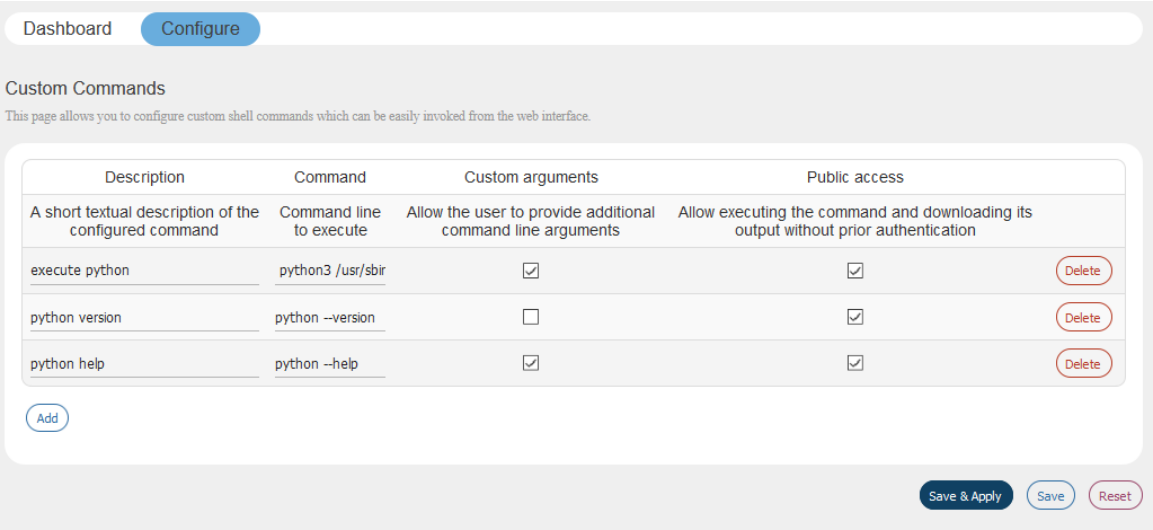


Figure 7.8-2: Custom Commands Configuration

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.
Add	Click to add an instance of a custom command.
Delete	Click to delete the custom command.

Table 7.8-2: Custom Commands Configuration

7.9 Reboot

System > Reboot

Router will be rebooted and will reload the configuration.

Note

- ***Any unsaved configuration will be lost when the router is rebooted.***

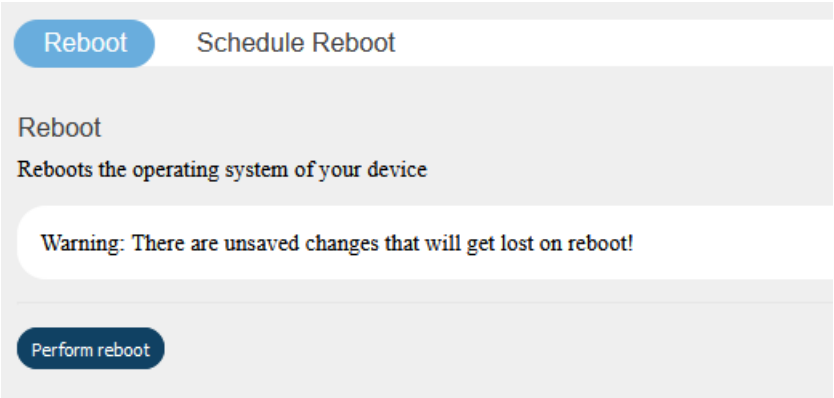


Figure 7.9-1: System Reboot

System > Reboot > Schedule Reboot

Set a schedule to periodically reboot the router. Frequency can be set by time of day (hour and minute), day of week, and day of month. The scheduled item must be enabled in order for the reboot to be performed.

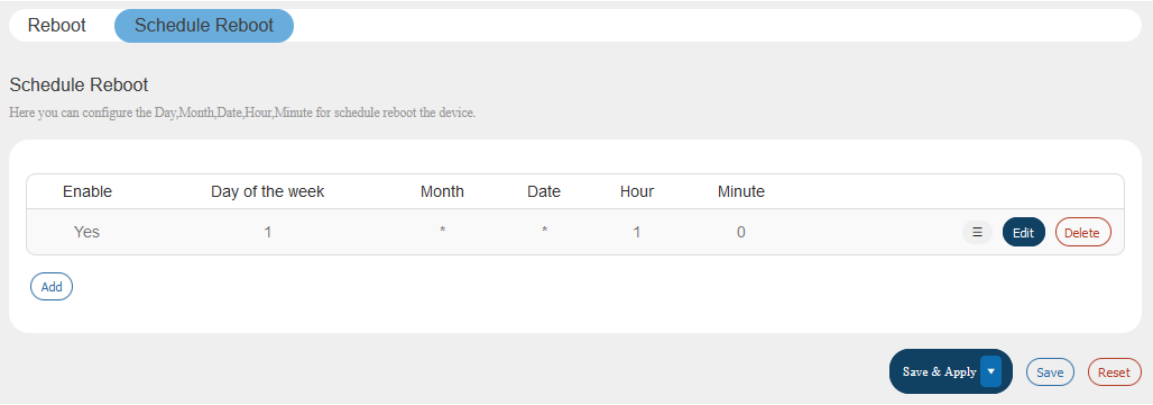


Figure 7.9-2: Schedule Reboot

8 VPN

VPN

A Virtual Private Network (VPN) is a tunnel, carrying traffic of a private network from one endpoint system to another over a public network such as the Internet. The traffic of private network so carried over public network does not know about the existence of the intermediate hops between the two endpoints. Similarly, the intermediate hops are also not aware that they are carrying the network packets that are traversing the tunnel. The tunnel may optionally compress and/or encrypt the data, providing enhanced performance and some measure of security.

Note

- ***The Lantronix E2xx routers support additional tunneling protocols. For L2TP, PPtP, or GRE protocol configuration, please see Section 8.1.2 Interface Protocols.***

8.1 IPSec (Internet Protocol Security)

VPN > IPSec

IP Security (IPSec) is a suite of protocols designed for cryptographically secure communication at the IP layer (layer 3). The router uses IPSec standard IPSec protocol to protect traffic. The identity of communicating users is checked with the user authentication based on Pre-shared keys or X.509 certificates.

The IPSec VPN instance can be started or stopped from the Web UI or by sending an SMS AT+VPN command. See *Figure 9.6-2* for command syntax.

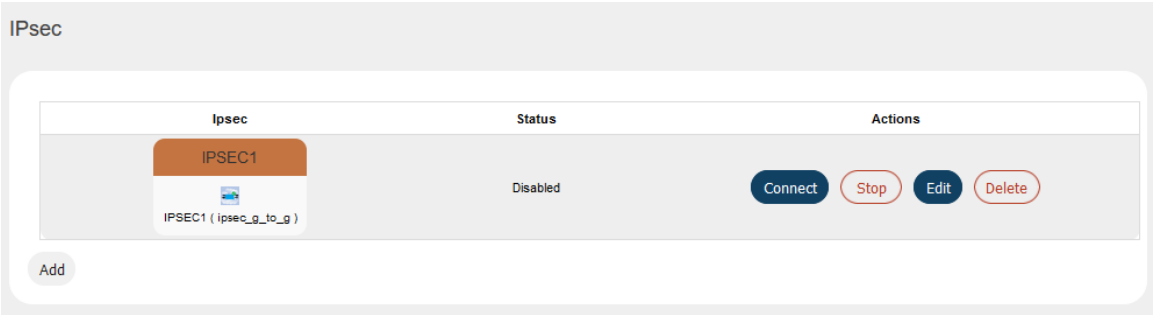


Figure 8.1-1: IPSec VPN Instance

IPSec is used for Gateway-to-Gateway VPN connection.

To create an IPSec interface instance:

1. Go to VPN > IPSec, and click **Add**.
2. Under Gateway to Gateway, click **Add**.

8.1.1 Gateway to Gateway

8.1.1.1 General Settings

VPN > IPSec > Edit > General settings

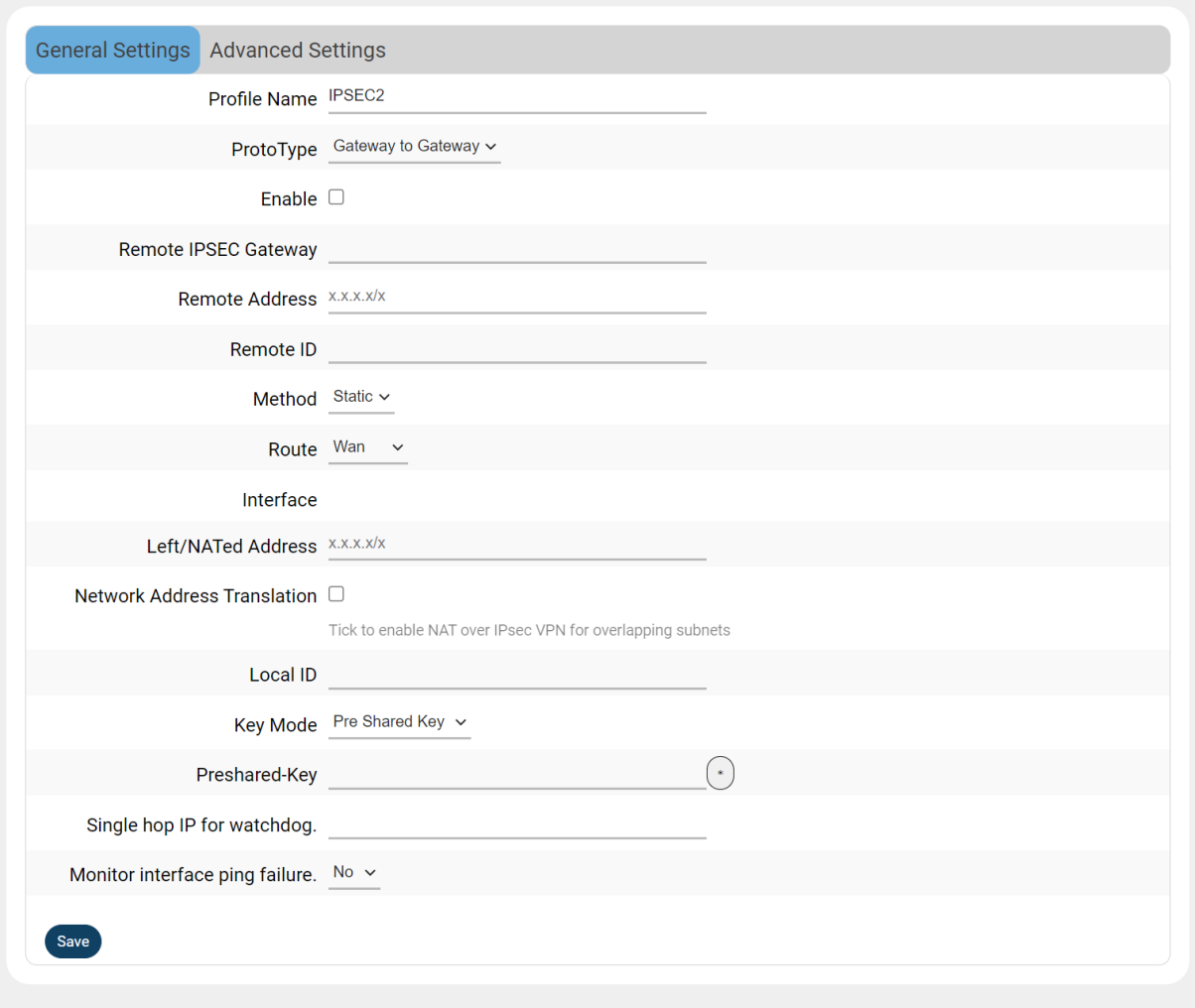


Figure 8.1-2: IPSec General Configuration

Parameters	Description
Profile Name	Enter the Profile Name to identify the Gateway–to-Gateway IPSec VPN connection.
Proto Type	Gateway to Gateway is the only available option.
Enable	Check to enable the connection.
Remote IPSec Gateway	Enter the remote WAN IP Address or domain name of the remote IPSec Gateway server.
Remote Address	Enter the remote LAN IP Address and subnet of the remote IPsec gateway server for use on the VPN connection.

Parameters	Description
Remote ID	Enter the ID of the remote network as configured on the remote IPSec gateway server.
Method	Select the interface used to establish the tunnel. *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	Available if Static is selected in Method field. Select the interface used to configure IPSec: *Wan* *Wifi* *Cellular*
Policy	Available if Auto is selected in Method field. Select the MWAN policy to use.
Interface	Displays the IP address of the interface used for the VPN connection.
Left/NATed Address	Local LAN IP address and subnet.
Network Addres Translation	Select to enable NAT over IPsec VPN for overlapping subnets.
Local Address	Enter the local network IP Address and subnet mask of the gateway for use on the VPN connection.
Local ID	Enter the ID of the local gateway as configured on the remote IPSEC gateway server. Note: On the remote server, it may be displayed as "remote ID."
Key Mode	Select the type of Key mode in use for VPN connection: *Pre shared Key* *X.509 certificate*
Preshared-Key	This field is available if Pre shared Key is selected in the Key Mode field. Enter the Pre shared key. The peer uses the key to authenticate each other from Internet Key Exchange.
Use Scep Client	This field is available if X.509 Certificate is selected as Key Mode. The Simple Certificate Enrollment Protocol (SCEP) is used to enroll the certificate from the SCEP server by providing server URL and password.
Certificate Name **Certificate Type**	These fields are available if Use SCEP client is selected. Select certificate enrolled in SCEP Client page as **Certificate Name**. Select **Certificate Type**: *pem* *der*

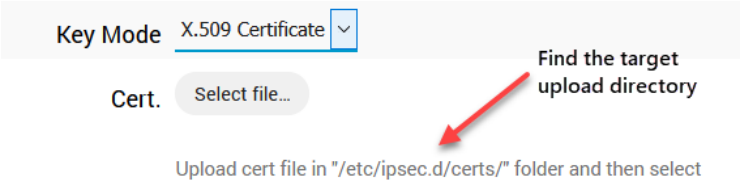
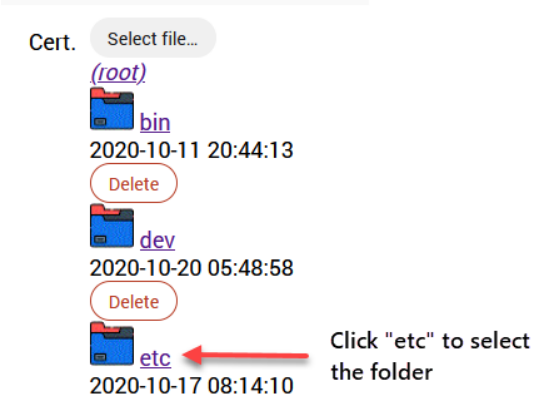
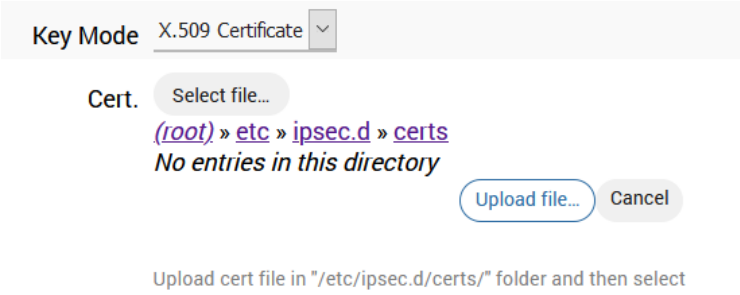
Parameters	Description
Cert. **Key** **CA Cert.**	These fields are available if Use SCEP client is not selected. The certificate files must be uploaded to the directory listed in the field.  For example, to upload the Cert. file in the "etc/ipsec.d/certs/" folder, click **Select file...** to open the root directory. Navigate to and click "etc" to open the "etc folder.  Navigate to the "ipsec.d" and "certs" folders in the same way. In the "certs" folder, click **Upload file...** and select the cert file to be uploaded.  Repeat this procedure with the **Key** and **CA Cert** files.
Single hop IP for watchdog	Enter the IP address to be used for monitoring purposes. The application will ping the IP defined here and will restart the device if the ping fails. This could be the LAN IP address of the IPSEC gateway 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.

Table 8.1-1: IPSec General Configuration

8.1.1.2 Advanced Settings

VPN > IPSec > Edit > Advanced settings

Advanced Settings contains IPSec policies defined in the remote IPSec gateway server.

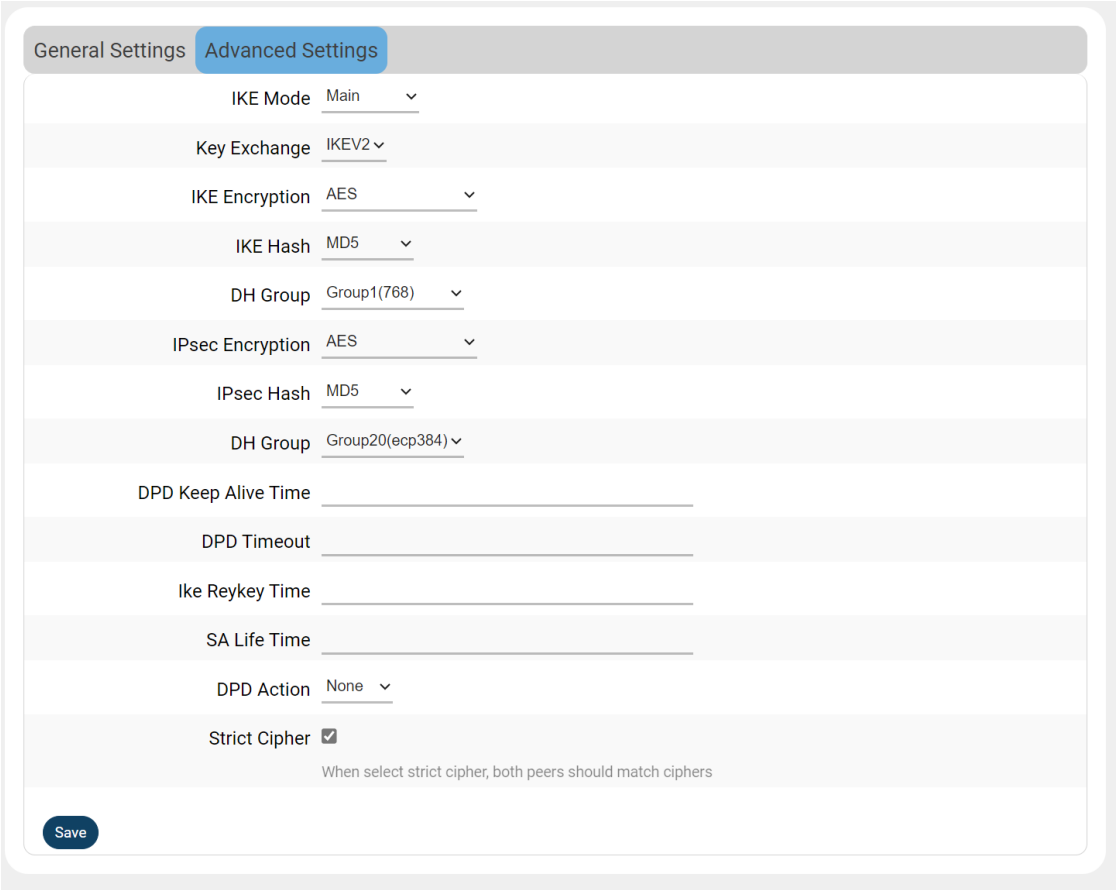


Figure 8.1-3: IPSec Advanced Configuration

Parameters	Description
IKE Mode	Select the mode that 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 of Internet Key Exchange is IKEV1.*
IKE Encryption	Select the cipher type to use for the internet key exchange (IKE): *Any* *AES*

Parameters	Description
	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 cipher type “Any” is the default IKE Encryption.
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: *Any* *MD5* *SHA1* *SHA2 256* *SHA2 384* *SHA2 512* The hash type “Any” is the default IKE hash.
IKE DH Group	Select the desired Diffie-Hellman group to use: *Group 1 (768)* *Group 2 (1024)* *Group 5 (1536)* *Group14 (2048)* *Group 15 (3072)* *Group 16 (4096)* *Group 19 (ecp256)* *Group 20 (ecp384)* Higher groups are more secure but also require longer to generate key. The group “Any” is selected by default.
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*

Parameters	Description
	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 cipher type "Any" is the default IPSec Encryption.
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: *Any* *MD5* *SHA1* *SHA2 256* *SHA2-384* *SHA2-512* The hash type "Any" is the default IPSec hash.
DH Group	Select the desired Diffie-Hellman group to use: *Group 1 (768)* *Group 2 (1024)* *Group 5 (1536)* *Group14 (2048)* *Group 15 (3072)* *Group 16 (4096)* *Group 19 (ecp256)* *Group 20 (ecp384)* Higher groups are more secure but also require longer to generate the key. The group "Any" is selected by default.
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.
DPD Action	Select the desired Dead Peer Detection action. This action must be taken when a dead Internet Key Exchange Peer is detected.
Strict Cipher	When enabled both routers should match ciphers.

Table 8.1-2: IPSec Advanced Configuration

8.2 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 User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) transports, multiplexing created SSL tunnels on a single TCP/UDP port. OpenVPN fully supports IPv6 as 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. These include IP addresses, routing commands, and a few connection options.

E210 and E220 series routers support OpenVPN client, server, and pass through.

8.2.1 OpenVPN Instances

VPN > OpenVPN

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 not only connect over available WAN but also switch between WANs when one WAN fails-over to another and also auto start on every reboot. The OpenVPN client must be enabled to be operational.

To create an OpenVPN instance, use the template based configuration or upload your own OVPN configuration file. The E210 and E220 routers come with pre-defined client templates and server templates.

Note

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

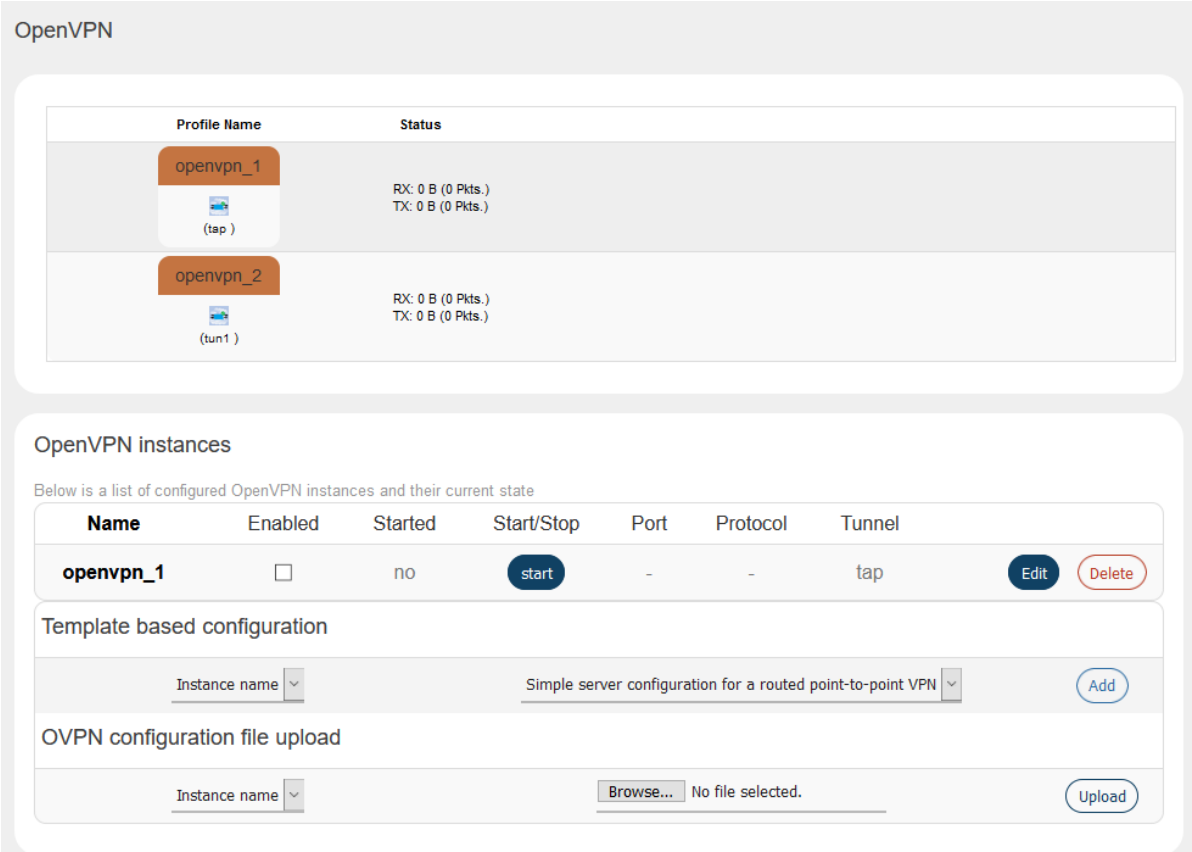


Figure 8.2-1: OpenVPN Service Configuration

Parameters	Description
OpenVPN instances	
Enabled	Click Enabled to allow restarting of OpenVPN in case the router is rebooted.
Started	Displays the status of OpenVPN instance, whether the instance is running or not. If the status is running, Yes is displayed along with Process ID (PID), else No.
Start/Stop	Click to start or stop the OpenVPN instance. ***Note:*** • ***The VPN instance can be started or stopped using SMS by sending an SMS AT+VPN command. See Figure 9.6-2 for command syntax.***
Port	Displays the port number. This port is for communication between the server (listening) and client.
Protocol	Displays the protocol used for communication. The available protocols are TCP and UDP. The default protocol is UDP.

Parameters	Description
Tunnel	Displays the type of networking interface to use for tunnel, via the TUN/TAP driver. Can be tun or tap. The default value is tun.
Template based configuration	Create a VPN instance for client or server based on templates. After adding the instance, you can edit its configuration. Instance name – select the OpenVPN instance Select template – select the client or server template to use as the basis for the instance. Click **Add** to add the instance. After successful upload, the new OpenVPN instance will appear under the OpenVPN Instances section. You can modify the OpenVPN configuration directly in the web interface
OVPN configuration file upload	Create a VPN instance using a configuration file. Select the OpenVPN instance name and then click **Browse** to locate the configuration file. Click **Upload** to upload the selected file and create the configuration for the OpenVPN instance.. After successful upload, the new OpenVPN instance will appear under the OpenVPN Instances section. Click Edit to view and modify the configuration file in an editor and to optionally, add the user and password authentication credentials for the OpenVPN server.

Table 8.2-1: OpenVPN Service Configuration

8.2.2 Edit OpenVPN Instance from Template

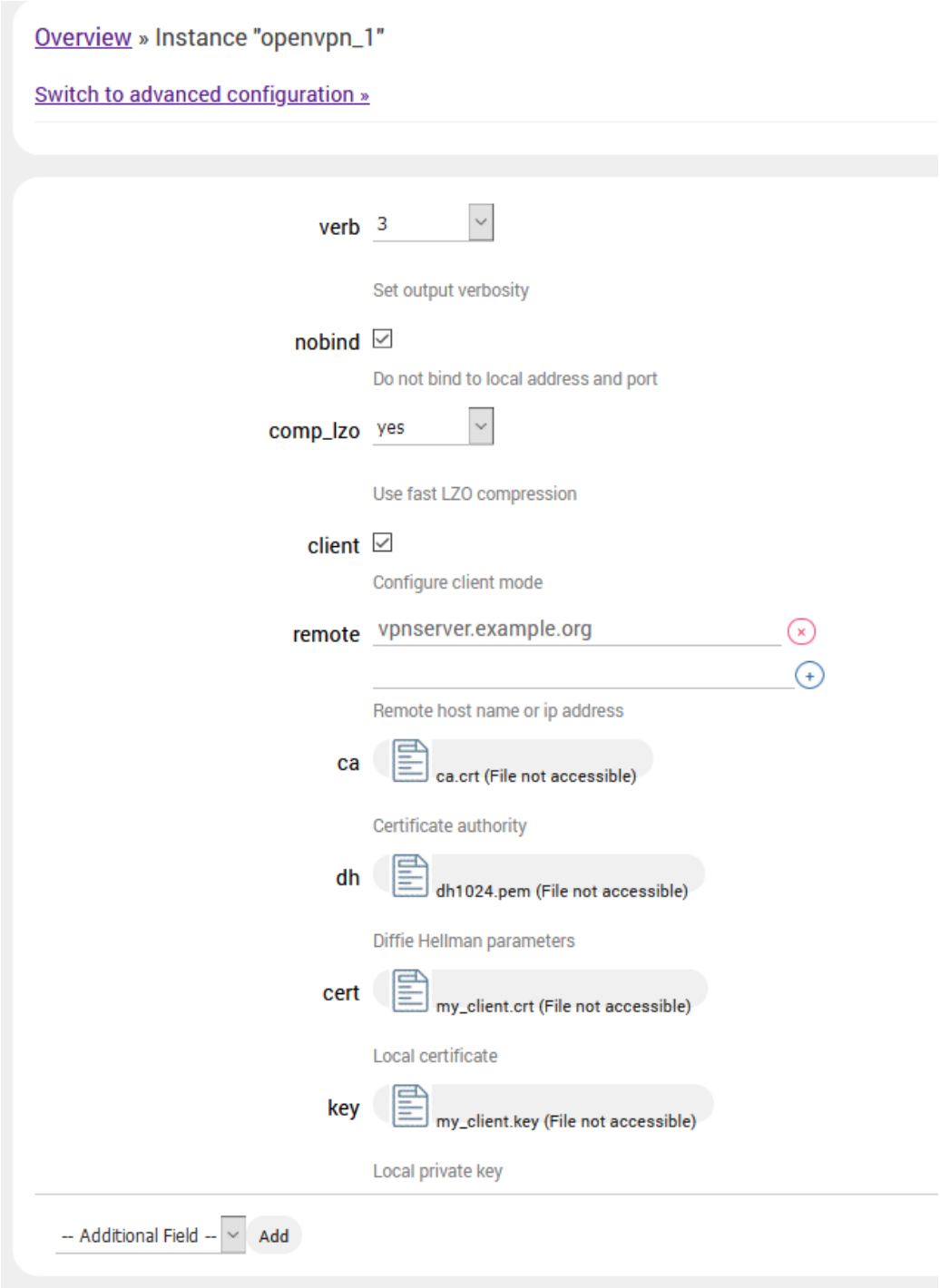
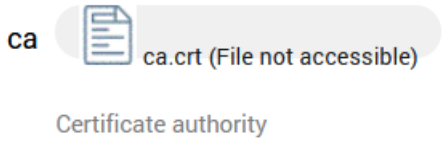
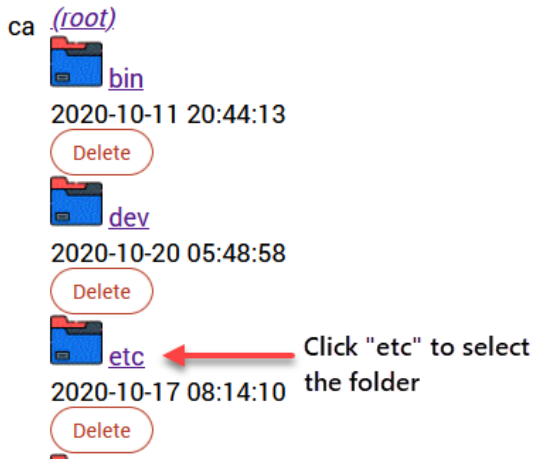


Figure 8.2-2: OpenVPN Service Configuration for Client Mode

Parameters	Description
OpenVPN Client	
Verb	Select the output verbosity level. Higher the verbosity, higher will be the internal log details.
nobind	If selected, do not bind to local address and port If you want to run multiple VPN clients on the same host, it's advisable to select "nobind".
comp_lzo	Select Yes to use fast lzo compression.
Client	Check to enable the OpenVPN client mode and disable the OpenVPN server mode.
remote	The IP address or host name of the remote server that the client will try to connect to. The client will attempt to connect in the order specified.
ca	Upload the Certificate authority file. The certificate and key files are uploaded to the /etc/openvpn/ folder on the router using the web interface. For example, to upload the CA cert file: Click the icon next to "ca" to display the directory structure of the router.  Navigate to and click "etc" to select the "etc" folder.  Next, navigate to and select the "openvpn" folder. Under /etc/openvpn/, click **Upload file...** and select the file to be uploaded.

Parameters	Description
	ca (root) » etc » openvpn No entries in this directory Upload file... Cancel Certificate authority Repeat this procedure with the other certificate and key files.
dh	Upload the Diffie Hellman parameters file. This parameter is required only in Server mode.
cert	Upload the local certificate file
key	Upload the local private key file
Additional Field – Add	Displays additional configuration parameters for the VPN instance or additional files that can be uploaded. Select the field and click Add.
OpenVPN Server	
verb	Verbosity level of the output. Higher verbosity level will produce more detailed internal log output.
server_bridge	Enter the IP Address and Subnet Mask for server mode
comp_lzo	Select Yes to use fast lzo compression.
keepalive	Server sends the keepalive packets to the client. Default is 10 60.
ca	Upload the Certificate authority file. The certificate and key files are uploaded to the /etc/openvpn/ folder on the router using the web interface. Please see the **ca** field in the OpenVPN Client section of this table for details describing the certificate upload procedure.
dh	Upload the Diffie Hellman parameters file
cert	Upload the local certificate file
key	Upload the local private key file
Additional Field – Add	Displays additional configuration parameters for the VPN instance or additional files that can be uploaded. Select the field and click Add.

Table 8.2-2: OpenVPN Service Configuration

8.2.3 Edit OpenVPN Instance from Configuration File

After uploading the OVPN configuration file, the new instance appears under OpenVPN Instances.

To edit the OpenVPN instance, click **Edit.** This displays the OVPN configuration file. You may also add the user and password authentication credentials for the OpenVPN server.

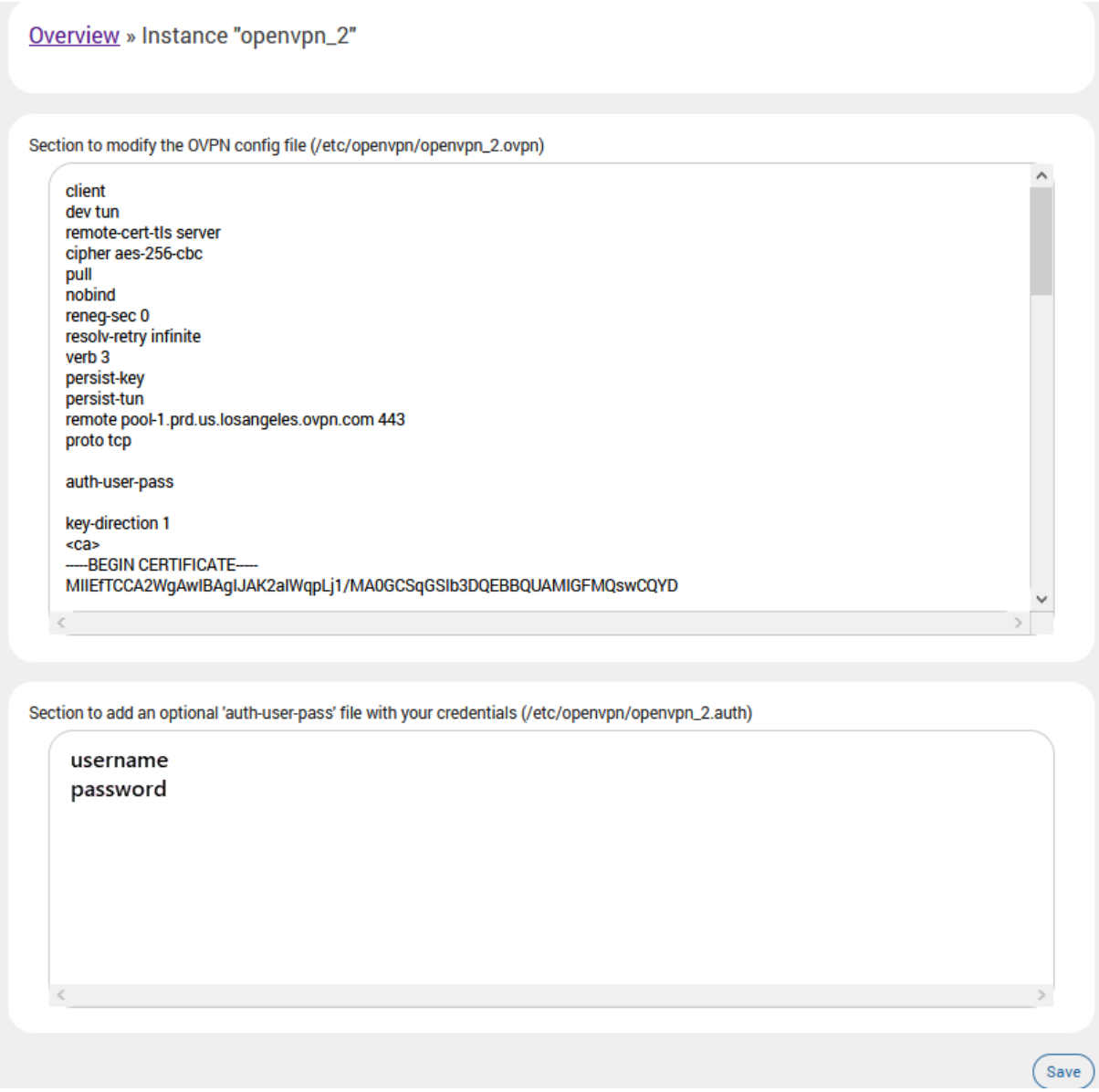


Figure 8.2-3: OpenVPN Edit Configuration File

9 Services

The E210 and E220 series routers are equipped with services complementing the routing features. These services include:

- Dynamic DNS
- Agents
- SD(HC)/MMC card
- SNMPD
- SNMPTRAPD
- Modbus Master
- Modbus Slave
- DNP3
- IEC 104 Master
- DNP3 to IEC104
- DOTA
- Page Selector
- SMS
- Reporting Agent
- GPS
- Keepalived
- Last Gasp
- Serial
- Service Actions
- Events
- GSM Update
- uHTTPd
- SCEP Client

9.1 Dynamic DNS

Services > Dynamic DNS

Dynamic DNS (Domain Name System) is 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.

This section lets you configure your DDNS service so that your router automatically updates your public IP to your DDNS provider. Before starting this configuration, you should already have registered a DNS name with a compatible DDNS service provider. Compatible DDNS providers are listed here: https://openwrt.org/docs/guide-user/services/ddns/client.

9.1.1 Basic Settings

Services > Dynamic DNS > Basic Settings

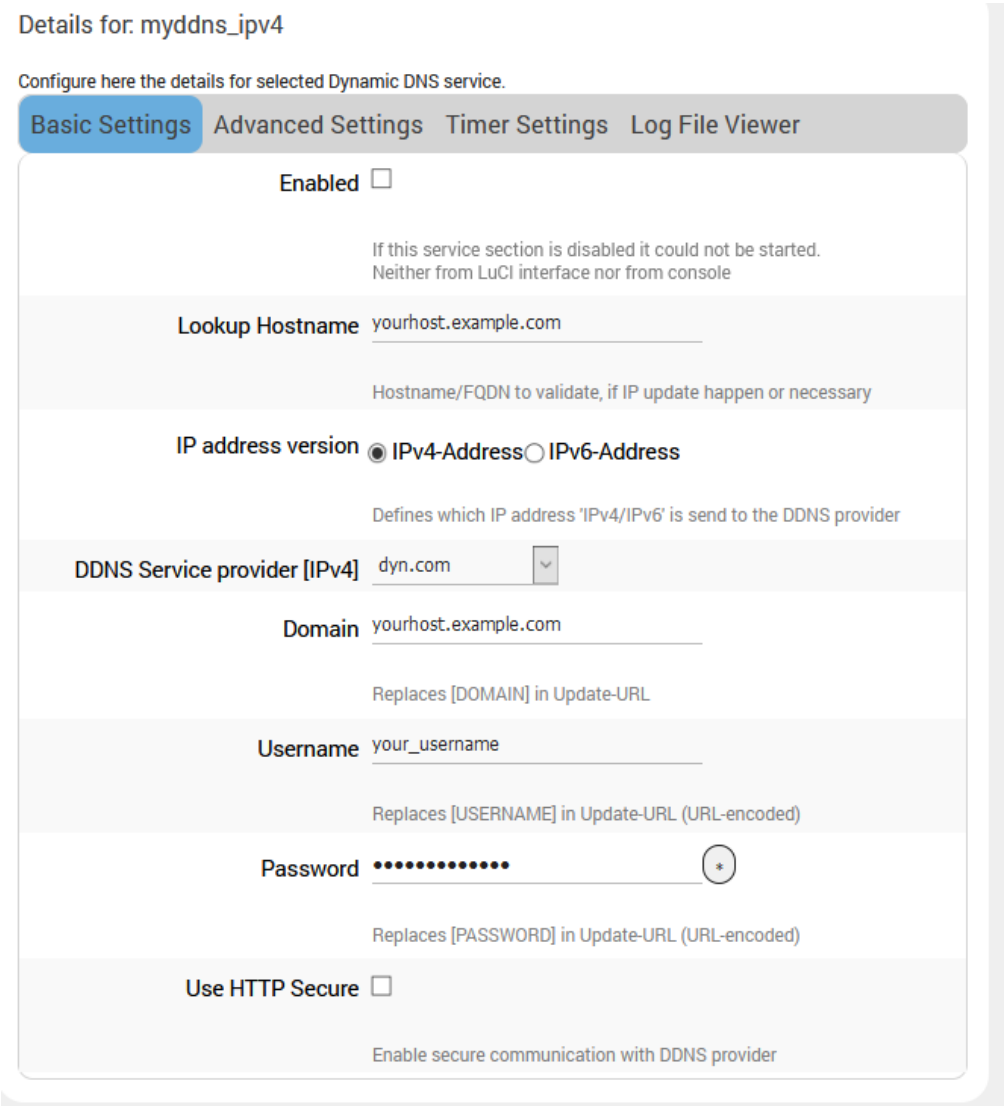


Figure 9.1-1: Dynamic DNS Basic Configuration

Parameters	Description
Enable	Select to enable Dynamic DNS. Clear to disable Dynamic DNS. Dynamic DNS allows the router 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.
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.

Table 9.1-1: Dynamic DNS Basic Configuration

9.1.2 Advanced Settings

Services > Dynamic DNS > Advanced Settings

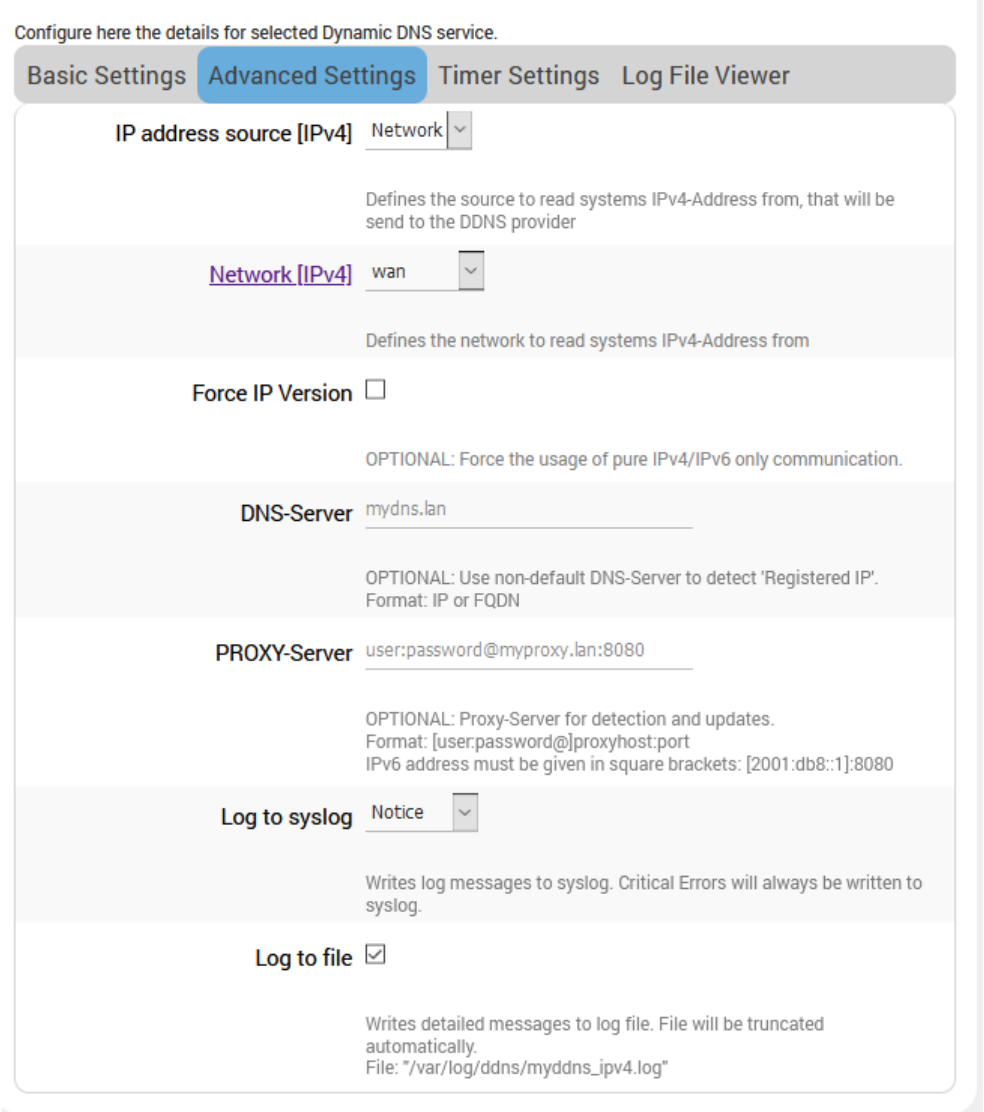


Figure 9.1-2: Dynamic DNS Advanced Configuration

Parameters	Description
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 name to read systems IPv4 address from.* Interface *Interface - Select the physical network interface from the available options*

Parameters	Description
	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* 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.
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 save the logs in Syslog server, or select No logging to save only critical errors. Available options: *No logging, Info, Notice, Warning, Error.* The default setting is Notice.
Log to file	Select to allow the detailed messages to be written to a log file.

Table 9.1-2: Dynamic DNS Advanced Configuration

9.1.3 Timer Settings

Services > Dynamic DNS > Timer Settings

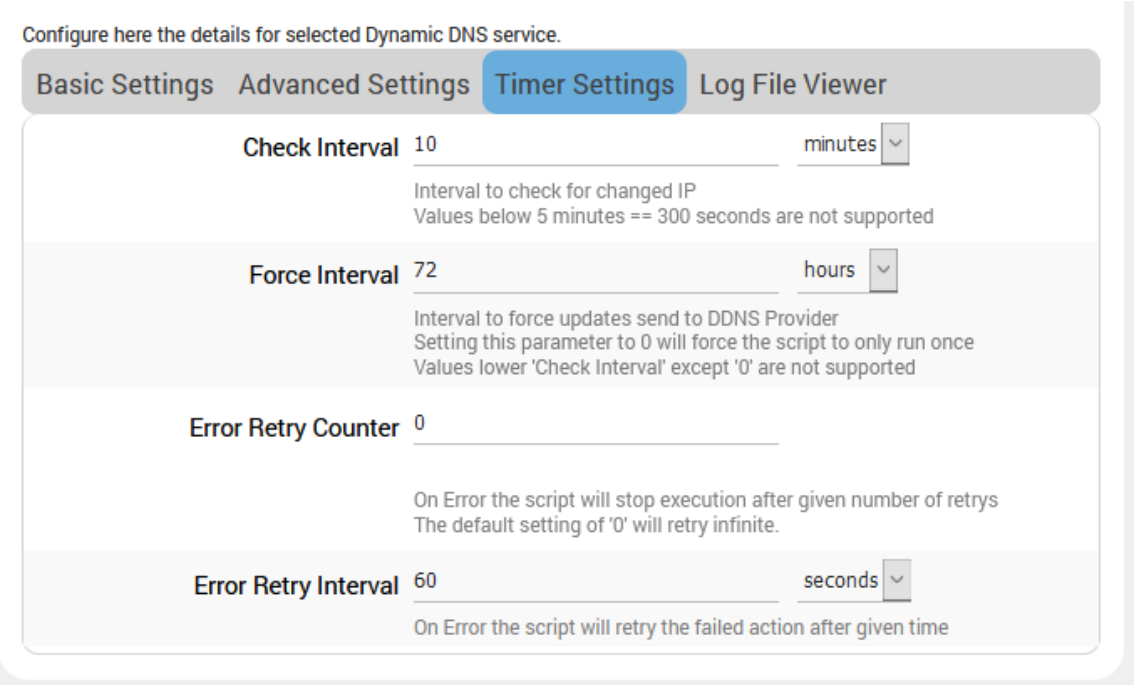


Figure 9.1-3: Dynamic DNS Timer Settings Configuration

Parameters	Description
Check Interval	Specify the time interval after which the DDNS server should check and update the IP address of the router. Default is 10 minutes.
Force Interval	Specify the time interval after which the DDNS server should check for and force update the IP address of your server even if it is not changed. The Force Interval should be greater than the Check Interval. Default 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	Enter the time interval after which the router must retry to update the obtained WN IP address with the DNS name or the host name. Default 60 seconds.

Table 9.1-3: Dynamic DNS Timer Settings Configuration

9.1.4 Log File Viewer

Services > Dynamic DNS > Log File Viewer

Click **Read/Reread log file** to display the Dynamic DNS service logs.

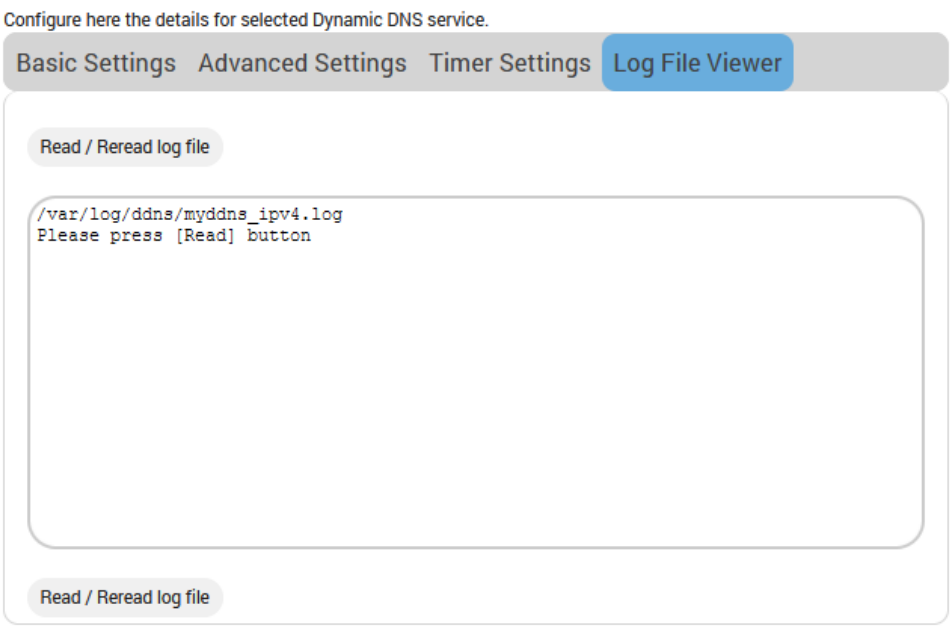


Figure 9.1-4: Dynamic DNS Log File Viewer

9.2 Agents

Services > Agents

Agents are customized applications loaded on the router that communicate with a specific device/data management platform.

By default, Lantronix Wireless Automation Server (MWAS) agent is loaded on the router, which facilitates bi-directional data communication between devices connected to the router (mainly using dynamic IP Address) and a centralized server through a kalkitech compatible MWAS server.

[Device/SCADA <=> Kalkitech(sever)] <=> [MWAS(agent) <=> Device/PLC]

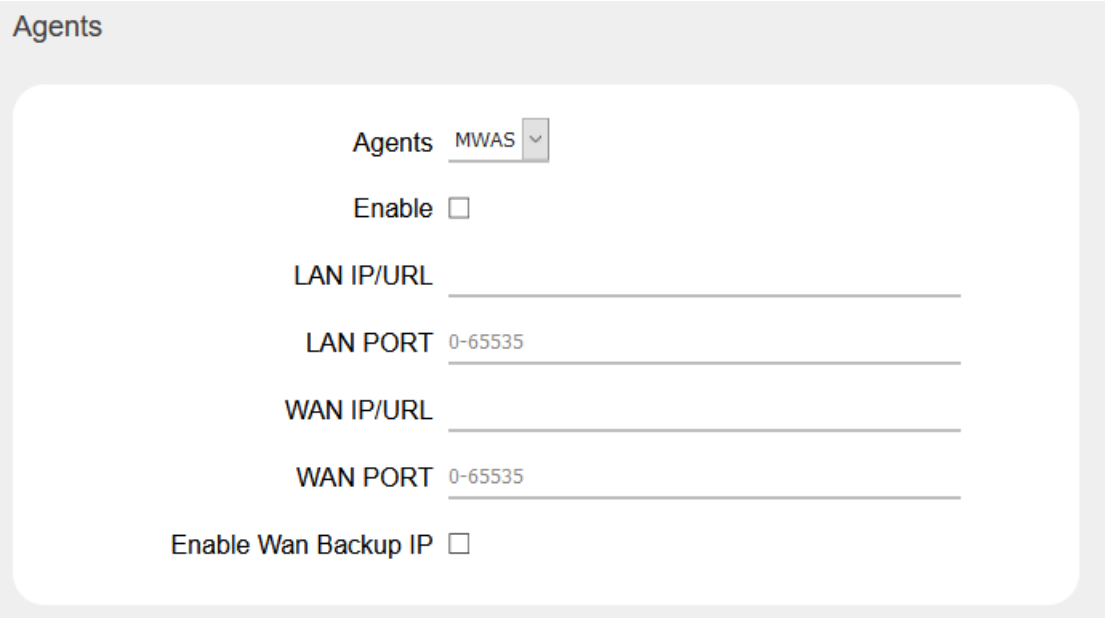


Figure 9.2-1: Agent Configuration

Parameters	Description
Agents	
Agents	Select the Agent from the dropdown list: *MWAS – Lantronix Wireless Acquisition System*
Enable	Click to enable the selected agent.
LAN IP/URL	Enter the IP Address of remote/field device.
LAN PORT	Enter the Port number of remote/field device.
WAN IP/URL	Enter the IP Address of the M2M Gateway.
WAN PORT	Enter the Port number of the M2M Gateway.
Enable WAN Backup IP	Click to enable the backup Gateway Server. *Backup WAN IP/URL - Enter the IP Address of backup M2M Gateway.* *Backup WAN Port - Enter the Port number of backup M2M*

Parameters	Description
	Gateway.

Table 9.2-1: Agent Configurations

9.3 SD(HC)/MMC Card

Services > SD(HC)/MMC Card

The E210 series devices provides one microSD-XC card slot that supports an SD(HC) card or MMC card for external file storage.

The SD(HC)/MMC card should be formatted before it is mounted in the E210 device.

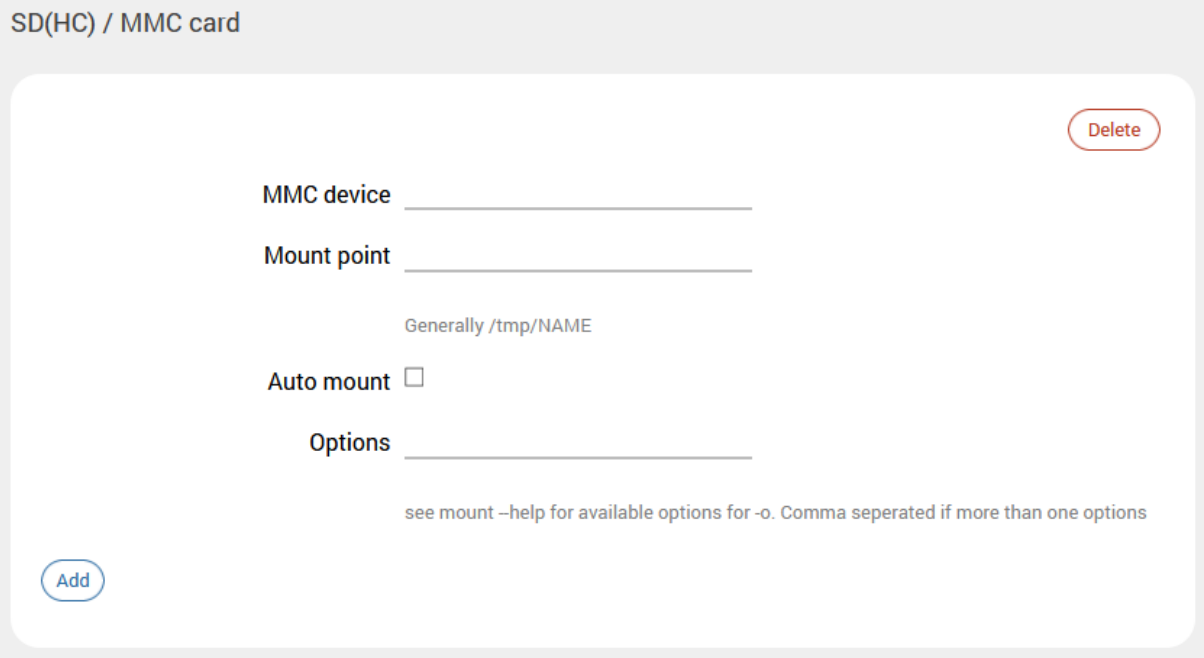


Figure 9.3-1: SD(HC)/MMC Card

Parameters	Description
MMC device	Enter the device name.
Mount point	Enter the mount point directory to the filesystem provided by the SD(HC)/MMC card, relative to the root directory.
Auto mount	Select to mount the device automatically when the router boots. If unselected, the device must be mounted manually.
Options	Enter Linux mount options to be run when the device is mounted.

Table 9.3-1: SD(HC)/MMC Card Configuration

9.4 SNMPD

Services > SNMPD

The E210 and E220 series gateways use 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), and write configuration on the device (snmpset).

The configuration of the SNMP agent and SNMP-TRAP application configuration files (mainly snmpd.conf and snmptrapd.conf) is 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.

9.4.1 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.

9.4.2 SNMP Versions

The E210 and E220 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.

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

Table 9.4-1: SNMP Security Models and Levels

9.4.3 SNMP Configuration

Services>SNMPD

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

SNMP Configuration consists of the following sections:

- General Settings
- View-based Access Control Model (VACM) Settings
- Trap Settings

9.4.3.1 SNMP General Settings

To view and configure SNMP **General Settings**, go to:

Services>SNMPD>General Settings

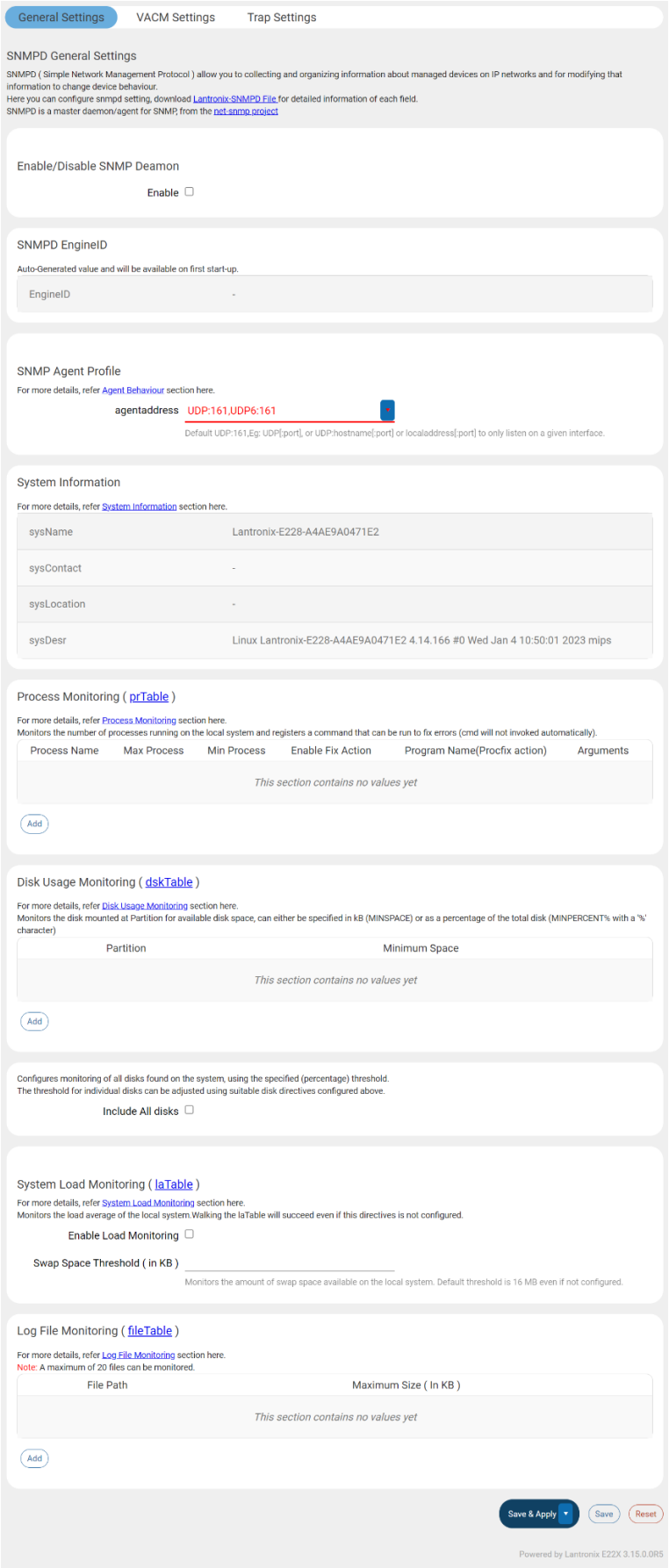


Figure 9.4-1: SNMP General Settings

The below table lists the configuration details for General Settings:

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-<Model Name>-<device MAC address* • *sysContact – default is root@localhost* • *sysLocation – default is Unknown* • *sysDesr – 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.

Parameters	Description
	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 are supported.
Disk Usage Monitorng	
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.

Parameters	Description
5 - Minute Max. Load	The five-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. 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.
Maximum Size	Maximum file size in KB before errors are triggered.

Table 9.4-2: SNMP General Settings Configuration

9.4.3.2 SNMP View-based Access Control Model (VACM) Settings

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.

To view and configure VACM Settings, go to:

Services>SNMPD>VACM Settings

General Settings | VACM Settings | Trap Settings

SNMPD v1/v2c/usm Configuration

For more details, refer VACM Configuration and Active Monitoring section here.

Com2Sec Configuration

Security Name	Source	Community
This section contains no values yet		

Add

Group Configuration

Group Name	Version	Security Name
This section contains no values yet		

Add

Access Configuration

Group Name	Context	Version	Level	Match	Read	Write	Notify
This section contains no values yet							

Add

View

Defines a named "view" - a subset of the overall OID tree.
Note: Mask - Take care while configuring Mask directive in the table. It is hex octets (optionally separated by '.' or ':')

View Name	Type	OID	Mask (Optional)
This section contains no values yet			

Add

Engine ID Configuration

These parameters are generic to all the forms of SNMPv3. For more details, refer SNMPv3 Configuration section here.
WARNING: Do not configure this unless you know what you are doing.

Enable ☐

SNMPv3 with (USM)

For more details, refer SNMPv3 with the User-based Security Model (USM) section here.
To use the USM based SNMPv3-specific users, you'll need to create them using following directives.
This section contains no values yet

Add

Save & Apply | Save | Reset

Powered by Lantronix E22X 3.15.0.0R5

Figure 9.4-2: SNMP VACM Settings

The below table lists the configuration details for 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 9.4-1 on page 96) 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.***

Parameters	Description
	• ***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.
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.
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.*

Parameters	Description
	• *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	
View	Creates a named view, which determines what part of the MIB the access control is applied to.

Parameters	Description
	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 sub identifiers in the view OID to match against. Recommended to ignore this field.
Engine ID Configuration	
Engine ID Configuration	Engine ID 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 engine ID. For this reason, it is recommended that you use the default values unless you know what you are doing.
Enable	Enables the engine ID.
engineID	Specifies that the engine ID 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 engine ID should use the following interface when determining the MAC address. Only required if engine ID Type 3 is specified. Default: eth0
SNMPv3 with (USM) Configuration	
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*

Parameters	Description
	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 9.4-3: SNMP VACM Settings Configuration

9.4.3.3 SNMP Trap Settings

The SNMP agent is configured to generate Trap Notifications.

To view and configure SNMPD Trap Sender settings, go to:

Services>SNMPD>Trap Settings

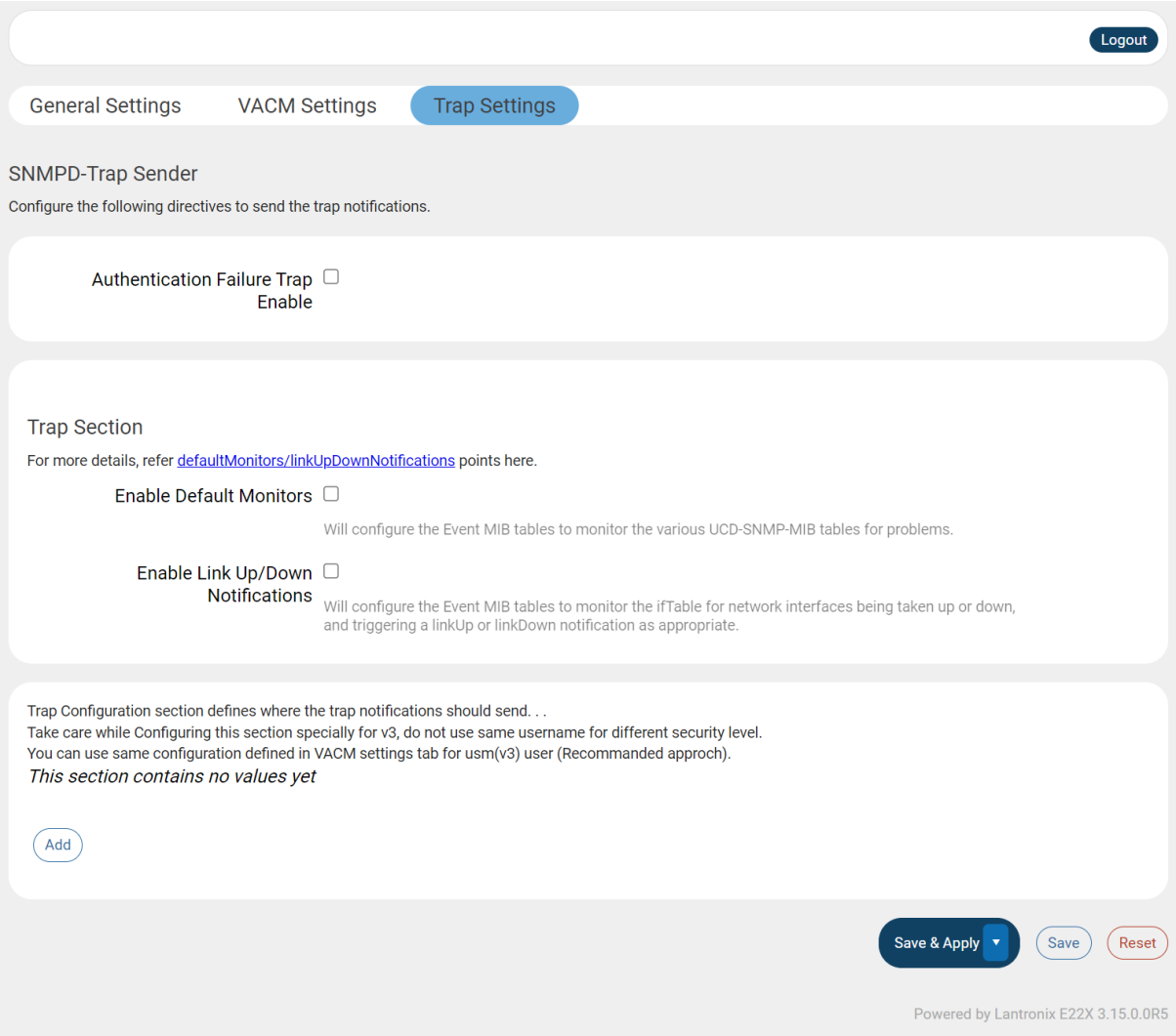


Figure 9.4-3: SNMP Trap Settings

The below table lists the configuration details for Trap Settings:

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 start-up 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.

Parameters	Description
	• *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.*
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.

Table 9.4-4: SNMP Trap Settings Configuration

9.5 SNMPTRAPD

Services > SNMPTRAPD

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.

9.5.1 SNMP-TRAP Configuration

To view and configure SNMP-TRAP settings, go to:

Services > SNMPTRAPD > General Settings

General Settings

SNMP-TRAP Receiver

SNMPTRAPD is an SNMP application that receives and logs SNMP TRAP and INFORM messages.
Here you can configure snmptrapd setting, download Lantronix-SNMPTRAPD File for detailed information of each field.

GENERAL

Enable ☐

Ignore Authorization Failure ☐

Instructs the receiver to ignore authenticationFailure traps.

SNMP TRAP Deamon Configuration

Specify the authorized user to accept the notifications.
This section contains no values yet

Add

Logging Configuration

For more details, refer Logging section here.

Log ☐

log the details of the notification either in a specified file, or via syslog.

Format1 %.4y-%.2m-%.2l %.2h:%.2j:%.2k %B [%b]: %N\n\t%W

specify the format used to display SNMPv1 TRAPs & Refer for FORMAT SPECIFICATIONS

Format2 %.4y-%.2m-%.2l %.2h:%.2j:%.2k %B [%b]: %N\n\t%W

specify the format used to display SNMPv2c and v3 TRAPs & Refer for FORMAT SPECIFICATIONS

Notifications Handling

For more details, refer Notifications Processing section here.

Execute ☐

pass the details of the trap to a specified handler program

Net ☐

forward the trap to another notification receiver.
Note: Do not use this directive for snmp v3 for any security level.

Save & Apply Save Reset

Powered by Lantronix E22X 3.15.0.0R5

Figure 9.5-1: SNMPTRAPD General Settings

The below table lists the configuration details for SNMPTRAPD General Settings:

Parameters	Description
General	
Enable	Enables the SNMPRAP application
Ignore Authorization Failure	Select to ignore authentication failure traps.
SNMP-TRAP Daemon Configiration	
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.
Username	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.
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 Configuartion	
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.

Parameters	Description
	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.

Table 9.5-1: SNMPD General Settings Configuration

9.6 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 the 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.

9.6.1 Serial Transmission Mode

The E210 and E220 series gateway can be configured to communicate on Modbus networks using RTU. Modbus RTU can use the available serial 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.

9.6.2 Ethernet Transmission Mode

The E210 and E220 series gateway can be set up to communicate on Modbus networks using TCP/IP. The Modbus Protocol header is added to the start of each Modbus message and the slave address and CRC are removed. Modbus TCP uses TCP port 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.

The below table shows the structure of the Modbus application protocol header.

9.6.3 Modbus Master Configuration

Services > Modbus Master > Configuration

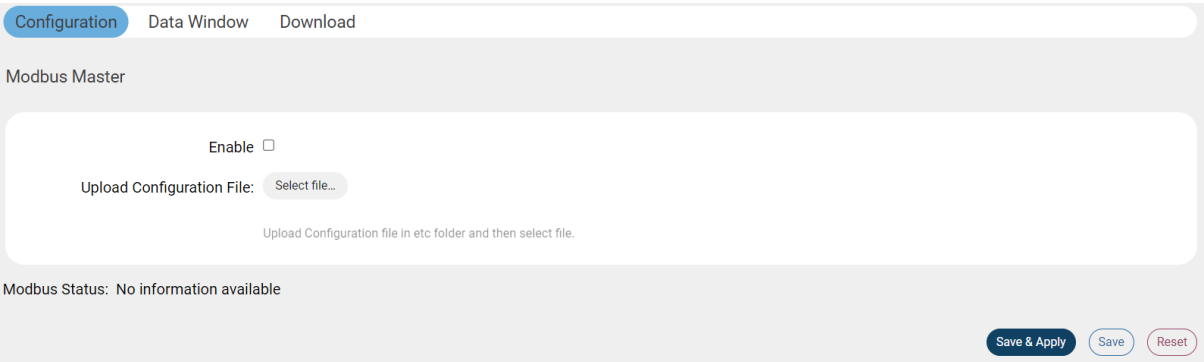


Figure 9.6-1: Modbus Master Configuration

This page lets you enable or disable the Modbus master, configure the Modbus master settings, 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.

The Modbus configuration settings are contained in a Modbus configuration file, which is a CSV formatted file that you can generate using the Modbus Configuration Utility at: https://modbus.d2sphere.com. The following configuration sections can be configured: the target server where the data will be reported, up to six (6) polling groups, up to five (5) upload groups, and Modbus logger details.

Parameters	Description
Enable	Click to enable Modbus Master on the selected interface.
Upload Configuration File	Upload the Modbus configuration file (CSV formatted file). This file contains all the configuration for the Modbus server. Generate the Modbus configuration file using https://modbus.d2sphere.com/. Click **Select file**... and then click **Upload file** to upload the configuration file from the local drive to the /etc folder on the gateway.

Table 9.6-1: Modbus Master Configuration Settings

Click **Save & Apply** after configuring the above settings.

9.6.4 Data Window

Services > Modbus Master > Data Window

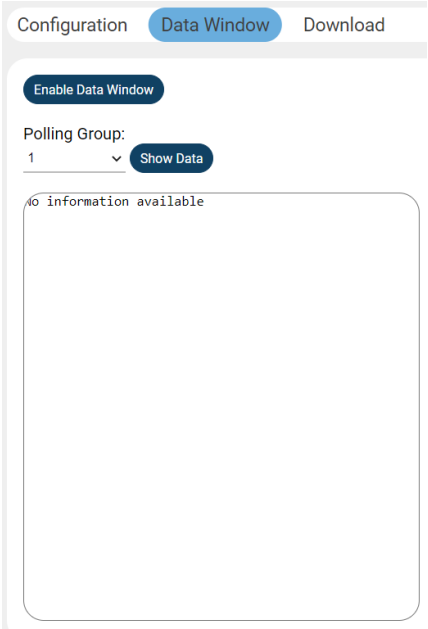


Figure 9.6-2: Modbus Master Data Window

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

9.6.5 Download

Services > Modbus Master > Download

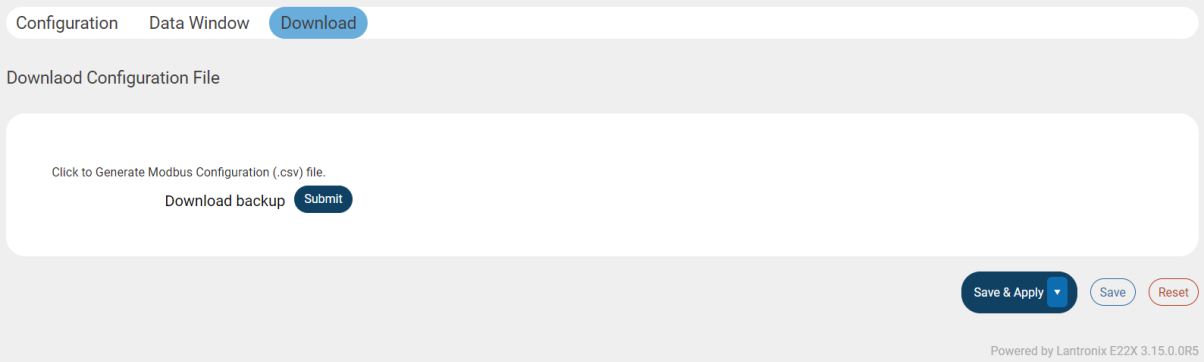


Figure 9.6-3: Modbus Master Download

This page allows you to download the Modbus configuration file in CSV format.

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.

9.7 Modbus Slave

Service>Modbus Slave

The Modbus protocol exchanges information using a request-reply mechanism between a master (client) and a slave (server). The master-slave principle is a model for a communication protocol in which one device (the master) controls one or more other devices (the slaves). The slaves can only send replies to the master.

The master initiates all communication transactions. Each slave has a unique id, responding to the master only when addressed by the master.

9.7.1 Modbus Slave Configuartion

Go to **Services>Modbus Slave**

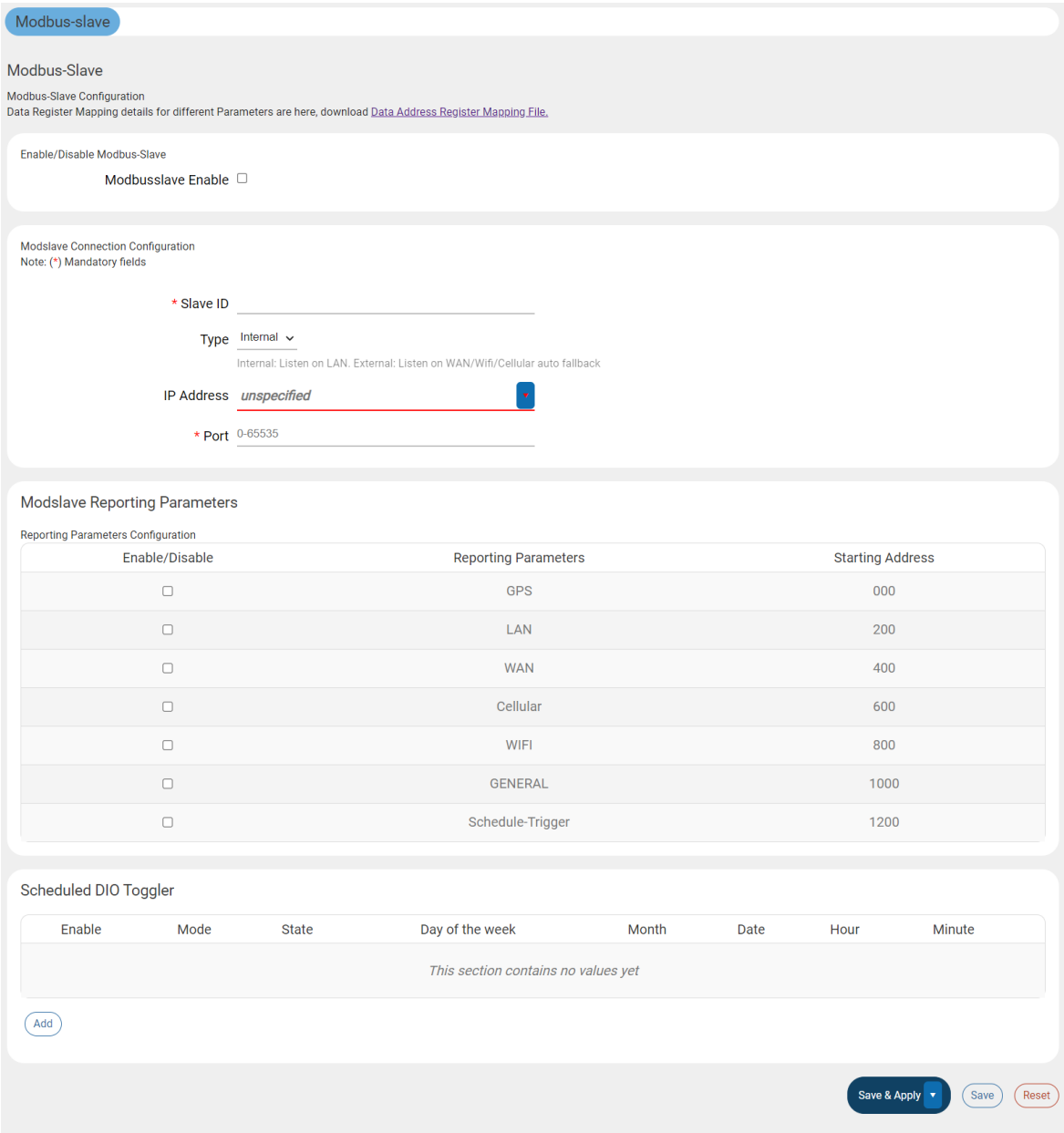


Figure 9.7-1: Modbus Slave Setings

Click **Data Address Register Mapping File** to display the register mapping addresses and description for the different parameters.

The various parameters reported by the Modslave are listed in the table below.

Parameters	Description
Enable/Disable Modbus Slave	
Modbusslave Enable	Select Enable to enable Modbusslave
Modslave Connection Configuration	
Slave ID	Each slave in a network is assigned a unique unit address from 1 to 247. When the master requests data, the first byte it sends is the Slave address. This way each slave knows after the first byte whether to acknowledge or ignore the message.
Type	Select the interface that the server listens on. Internal – listens on LAN. Select IP and enter port. External – listens on WAN/WiFi/Cellular with automatic fallback.
IP Address	IP address of the device
Port	Port number used
Modslave Reporting Parameters	
GPS	Select Enable for the parameter to enable it.
LAN	
WAN	
Cellular	
WIFI	
GENERAL	
Schedule-Trigger	
Schedule DIO Toggler	
Click **Add** to view and select the parameter options.	
Enable	Select Enable to enable DIO toggler
Mode	Select Mode *Digital IO 1* *Digital IO 2*
State	Select State *Low* *High*
Day of the week	Select Day of the week
Month	Select Month
Date	Select Date

Parameters	Description
Hour	Select Hour
Minute	Select Minute
Click Save & Apply	

Table 9.7-1: Modbus Slave Configuaration

9.8 DNP3

Services > DNP3

The E210 and E220 series gateway acts as a DNP3 outstation. DNP3 is an open standard communication protocol used in many SCADA environments. DNP3 facilitates Modbus RTU to DNP3 conversion which enables DNP3 master (DNP3 SCADA) to connect and monitor The Modbus RTU device.

9.8.1 Configuring DNP3 Outstation for Modbus RTU to DNP3 conversion

To view and configure DNP3 Outsation, go to:

Services > DNP3 > Outstation

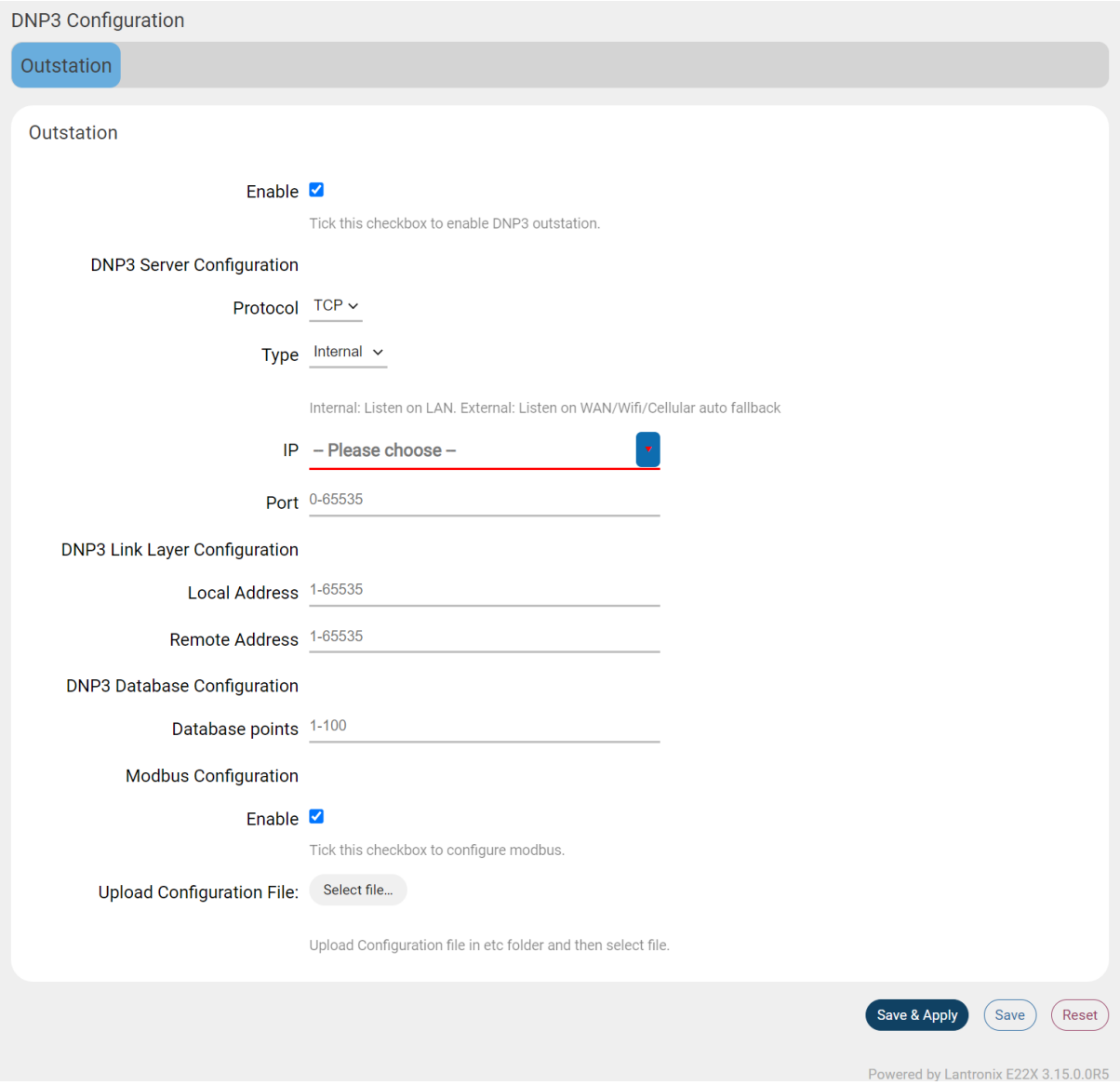


Figure 9.8-1: DNP3 Outstation Settings

Parameters	Description
Outstation	
Enable	Select to enable DNP3
DNP3 Server Configuartion	
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
DNP3 Link Layer Configuartion	
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
DNP3 Database Configuration	
Database points	
Modbus Configuartion	
Enable	Select Enable to add Modbus configuration.
Upload Configuration File	Upload and then select the Modbus Master configuration file in CSV format.

Table 9.8-1: DNP3 Outstation Settings Configuration

9.8.2 Modbus Master configuration file for DNP3 Outstation

To configure the Modbus Master configuration file:

1. Go to Services> Modbus Master>Configuration
2. Generate the Modbus Master configuration file using the Modbus Configuration Utility at: https://modbus.d2sphere.com. The sections that can be configured by the tool are: the target server where the data will be reported, up to six (6) polling groups, up to five (5) upload groups, and Modbus logger details. The configuration file is generated as a CSV file.
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, Sample CSV with DNP3 Parameters
4. Save the configuration file in CSV format.

9.8.3 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,,,,,,,,,,,
```

9.8.4 DOTA

Services > DOTA

DOTA (download over the air) will allow you to remotely update your firmware using the Lantronix server or your custom server.

9.8.5 Lantronix Server

Services > Dota > Lantronix Server

This page allows you to check for available firmware and to upgrade or downgrade the firmware from the Lantronix D2Sphere server.

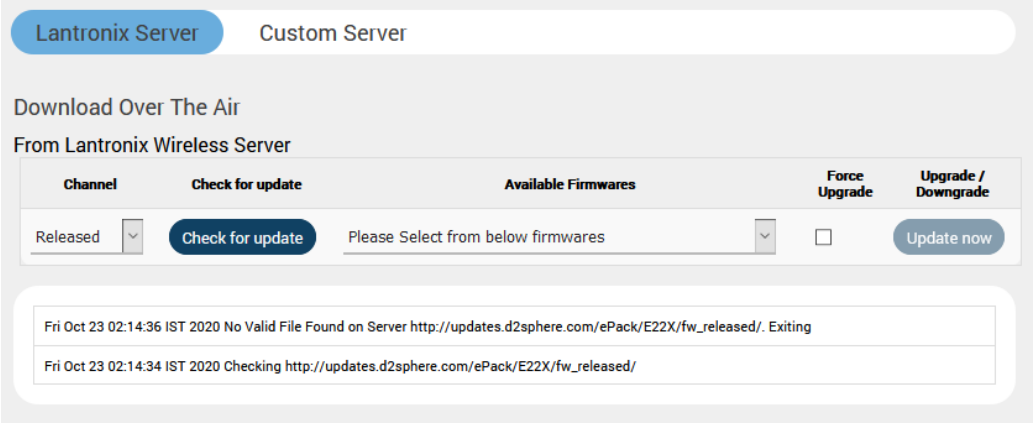


Figure 9.8-1. Download over the Air (DOTA) using Lantronix server

Parameters	Description
Channel	Select the D2Sphere 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 on D2Sphere.
Available Firmware	Displays a list of firmware for the router that is available on the server. Select the firmware from this list and click **Update now** to upgrade or downgrade on the router.
Force Upgrade	Check this box for forceful upgrade or downgrade of the router's firmware version.
Upgrade/Downgrade	Click **Update now** to download the firmware selected in the Available Firmware list.

Table 9.8-1: DOTA for Lantronix Server

9.8.6 Custom Server

Services > Dota > Custom Server

This page allows you to update the router firmware using a custom download over- the-air (DOTA) server.

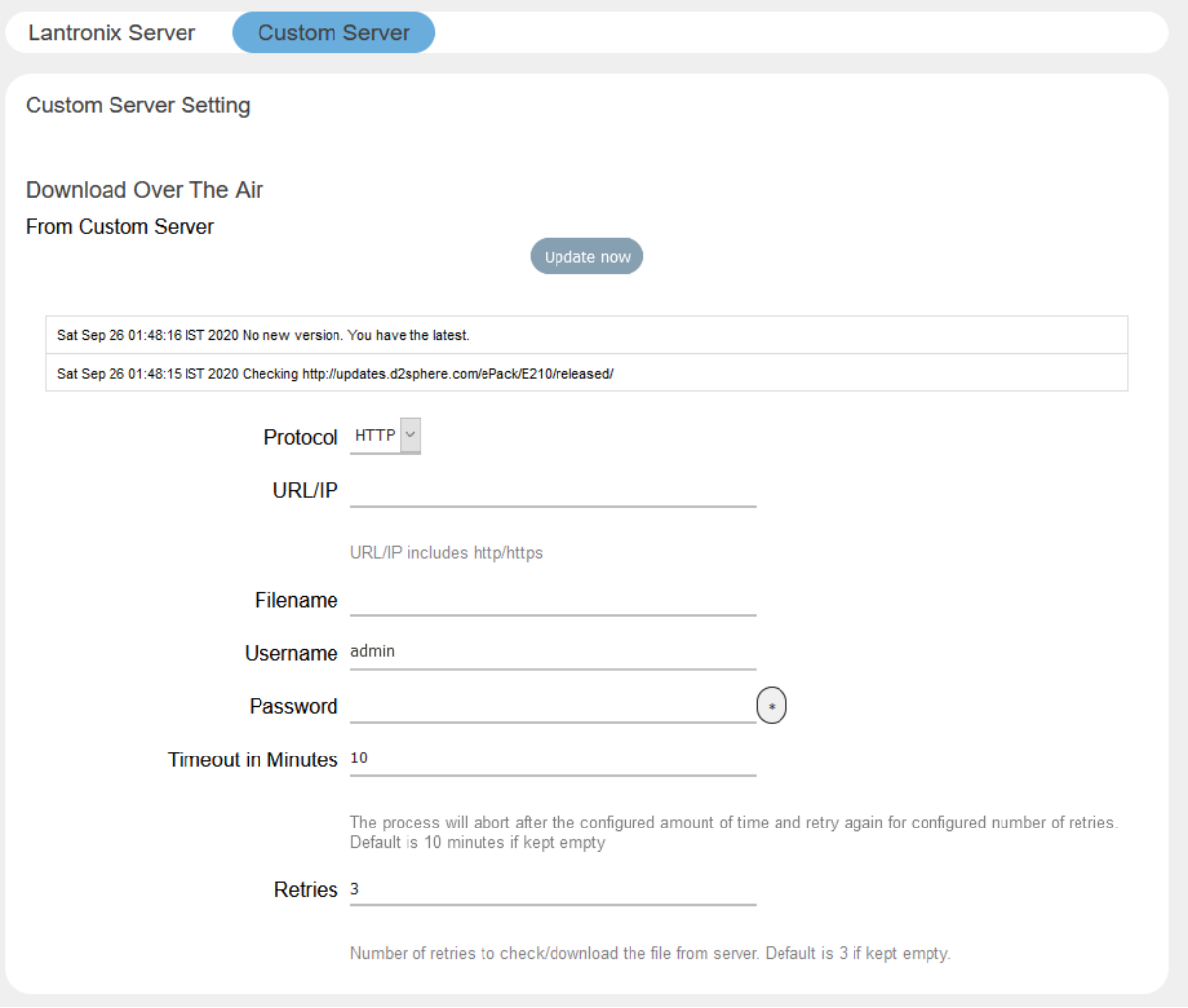


Figure 9.8-2: DOTA Custom Server Settings

Parameters	Description
Update now	After setting the parameters on the Custom Server page, click **Update now** to download the firmware pointed to by the URL and the filename below.
Custom Server Settings	
If the custom server is not configured, DOTA service will configure the D2Sphere server.	
Protocol	Select HTTP or HTTPS as the protocol of the custom server.
URL/IP	Enter the URL or the IP address of the custom DOTA server. The entry must include http/https.

Parameters	Description
Filename	Enter the name of the router firmware file to be accessed for the update.
Username	Enter the server login username.
Password	Enter the server login password.
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.

Table 9.8-2: DOTA Custom Server Configuration

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. See Figure 9.9-2 for syntax details.***

9.9 IEC 104 Multi-master

Services>IEC 104 Master

The E210 and E220 series routers support the IEC104 protocol to monitor remote devices.

9.9.1 IEC 104 Multi-master Configuartion

Got to **Services>IEC 104 Master**

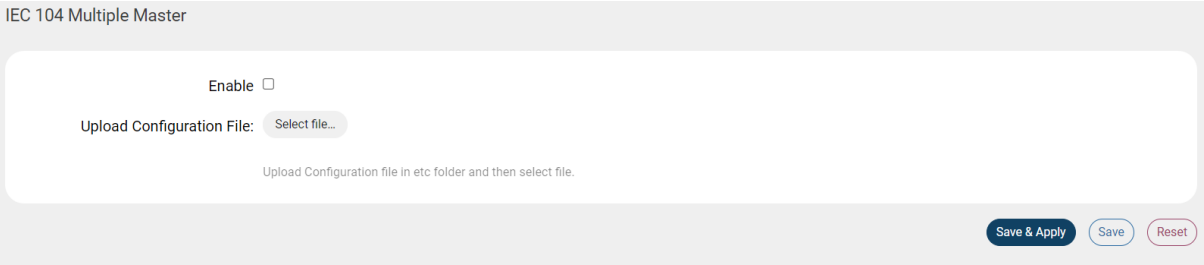


Figure 9.9-1: IEC 104 Multi-master settings

Parameters	Description
Enable	Click to enable IEC104 Multi-master on the selected interface.
Upload Configuration File	Upload the IEC 104 Multi-master configuration file (CSV formatted file). This file contains all the configuration for the IEC 104 Multi-master server. Click **Select file**... and then click **Upload file** to upload the configuration file from the local drive to the /etc folder on the gateway.

Table 9.9-1: IEC 104 Multi-master configuration

9.10 DNP3 to IEC104

Services>DNP3 to IEC104

The E210 and E220 series routers support protocol conversion from DNP3 to IEC104

9.10.1 DNP3 To IEC104 Configuration

Go to **Services>DNP3 to IEC104**

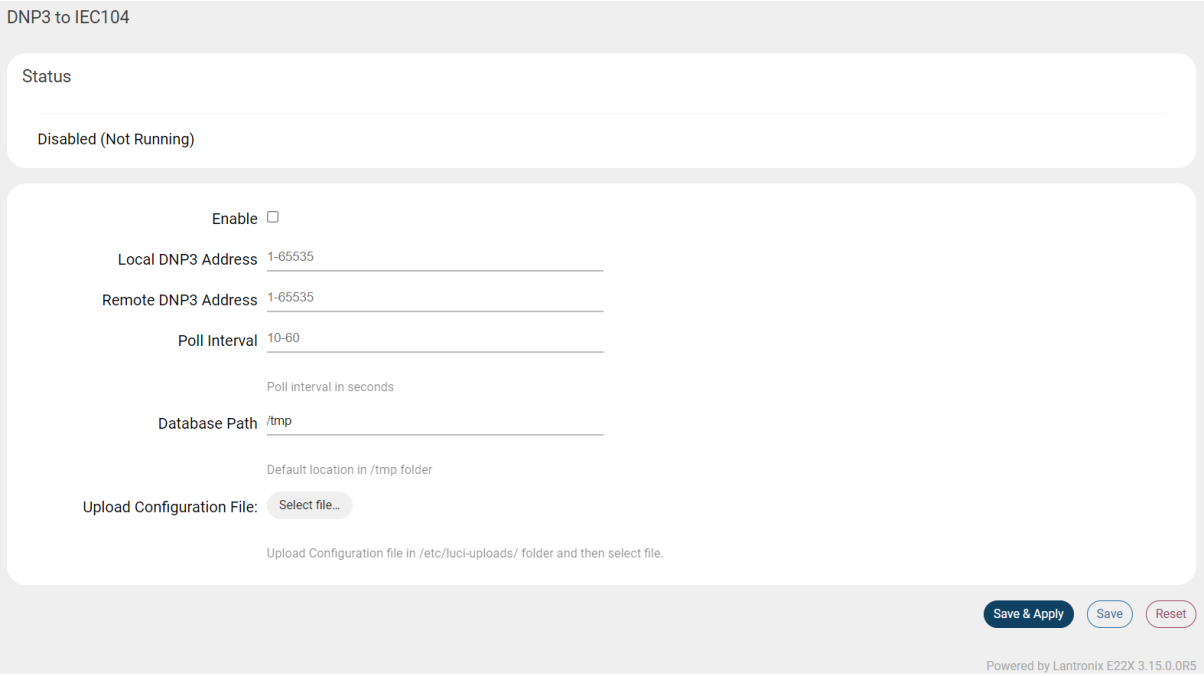


Figure 9.10-1: DNP3 to IEC104 Settings

Parameters	Description
Enable	Click to enable DNP3 to IEC104
Local DNP3 Address	DNP3 master address
Remote DNP3 Address	Remote DNP3 outstation address
Poll Interval	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.
Database Path	Location on the device.
Upload Configuration File	Upload the IEC 104 Master configuration file (CSV formatted file). This file contains all the configuration for the IEC 104 Master server. Click **Select file**... and then click **Upload file** to upload the configuration file from the local drive to the /etc folder on the gateway.

Table 9.10-1: DNP3 to IEC104 Configuration

9.11 Page Selector

This page allows a root user to hide certain pages from the admin user view.

9.12 SMS

Services > SMS

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

9.12.1 SMS Configuration

Services > SMS > SMS Configuration

You can configure up to four administrator mobile numbers to receive SMS messages containing router 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

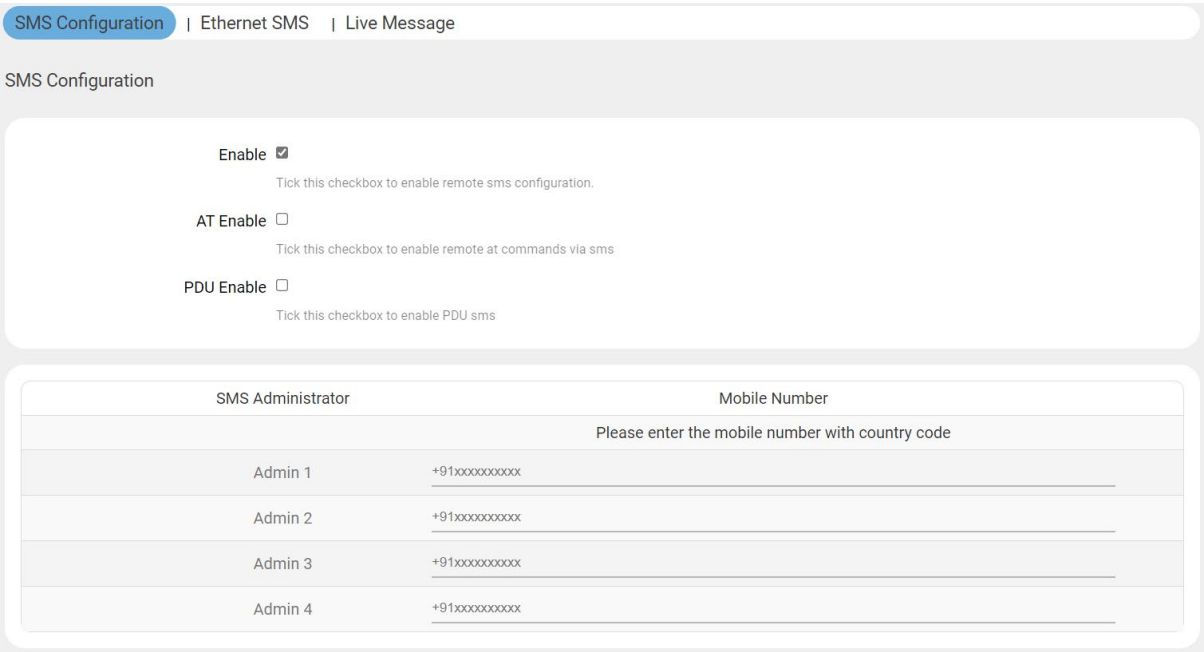


Figure 9.12-1: SMS Configuration

Parameters	Description
SMS Configuration	
Enable	Enable remote SMS configuration.
AT Enable	Enable remote AT commands using SMS
PDU Enable	Enable PDU to support long SMS messages and to send Flash SMS messages. Now SMS Text and PDU mode support 16-bit data

Parameters	Description
SMS Administrator	Displays up to four Administrators configured to receive the diagnostics information of the router via SMS after an SMS command is sent. ***Note*** • ***If no number is configured, then the router 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

Table 9.12-1: SMS Service Configuration

SMS AT Commands

The following figure shows the supported SMS command syntax.

List of Commands

Command name	Command
Reboot	AT+REBOOT=1
Cell Diagnostics	AT+CELLDIAG?
LAN Diagnostics	AT+LANDIAG?
WAN Diagnostics	AT+WANDIAG?
WAN Ping	AT+WANPING=<IPA>
LAN Ping	AT+LANPING=<IPA>
WWAN Ping	AT+WWANPING=<IPA>
CELL Ping	AT+CELLPING=<IPA>
Enable Remote access	AT+REMACC=<1/0>
Hardware information	AT+HWI?
Software information	AT+SWI?
Start Stop VPN	AT+VPN=<VPN Type>,<VPN Name>,<start/stop>
Install/Update IPK	AT+IPKDOTA=<Name of IPK file>,<install/upgrade/remove/autoremove>,<For install/upgrade: 0-Both Default & Custom URL, 1-Default URL, 2-Custom URL>
Lan Settings	AT+IPLAN=<IPv4 address>,<SubnetMask>
Dota Custom Settings	AT+DOTASETTINGS=<HTTP/HTTPS>,<Server URL>,<File name>,<Username>,<Password>,<Timeout>,<Retry>
OPKG Configuration Settings	AT+OPKGSETTINGS=<Server URL>
Manage Digital Output	AT#OUT=<GPO1/GPO2>,<OPEN/CLOSE>
AT Command	AT#ATCMD='<AT command string>',<Timeout>
Dota Action	AT+DOTA=<C/M>,<update/check>[,<released/beta/development>,<filename>]
Cellular Settings	AT+IPGPRS=<1/2>,<Apn>,<Username>,<Password>,<Auth-Type>,<Data-Roam>
Get Serial FTP Configuration	AT+SERIALFTPCONFIG?
Set Serial FTP Configuration	AT+SERIALFTPCONFIG=<File Name>,<IMEI-0/1>,<Server Address>,<Port>,<Username>,<Password>,<Directory Path>
Send Serial Data	AT+SERIALDATA=<Data>
Change SIM Priority	AT+SIMPRIORITY=<1/2>
Module Dota	AT+MODULEDOTA=<M/C>,<update/check>,<sierra_fw/volte_patches>,<firmware/patch filename>
Module Dota Custom Settings	AT+MODULEDOTASETTINGS=<Server URL>,<File name>

Save & Apply Save Reset

Powered by Lantronix E21X 3.16.0.0R1

Figure 9.12-2: SMS AT Commands

The following table describes the command syntax:

#	Name	Command Syntax
1	Reboot	AT+REBOOT=1
2	Cell Diagnostics	AT+CELLDIAG?
3	LAN Diagnostics	AT+LANDIAG?
4	WAN Diagnostics	AT+WANDIAG?
5	WAN Ping	AT+WANPING=<IPA> Parameter:

#	Name	Command Syntax
		IPA- IP address of the WAN interface to ping.
6	LAN Ping	AT+LANPING=<IPA> Parameter: *IPA – IP address of the LAN interface to ping*
7	WWAN Ping	AT+WWANPING=<IPA> Parameter: *IPA- IP address of the WAN interface to ping.*
8	CELL Ping	AT+CELLPING=<IPA> Parameter: *IPA- IP address of the WAN interface to ping.*
9	Enable Remote Access	AT+REMACC=<1/0> Parameter: *1/0 – Set 1 to enable, set 0 to disable remote access*
10	Hardware Information	AT+HWI?
11	Software Information	AT+SWI?
12	Start/Stop VPN	AT+VPN=<VPN Type>,<VPN Name>,<start/stop> Parameters: *VPN type – Openvpn or ipsec* *VPN name – VPN instance name* *Start/stop – action to start or stop the vpn*
13	Install/Update IPK	AT+IPKDOTA=<Name of IPK file>,<install/upgrade/remove/autoremove>,<For install/upgrade: 0-Both Default & Custom URL, 1-Default URL, 2-Custom URL> 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*
14	Lan Settings	AT+IPLAN=<IPv4 address>,<SubnetMask> Parameters: *IPv4 address – The IP address of the LAN interface* *Subnet mask – Subnet mask of the LAN IP address*
15	Dota Custom Settings	AT+DOTASETTINGS=<HTTP/HTTPS>,<Server URL>,<File name>,<Username>,<Password>,<Timeout>,<Retry>

#	Name	Command Syntax
		Parameters: *HTTP/HTTPS – protocol of the custom server* *Server URL – server URL, must include http: or htttps:* *File name – name of the file to be accessed for the update* *Username – server user name* *Password – server password* *Timeout – period of time to wait for the download to complete (minutes)* *Retry Parameters – number of retry attempts to check and download the file from the server.*
16	OPKG Configuration Settings	AT+OPKGSETTINGS=<Server URL> Parameter: *Server URL – Enter the URL of the*
17	Manage Digital Output	AT#OUT=<GPO1/GPO2>,<OPEN/CLOSE> Parameters: *GPO1/GPO2 – the pin to be configured* *OPEN/CLOSE – Set OPEN for low, or CLOSE for high.*
18	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 – 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 - to check signal strength*
19	DOTA Action	AT+DOTA=<C/M>,<update/check>[,<released/beta/development>,<filename>] Parameters: *C/M – C for custom server, M for D2Sphere* *update/check – whether to update the router with the specified filename or to check for available updates* *released/beta/development – the release channel on the D2Sphere server to use for the update/check* *filename – filename of the package to use for the update*
20	Cellular Settings	AT+IPGPRS=<1>,<Apn>,<Username>,<Password>,<Auth-Type>,<Data-Roam> Parameters: *1 or 1/2 – SIM slot number. 1 slot is supported on E22x models. 2 slots are supported on E21x models only.* *Apn – access point name provided by the cellular network provider* *Username – username if auth type is pap, chap, or pap/chap*

#	Name	Command Syntax
		Password – password if auth type is pap, chap, or pap/chap *Auth-type – none, pap, pap/chap, or chap (the auth-type parameter is case sensitive, must be all lowercase)* *Data-Roam – Enter 0 for disabled or 1 for enabled*
21	Get Serial FTP Configuration	AT+SERIALFTPCONFIG?
22	Set Serial FTP Configuration	AT+SERIALFTPCONFIG=<File Name>,<IMEI-0/1>,<Server Address>,<Port>,<Username>,<Password>,<Directory Path> Parameters: *File Name – Destination file name* *IMEI-0/1 - 0 to exclude IMEI number and 1 to include IMEI number.* *Server Address – FTP server addres* *Port – Port No. used* *Username – FTP username* *Password – FTP password* *Directory Path – Location on the server*
23	Send Serial Data	AT+SERIALDATA=<Data>
24	Change SIM Priority	AT+SIMPRIORITY=<1/2> Parameters: *1/2 – SIM slot number* Only for E210 devices.
25	Module Dota	AT+MODULEDOTA=<M/C>,<update/check>,<sierra_fw/volte_patches>,<firmware/patch filename> Parameters: *M – Lantronix Server* *C – Customserver* *update – Update firmware* *check – Check availablity* *sierra fw – Cellular firmware* *volte pacthes – Patches* *firmware filename – Fimware filename* *patch filename – Patch filename* ***Note:*** ***If you want to use custom server, first execute command no.26 AT+MODULEDOTASETTINGS to the set custom URL, filename and then execute this command.***
26	Module Dota Custom Settings	AT+MODULEDOTASETTINGS=<Server URL>,<File name> Parameters: *Server URL: URL of custom server* *File name: Firmware or Patch File name*

Table 9.12-2: SMS AT Command Syntax

9.12.2 Ethernet SMS

Services > SMS > Ethernet SMS

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

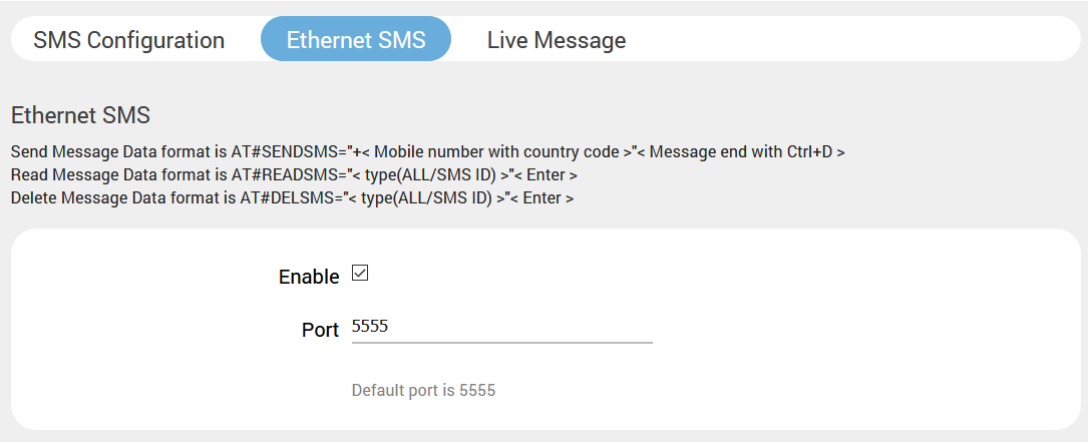


Figure 9.12-3: Ethernet SMS Configuration

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

Table 9.12-3: Ethernet SMS Configuration

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 with CTRL+D>
```

To read an incoming SMS

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

To delete an SMS

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

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

9.12.3 Live Message

Services > SMS > Live Message

Sends SMS from the web interface: You can also send SMS, read SMS and delete SMS from the web interface as shown in the screenshot below.

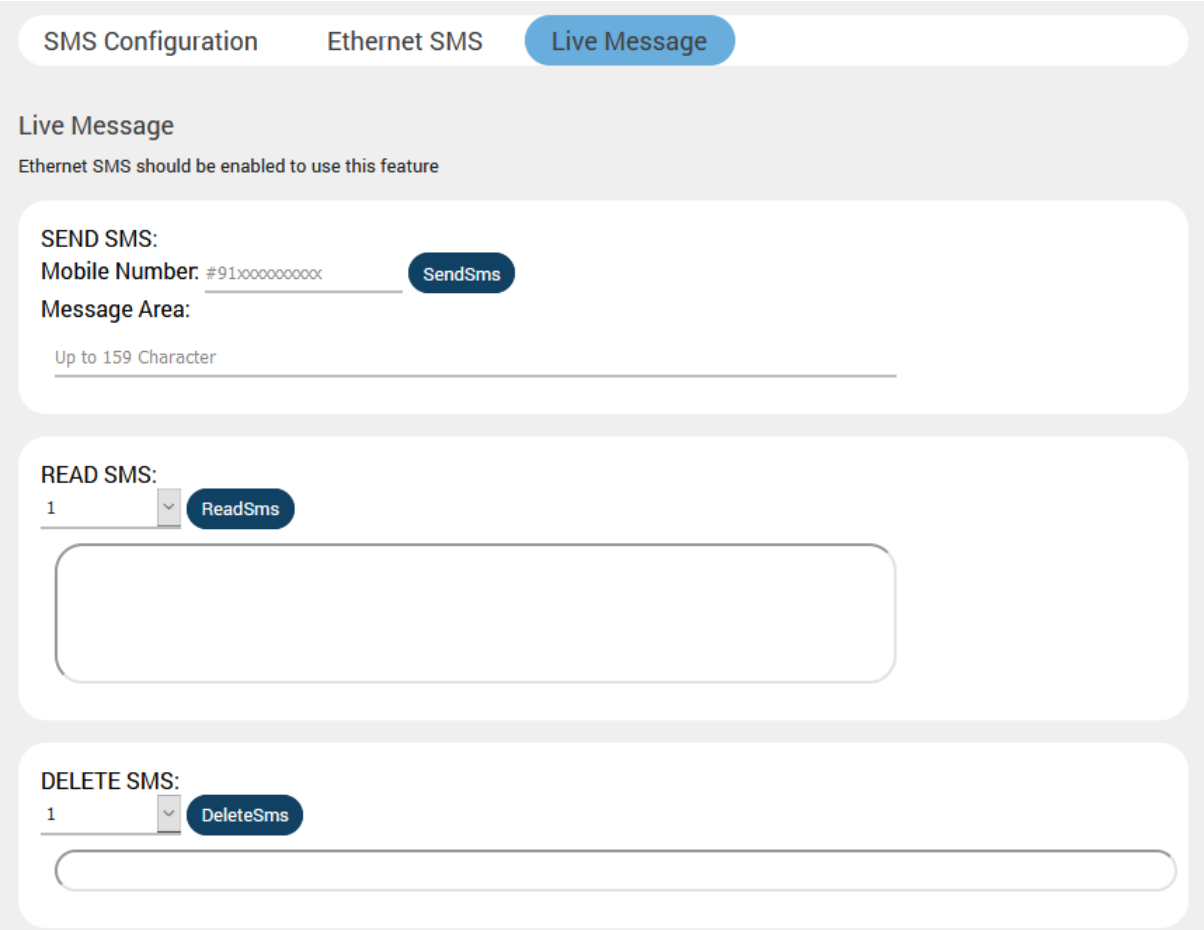


Figure 9.12-4: SMS Live Message Configuration

Note:

- ***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.***

9.13 Reporting Agent

Services > Reporting Agent

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

The information obtained from the router includes device information and the following groups:

- LAN
- WAN
- Cellular
- Wi-Fi
- GPS

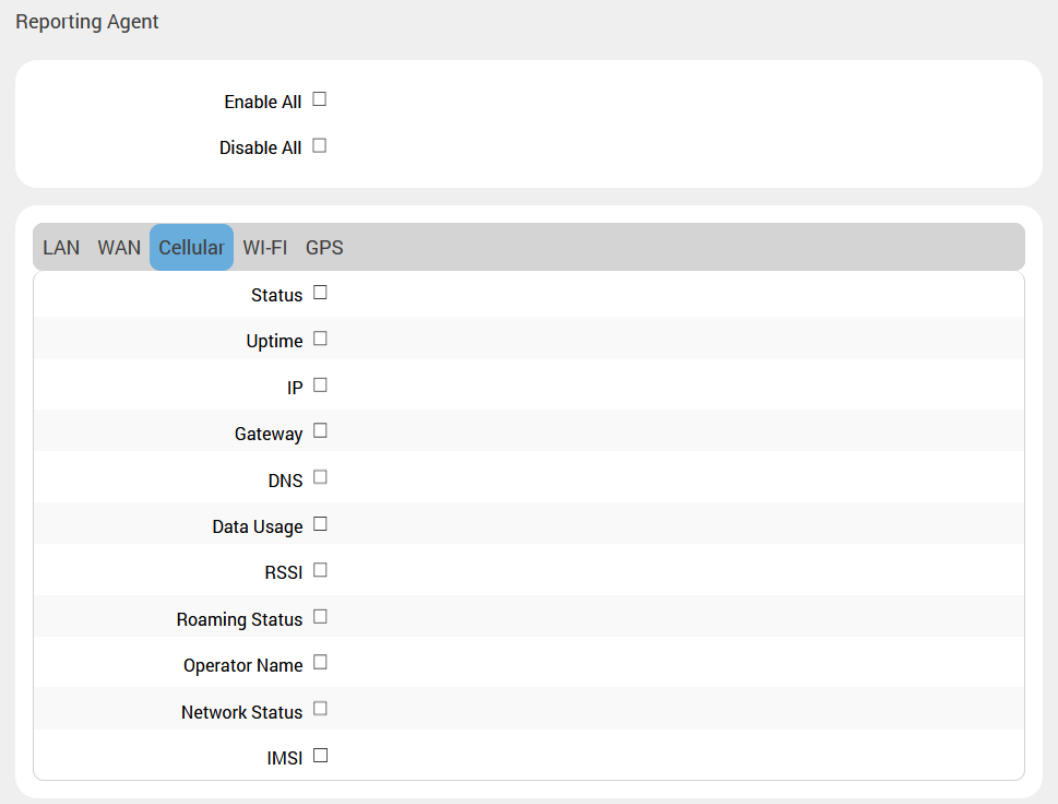


Figure 9.13-1. Reporting Agent (Cellular shown)

Parameters	Description
Enable All	Select check box to enable all settings for all interfaces.
Disable All	Select check box to clear all settings for all interfaces.
LAN Parameters	
LAN	Select to enable individual LAN settings. • Status • Uptime • IP

Parameters	Description
	• Data usage
WAN Parameters	
	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

Table 9.13-1: Reporting Agent Configuration

9.13.1 Sending Data

Services > Reporting Agent > Enable data Send

The reporting agent sends captured data using any of the following protocols: TCP/UDP/HTTP/HTTPS.

When sending data over TCP, you can define a custom string sequence for start of frame and end of frame. You can also configure a backup server. The router will send data to the backup server after three unsuccessful retries to the primary device management server. It will continue to send data to the backup server until the backup server fails or the device reboots.

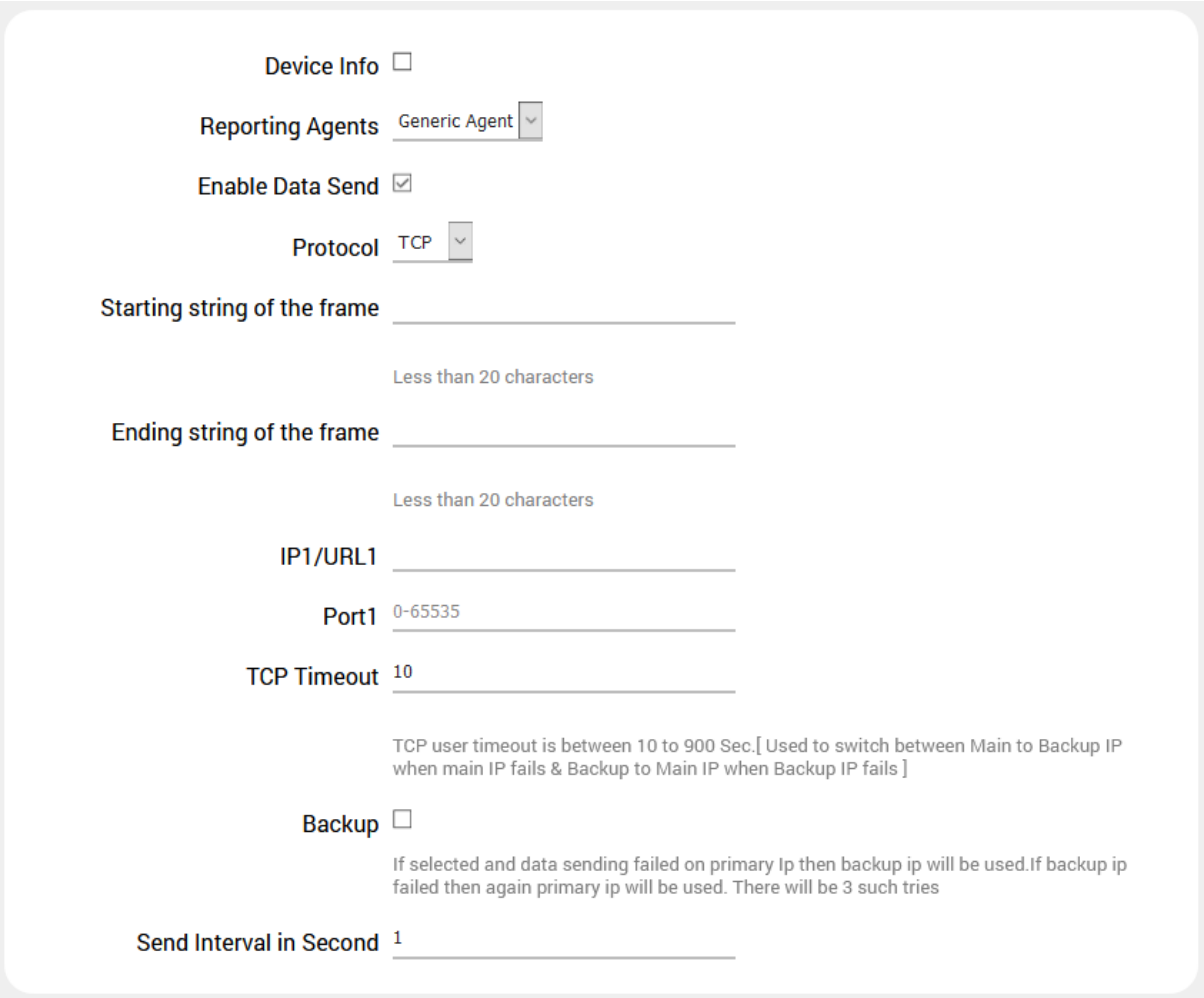


Figure 9.13-2 Reporting Agent Enable Data Send (TCP)

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 somewhat.
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.

Table 9.13-2: Reporting Configuration Agent Data Send

9.13.2 Data Format

The following example shows the data format of the output considering all parameters selected in the interfaces and TCP protocol selected

```
@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
Info={(MAC;IP;TX;RX)(6C:19:8F:0B:7A:78;192.169.2.1;305;5209)},Time(GMT)=,Latitude(d
egree.mmsss)=,Longitude(degree.mmsss)=,Altitude(in meters)=,Model=E225LITE,Kernel
Version=3.10.49,Local Time=Tue Mar 14 06:11:25 GMT 2017,System
```

```
Uptime(Seconds)=329530,Firmware Version=Lantronix E220 2.2.0
RC8,DI1=,DO1=,DI2=,DO2=#



@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)=x.x.x.x,
Cellular uptime(Seconds)= abc,
Cellular Gateway=y.y.y.y,
Cellular DNS=z.z.z.z,
Cellular TX bytes=xxx,
Cellular RX bytes=yyy,
RSSI(ASU)=22,
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,
WifiClientInfo={(MAC;IP;TX;RX)(6C:19:8F:0B:7A:78;192.169.2.1;305;5209)},

Time(GMT)=,
Latitude(degree.mmsss)=,
Longitude(degree.mmsss)=,
Altitude(in meters)=,

Model=E225LITE,
Kernel Version=3.10.49,
Local Time=Tue Mar 14 06:11:25 GMT 2017,
System Uptime(Seconds)=329530,
Firmware Version=Lantronix E220 2.2.0 RC8,

DI1=,
DO1=,
DI2=,
DO2=#
```

9.14 GPS

Services > GPS

Some E210 and E220 series router models have a built-in GPS receiver that receives GPS data from GPS satellites for synchronizing the GPS time and position data.

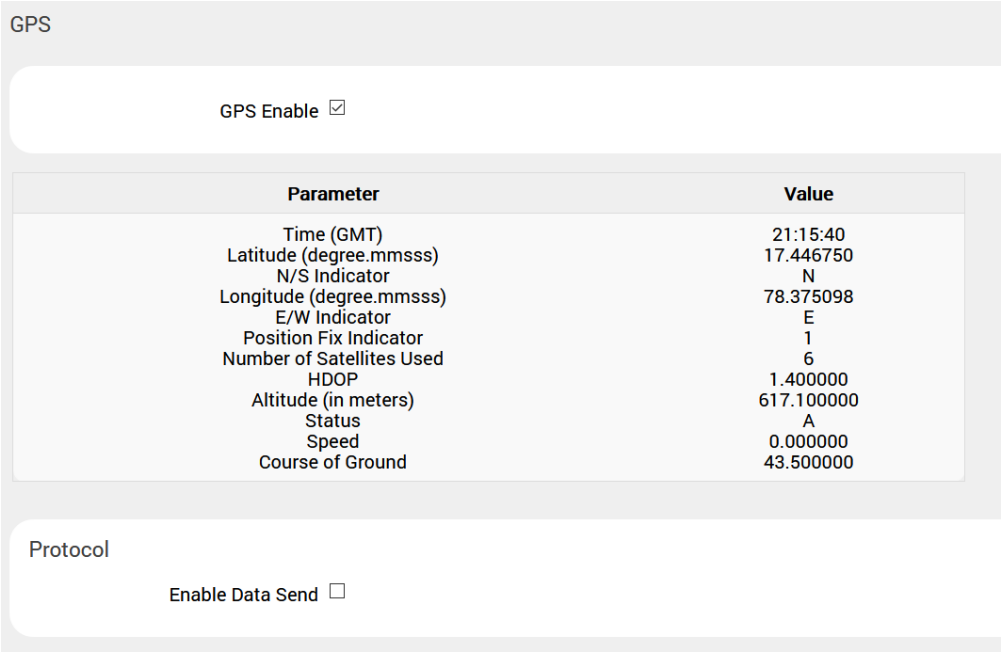


Figure 9.14-1: Services > GPS enable data

The GPS data can be sent in NMEA data format to an external TCP/UDP/HTTP/HTTPS server on a real-time basis.

You can also configure a backup server. The router will send data to the backup server after three unsuccessful attempts to the primary device management server. It will continue to send data to the backup server until the backup server fails or the device reboots.

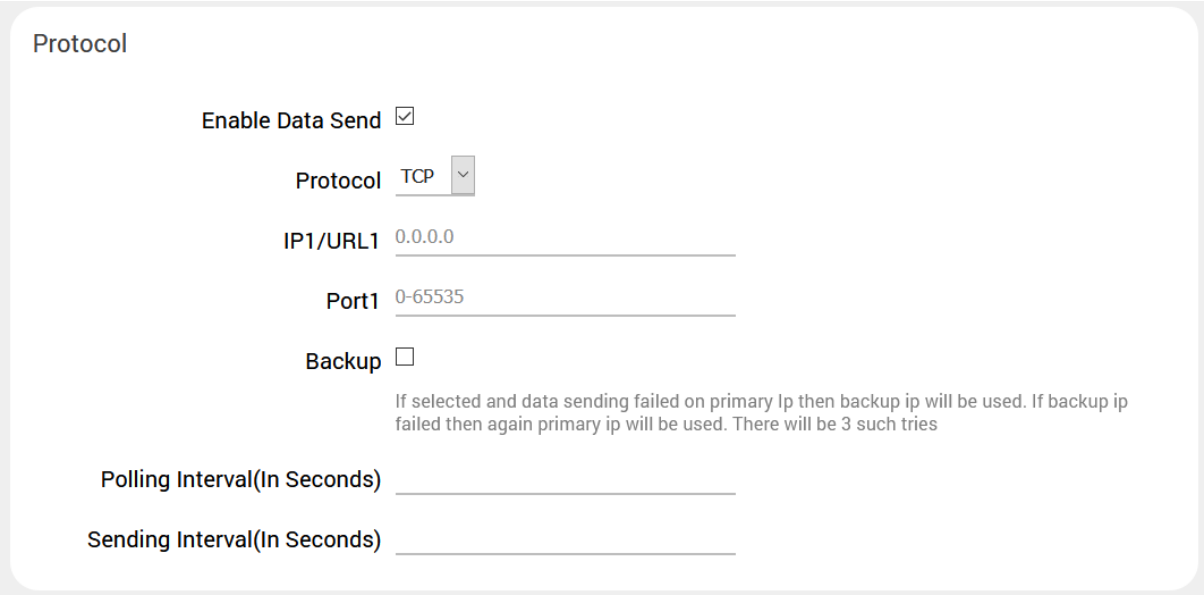


Figure 9.14-2: GPS Service Configuration

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
Status	Displays the status. A = Data valid V = Data not valid

Parameters	Description
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 allow using of backup IP, in case sending of the data fails using primary IP Address. In case the backup IP Address fails, primary IP Address will be used. Three such trials will be executed. *IP2 – 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.

Table 9.14-1: GPS Service Configuration

9.14.1 Sample GPS Frames

9.14.1.1 GSV Format

- $GPGSV,4,1,16,21,50,358,38,22,28,272,37,29,53,164,36,18,51,319,31*7E

IMEI number is added at the start of every frame

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	Channel 4 (Range 1 – 32) Example – 18
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

Table 9.14-2: GSV Data Format

[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.

9.14.1.2 GGA Format

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

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	-

Parameters	Description
Checksum	*42
<CR><LF>	End of message termination

Table 9.14-3: GGA Data Format

9.14.1.3 VTG Format

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

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
<CR><LF>	End of message termination

Table 9.14-4: VTG Data Format

[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.

9.14.1.4 RMC Format

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

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)

Parameters	Description
	S *– Simulator* Example – A
Checksum	*1E
<CR><LF>	End of message termination

Table 9.14-5: RMC Data Format

(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.

9.14.1.5 GSA Format

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

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

Table 9.14-6: GSA Data Format

(1) Satellite used in solution.

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

9.15 Keepalived

Services > Keepalived

The Keepalived service (Keepalived is a Linux daemon that provides frameworks for load balancing and high availability of the servers connected to the router) 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).

9.15.1 General

Services > Keepalived > General

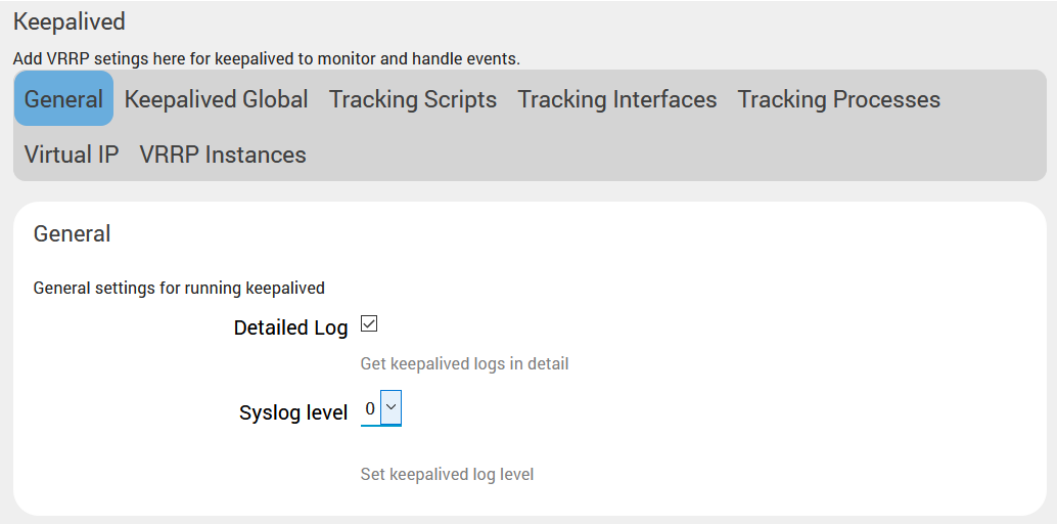


Figure 9.15-1 Keepalived General settings

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.

Table 9.15-1: Keepalived General Configuration

9.15.2 Keepalived Global

Services > Keepalived > Keepalived Global

This provides general settings for the Keepalived service.

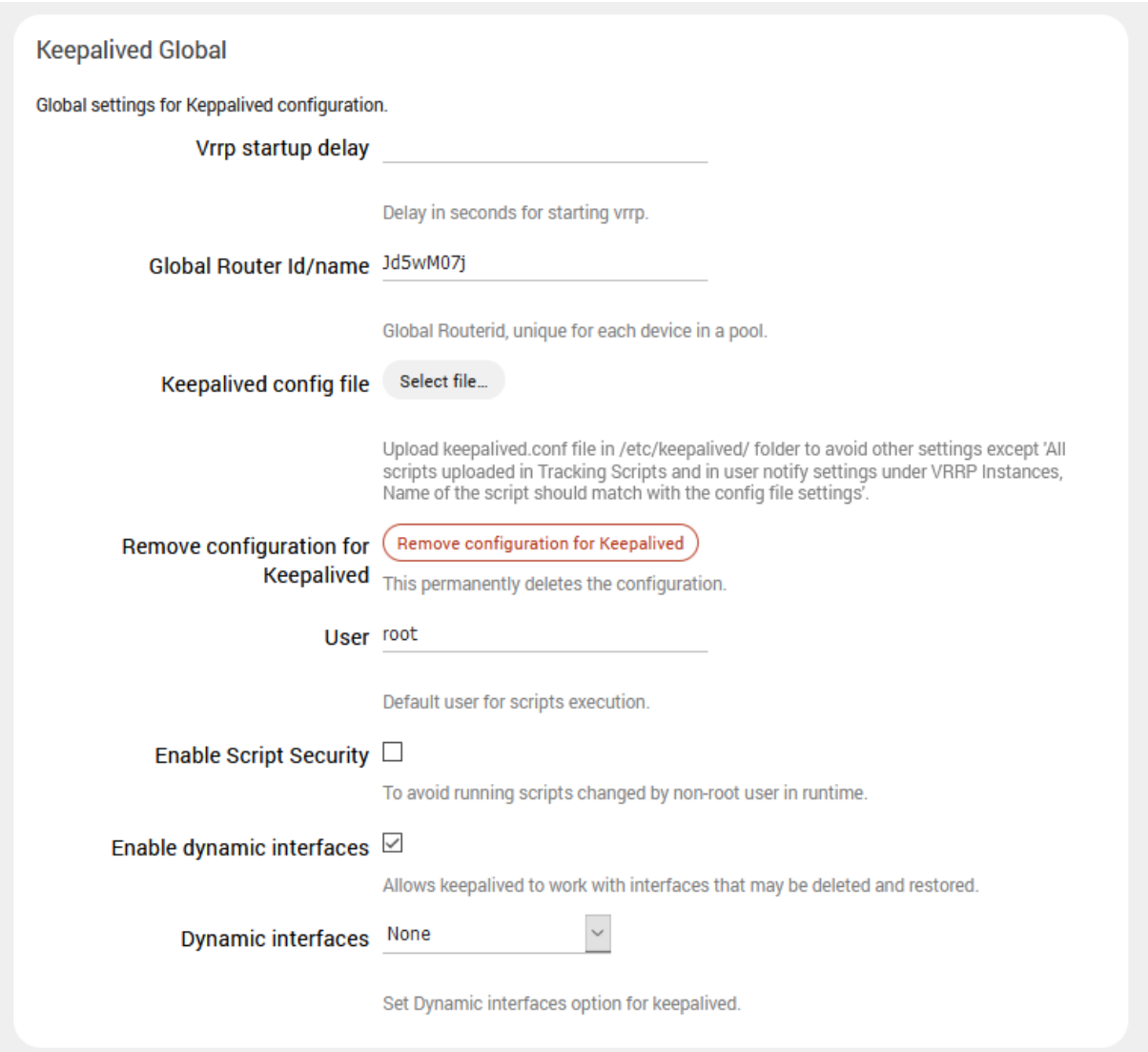


Figure 9.15-2: Keepalived Global Configuration

Parameters	Description
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

Parameters	Description
	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

Table 9.15-2: Keepalived Global Configuration

9.15.3 Tracking Scripts

Services > Keepalived > Tracking Scripts

This page is used to create blocks of tracking scripts that can be used by various Keepalived instances to be configured in the same router. Keepalived will run the tracking script to determine the health of the host and increase or decrease the priority of the router by the value of the weight.

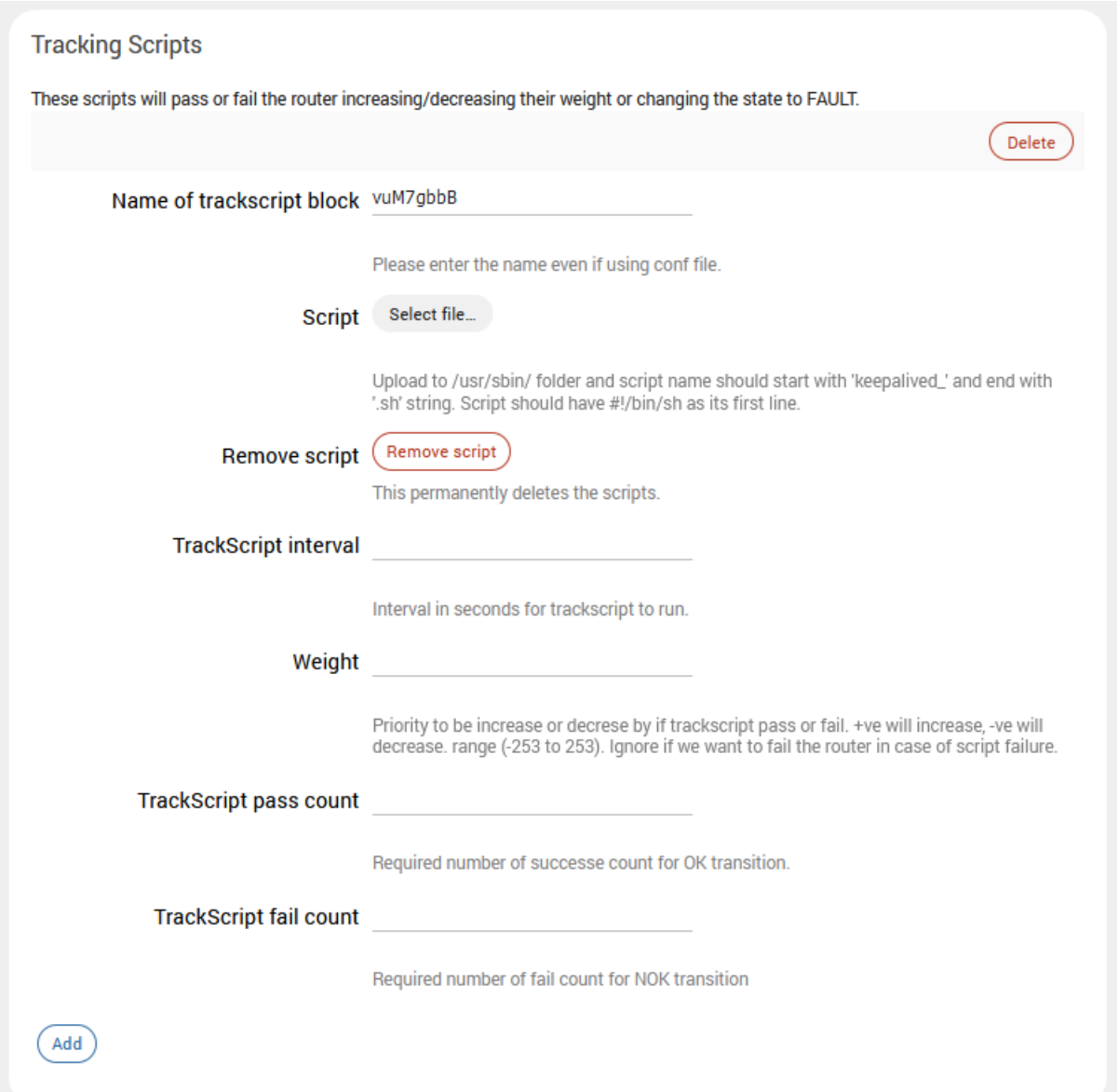


Figure 9.15-3: Keepalived Tracking Scripts Configuration

Parameters	Description
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".

Parameters	Description
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.

Table 9.15-3: Keepalived Tracking Scripts Configuration

9.15.4 Tracking Interfaces

Services > Keepalived > Tracking Interfaces

This page is used to 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.

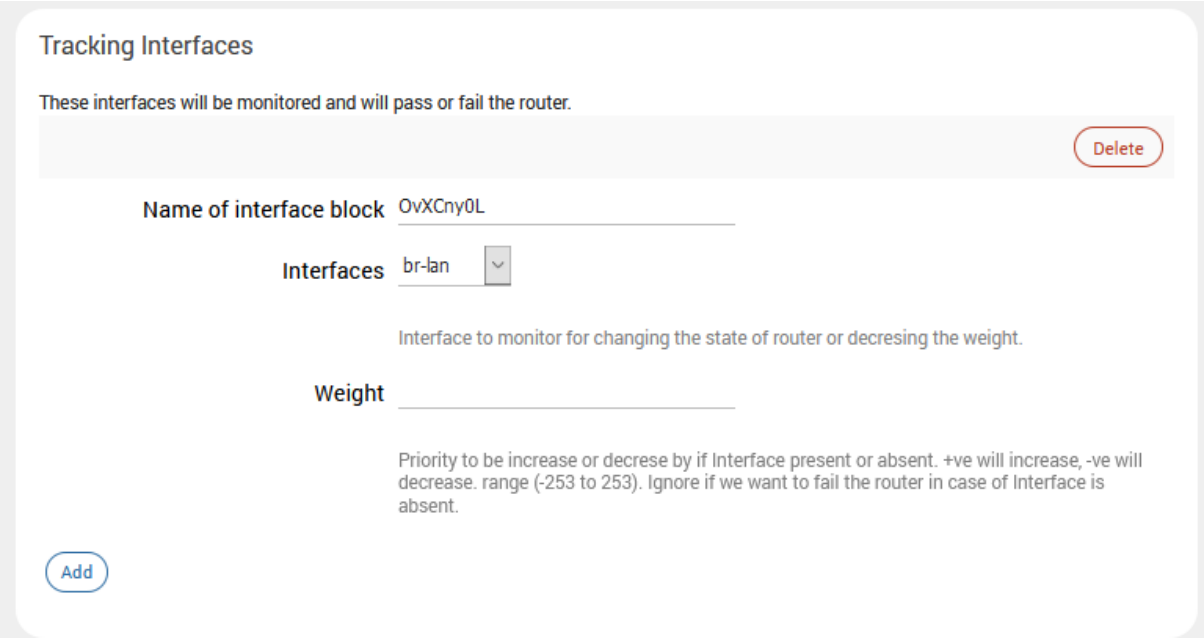


Figure 9.15-4: Keepalived Tracking Interfaces Configuration

Parameters	Description
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.
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.

Table 9.15-4: Keepalived Tracking Interfaces Configuration

9.15.5 Tracking Processes

Services > Keepalived > Tracking Processes

This page is used to 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.

Note:

- ***To monitor a process after you've added it, you must restart the Keepalived service manually.***

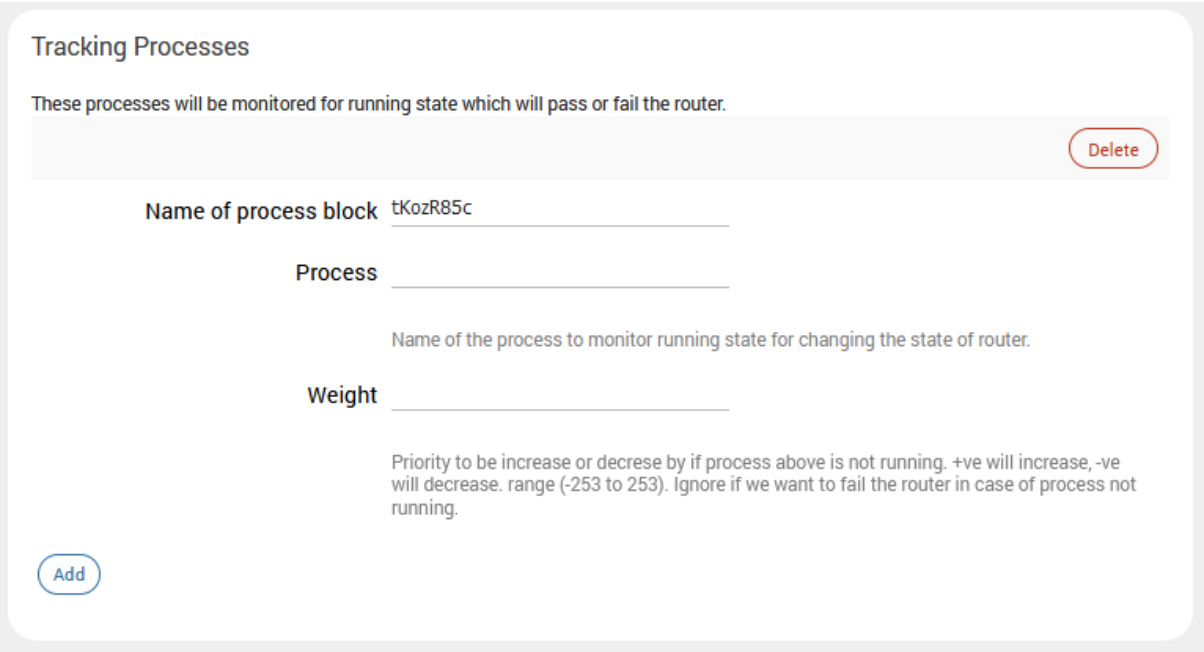


Figure 9.15-5: Keepalived Tracking Processes Configuration

Parameters	Description
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.

Table 9.15-5: Keepalived Tracking Processes Configuration

9.15.6 Virtual IP

Services > Keepalived > Virtual IP

Configure the Virtual IP address for the VRRP instance.

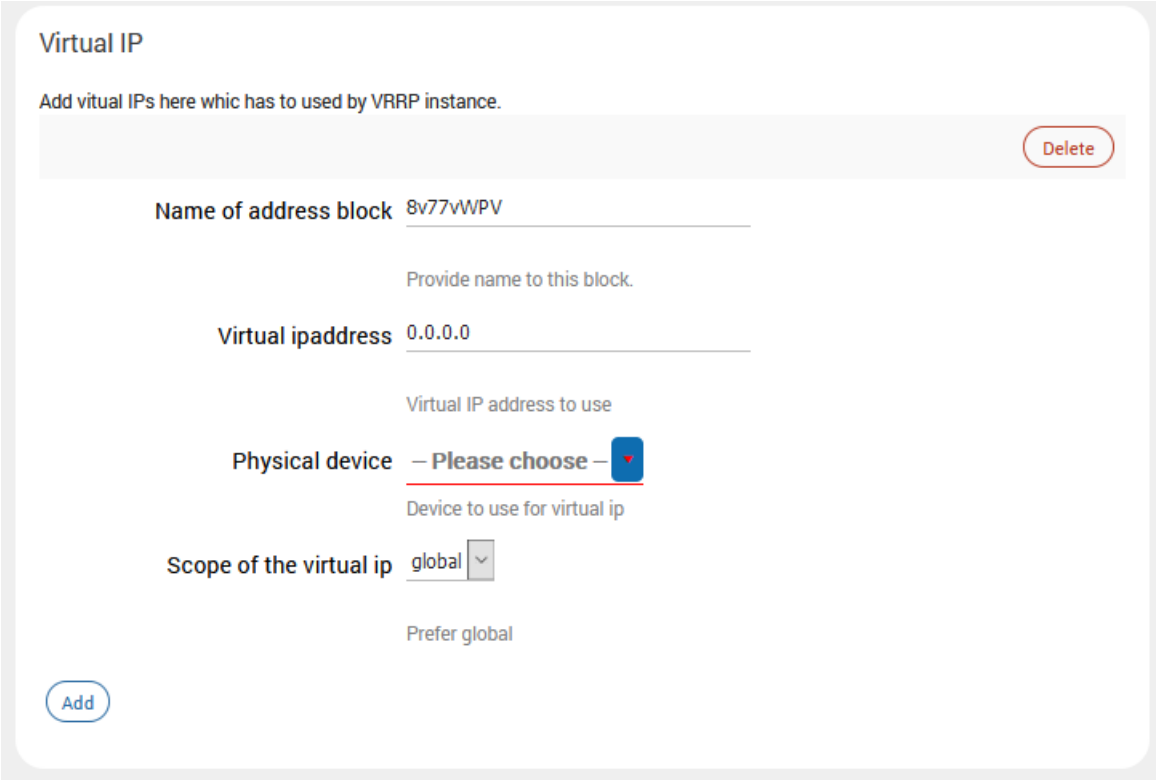


Figure 9.15-6: Keepalived Virtual IP

Parameters	Description
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.

Table 9.15-6: Keepalived Virtual IP Configuration

9.15.7 VRRP Instances

Services > Keepalived > VRRP Instances

The VRRP instance is the individual instance of the VRRP protocol running on an interface to be monitored by Keepalived.

The General and Advanced settings define the VRRP instance. The User Notify settings allow Keepalived to run specified scripts when the router transitions from backup to master state or master to backup state.

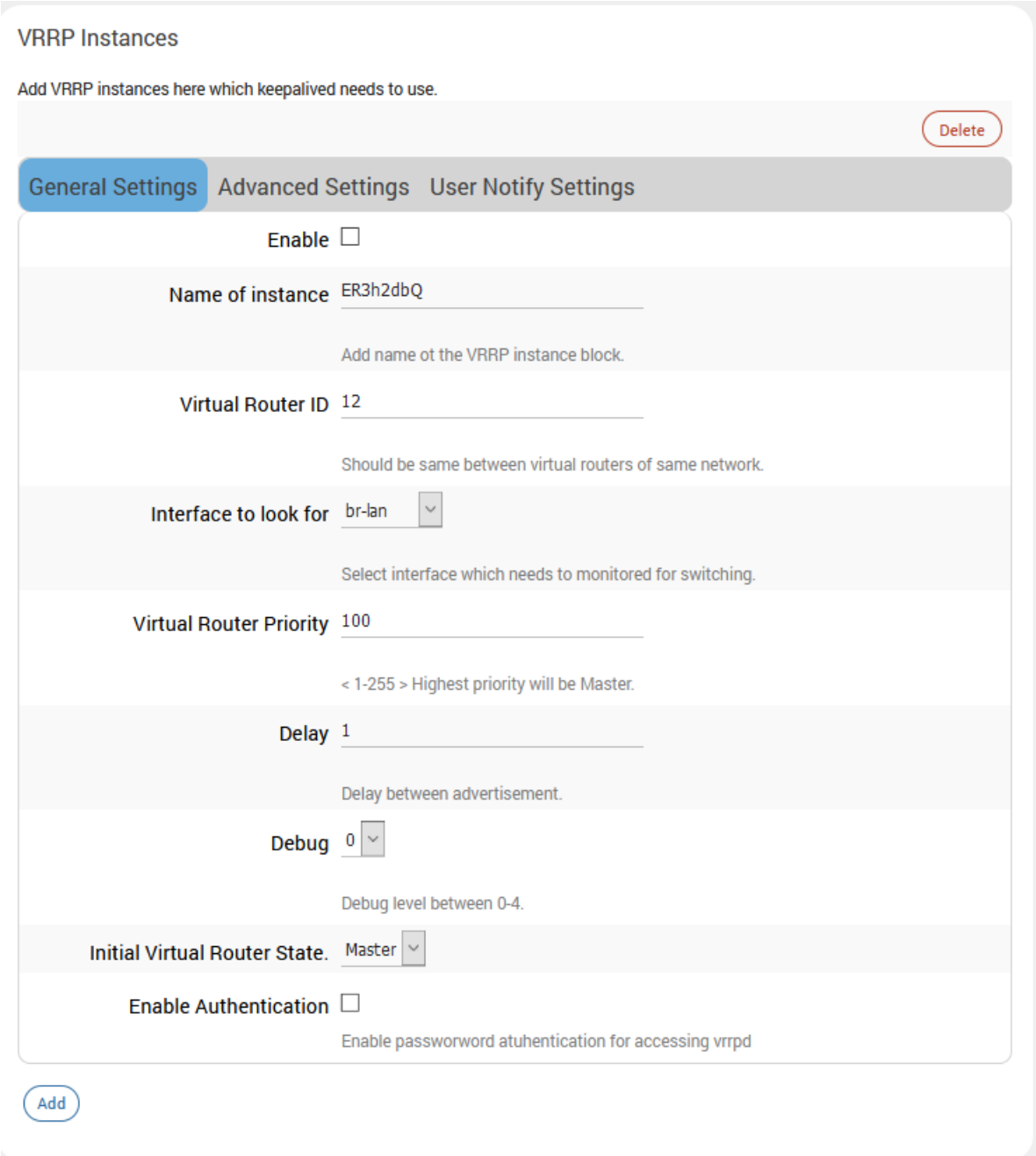


Figure 9.15-7: Keepalived VRRP Instances (General Configuration)

Parameters	Description
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.
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

Parameters	Description
	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.

Table 9.15-7: Keepalived VRRP Instances Configuration

9.16 Last Gasp

The Last Gasp feature is available on E220 series routers only. The Last Gasp feature sends a last gasp message to a mobile number to report the abrupt loss of power to the router.

Last Gasp configuration includes a mobile number that Last Gasp will attempt to contact, and short text messages for power restore or power. Last Gasp is enabled by default.

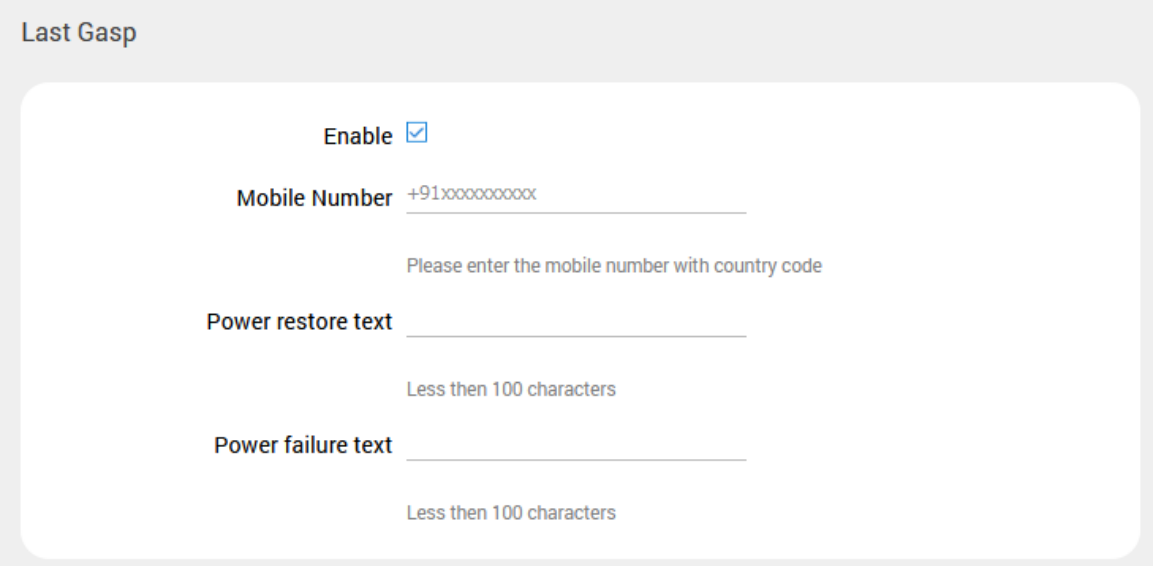


Figure 9.16-1 Last Gasp (E220 series devices only)

Parameters	Description
Last Gasp	
Enable	Select to enable last gasp. Enabled by default.
Mobile Number	Enter the mobile number that Last gasp will attempt to contact when power is lost.
Power restore text	Enter the message for power restore.
Power failure text	Enter the message for power failure.

Table 9.16-1: Last Gasp Configuration (E220 series devices only)

9.17 Serial

Services > Serial

The E220 series router provides one RS-485 serial port, which can be configured in half-duplex or full-duplex mode by means of a switch on the E220 series hardware.

The E210 router provides one RS-232 9-pin serial port. Optionally, the RS-232 port can be converted to an RS-485 port using the Snap Cap™ SC485 add-on. The RS-485 port can be configured in half-duplex or full-duplex mode by means of a switch on the Snap Cap SC485 add-on.

For wiring configuration details for the E220 series RS-485 in half-duplex mode, see *Appendix A. Wiring Diagrams.*

9.17.1 Serial Configuration

The Serial configuration parameters such as baud rate must be configured for the data connection to the serial port. You can set the serial configuration mode as:

- Transparent
- Modbus RTU to Modbus TCP
- AT command

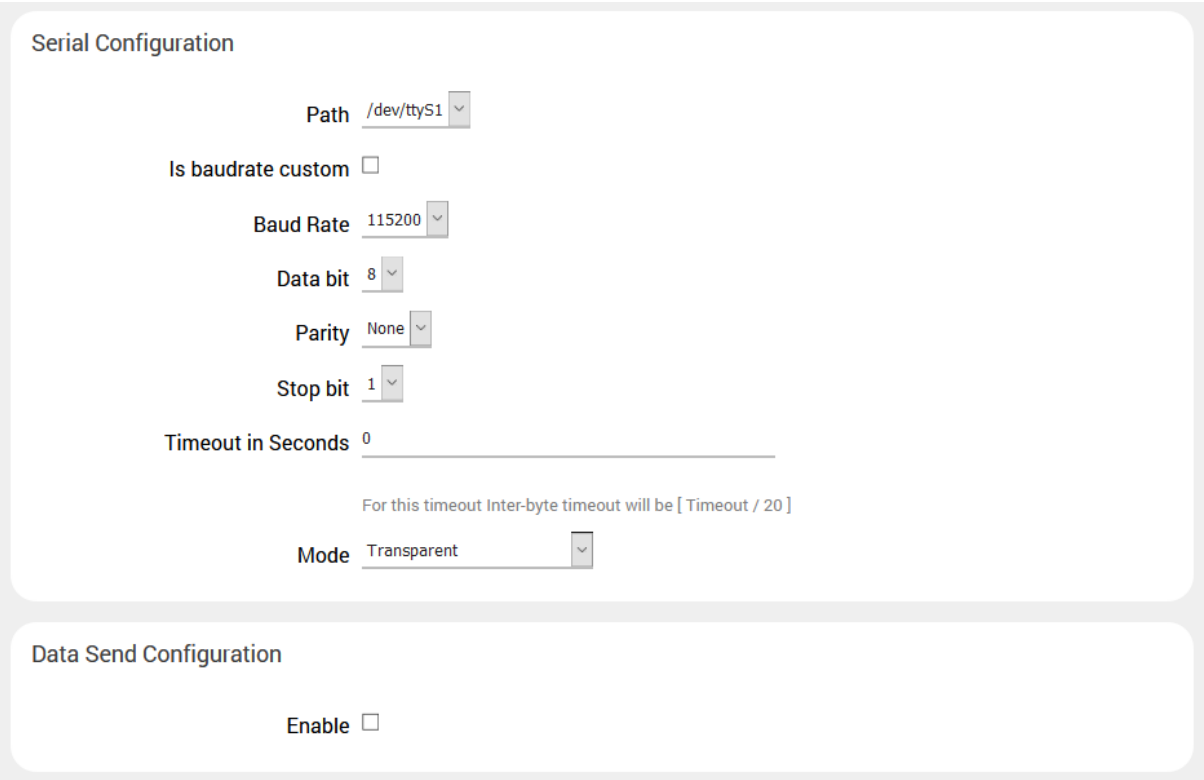


Figure 9.17-1: Serial Configuration

Parameters	Description
Serial Configuration	
Path	The path to the serial device. The default path is "dev/ttyS1".
Is baudrate custom	Select the box to add a custom baud rate between 2400 bps and 230400 bps in the Baud Rate field.
Baud Rate	Select a baud rate from the list of pre-defined options or enter the custom baud rate between 2400 bps and 230400 bps. The default baud rate is 115200.
Data bit	Select the number of data bits: The valid range is from 5 to 8. The default data rate is 8.
Parity	A parity bit is added to the end of the string of binary code that checks if the number of bits in the string with value one is even or odd. It is used for detecting error. Select the parity bit: *Odd* *Even* *None* The default is None.
Stop bit	Select the number of stop bits: *1* *2* The default stop bit is 1.
Timeout in Seconds	Enter the idle timeout in seconds for serial data completion.
Mode	Select the mode of serial communication: Transparent *Transparent mode of communication does not alter any data structure before or during the data communication.* Modbus RTU to Modbus TCP: *This mode converts the Modbus RTU data to/from serial to Modbus TCP before transmitting over TCP network.* AT command: *Enables to send and receive SMS via AT commands.*

Table 9.17-1: Serial Configuration

9.17.2 Serial Data Send Configuration

The Data Send configuration is used to select the protocol and serial operating mode settings. If the TCP protocol is selected, the router can operate in TCP server or TCP client mode. In TCP server mode, the router will listen on the local port for network communication from TCP clients on the LAN interface (type=internal) or the WAN interface (type=external). In TCP client mode, the serial device connects to a remote TCP server at a specified IP and port, or to a backup server, for the data

transmission. The data from the serial port can be sent via TCP using any of the available TCP interfaces.

The other protocol option is FTP, which allows the serial device to send a file to an FTP server. See Section 9.14.2.3 Data Send Configuration for FTP

9.17.2.1 TCP Server Mode Configuration

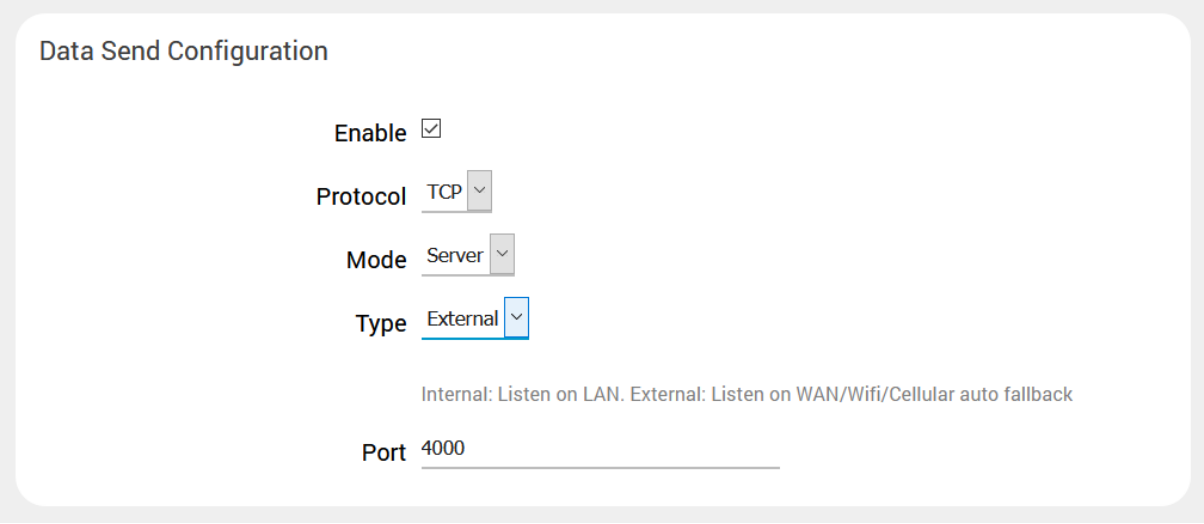


Figure 9.17-2: Data Send Configuration – Server Mode on WAN Interface

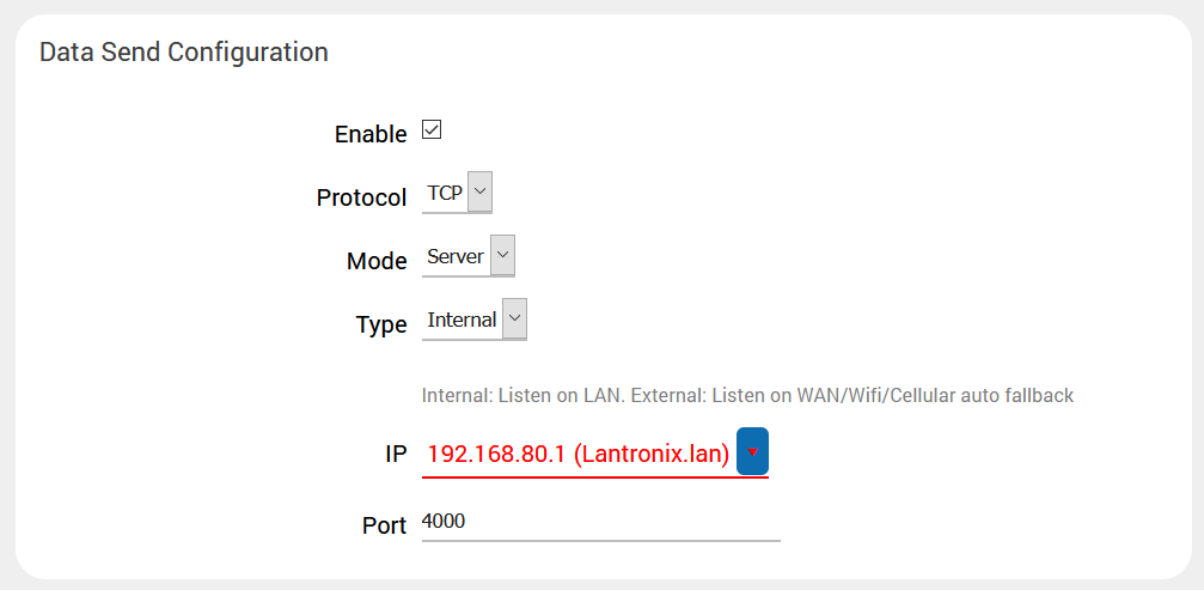


Figure 9.17-3: Data Send Configuration – Server Mode on LAN Interface

Parameters	Description
Enable	Select the box to enable sending serial data
Protocol	Select the protocol. *For TCP, select TCP.*

Parameters	Description
	For FTP transport, select FTP.
Mode	Select the serial operating mode. ***Note:*** • ***Server mode operation requires a public IP address on the external interface (WAN).*** *For TCP server mode, select Server.* *For TCP client mode, select Client*
Type	This setting is available if TCP Protocol and Server Mode settings are selected. *Select External to listen for network connections on the WAN interface.* *Select Internal to listen for network connections on the LAN interface.*
External – serial port listens on WAN interface	
Port	Enter the WAN port to listen on.
Internal – serial port listens on LAN interface	
IP	Enter the IP address of the LAN interface to listen on
Port	Enter the port of the LAN interface to listen on

Table 9.17-2: Data Send Configuration - Server Mode

9.17.2.2 TCP Client Mode Configuration

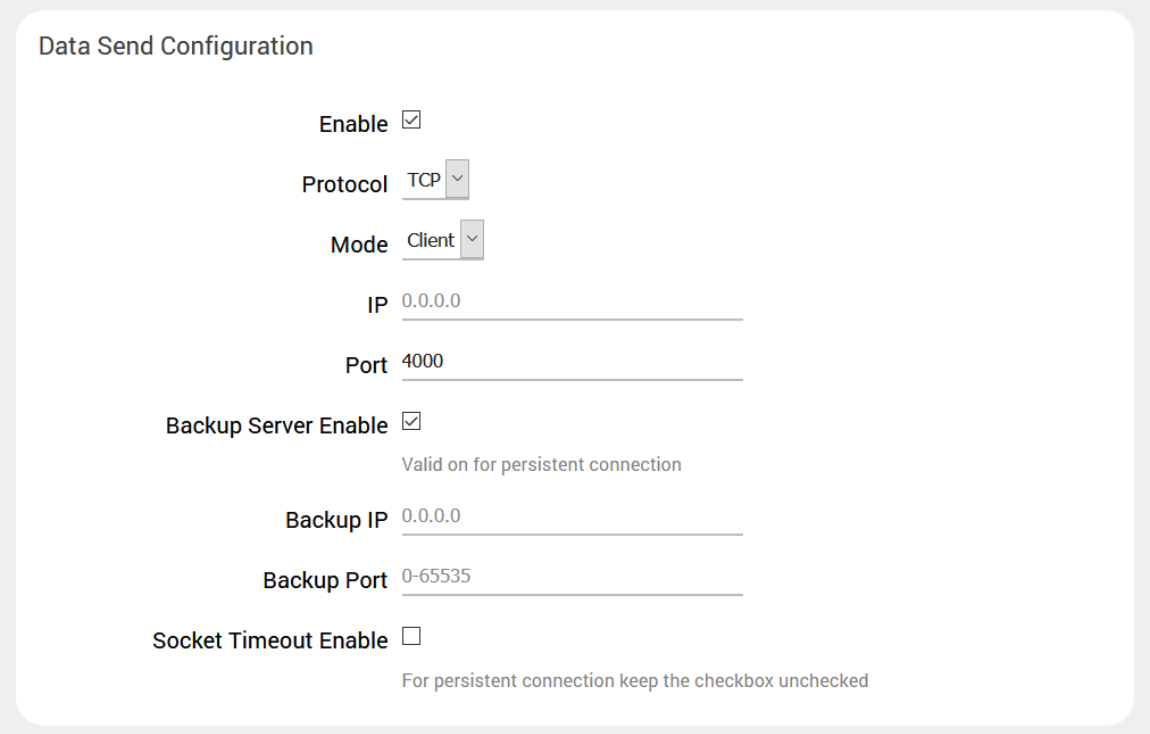


Figure 9.17-4: Data Send Configuration – Client Mode

Parameters	Description
Enable	Select the box to enable sending serial data
Protocol	Select the protocol. *For TCP, select TCP.* *For FTP transport, select FTP.*
Mode	Select the serial operating mode. *For TCP server mode, select Server.* *For TCP client mode, select Client*
IP	Enter the IP address of the remote TCP server
Port	Enter the port of the remote TCP server
Backup Server Enable	Select the box to enable a backup TCP server
Backup IP	Enter the IP address of the remote backup TCP server
Backup Port	Enter the port of the remote backup TCP server
Socket Timeout Enable	Select the box to enable a socket timeout value.
Inactivity Timeout in Seconds	If Socket Timeout is enabled, enter the inactivity timeout value in seconds.

Table 9.17-3: Data Send Configuration - Client Mode

9.17.2.3 Data Send Configuration for FTP

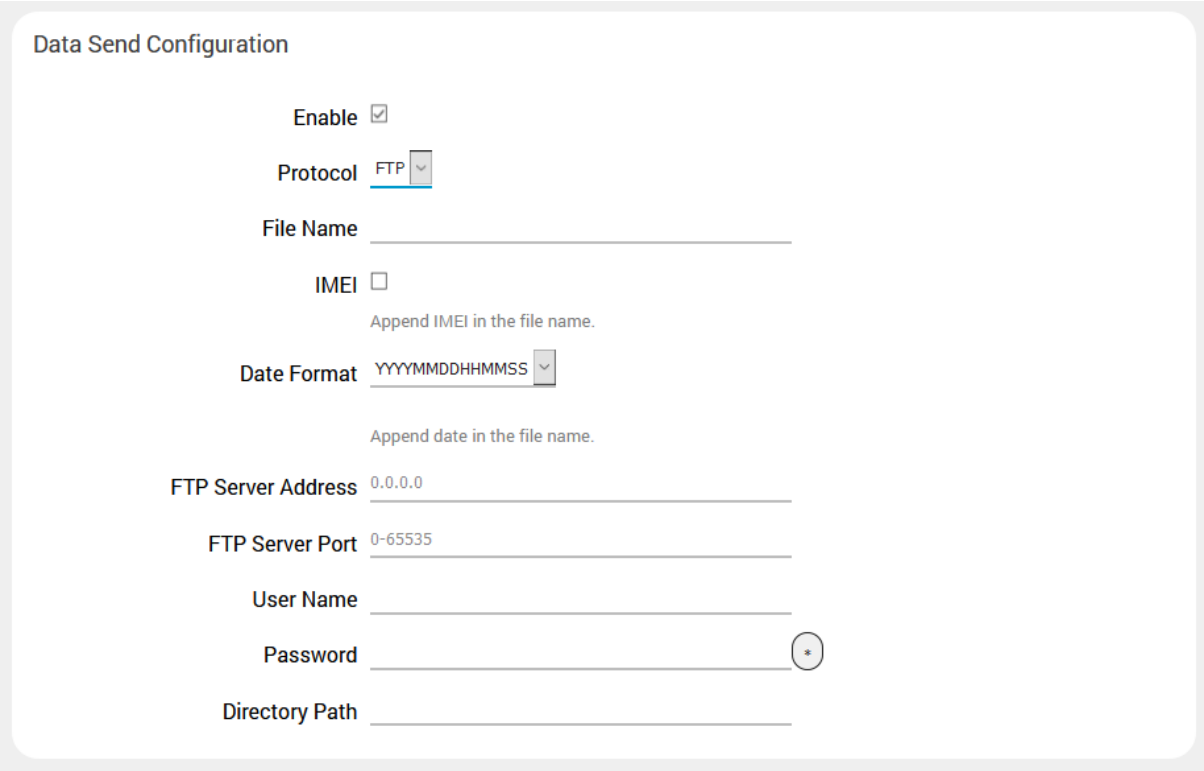


Figure 9.17-5: Data Send Configuration FTP Protocol

Parameters	Description
Enable	Select the box to enable sending serial data.
Protocol	Select the protocol. *For TCP, select TCP.* *For FTP transport, select FTP.*
File Name	Enter the file name of the file to transmitted.
IMEI	Select the box to add the IMEI to the file name.
Date Format	Select the date format to be appended to the file name.
FTP Server Address	Enter the IP address of the FTP server.
FTP Server Port	Enter the port number of the FTP server.
User Name	Enter the FTP server user name.
Password	Enter the FTP server password.
Directory Path	Enter the directory path on the FTP server where the file will be placed.

Table 9.17-4: Data Send Configuration FTP Protocol

9.18 Service Actions

Services > Service Actions

This page displays a list of all the available services and allows the administrator to manage 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

- ***Only perform service actions if you understand the outcome. Stopping or disabling certain services could adversely affect the operation of the router and require a device reset.***

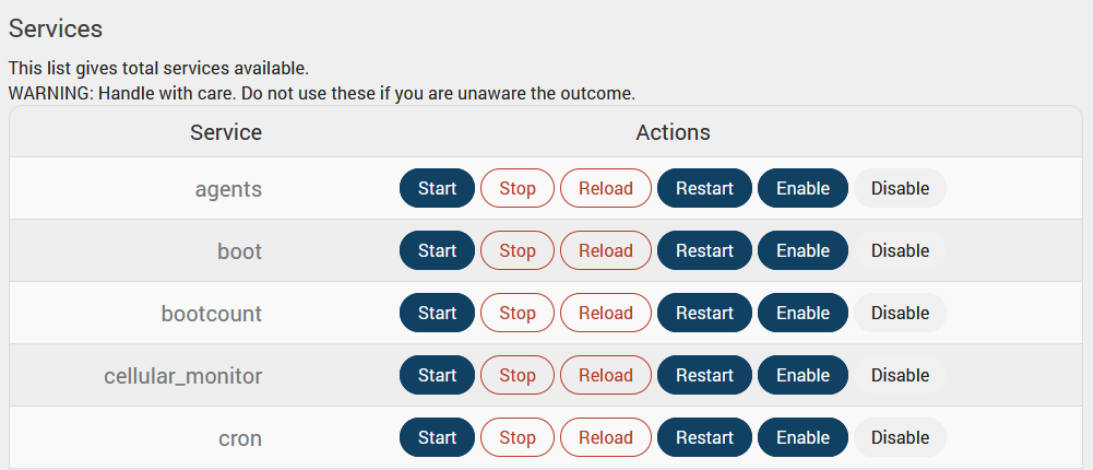


Figure 9.18-1: Service Actions

9.19 Events

Services > Events

E210 and E220 routers are equipped with two digital inputs/outputs (I/O). Digital inputs range is 3V to 24V and the same input pins are also available to be used as open collector digital output with maximum 200mA @ 24V. The Event Management page allows you to map actions to events respective to the digital I/Os.

9.19.1 Event Management

Services > Events

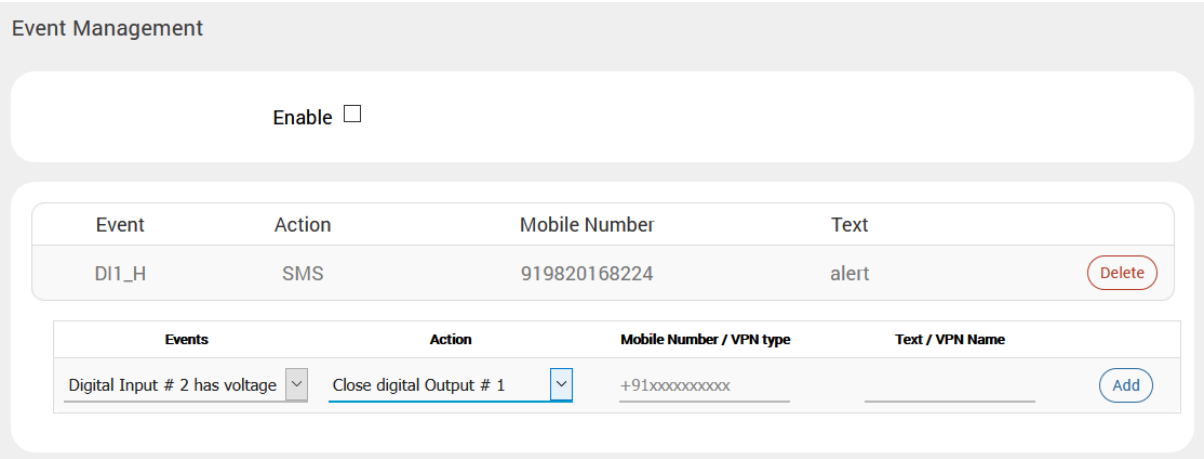


Figure 9.19-1: Event Service Configuration

Parameters	Description
Event Management	
Enable	Click to enable the events
Event	Select the event from the available options DIO is by default are pulled up to high voltage level.
Action	Select the action from options. *Close/Open digital Output # 1/2 – to close or open the digital pin* *Start VPN – start VPN* *Stop VPN – stop VPN* *SMS – to send the event details using the SMS.* *Switch Digital Output – Change the state of Digital Output* *Reboot – To reboot the router.* *POWER_SAVEMODE_ON* *POWER_SAVEMODE_OFF*
Mobile Number/VPN Type	Enter the mobile number. The mobile number format must be: <countrycode><phonenumber>. If the action is to start or stop the VPN, then enter the type of the

Parameters	Description
	VPN such as ipsec, pptp, l2tp, or openvpn.
Text/VPN Name	Enter the text message that will be sent to the configured mobile number in case of event occurs. If the action is to start or stop the VPN, then enter the VPN instance name.

Table 9.19-1: Event Service Configuration

9.20 GSM Update

Services>GSM Update

The GSM Update feature allows you to remotely upgrade the cellular module firmware and VOLTE Patch. You can use **Lantronix Server** or **Custom Server** as the source for available firmwares.

9.20.1 Lantronix Server

Service>GSM Update>Lantronix Server

This page allows you to check for available firmware and to upgrade the firmware from the Lantronix D2Sphere server.

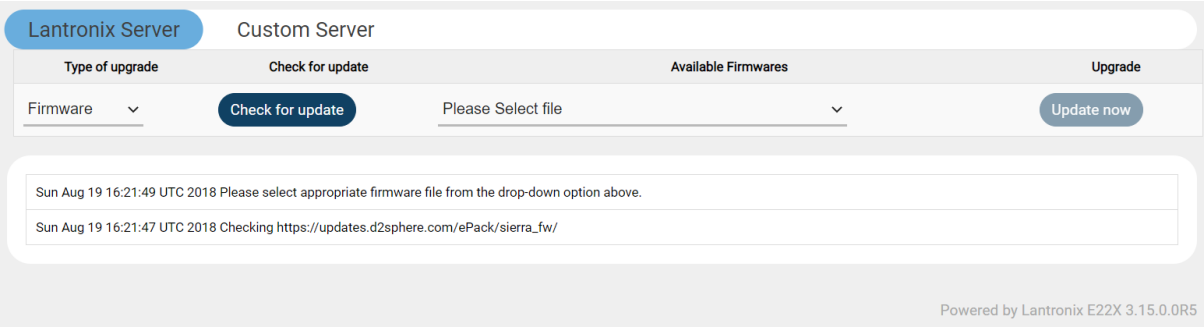


Figure 9.20-1: GSM Update Lantronix Server

Parameters	Description
Type of Upgrade	Select the type of upgrade. • *Firmware* • *Volte Patch*
Check for update	Click to check for available updates on D2Sphere.
Available Firmware	Displays a list of firmwares for the cellular module, available on the server. Select the firmware from this list.
Upgrade	click **Update now** to upgrade the router.
Upgrade/Downgrade	Click **Update now** to download the firmware selected in the Available Firmware list.

Table 9.20-1: GSM Update configuration for Lantronix Server

9.20.2 Custom Server

Services>GSM Update>Custom Server

This page allows you upgrade the router firmware from a custom server.

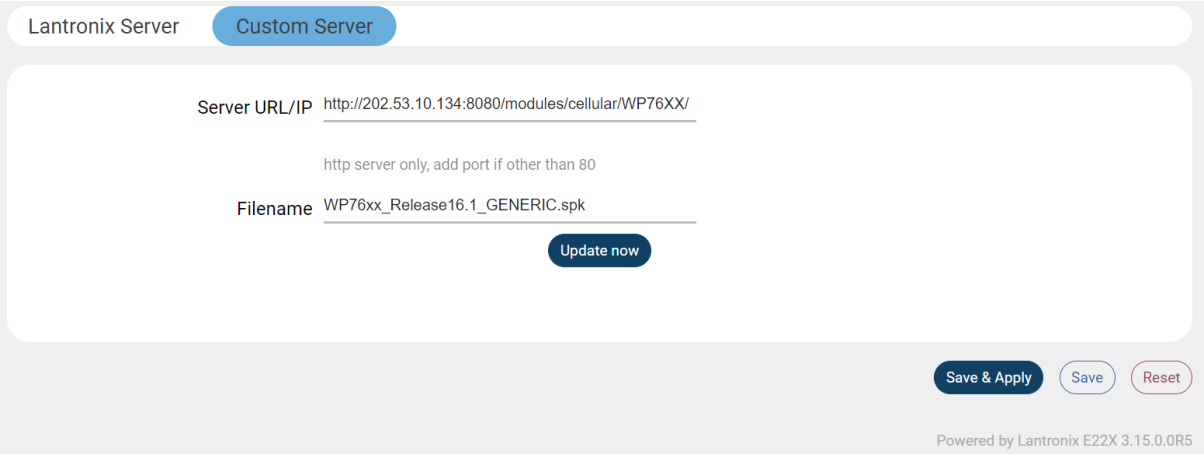


Figure 9.20-2: GSM Update Custom Server

Parameters	Description
Server URL/IP	Enter URL/IP of the custom server
Filename	Add the required firmware version. Click **Save & Apply** and then click **Update now**.

Table 9.20-2: GSM Update configuration for Custom Server

Note:
GSM update can also be triggered using SMS by sending the SMS AT+MODULEDOTA command from a registered mobile number. For custom server use the command AT+MODULEDOATSETTINGS after setting the configuration from the Web UI (shown above). See Figure 9.12-2 for syntax details.

9.21 uHTTPd

uHTTPd is the standard web server that runs the web interface and provides support for multiple instances, TLS (SSL), and other web server features.

9.21.1 General Settings

Services > uHTTPd > General Settings

The uHTTPd Main instance is provided by default and is used for configuring the router. You can create new instances and configure the server settings by clicking the **Add** button.

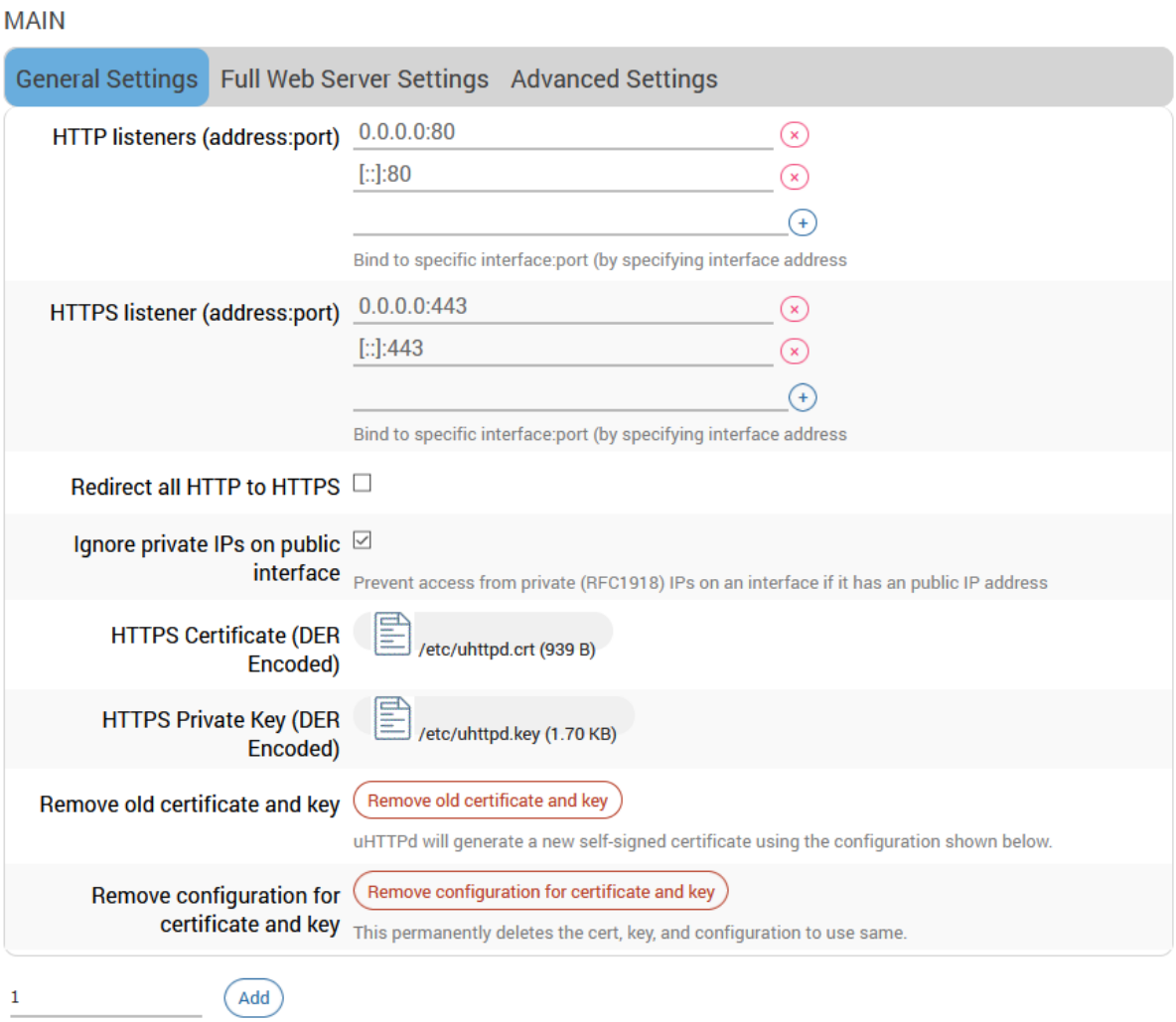


Figure 9.21-1: uHTTPd Service General Settings Configuration

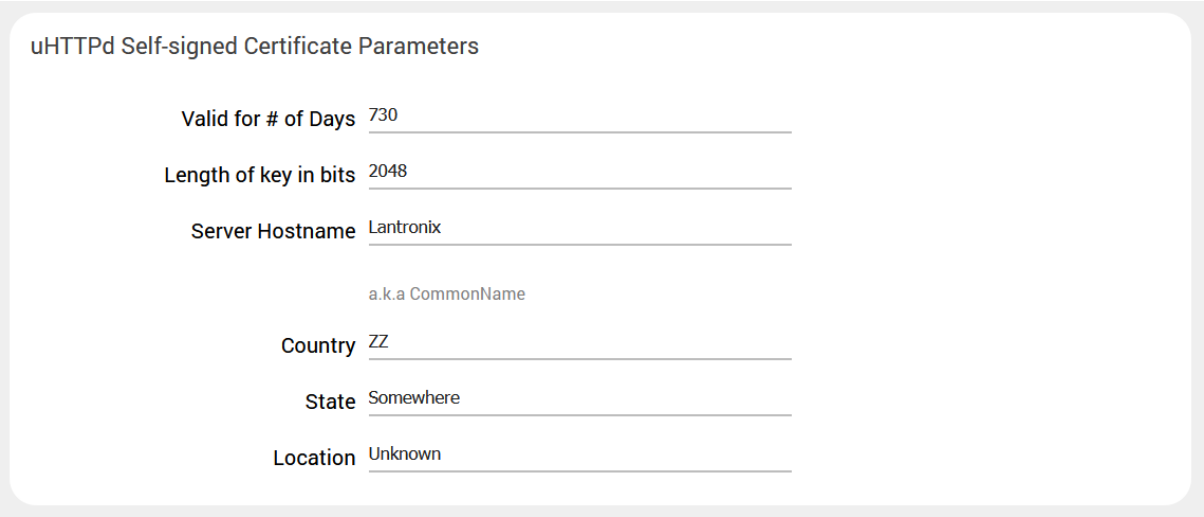


Figure 9.21-2: uHTTPd Self-signed Certificate Configuration

Parameters	Description
MAIN	
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.
Add	Click to add another instance.
uHTTPd Self-signed Certificate Parameters	
Valid for # of Days	Enter the validity time (number of days) of the generated certificate. Default: 730 days

Parameters	Description
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

Table 9.21-1: uHTTPd Service General Configuration

9.21.2 Full Web Server Settings

Services > uHTTPd > Full Web Server Settings

Full Web Server Settings provide additional configuration for the uHTTPd service.

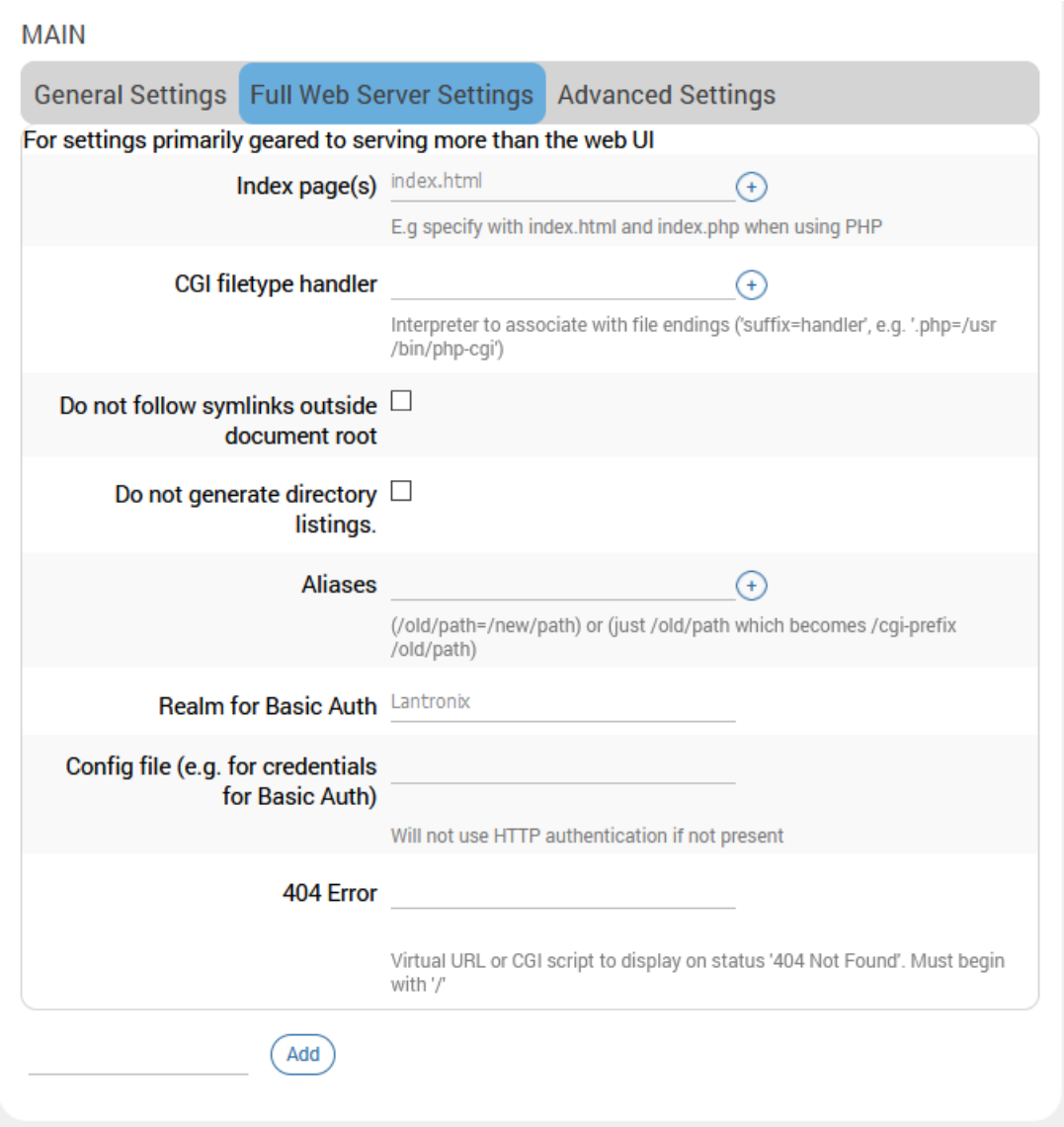


Figure 9.21-3: uHTTPd Service Full Web Server Configuration

Parameters	Description
MAIN	
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.

Parameters	Description
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. 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 '/'.
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

Table 9.21-2: uHTTPd Service Full Web Server Configuration

9.21.3 Advanced Settings

Services > uHTTPd > Advanced Settings

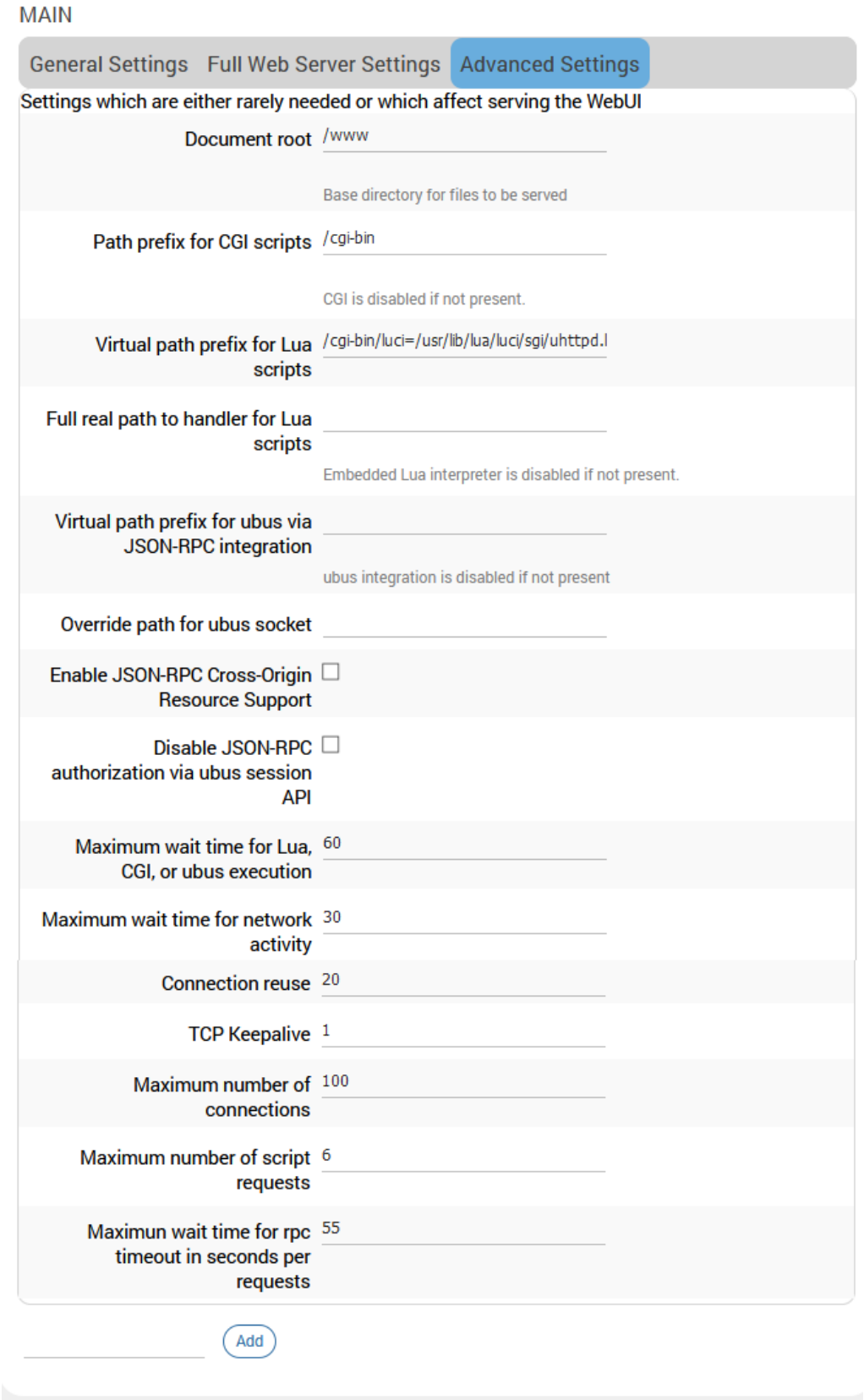


Figure 9.21-4: uHTTPd Service Advanced Configuration

Parameters	Description
MAIN	
Document root	Enter the directory path to the server document root. By default the 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.
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	Enter the maximum wait time for RPC timeout in seconds. Default: 55

Parameters	Description
requests	
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

Table 9.21-3: uHTTPd Service Advanced Configuration

9.22 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 status and validity. This page allows you to perform the following actions related to certificates:

- Add – Add a new certificate.
- Edit – Edit a certificate.
- Delete – Delete a certificate.
- Enroll – Enroll a newly created certificate.
- Renew – Renew an expired certificate.

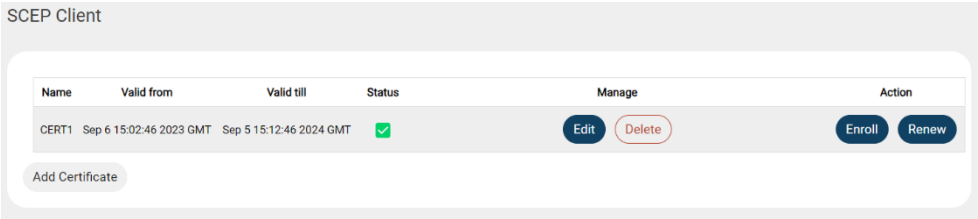


Figure 9.22-1: SCEP Client Page

Click **Add Certificate** to create a new certificate.

9.22.1 Certificate Details

Services > SCEP Client > Add Certificate

The **Certificate Details** page displays.

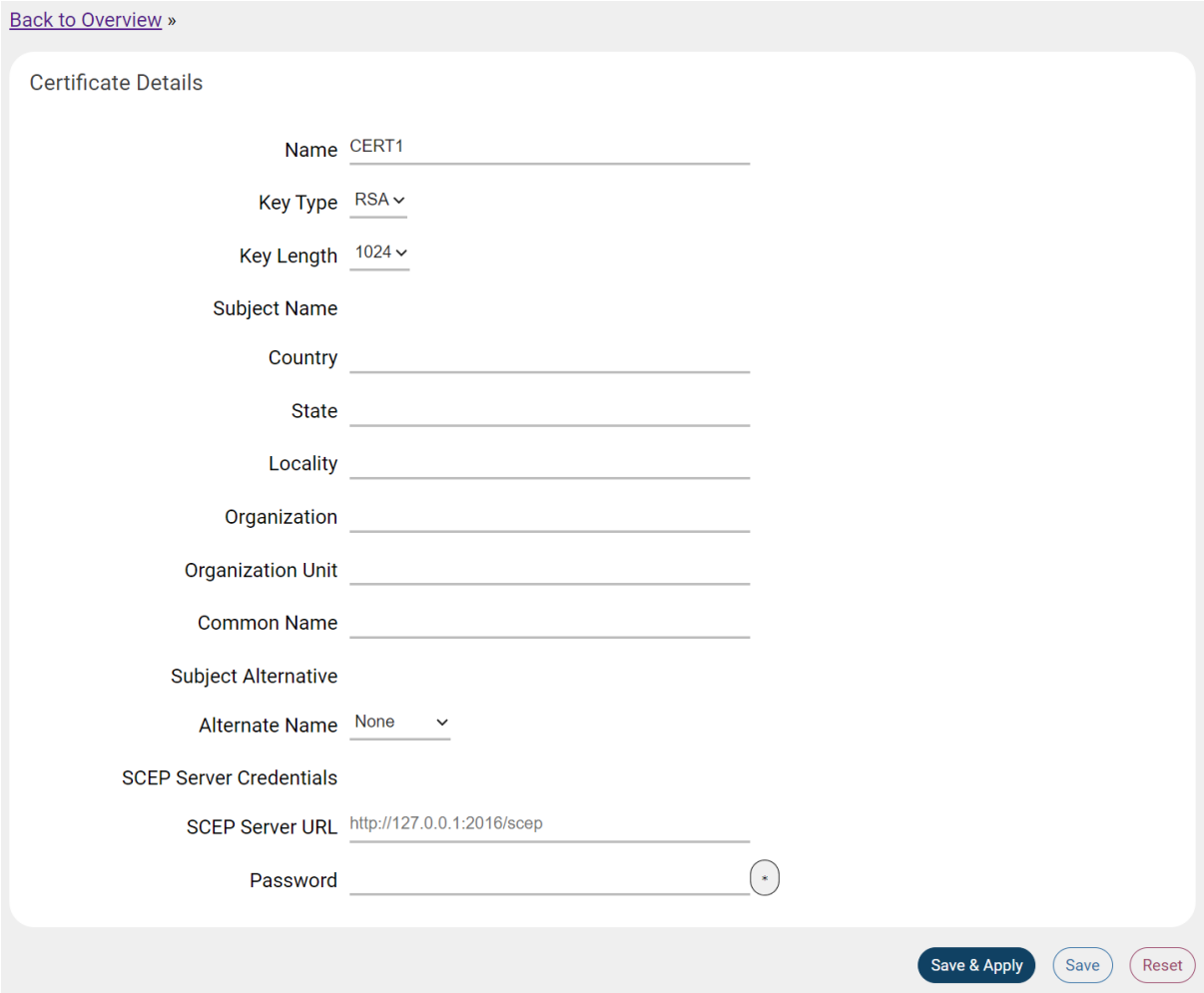


Figure 9.22-2: SCEP Client Certificate Details

Parameters	Description
Name	Enter a name for the certificate.
Key Type	Select key type: *RSA (default)*
Key Lenth	Select key length: *768* *1024 (default)* *2018* *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.
Organization	Enter organization name.
Organization Unit	Enter organization unit name.

Parameters	Description
Common Name	Enter a common name.
Subject Alternative	
Alternate Name	Select an alternate name: *Cert IP* *Cert DNS* *Cert Email* *None (default)*
SCEP Server Credentials	
SCEP Server URL	Enter the URL for SCEP server.
Password	Enter SCEP server password.

Table 9.22-1 : SCEP Client Certificate Details Configuration

Note: The Subject Name is a combination of the fields under it. The Subject Name should be unique for every certificate.

Once you enter values for all the fields, click **Save & Apply**. The new certificate displays on the **SCEP Client** page.

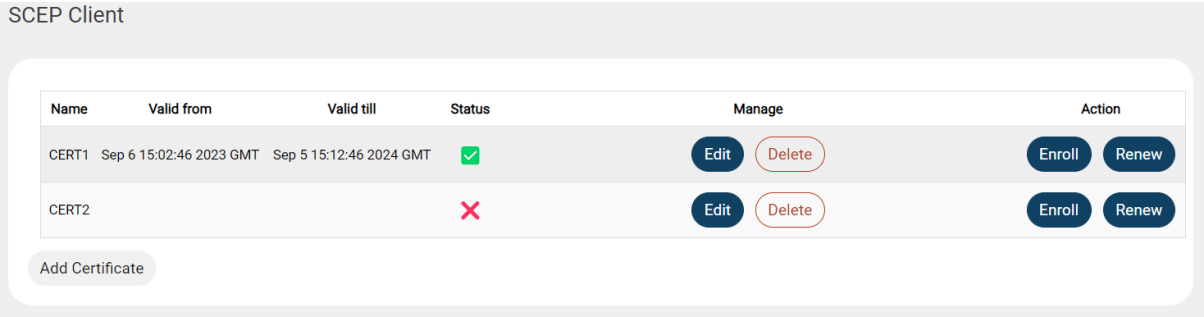


Figure 9.22-3: SCEP Client page with new certificate

Click **Enroll**. The **Certificate Enrolled Successfully** message displays. Click **OK**. The status of the new certificate changes.

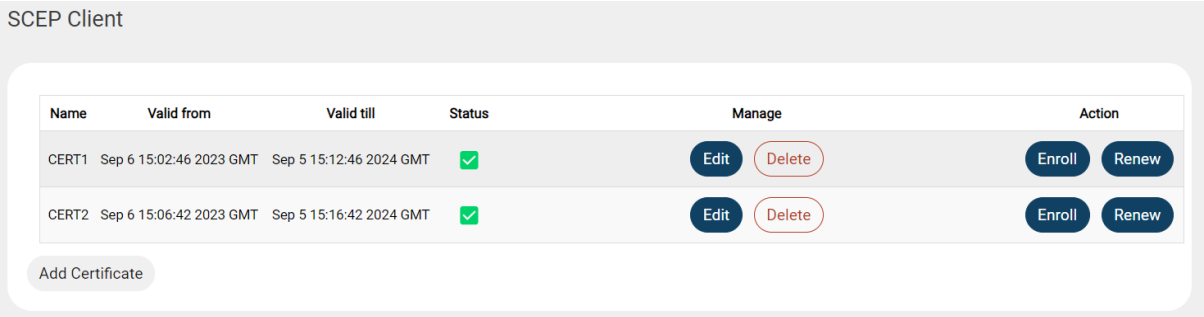


Figure 9.22-4: SCEP Client page with new certificate enrolled

In the case a certificate expires, click **Renew** to renew the certificate.

10 Network

The ePack software provides the administrator several options to customize the Network configurations adhering to the organization's requirements. To configure the Network parameters, the following sub-sections are available:

- Interfaces
- Wireless
- Switch
- DHCP and DNS
- Hostnames
- Static Routes
- Diagnostics
- Firewall
- Load Balancing

10.1 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 protocol assignment, gateway metric, DNS configuration, bridge interface configuration, firewall zone assignment, and DHCP server configuration according to your requirements.

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

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

- CELLULAR
- LAN
- WAN/WAN6
- WWAN/WWAN6

10.1.1 Interfaces Overview

Network > Interfaces

This page provides a summary view of the interfaces on the router and general interface settings.

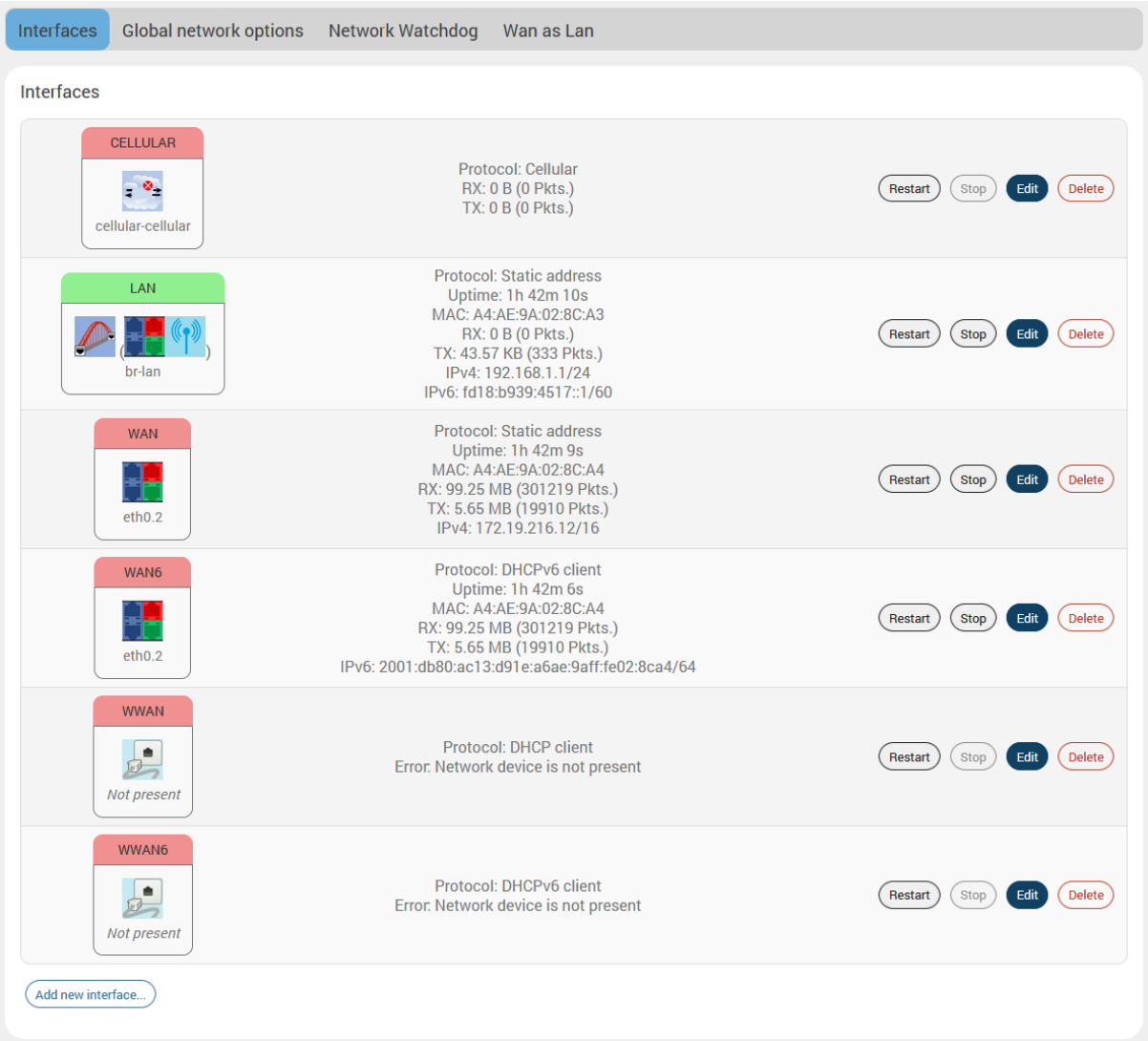


Figure 10.1-1: Interfaces Overview

Parameters	Description
Interfaces Overview	
Network	Displays all the configured Network Interfaces. The default interfaces are: LAN, CELLULAR, WAN, WAN6, WWAN, WWAN6 In addition, it displays any custom interfaces that have been added. ***Note*** • ***When Wi-Fi is configured as Client, Interface WWAN will become active.***
Status	Displays the status of the interface. See Section *10.1.2.*

Parameters	Description
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.* ***Detete*** *– Deletes the interface.* ***Note*** • ***Default interfaces have pre-defined configurations and should not be deleted.***
Add new interface	Click **Add new interface** to add a virtual interface. See Section *10.1.8*.
Global Network Options	
IPv6 ULA-Prefix	Displays the IPv6 Unique Local Address (ULA)-Prefix
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 router 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 router.

Table 10.1-1: Network Interfaces Overview

10.1.2 Interface Status

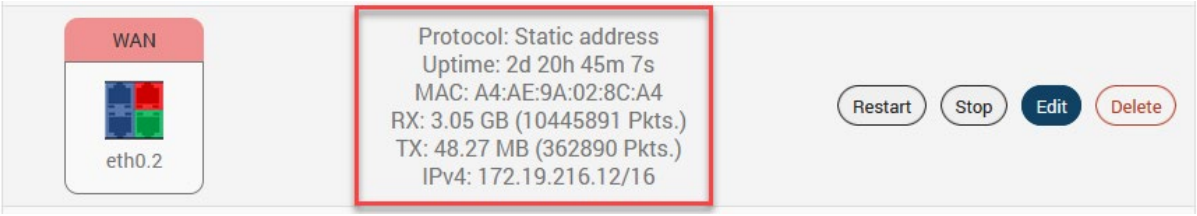


Figure 10.1-2: WAN Interface Status

The Interface Status displays the following details associated to interface:

- **Protocol –** Displays the protocol assigned to the interface.
- **Uptime –** Displays the amount of time that the interface has been active since the last interface connection/reconnection. The format is dd:hh:mm:ss, and is displayed in 24 hour clock format. Uptime is displayed for all active interfaces.
- **MAC-Address –** MAC Address of the physical interfaces.

Note

- ***MAC Address is displayed for LAN, WAN, WWAN and OpenVPN interfaces.***

- **RX –** Amount of data received in bytes over an Interface. RX is displayed for all the interfaces for a particular session.
- **TX –** Amount of data transmitted in bytes over an Interface. TX is displayed for all the interfaces for a particular session.
- **IPv4 –** Displays IPv4 Address of the interface.
- **IPv6 –** Displays IPv6 Address of the interface.

10.1.3 Interface Protocols

The **Protocol** field on the **Edit Interface > General Settings** page allows assigning the protocol with respect to the router model number. Table 10.1-2 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.

Interface → / Protocols ↓	LAN	WAN	WWAN	Cellular
Static Address	✓	✓	✓	✗
DHCP client	✗	✓	✓	✗
DHCPv6 client	✗	✓	✓	✗
GRE	✗	✗	✗	✗
L2TP	✗	✗	✗	✗
Unmanaged	✓	✓	✓	✗
PPP	✗	✗	✗	✗
PPPoE	✗	✓	✗	✗
PPtP	✗	✗	✗	✗
Cellular	✗	✗	✗	✓
QMI Cellular	✗	✗	✗	✓
Relay Bridge	✗	✗	✗	✗

Table 10.1-2: Network Interface Protocols

The protocols should be assigned to interfaces as shown in *Table 10.1-2* based on how the user wants the interfaces to work. The interface requires additional selection or configuration of settings such as default gateway, gateway metric, DHCP server, and firewall zone to name a few. These settings may be mandatory, optional, or not used by the interface; the interface configuration depends on both the protocol selected as well as the organization's requirements.

Please review the following before configuring the LAN, WAN, and WWAN interfaces.

- If any two interfaces in Table 11.1-2 have the same protocol (for example, Static Address is assigned to LAN and WAN interfaces), the settings for configuring the interface will be nearly the same. For this reason, the protocols are described below. Refer to Sections *10.1.3.1* to *10.1.3.6* for descriptions of the protocol settings.

- The LAN interface should use Static Address. On the LAN interface, the Gateway is not required and DHCP server is optional, It can be used if you want the router (DHCP server) to dynamically assign IP addresses to clients connecting to the LAN.
- WAN and WWAN interfaces should use either Static Address, DHCP client, or DHCPv6 client. WAN also supports using PPPoE protocol. On the WAN and WWAN interfaces with Static Address as the assigned protocol, gateway is required for external interface, but it is not used for internal use. On the WAN and WWAN interfaces, the DHCP server should be disabled ("Ignore interface" will be selected).

All the other protocols listed in *Table 10.1-2* are supported after you add a virtual interface based on the requirement. For example, if an L2TP VPN is set up, a virtual interface with L2TP protocol should be used to configure the L2TP VPN connection. For descriptions on these protocols, see Section *10.1.8 Add Virtual Interface*.

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

10.1.3.1 Static Address

The following table describes the 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 Router. The default IP Address is 198.162.1.1 for LAN.
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.*

Parameters	Description
	IPv6 routed prefix - *Enter the public prefix to direct the client distribution to the router.* 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.
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 Server - DHCP Server is used only for LAN interfaces	
DHCP > General Setup	
Ignore Interface	Check to disable the DHCP interface.

Parameters	Description
	Note • ***If DHCP server is disabled for the interface, all the LAN devices connected to the router should have a static LAN IP configured.***
Start	Lowest leased address as offset from the network address. ***Example*** • ***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 which the device can use the DHCP server leased IP Address. ***Note*** • ***IP address allocated by the router will disappear from the Wi-Fi / Overview / Associates 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.
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.

Parameters	Description
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	If ticked 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.

Table 10.1-3: Static Address Protocol Settings

10.1.3.2 DHCP Client

The following table describes the 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 router
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 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

Parameters	Description
	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.

Table 10.1-4: DHCP Client Protocol Settings

10.1.3.3 DHCPv6 Client

The following table describes the 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

Parameters	Description
	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 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.

Table 10.1-5: DHCPv6 Client Protocol Settings

10.1.3.4 PPPoE

The following table describes the PPPoE protocol settings.

Parameters	Description
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 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.
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*

Parameters	Description
	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.

Table 10.1-6: PPPoE Protocol Settings

10.1.3.5 Cellular

The following table describes the Cellular protocol settings.

Parameters	Description
General Settings	
Protocol	Cellular - CDMA, UMTS, or GPRS connection using an AT-style 3G *modem*
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 cellular network.
Cellular Module	Displays the Cellular module
Modem device	Displays the cellular modem device
Service Type	Select the cellular service type to use or select Automatic to let the device use the best available network
IP Protocol	Select from IPv4, IPv4 + IPv6, or IPv6.
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 on PPP link	Click to enable IPv6 negotiation on PPP link.
Modem init timeout	Enter the maximum wait time in seconds for the modem to

Parameters	Description
	become ready. The default modem initiation timeout 20 seconds.
Use default gateway	Click to configure a default gateway route. None of the gateway routes are configured by default.
Use gateway metric	Enter the gateway metric. The default metric is 5.
Use DNS servers advertised by peer	For Cellular protocol only. Select the box to use DNS servers advertised by peer.
MTU Size/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
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.
SIM Settings (E220 series) or SIM1/SIM2 Settings (E210 series)	
PDP Type	Enter the IP stack mode as IPv4, IPv6, or IPv4/IPv6 (dual stack).
Service Type	Select the cellular service type to use or select Automatic to let the device use the best available network.
APN	Enter the Access Point Name provided by the cellular network operator.
PIN	Enter the PIN of 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, PAP/CHAP, CHAP (these require username and password) or None
Enable roaming	Enable data roaming on the cellular interface
Cid	Only on E220 series. Enter Cid value or leave as default

Table 10.1-7: Cellular Protocol Settings

10.1.3.6 QMI Cellular

The following table describes the 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 cellular network through epack router.
Modem device	Displays the modem device
Primary SIM	Only available on E210 series devices that have dual SIM support. SIM1 or SIM2
Retries	Only available on E210 series devices that have dual SIM support. Enter the number of retry attempts to make on the primary SIM before switching to the secondary SIM in case of data connection failures. After the retry limit has been reached, the device will connect via the secondary SIM.
Period after which the router will try and return to primary SIM	Only available on E210 series devices that have dual SIM support. 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.
Routine switch to secondary SIM	Only available on E210 series devices that have dual SIM support. 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 on PPP link	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.
Use default gateway	Click to configure a default gateway route.

Parameters	Description
	None of the gateway routes are configured by default.
Use gateway metric	Enter the gateway metric. The default metric is 5.
MTU Size/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
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.
SIM Settings (E220 series) or SIM1/SIM2 Settings (E210 series)	
PDP Type	Enter the IP stack mode as IPv4, IPv6, or IPv4/IPv6 (dual stack).
Service Type	Select the cellular service type to use or select Automatic to let the device use the best available network.
APN	Enter the Access Point Name provided by the cellular network operator.
PIN	Enter the PIN of 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, PAP/CHAP, CHAP (these require username and password) or None
Enable roaming	Enable data roaming on the cellular interface
Cid	Enter Cid value or leave as default

Table 10.1-8: QMI Cellular Protocol Settings

10.1.4 CELLULAR Interface

Network > Interfaces > CELLULAR

This page allows you to configure the Cellular interface parameters. Actual parameters may differ based on your router model number. When the Cellular interface is first enabled or when the router is factory reset, the router detects the GSM module and assigns the appropriate protocol. The protocol can be either Cellular for Sierra HL GSM modules or QMI Cellular for Sierra WP GSM modules.

Interface configuration settings will vary depending on the assigned protocol. For descriptions of the Cellular protocol and QMI Cellular protocol settings, see Section *10.1.3.5* and Section *10.1.3.6*, respectively.

To edit the interface:

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

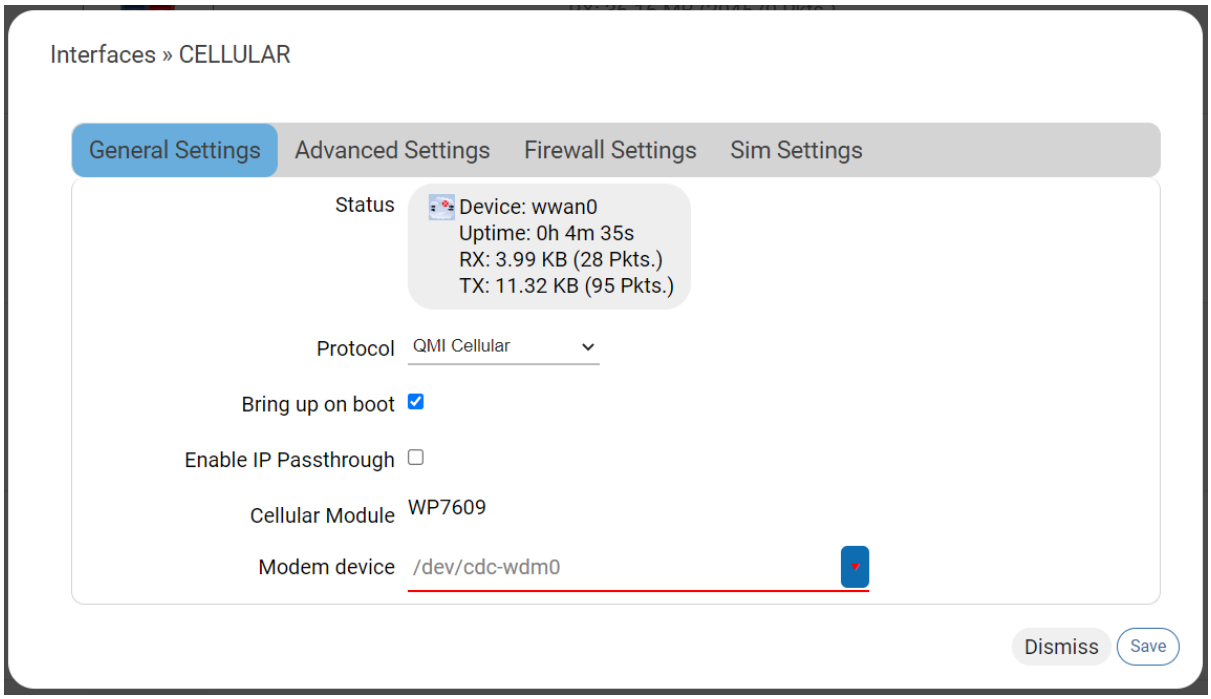


Figure 10.1-3: Cellular Interface General Settings

2. Configure the interface settings respective to the router model number.
   a. See Section *10.1.3.5* for Cellular or Section *10.1.3.6* for QMI Cellular protocol settings.
   b. **General Settings** - Protocol should not be changed for the cellular interface.
   c. **Firewall Settings** - Firewall zone should be set as WAN zone.
   d. **SIM Settings** – For E210 series models that support dual SIM, two SIM settings tabs will be displayed. See the figure below. For devices that support only a single SIM, one SIM Settings tab will be displayed.

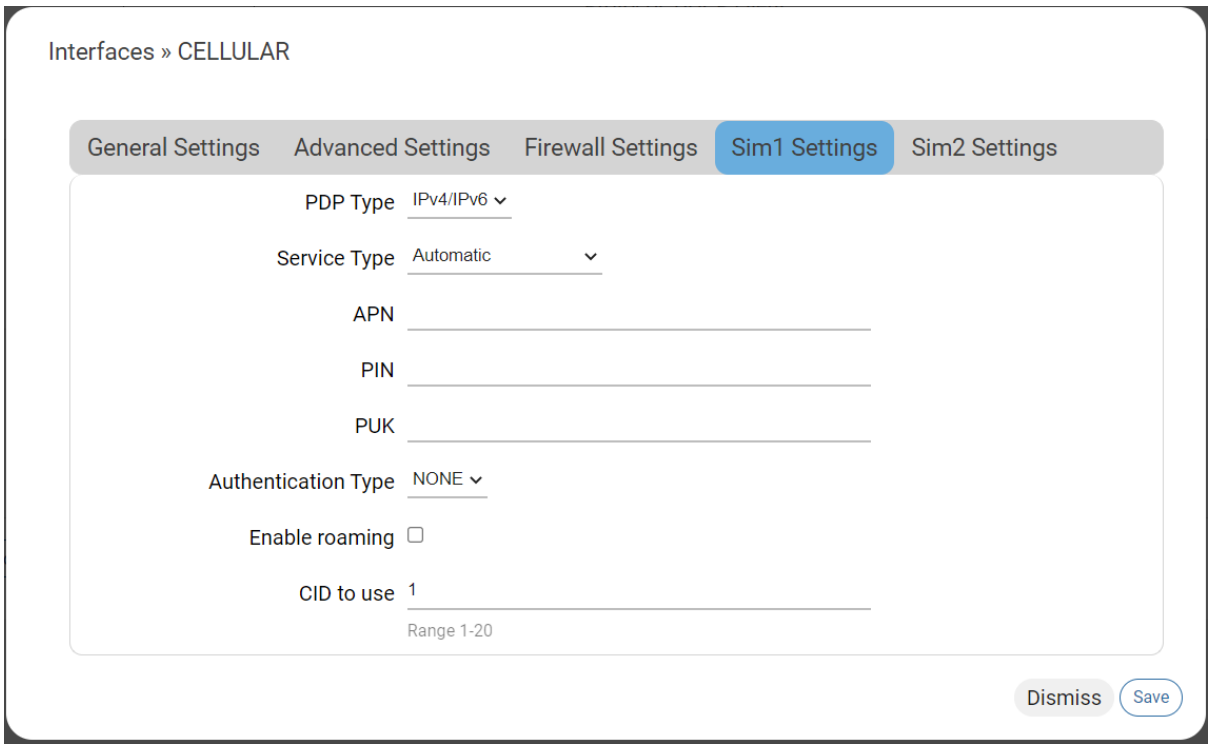


Figure 10.1-4: Cellular Interface SIM Settings

3. Click **Save**.
4. On the Network Interfaces overview page, click **Save & Apply** to save the configuration on the router.

10.1.5 LAN Interface

Network > Interface > LAN

This page allows you to configure the LAN interface with respect to the router model number.

The LAN interface should use Static Address. Gateway 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 router should have a static LAN IP configured.

DHCP Server

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, and 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.

The router acts as the DHCP server and assigns the IP Address to device(s) connected to the network.

Interface configuration settings are determined mainly by the protocol selection. For a description of the Static Address protocol settings, see Section *10.1.3.1.*

To edit the interface:

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

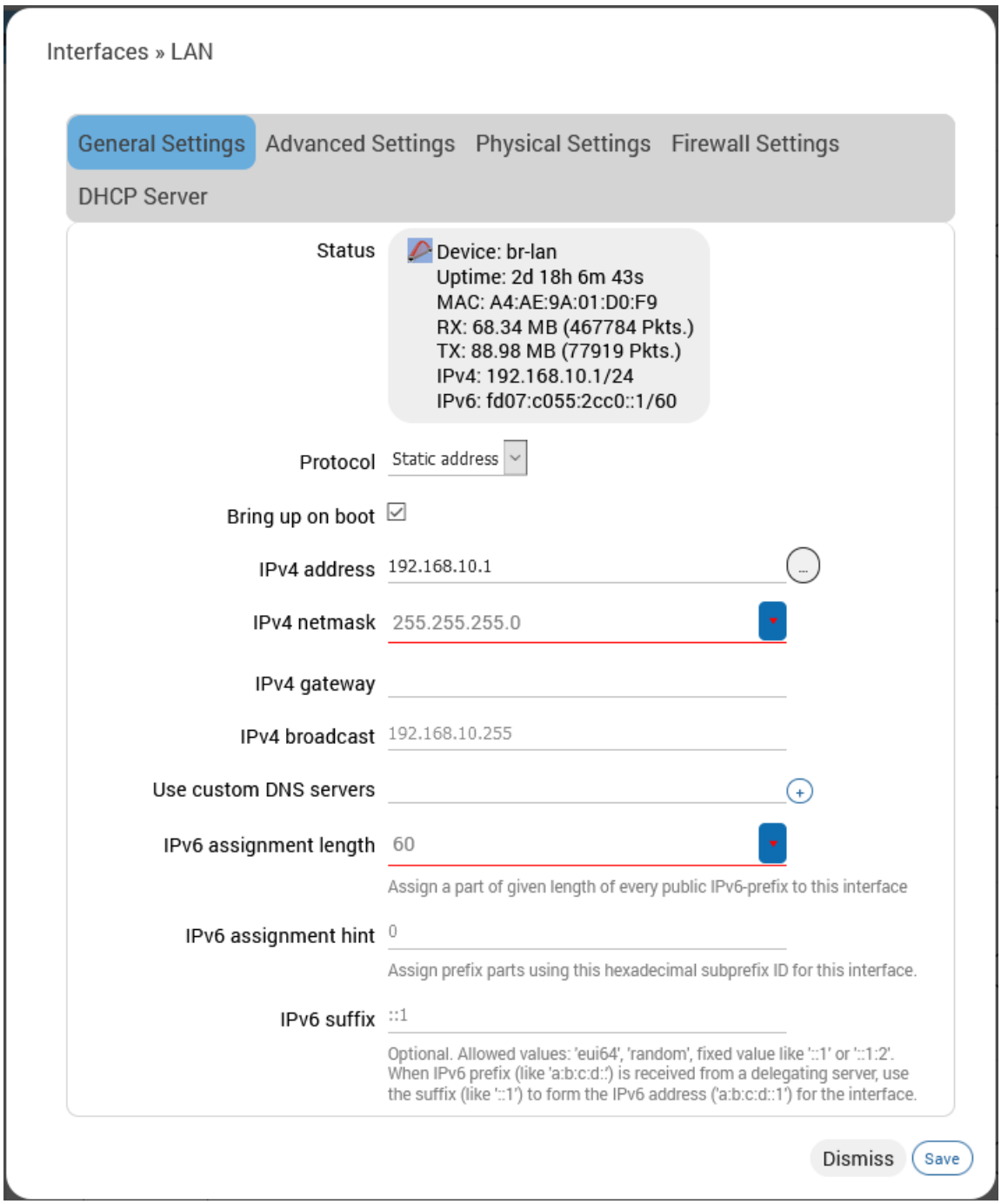


Figure 10.1-5: Lan General Settings

2. Configure the interface settings respective to the router model number.
   a. See Section *10.1.3.1* for Static Address protocol settings.
   b. **General Settings** – Protocol should be Static Address for the LAN interface. Gateway is not required.
   c. **Physical Settings** – By default, the LAN interface bridges the eth0.1 and wlan0 physical interfaces.

d. **Firewall Settings** - Firewall zone should be set as LAN zone.

e. **DHCP Server** – DHCP server may 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. On the Network Interfaces overview page, click **Save & Apply** to save the configuration.

10.1.6 WAN and WAN6 Interface

Network > Interface > WAN or WAN6

This page allows you to configure the WAN and WAN6 interface parameters.

WAN interface supports IPv4 or dual mode IPv4/IPv6. WAN6 interface supports IPv6 mode. Otherwise, the WAN and WAN6 interfaces provide similar functionality and are configured in a similar manner.

The WAN or WAN6 interface will use either Static Address, DHCP client, DHCPv6 client, or PPPoE protocol. 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.

The interface configuration parameters will depend on the assigned protocol. For descriptions of the Static Address, DHCP Client, or PPPoE protocol settings, see Section *10.1.3.1*, Section *10.1.3.2*, or Section *10.1.3.4*, respectively. For DHCPv6 Client, see Section *10.1.3.3*.

To edit the interface:

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

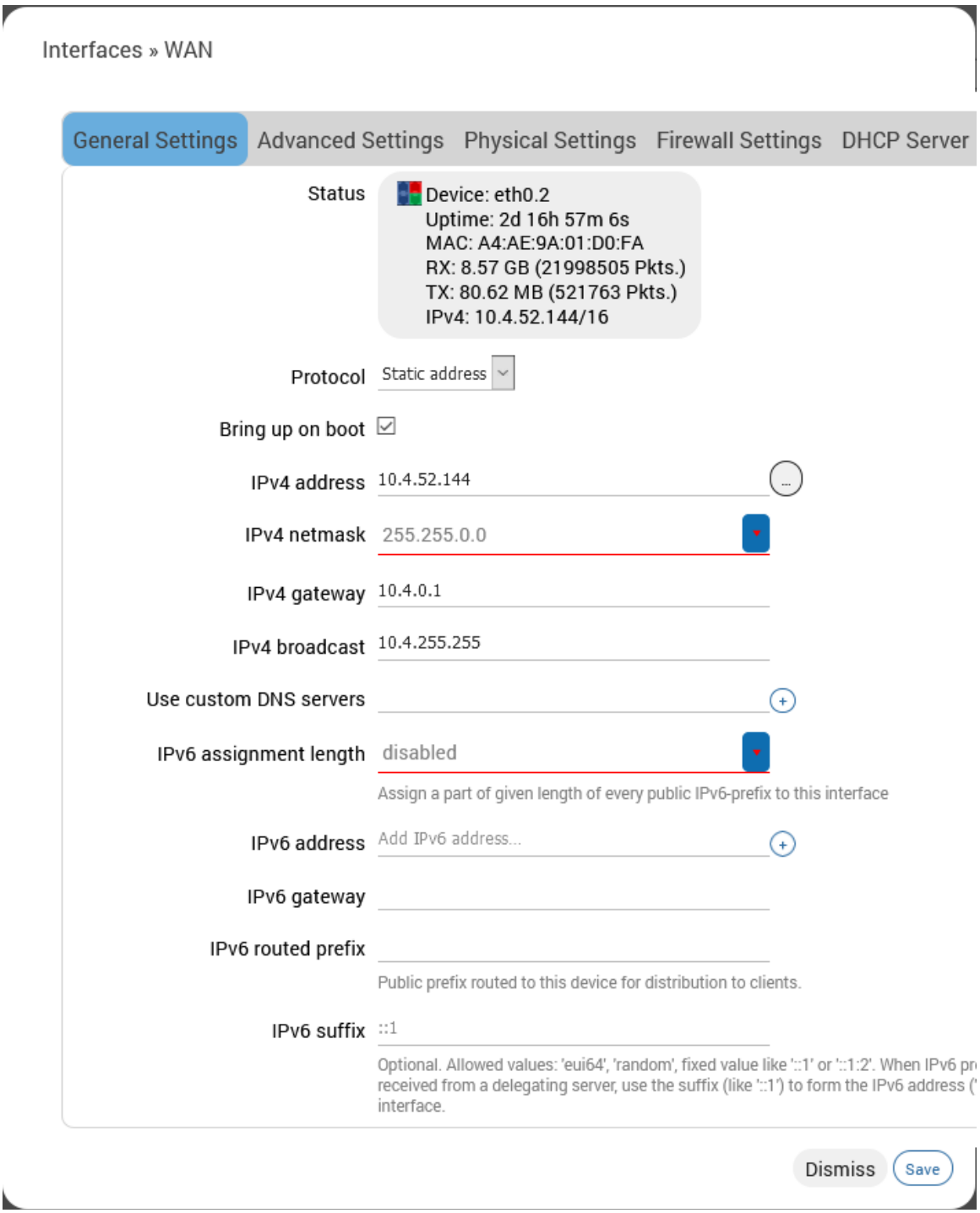


Figure 10.1-6: WAN Interface (Static Address)

2. Configure the interface settings respective to the router model number.

   a. See Section *10.1.3.1* for Static Address, Section *10.1.3.2* for DHCP client, or Section *10.1.3.4* for PPPoE protocol settings.

   b. **General Settings** – To update the WAN protocol, select the protocol and click the **Switch Protocol** button. IPv4 gateway is required for external interface but should not be used for internal use.

c. **Firewall Settings** - Firewall zone should be set as WAN zone.

d. **DHCP Server** – DHCP server should be disabled. Make sure to select "Ignore Interface."

3. Click **Save**.
4. On the Network Interfaces overview page, click **Save & Apply** to save the configuration.

10.1.7 WWAN and WWAN6 Interface

Network > Interface > WWAN or WWAN6

This page allows you to configure the WWAN and WWAN6 interface parameters. When the Wireless interface is configured as Client, the WWAN interface will become active.

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 Static Address, DHCP Client or DHCPv6 Client, see Section *10.1.3.1,* Section *10.1.3.2*, or Section *10.1.3.3,* respectively.

To edit the interface:

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

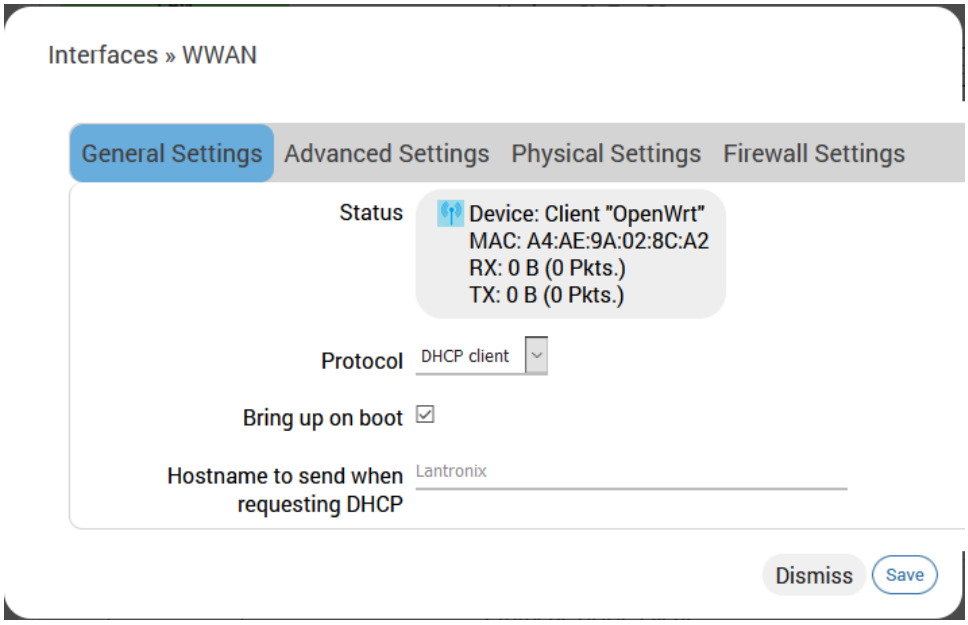


Figure 10.1-7: WWAN General Settings

2. Configure the interface settings respective to the router model number.
   a. See Section *10.1.3.1* for Static Address or Section *10.1.3.2* for DHCP protocol settings.
   b. **General Settings** – To update 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.

c. **Advanced Settings** - Similar to WAN DHCP settings, except the metric is fixed by default for other features to work as per requirement.
d. **Firewall Settings** - Firewall zone should be set as WAN zone.
e. **DHCP Server** – DHCP server should be disabled. Make sure to select "Ignore Interface."

3. Click **Save**.
4. On the Network Interfaces overview page, click **Save & Apply** to save the configuration.

10.1.8 Add Virtual Interface

You can create a virtual network interface to configure a VPN tunnel that encapsulates data inside a transport protocol. GRE, L2TP, PPP, and PPtP, are examples of tunneling protocols that the ePack software supports.

In general, virtual interfaces can also be used for other reasons, such as to configure a relay bridge to extend the wireless network or for VLANs (see Section *10.3 Switch*).

Note

- ***Adding a virtual interface may require complex configuration modifications in the load balancer settings. For more details, please visit Lantronix Technical Support.***

To add a new interface:

1. Go to **Networks > Interfaces**, and click **Add new interface** below the list of existing interfaces.
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** to create the interface.
5. Configure the interface settings relative to the selected protocol.
    a. The first field below the protocol selection is **Bring up on boot**. This is enabled by default and will start the interface when the router is booted.
    b. For the remaining configuration details, refer to *Table 10.1-9: Tunnel Protocols Configuration*.
6. Click **Save** to save the new interface.
7. Click **Save & Apply** to apply the configuration to the router.

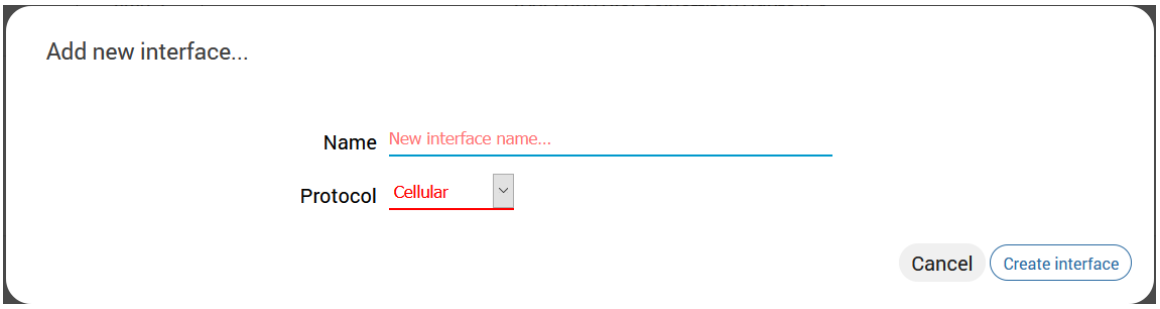


Figure 10.1-8: Add New Interface

Protocol	Parameters
GRE	GRE point-to-point tunnel over IPv4 **General Settings** ***Bring up on boot*** *– Start the interface when the device is*

Protocol	Parameters
	booted. Selected by default. ***Enable GRE tunnel** – Enable GRE on 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 router* ***Local Tunnel Address** – Enter the local IP address of the router 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.* **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.* **Firewall Settings** *Select the WAN zone as the firewall zone.*
L2TP	PPP over L2TP pseudowire tunnel **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.* **Advanced Settings** Advanced settings are similar to those of PPPoE with a few exceptions as noted below. See Section 10.1.3.6 for a description of the configuration. *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*. **Firewall Settings** *Select the WAN zone as the firewall zone.*
PPP	PPP protocol for dialup modem connections **General Settings**

Protocol	Parameters
	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.* **Advanced settings** Advanced settings are similar to those of PPPoE. See Section 10.1.3.6 for a description of the configuration. **Firewall Settings** *Select the WAN zone as the firewall zone.*
PPtP	Point to Point Tunneling Protocol (PPtP) VPN **General Settings** ***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.* **Advanced Settings** Advanced settings are similar to those of PPPoE. See Section 10.1.3.6 for a description of the configuration. One additional setting is described below: ***Use mppe*** *– Select to enable encryption if this setting is enabled on the remote server.* **Firewall Settings** *Select the WAN zone as the firewall zone.* ***Note:*** • ***Enabling PPtP will also enable a 20mins PPtP watchdog which will reboot the router in absence of an active PPtP connection for a period of 20 mins.***

Table 10.1-9: Tunnel Protocols Configuration

10.1.8.1 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.

10.2 Wireless

Network > Wireless

The Wireless interface on the router can work in different modes:

- **Master mode as a Wi-Fi access point –** The router provides Internet to other host machines in its network over Wi-Fi. It can get Internet connection from WAN or cellular.
- **Client mode as a Wi-Fi client –** The router will act as a client to existing wireless networks. The router will accept the Internet access through wireless access provided by another service provider and then distribute the access to the machines connected to the router on its LAN interface.
- **WDS access point and WDS client modes –** Wireless Distribution System (WDS) allows the interconnection of access points in an IEEE 802.11 network. It allows you to bridge two routers (as WDS access points) wirelessly to extend the Wi-Fi network. WDS client mode allows a router to connect to a WDS access point. WDS with WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK Mixed Mode encryption modes are supported.
- **802.11s mode –** The IEEE 802.11s amendment for mesh networking to the IEEE 802.11 Wireless LAN standard focuses on mechanisms for connecting wireless devices without having to set up infrastructure. The 802.11s mode allows interconnecting routers to implement a mesh network.
- **Ad-hoc and Pseudo Ad-hoc (ahdemo) modes –** Ad-hoc mode is used to allow two stations to communicate directly without an intermediary. Pseudo ad-hoc (ahdemo) mode is a variant of ad-hoc mode. Ad-hoc and pseudo ad-hoc modes were used in earlier implementations of mesh networks, but have been succeeded by 802.11s mesh networks.
- **Monitor mode –** this is a client mode setting in which the wireless interface will listen to all traffic, not just its own.

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

Figure 10.2-1: Wireless Overview

Parameters	Description
Wireless Overview	
Status and Details	Displays the following details: ***SSID –*** *A Service Set Identifier (SSID) is a public identifier of 32 characters that uniquely names a Wi-Fi connection.* ***Mode –*** *Displays the mode of WLAN interface like Access Point Mode or Client Mode.* ***BSSID –*** *Displays Basic Service Set Identification (BSSID); 24 bit MAC Address of Wireless Access Point.* ***Encryption –*** *Displays the data encryption method.* ***Channel –*** *Wi-Fi channel* ***Tx-Power*** *– Transfer power limit* ***Signal Strength –*** *Displays the signal strength in percentage* ***Bitrate –*** *Data transfer rate* ***Country –*** *country code*
Scan	Click to scan and detect the available wireless connections. Scanning must be done when the router is changed from Master mode to client mode.
Restart	Click to restart the radio interface.
Add	Click to add an new network instance.
Enable/Disable	Click to enable or disable the network instance.
Edit	Click to edit the network instance.
Remove	Click to remove the network instance.
Associated Station	
Network	Displays the SSID that the station is connected to.
MAC-Address	Displays the MAC Address of the computers and/or devices that are connected to the router.
Host	Displays the Host name of the computers and/or devices that are connected to the router.
Signal/Noise	Displays the signal strength in dBm. Noise in dBm.
RX Rate/TX Rate	Displays the data transfer rate at which the data is received. Data transfer rate at which the data is transmitted.

Table 10.2-1: Wireless Connection and Associated Stations Overview

10.2.1 Wireless Network Configuration

Network > Wireless > Add/Edit

Wireless network configuration consists of device and interface settings. The wireless device settings specify radio properties such as channel, driver type and power. The wireless interface configuration defines the wireless network settings on top of the wireless device.

10.2.1.1 Device Configuration

Network > Wireless > Add/Edit

The wireless device configuration parameters are shown in the top half of the Wireless Configuration page. The following figure shows an example of the device configuration settings.

General Setup

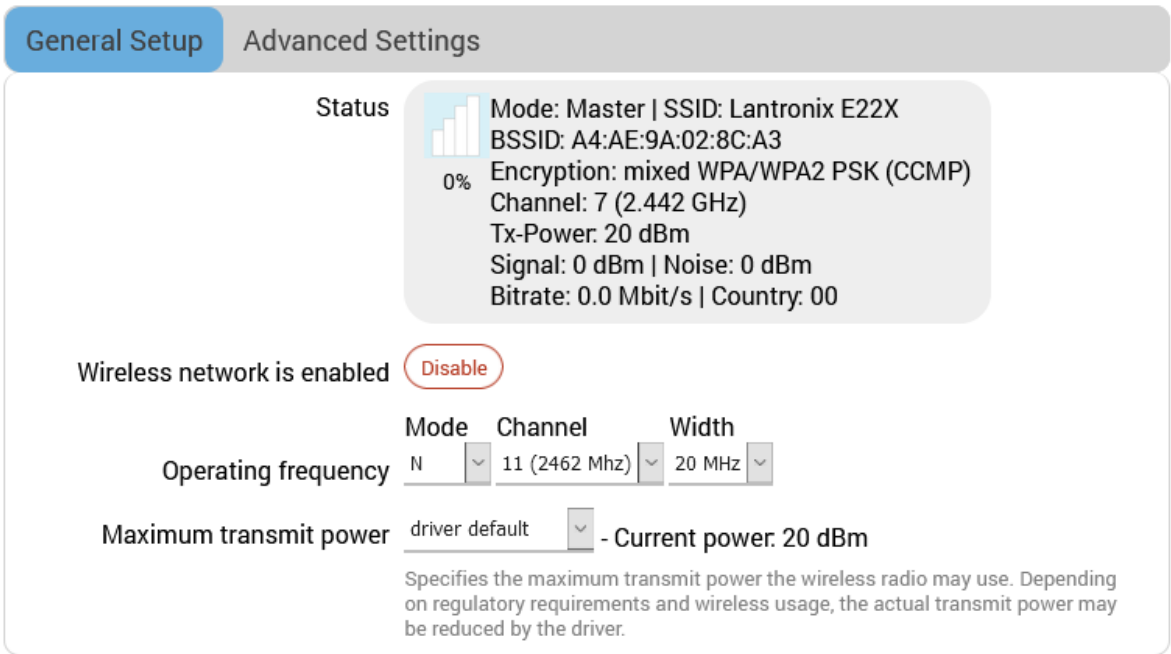


Figure 10.2-2: Wireless Device General Configuration (E228 device)

Parameters	Description
Status	Displays the following details: ***Mode –*** *Displays the mode of the wireless interface.* ***SSID –*** *A Service Set Identifier (SSID) is a public identifier of 32 characters that uniquely names a Wi-Fi connection.* ***BSSID –*** *Displays Basic Service Set Identification (BSSID); 24 bit MAC Address of Wireless Access Point.* ***Encryption –*** *Displays the data encryption method.* ***Channel –*** *Displays the channel and frequency* ***Tx-Power*** *– Displays the transmit power in dBm*

Parameters	Description
	Signal/Noise *– Displays the signal strength and noise in dBm* ***Bitrate/Country*** *– Displays the bit rate and country code*
Wireless network is enabled	This field allows you to enable or disable the network. The label displays either "Wireless network is enabled" or "Wireless network is disabled." Click **Enable** or **Disable** to update the network operation status.
Operating Frequency /Channel	Choose the channel frequency and width from the drop down menu, or choose 'auto', to select it automatically. Channels are defined in 5 MHz increments and are 20 MHz wide, so 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. You may also add a custom channel.
Maximum Transmit Power	Select the transmit power. The default selection is 20dBm or 100mW.

Table 10.2-2: Wireless Device General Configuration

Advanced Settings

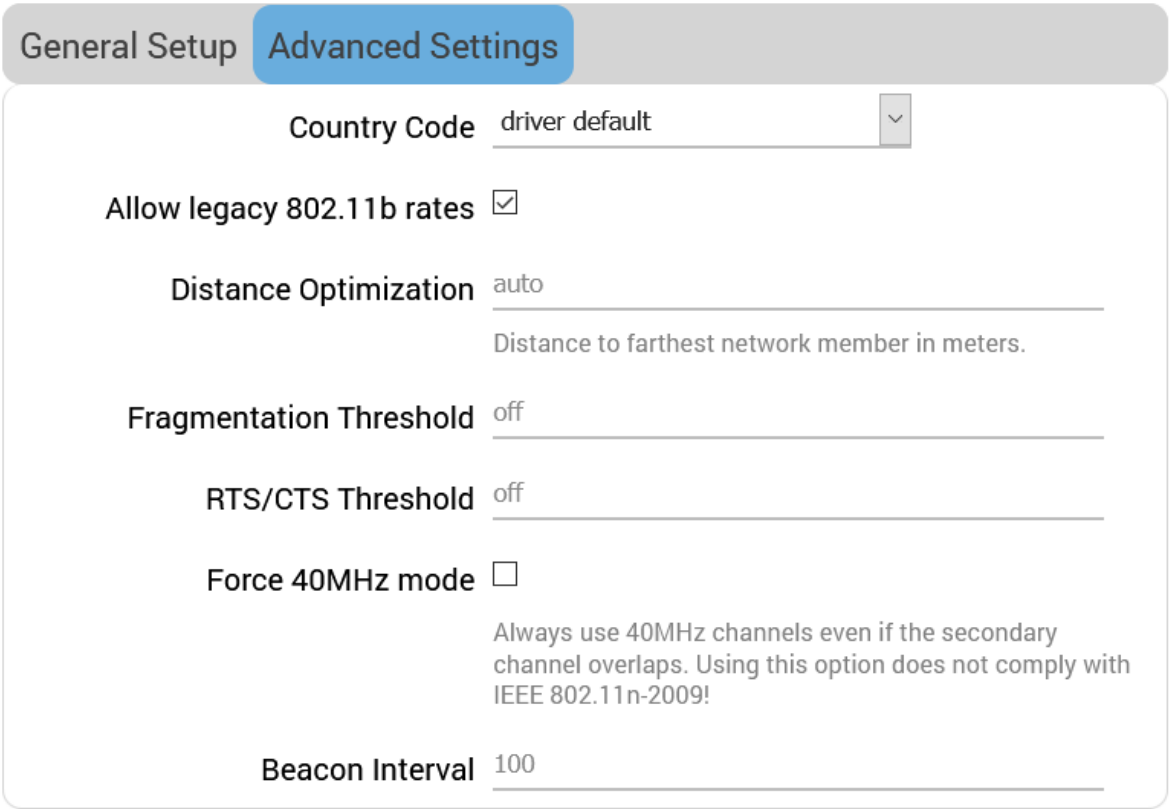


Figure 10.2-3: Wireless Network Device Advanced Configuration

Parameters	Description
Country Code	Choose the country code corresponding to the country where the router is operational. This ensures that the channels available in that country are enabled. You can choose driver default to allow the driver to make the selection. By choosing '00' (World), the router will select the appropriate channel in your country.
Allow legacy 802.11b rates	Select to allow 802.11b rates
Distance Optimization	Displays the distance (in meters) of the farthest machine in your network from the router. Used to optimize the operation of the Wi-Fi network. Default is auto.
Fragmentation Threshold	Displays the Fragmentation threshold value (in number of bytes). Fine-tuning Fragmentation Threshold parameter can result in good throughput but a wrong value can result in low throughput. The range of values is 256 to 2346 bytes. In a noisy environment, a smaller value of Fragmentation Threshold may result in more efficient communication. Default is off.
RTS/CTS Threshold	Displays the RTS/CTS threshold between 0 to 2347 bytes, typical value being 500. This setting is for advanced users. It prevents collision of wireless packets, particularly in case of hidden nodes or in a noisy environment. Default is off. ***Note*** • ***In case of access point setting, it is recommended not to use RTS/CTS threshold.***
Beacon Interval	Displays the interval between each of the beacons sent by the access point. Value is in milliseconds. Default is 100.

Table 10.2-3: Wireless Device Advanced Configuration

10.2.1.2 Interface Configuration

Wireless > Add/Edit

The wireless interface configuration parameters are shown in the bottom half of the Wireless Configuration page. To configure the interface settings, first select the Mode. The Mode and your specific network requirements will determine how you configure the interface settings. In general, the wireless interface mode will be one of the following: access point (master), client, point-to-point or a mesh network. The wireless interface may also operate in monitor mode, in which it simply listens to all wireless traffic, not just its own.

Figure 10.2-4 shows the General Setup tab of the Wireless Interface configuration in Access Point (Master) mode.

Table 10.2-4 shows the configuration parameters for the General Setup tab for all modes. 802.11s general settings are described separately from the other mode settings.

The remaining Wireless Interface configuration settings are also described in this section.

General Setup

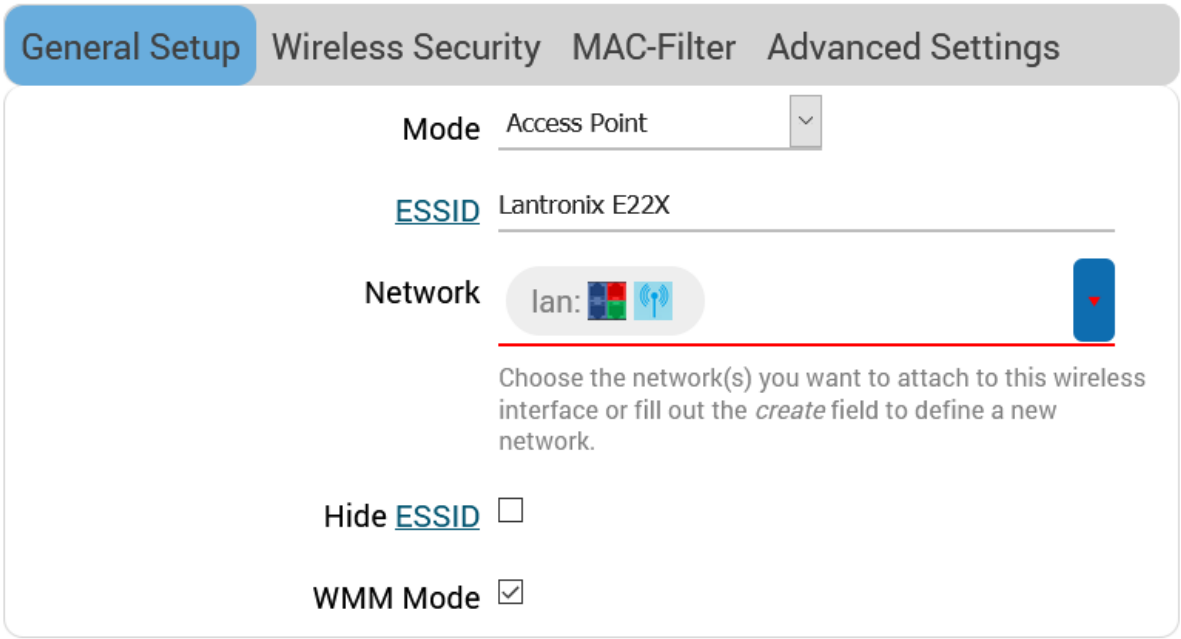


Figure 10.2-4: Wireless Interface General Configuration (Access Point mode)

Parameters	Description
Mode	Select the Wi-Fi Interface mode. **Available Options** *Access Point – router will act as an access point (master mode)* *Client - router will act as a wireless client* *Ad-Hoc – point to point connection between two stations without an intermediary* *802.11s – used for mesh networking* *Pseudo Ad-Hoc (ahdemo) – variant of ad-hoc mode that provides a point to point connection between two stations without an intermediary* *Monitor – client mode setting where wireless interface will listen to all traffic, not just its own.* *Access Point (WDS) – used for bridging two routers as WDS access points wireleslly to extend the Wi-Fi network. WDS with WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK Mixed Mode encryption modes are supported.* *Client (WDS) - WDS client mode allows a router to connect to a WDS access point.* The default mode is Access Point.

Parameters	Description
Mode: All modes except 802.11s	
ESSID	Displays the device name assigned to the router. The default name is *Lantronix E22X* for E220 series routers or *Lantronix E21X* for E210 series routers.
BSSID	This field is displayed for Client, Client (WDS), and Ad-Hoc modes only. Basic Service Set Identifier (BSSID) - 48-bit MAC address for the access point of the BSS. This can be left blank.
Network	Select LAN for the Access Point or WWAN for Client Mode to configure the Router as LAN or WWAN respectively.
Hide ESSID	Select Hide ESSID, to hide ESSID when client machines scan for available Wi-Fi networks.
WMM Mode	This field is displayed for Access Point and Access Point (WDS) only. Wi-Fi Multimedia (WMM) is a subset of the 802.11e wireless LAN (WLAN) specification that enhances quality of service (QoS) on a network by prioritizing data packets. ***Note*** • ***802.11n spec requires devices to support 802.11e (Quality of Service [QoS] enhancements for wireless LAN) in order to use HT (High Throughput) link rates, i.e. higher than 54 Mbps. WMM's Traffic Identifier (TID) field is key to aggregation mechanisms, including block acknowledgement (block ACK), that enable 802.11n's high throughput rates.*** Since WMM support is required for products to be certified for 802.11n, WMM comes enabled by default in all Wi-Fi Certified n APs and wireless routers. So even if you don't have any WMM-aware devices on your network, leave WMM enabled or you may find your clients connecting only at 54 Mbps rates.
Mode: 802.11s	
Mesh Id	Enter the Mesh ID to uniquely identify the Mesh BSS (Basic service set). This should be 0 to 32 byte ASCII string. The Mesh ID is similar to the SSID.
Network	Select LAN to configure as a LAN network.

Table 10.2-4: Wireless Interface General Configuration

Wireless Security

Allows you to configure the encryption mode for the wireless interface.

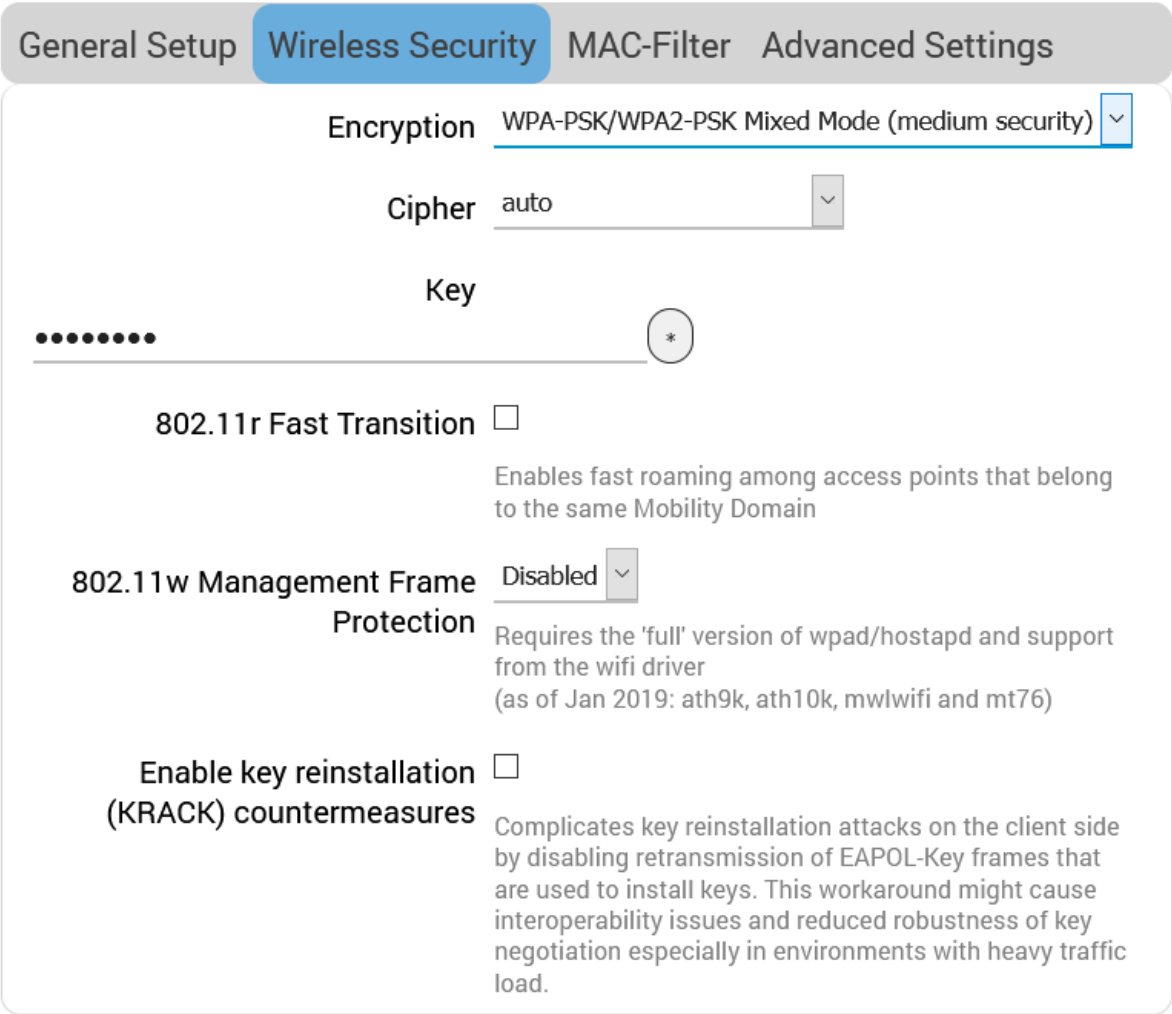


Figure 10.2-5: Wireless Interface Wireless Security Configuration (Access Point mode)

Parameters	Description
Encryption	Select the Encryption mode for Wi-Fi network. **Available Options** *No Encryption* *WPA-PSK/WPA2-PSK Mixed mode* *WPA2-PSK* *WPA-PSK* *WEP Shared Key* *WEP Open System* The default encryption mode is WPA-PSK/WPA2-PSK Mixed mode. Note: If 802.11s or Pseudo Ad-hoc mode is selected, the encryption mode should be set to No Encryption.

Parameters	Description
Cipher	For all encryption modes except No Encryption. Select the cipher suitable to the Router. **Available 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
802.11r Fast Transition	This setting is displayed only if the interface is an Access Point. Select to enable fast roaming among access points that belong to the same Mobility Domain. This setting is disabled by default.
802.11w Management Frame Protection	This setting is displayed if the interface is an Access Point or Client. Select the 802.11w MFP option. The options are Disabled, Optional, and Required. The default value is Disabled.
Enable key reinstallation (KRACK) countermeasures	This setting is displayed only if the interface is an Access Point. Select to enable KRACK countermeasures. This setting is disabled by default.

Table 10.2-5: Wireless Interface Wireless Security Configuration

MAC-Filter

The MAC-Filter settings apply to the interface configuration only when Access point mode (or Access point -WDS) is selected.

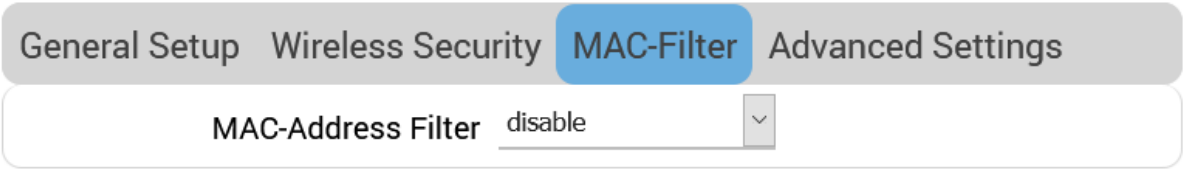


Figure 10.2-6: Wireless Interface MAC-Filter Configuration (Access Point mode)

Parameters	Description
MAC-Address Filter	MAC Address Filter is use to allow or block certain client MAC Addresses. **Available Options** *Disable* ***Allow listed only** – If this option is selected, choose the client MAC Addresses to allow.*

Parameters	Description
	Allow all except listed *– If this option is selected, choose the client MAC Addresses to block.* This setting is disabled by default.

Table 10.2-6: Wireless Interface MAC Filter Configuration

Advanced Settings

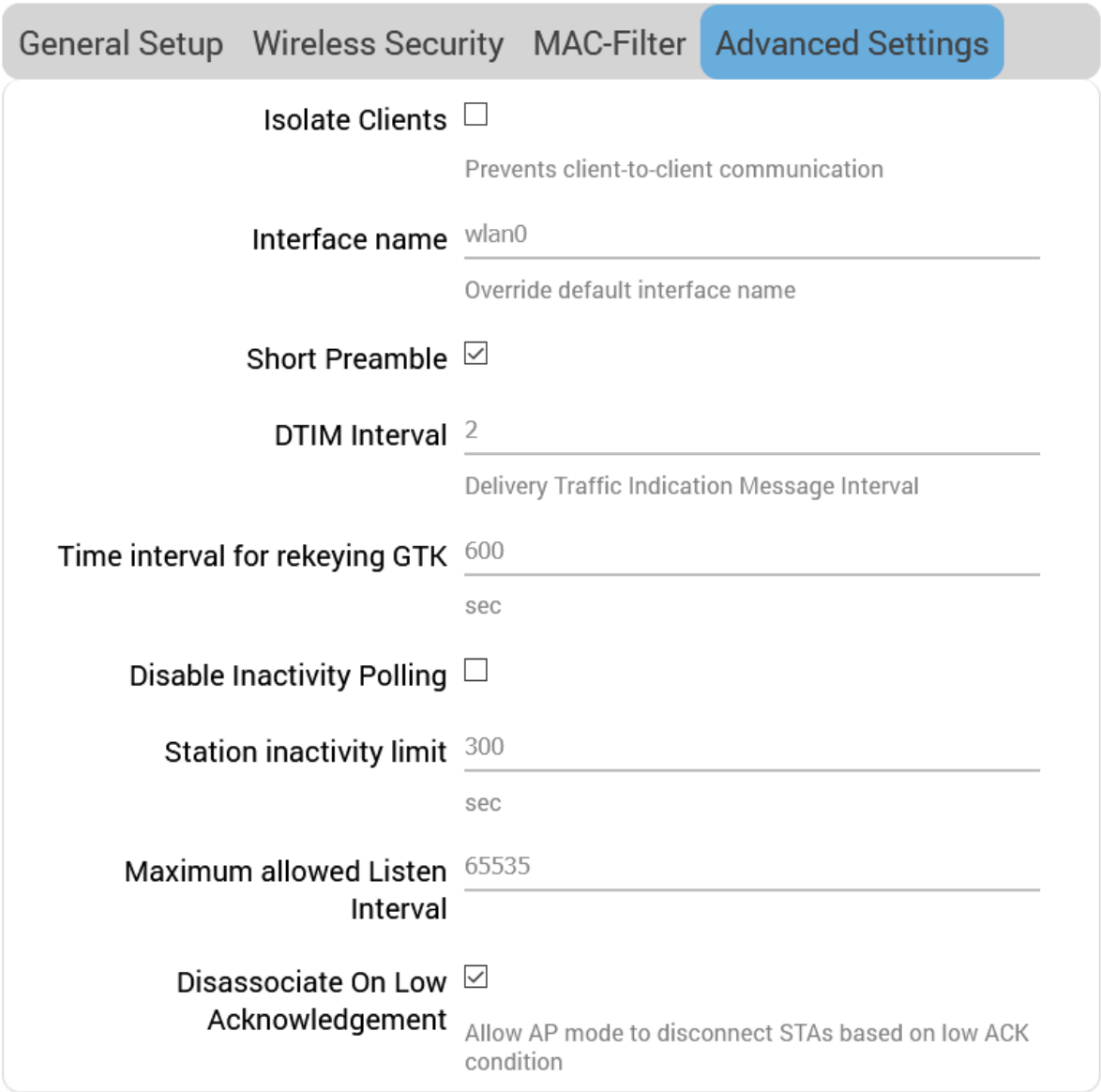


Figure 10.2-7: Wireless Network Interface Advanced Configuration (Access Point mode)

Parameters	Description
Isolate Clients	This setting appears in Access Point or Access Point (WDS) mode only. Prevent wireless clients on the wireless network from interacting with each other.
Forward mesh peer traffic	This setting appears in 802.11s mode only. By default this setting is selected to enable the interface to forward mesh peer traffic.

Parameters	Description
	Clear the box to disable.
RSSI threshold for joining	This setting appears in 802.11s mode only. Set the minimum RSSI value that peer radios must have for the station establish a link with it. Other options: Enter 0 to ignore an RSSI threshold. Enter 1 to use the driver default.
Interface name	Specifies a custom name for the Wi-Fi interface, which is otherwise automatically named.
Short Preamble	Select to enable optional use of short preamble.
DTIM Interval	Displays the Delivery Traffic Indication Message (DTIM) period value which determines how often a beacon frame includes a DTIM. This option only impacts access point interfaces. Default is 2. Range is 1-255.
Time interval for rekeying GTK	GTK rekey interval of WPA security in seconds. Default is 600.
Disable Inactivity Polling	Select to disable inactivity polling. Disabling the inactivity polling allows the router to disconnect stations based on inactivity timeout so that idle stations are more likely to be disconnected even if they are still in range of the access point.
Station inactivity limit	Specify the station inactivity limit in seconds. If a station does not send anything within this time period, the router sends a request to verify whether it is still in range. If the request is not acknowledged, the station will be disassociated and de-authenticated. Default is 300 seconds.
Maximum allowed Listen interval	Displays the number of beacon periods that stations are allowed to remain asleep. Default 65535
Disassociate on Low Acknowledgement	Select to enable or disable. Disassociate stations based on excessive transmission failures or other indications of connection loss. Availability depends on driver capabilities. Enabled by default.

Table 10.2-7: Wireless Network Interface Advanced Configuration

10.3 Switch

Network > Switch

The E210 and E220 routers provide a common default VLAN configuration that contains a single network interface (eth0), leading to a 5-port VLAN enabled switch that is virtually partitioned into a LAN and WAN network by using VLANs.

By default, VLAN functionality is enabled as shown by the check box in the image below.

Note

- ***For assistance configuring the switch functionality, please contact Lantronix Technical Support.***

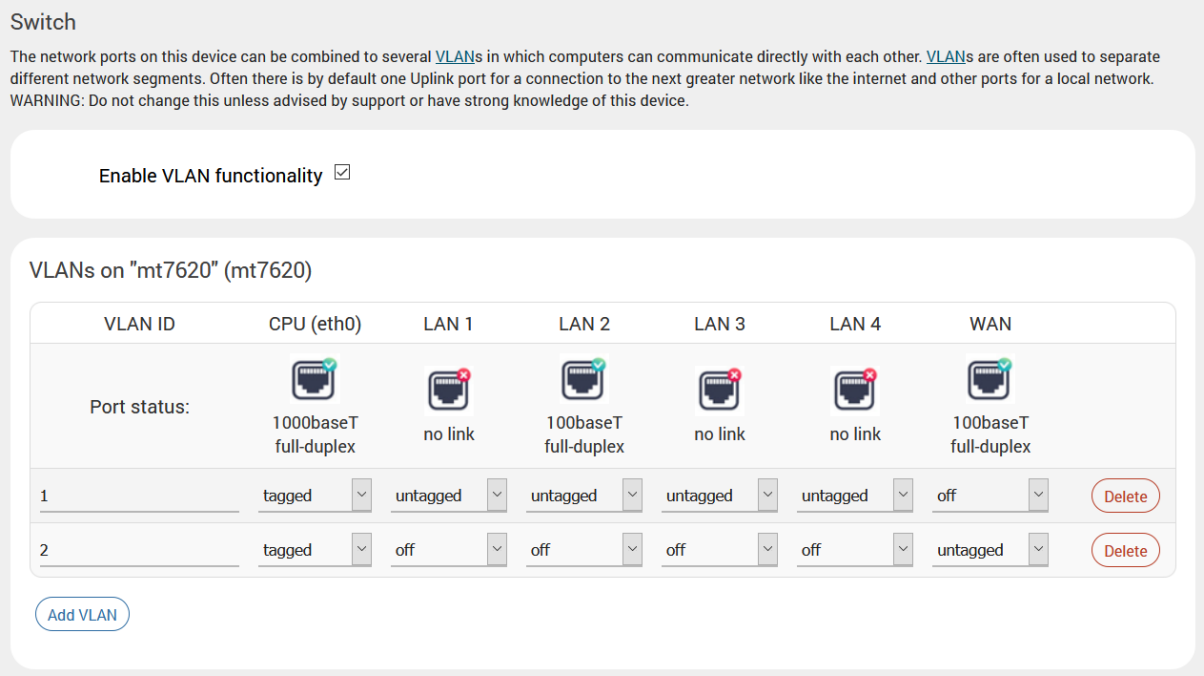


Figure 10.3-1: Switch Configuration

10.4 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 more details about basic setup of DHCP server on the LAN side refer to Network > LAN > DHCP Server.

DHCP and DNS sub-sections allows you to configure the advanced options like custom DNS servers, custom lease files, advanced TFTP settings and MAC Address based IP Address allocation.

10.4.1 General Settings

Network > DHCP and DNS > General Settings

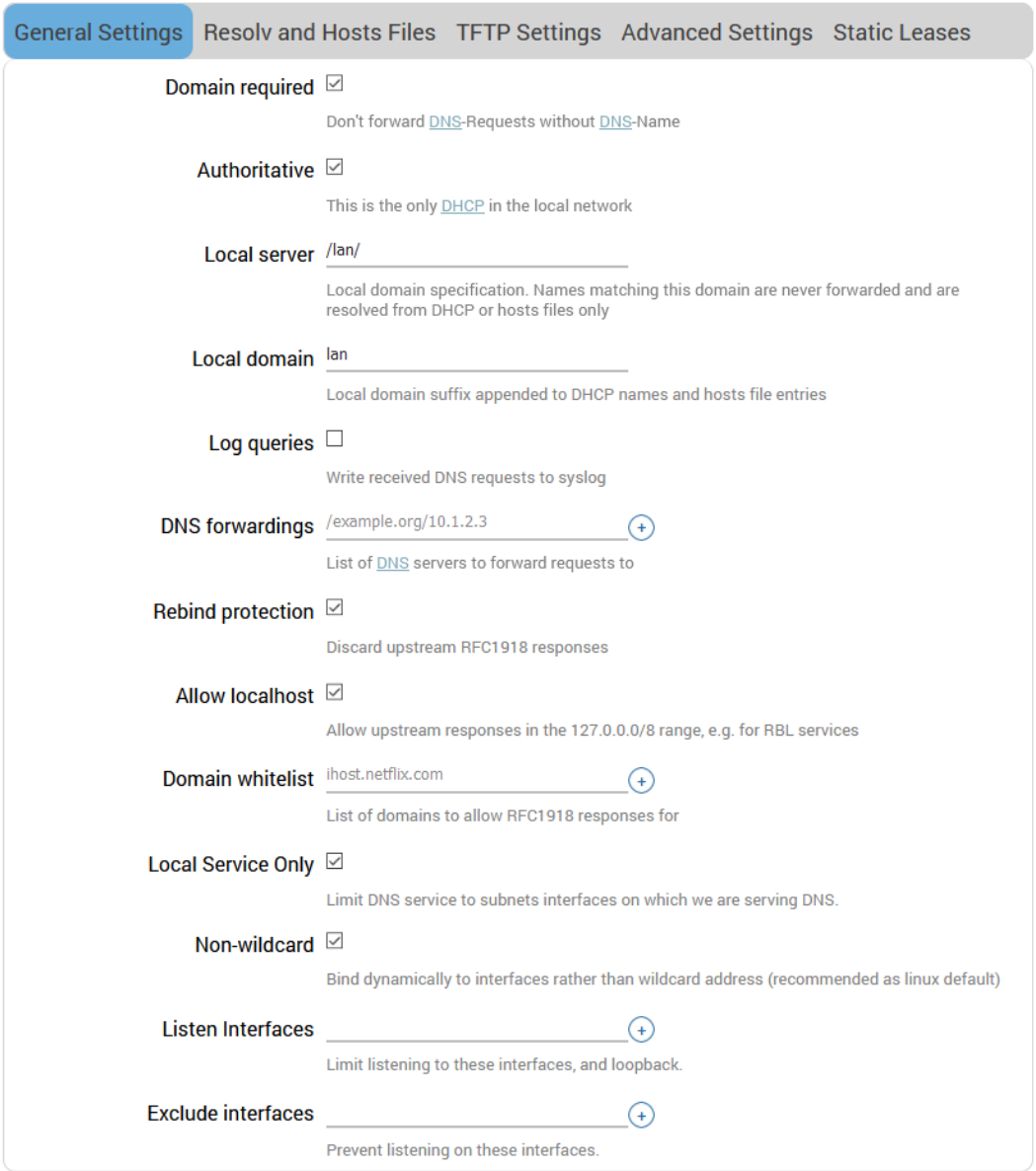


Figure 10.4-1: DHCP Server and DNS Forwarder General Configuration

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 resoled using DHCP or host files.
Local domain	Enter the local domain suffix appended to DHCP names and host

Parameters	Description
	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	
Hostname	Name of the device that is connected to the router and has been leased an IP Address by DHCP server.
IPv4-Address	IPv4 Address assigned to the device connected to the router.
MAC-Address	MAC address of the device connected to the router.
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 router and has been leased an IPv6 Address by DHCPv6 server.
IPv6-Address	IPv6 Address assigned to the device connected to the router.
DUID	DUID (Device Unique Identifier) of the device connected to the router
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 router and has been assigned a static IP Address.
MAC-Address	MAC address of the device connected to the router.
IPv4-Address	IPv4 Address to be assigned to the device connected to the router.
IPv6-Suffix (hex)	IPv6 Address to be assigned to the device connected to the router.

Table 10.4-1: General Configuration of DHCP Server and DNS-Forwarder

10.4.2 Resolv and Host Files

Network > DHCP and DNS > Resolv and Host File

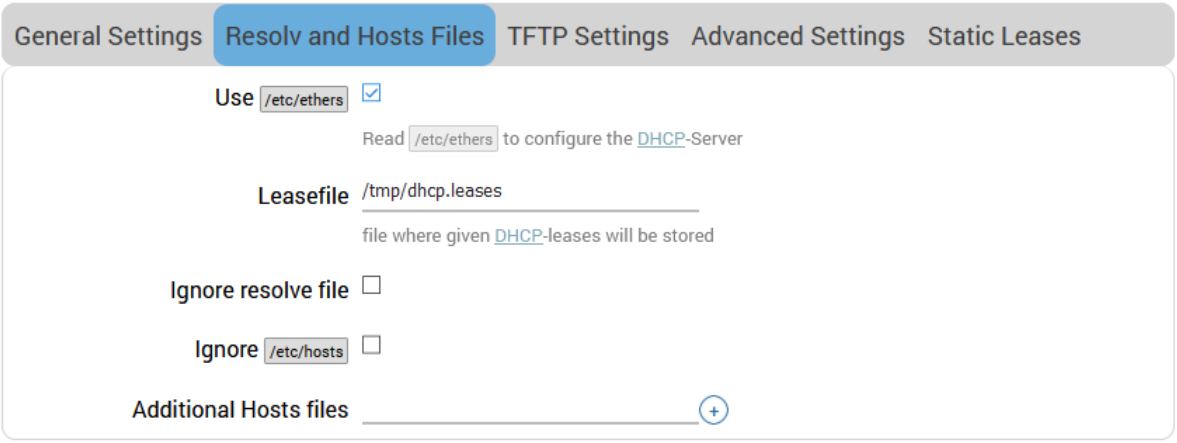


Figure 10.4-2: DHCP and DNS Resolv and Host File Configuration

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.

Table 10.4-2: Resolv and Host File Configuration for DHCP and DNS

10.4.3 TFTP Settings

Network > DHCP and DNS > TFTP Settings

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

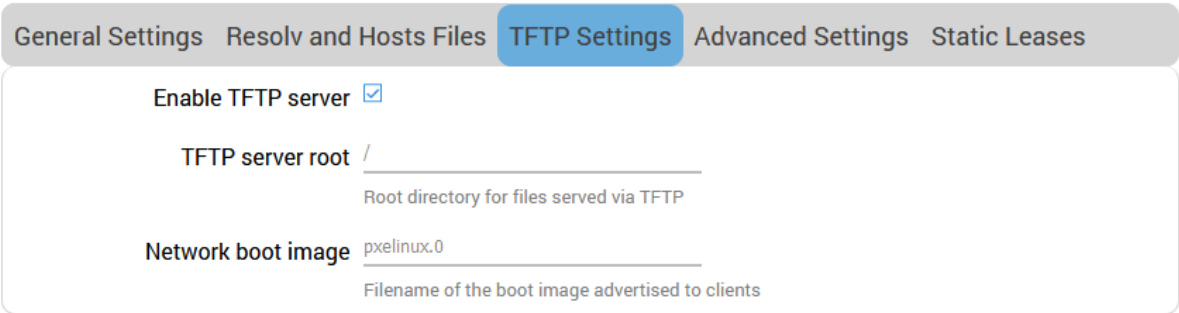


Figure 10.4-3: DHCP and DNS TFTP Configuration

Parameters	Description
Server Settings	
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.*

Table 10.4-3: TFTP Configuration for DHCP and DNS

10.4.4 Advanced Settings

Network > DHCP and DNS > Advanced Settings

General Settings | Resolv and Hosts Files | TFTP Settings | Advanced Settings | Static Leases

Suppress logging ☐
Suppress logging of the routine operation of these protocols

Allocate IP sequentially ☐
Allocate IP addresses sequentially, starting from the lowest available address

Filter private ☑
Do not forward reverse lookups for local networks

Filter useless ☐
Do not forward requests that cannot be answered by public name servers

Localise queries ☑
Localise hostname depending on the requesting subnet if multiple IPs are available

Expand hosts ☑
Add local domain suffix to names served from hosts files

No negative cache ☐
Do not cache negative replies, e.g. for not existing domains

Additional servers file
This file may contain lines like 'server=/domain/1.2.3.4' or 'server=1.2.3.4' for domain-specific or full upstream DNS servers.

Strict order ☐
DNS servers will be queried in the order of the resolvfile

All Servers ☐
Query all available upstream DNS servers

Bogus NX Domain Override 67.215.65.132 ⊕
List of hosts that supply bogus NX domain results

DNS server port 53
Listening port for inbound DNS queries

DNS query port any
Fixed source port for outbound DNS queries

Max. DHCP leases unlimited
Maximum allowed number of active DHCP leases

Max. EDNS0 packet size 1280
Maximum allowed size of EDNS.0 UDP packets

Max. concurrent queries 150
Maximum allowed number of concurrent DNS queries

Size of DNS query cache 150
Number of cached DNS entries (max is 10000, 0 is no caching)

Figure 10.4-4: DHCP and DNS Advanced Configuration

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.
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.

Table 10.4-4: Advanced Configuration for DHCP and DNS

10.4.5 Static Leases

Network > DHCP and DNS > Static leases

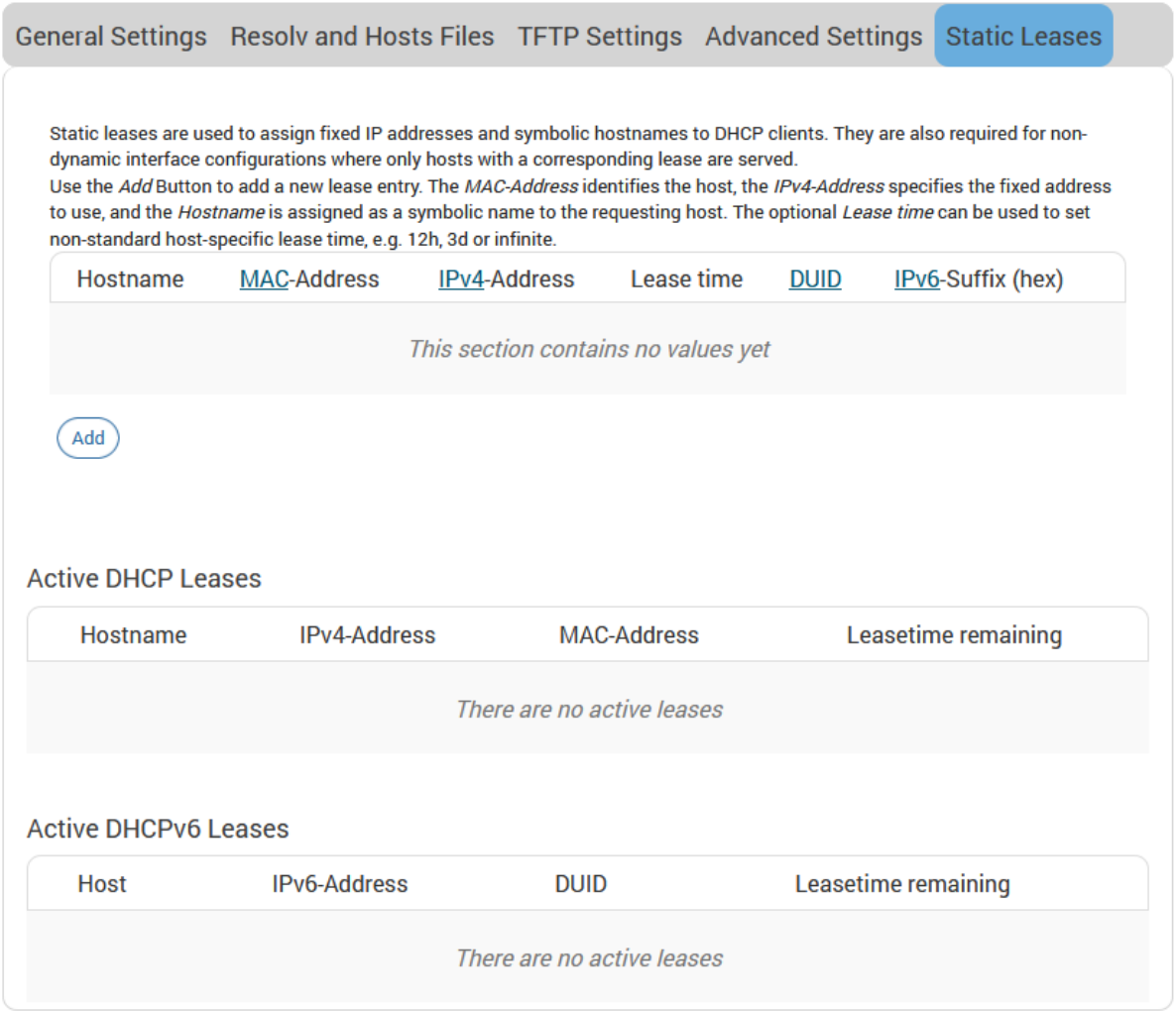


Figure 10.4-5: DHCP and DNS Static Leases

Parameters	Description
Active DHCP Leases	
Hostname	Name of the device that is connected to the router and has been leased an IP Address by DHCP server.
IPv4-Address	IPv4 Address assigned to the device connected to the router.
MAC-Address	MAC address of the device connected to the router.
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 router and has been leased an IPv6 Address by DHCPv6 server.

Parameters	Description
IPv6-Address	IPv6 Address assigned to the device connected to the router.
DUID	DUID (Device Unique Identifier) of the device connected to the router
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 router and has been assigned a static IP Address.
MAC-Address	MAC address of the device connected to the router.
IPv4-Address	IPv4 Address to be assigned to the device connected to the router.
IPv6-Suffix (hex)	IPv6 Address to be assigned to the device connected to the router.

Table 10.4-5: DHCP and DNS Static Leases

10.5 Hostnames

Network > Hostnames

Figure 10.5-1: Hostnames Configuration

Parameters	Description
Host entries	
Hostname	Enter the Hostname.
IP address	Enter the IP Address of the host.

Table 10.5-1: Hostnames Configuration

10.6 Static Routes

Network > Static Routes

You can configure the static routes to define the method for communication between two different networks located in two different domains.

10.6.1 Static IPv4 Routes

Network > Static Routes > Static IPv4 Routes

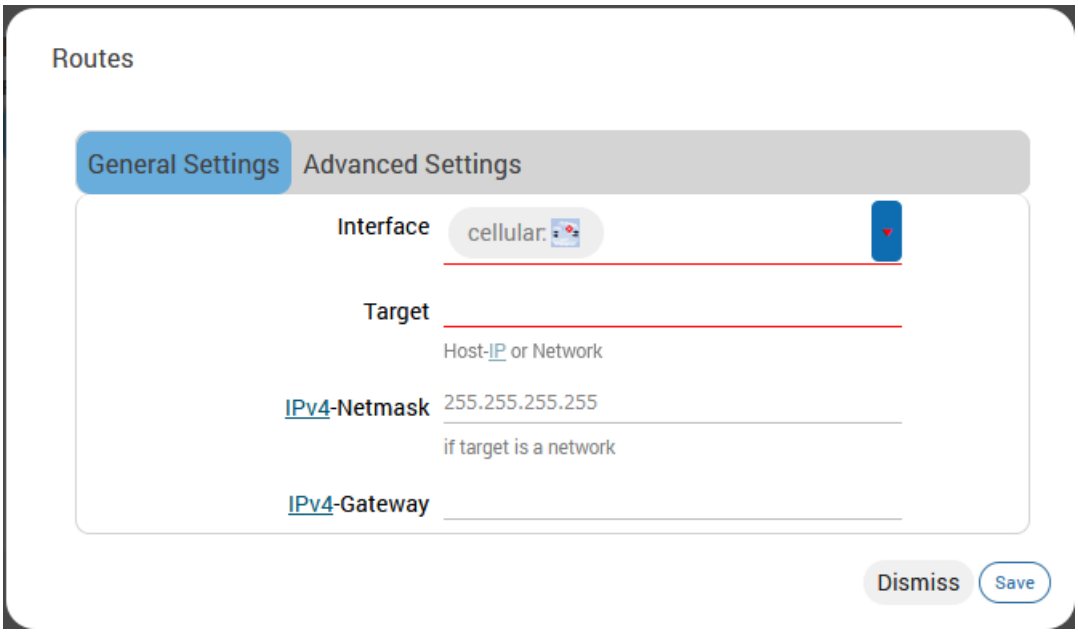


Figure 10.6-1: Static IPv4 Routes Configuration

Parameters	Description
General Settings	
Interface	Select the name of the logical interface assigned the static IPv4 Address.
Target	Enter the target host IPv4 Address or Network if the target is a network.
IPv4-Netmask	Enter the IPv4 Netmask of the static route.
IPv4-Gateway	Enter the IPv4 Gateway of the static route.
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.

Parameters	Description
Route type	Select the route type. Available options: ***unicast*** *– route entry describes real paths to the desitnations 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 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.

Table 10.6-1: Static IPv4 Routes Configuration

10.6.2 Static IPv6 Routes

Network > Static Routes > Static IPv6 Routes

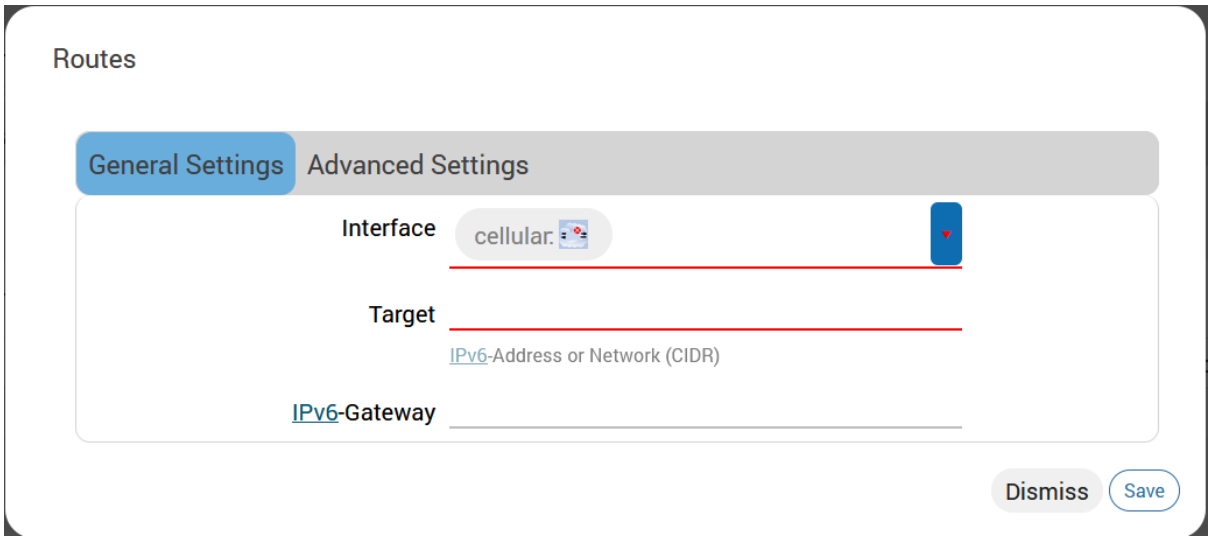


Figure 10.6-2: Static IPv6 Routes Configuration

Parameters	Description
General Settings	
Interface	Select the logical interface assigned the static IPv6 Address.
Target	Enter the target host IPv6 Address or Network CIDR if the target is a network.
IPv6-Gateway	Enter the IPv6 Netmask of the static route.
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. Blank value represents auto MTU size
Route type	Select the route type. Available options: ***unicast*** *– route entry describes real paths to the desitnations 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.

Table 10.6-2: Static IPv6 Routes Configuration

10.7 Diagnostics

Network > Diagnostics

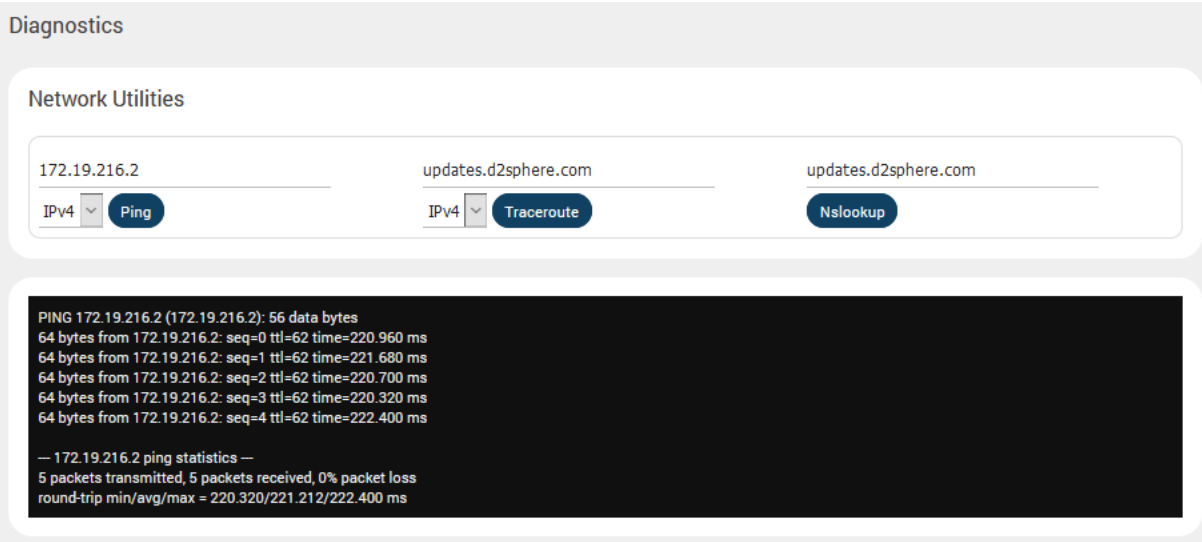


Figure 10.7-1: Diagnostics Network Utilities

Parameters	Description
Network Utilities	
Ping	IP Address or fully qualified domain name to be pinged. It determines network connection between Router and host on the network. The output shows if the response was received, packets transmitted and received, packet loss if any.
Traceroute	IP Address or fully qualified domain name It determines network connection between Router and host on the network. The output shows all the routers 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 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, and if you enter an IP address, then you get back the domain name to which it corresponds. In other words, it reaches out over the Internet to do a DNS lookup from an authorized name server, and displays the information in the user understandable format.

Table 10.7-1: Diagnostics Configuration

10.8 Firewall

Network > Firewall

E210 and E220 routers follow a Zone Based firewall concept.

Every interface of the E210 or E220 router, physical or virtual, needs to be assigned to a Firewall Zone, however one firewall zone can have multiple interfaces.

By default, there are two zones, the LAN zone and WAN zone.

You can create a new LAN or WAN zone either from the Firewall section or when you create an additional network interface. You can associate multiple interfaces to the Firewall Zones and define the rules of communication between them.

10.8.1 General Settings

Network > Firewall > General Settings

Concept of zone based Firewall

A zone section groups one or more interfaces and serves as source or destination for forwarding, rules, and redirects. Masquerading (NAT) of outgoing traffic is controlled on a per zone basis. Note that masquerading is defined in the outgoing interface.

- INPUT rules for a zone describe what happens to traffic trying to reach the router itself through an interface in that zone.
- OUTPUT rules for a zone describe what happens to traffic originating from the router itself going through an interface in that zone.
- FORWARD rules for a zone describe what happens to traffic passing between different interfaces in that zone.

By default, there are 2 zones which are already created in the Router, LAN Zone and WAN Zone. All traffic from LAN to WAN has no restrictions but all incoming traffic on WAN side is blocked unless a port forwarding rule is set or unless a particular port is opened.

Drop vs Reject

DROP

- less information is exposed
- less attack surface
- client software may not cope well with it (hangs until connection times out)
- may complicate network debugging (where was traffic dropped and why)

REJECT

- may expose information (like the ip at which traffic was actually blocked)
- client software can recover faster from rejected connection attempts
- network debugging easier (routing and firewall issues clearly distinguishable)

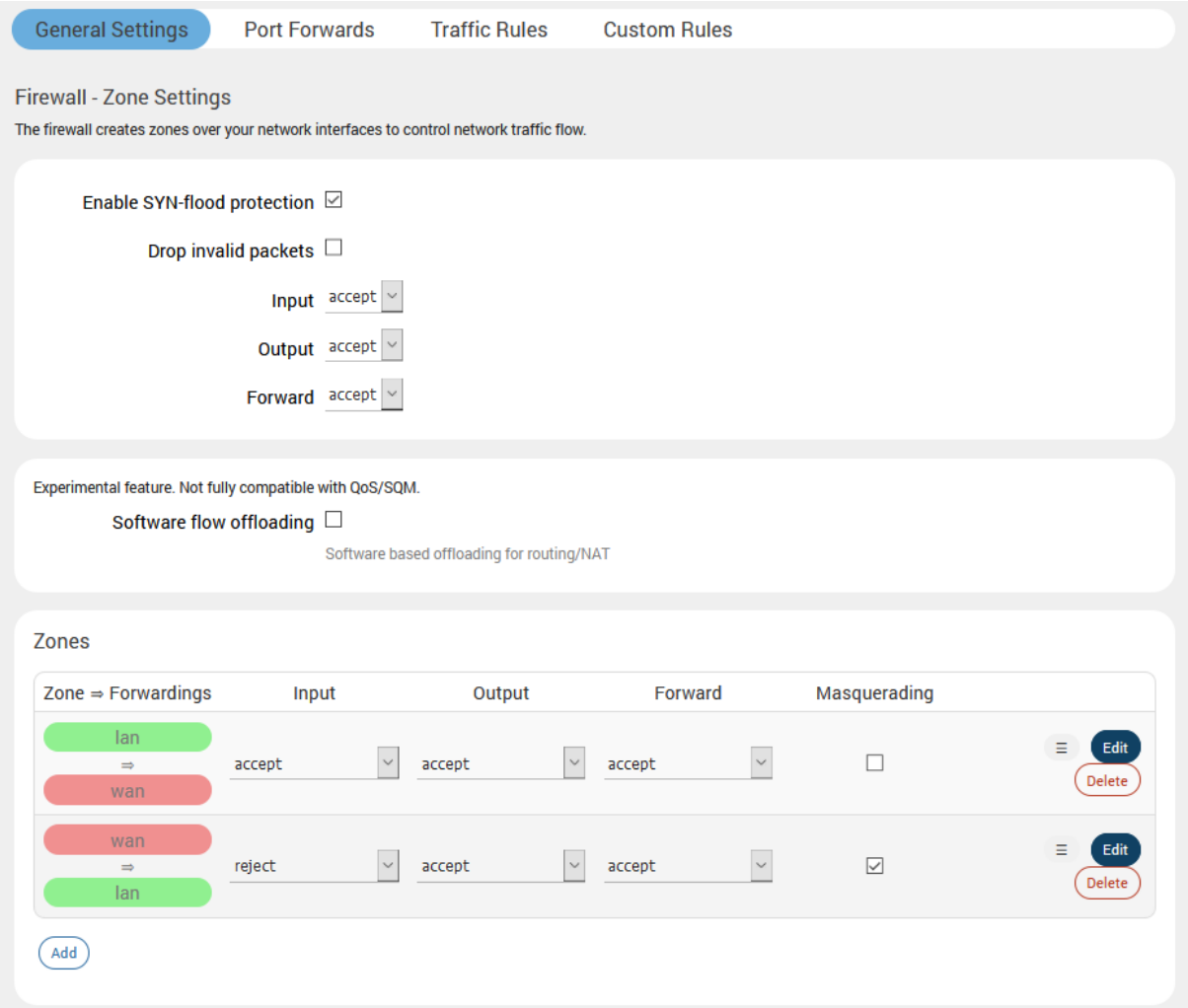


Figure 10.8-1: Firewall Zones General Configuration

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.
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.
Zones (Applies to configured zone)	
Zone Forwarding	Select the zones between which the Zone forwarding rule will be

Parameters	Description
	applicable.
Input	Select to accept or reject the inbound traffic to all the configured zones.
Output	Select to accept or reject the outbound traffic from all the configured zones.
Forward	Select to accept or reject the forwarded traffic from all the configured zones.
Masquerading	Check to allow IP Masquerading.

Table 10.8-1: General Configuration for Firewall Zone

10.8.1.1 Add/Edit Firewall Zone

Network > Firewall > General Settings > Add/Edit

General Settings

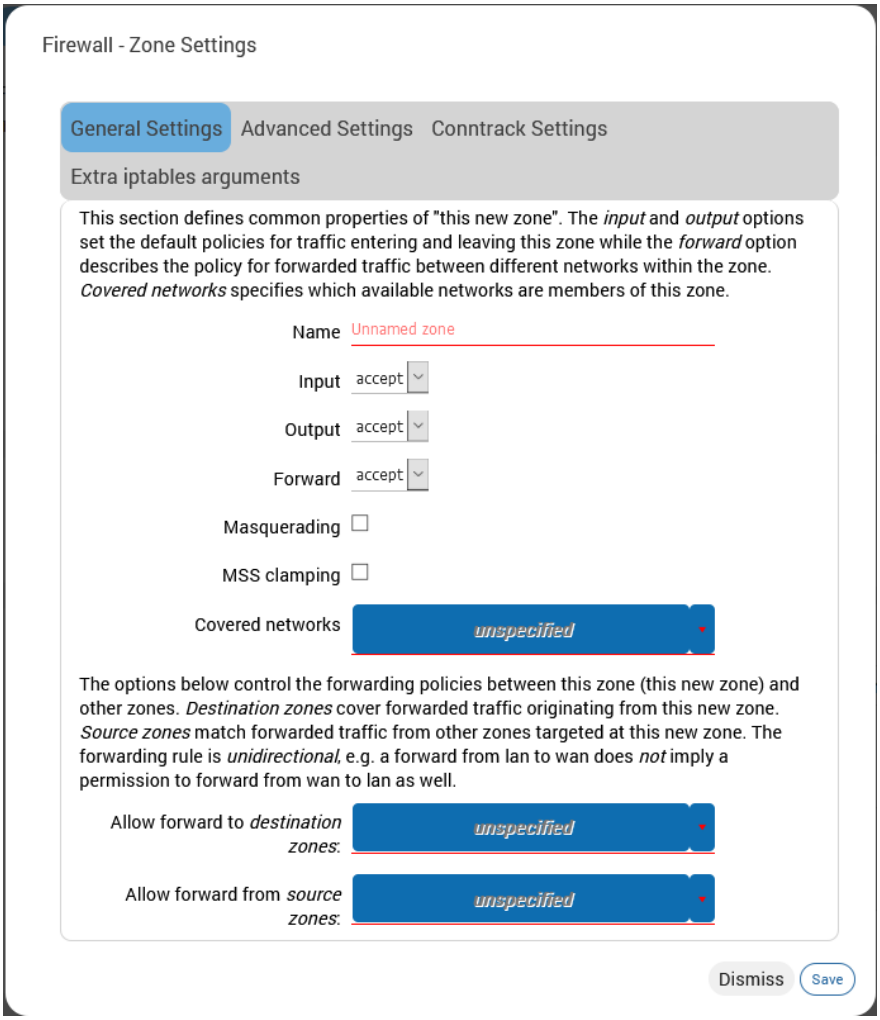


Figure 10.8-2: Firewall Zone General Configuration

Parameters	Description
Static IPv4 Routes	
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.
MSS clamping	Check to allow MSS clamping.
Covered networks	Select the network interfaces that must be included in the zone configuration.
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.

Table 10.8-2: General Configuration for Firewall Zone (LAN)

Advanced Settings

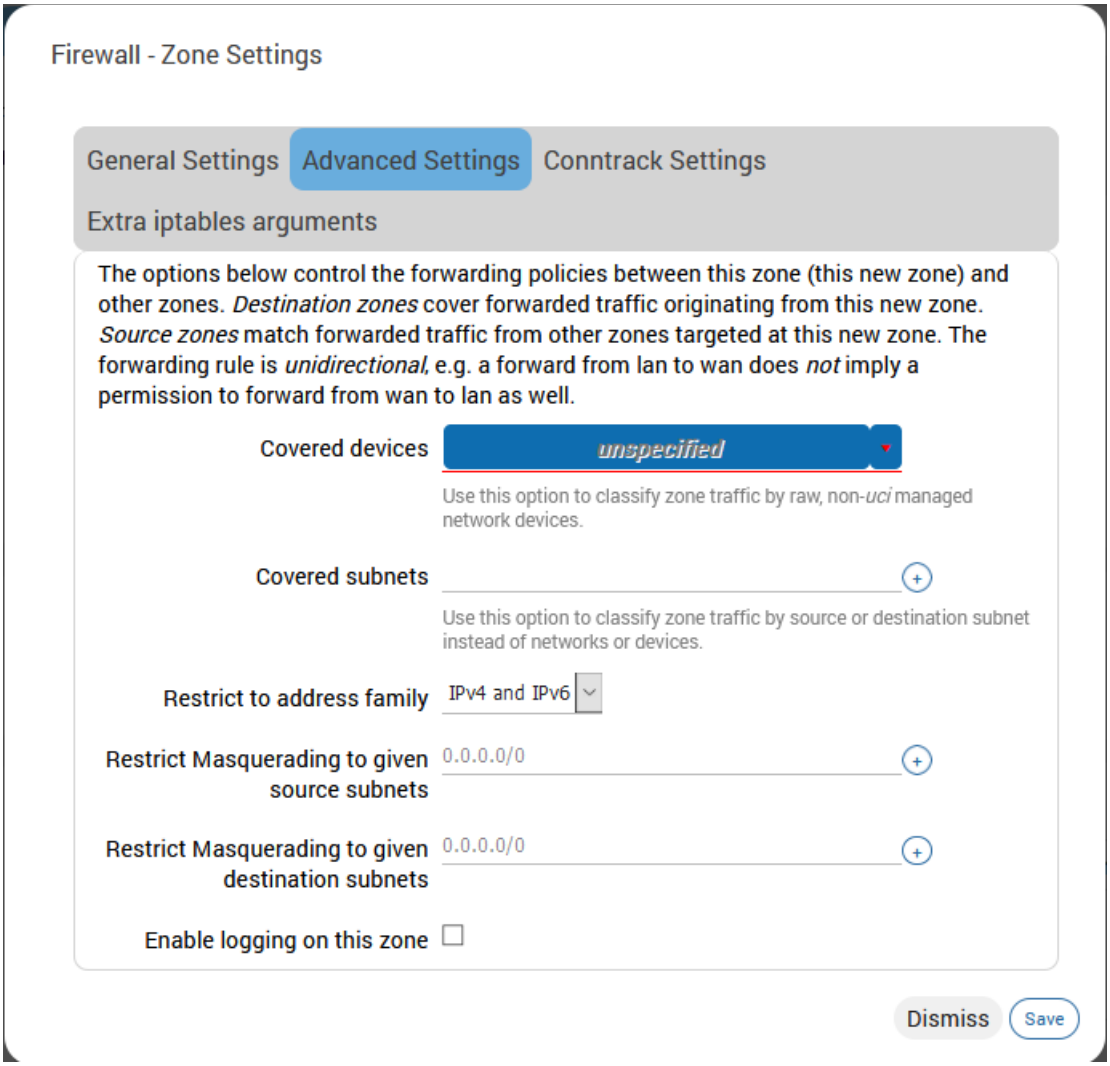


Figure 10.8-3: Firewall Advanced Configuration

Parameters	Description
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.

Parameters	Description
Enable logging on this zone	Check to enable logging of all the activities on the Zone.

Table 10.8-3: Advanced Configuration for Firewall Zone (LAN)

Conntrack Settings

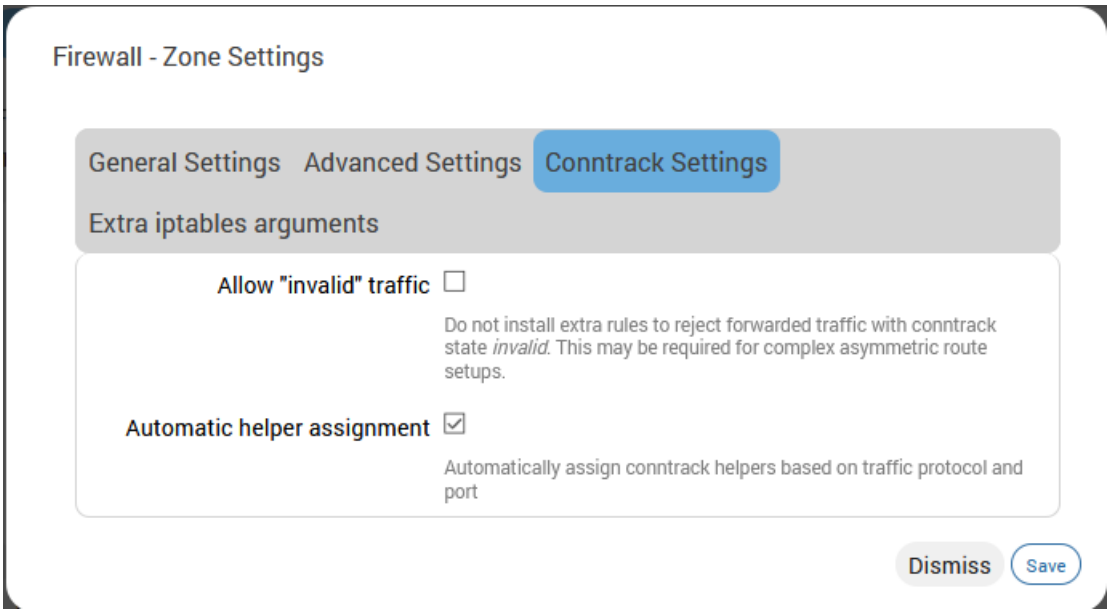


Figure 10.8-4: Firewall Conntrack Configuration

Parameters	Description
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.

Table 10.8-4: Firewall Conntrack Configuration

Extra iptables arguments

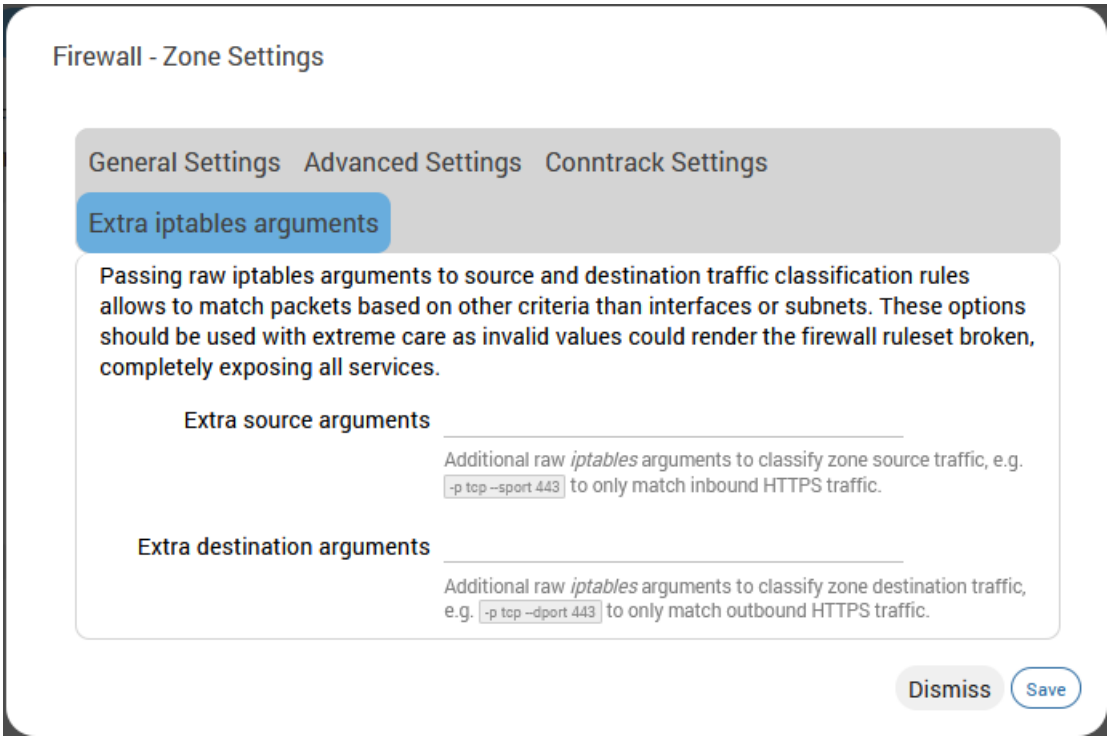


Figure 10.8-5: Firewall IPtables arguments configuration

Parameters	Description
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

Table 10.8-5: Firewall iptables arguments configuration

10.8.2 Port Forwards

Network > Firewall > Port Forwards

By default, all WAN side ports are closed. Port forwarding allows remote computers to connect to a specific computer or service within the LAN by opening the WAN port and redirecting the connection (and data) on that port to an internal LAN IP and port.

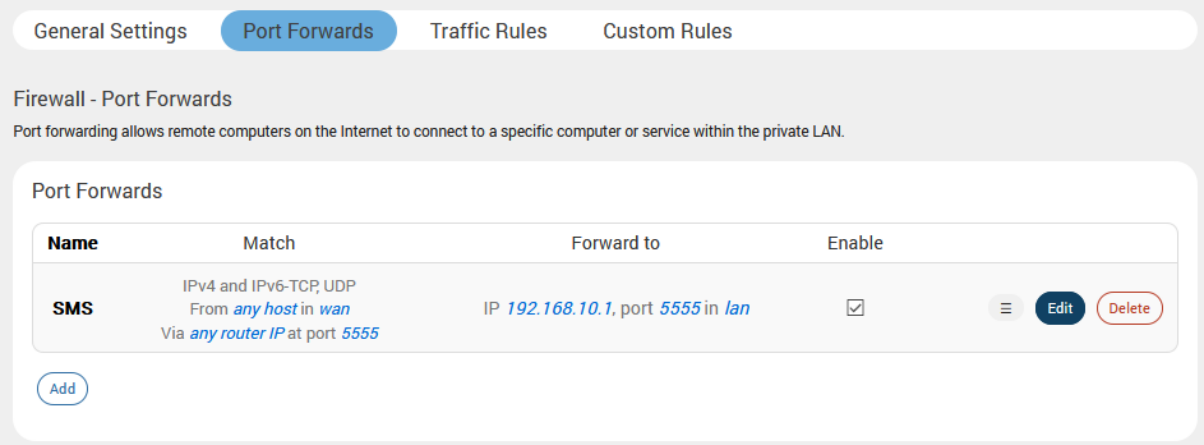


Figure 10.8-6: Firewall Port Forwards

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.

Table 10.8-6: Firewall Port Forwards

10.8.2.1 Add Port Forwarding Rule

All the WAN side ports on the E210 and E220 routers are closed by default. For any WAN side connection to reach the internal LAN, a port-forwarding rule must be configured that maps the WAN port to an internal LAN IP Address and port. Also, the router provides advanced port-forwarding configurations, where in addition to WAN port; the WAN IP Address can be mapped with LAN IP Address and LAN port.

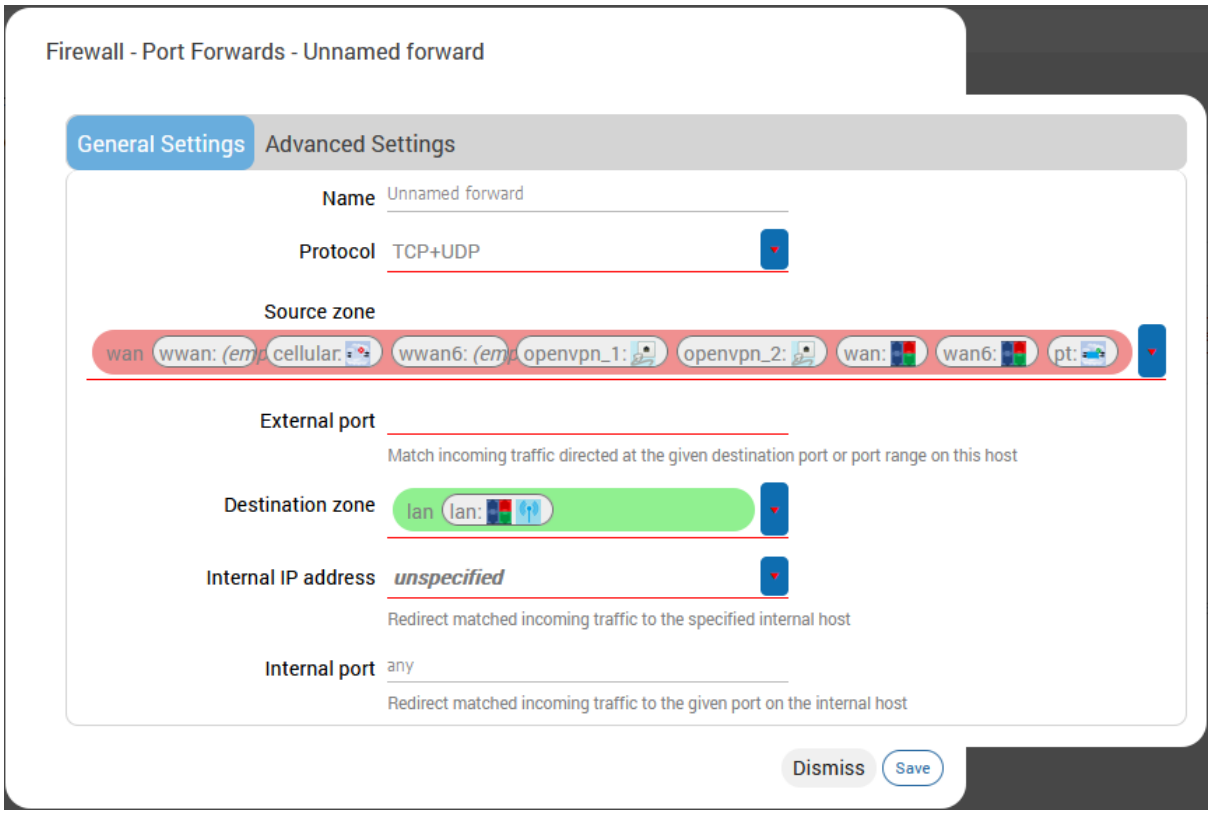


Figure 10.8-7: Firewall Port Forwards General Configuration

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

Parameters	Description
	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.
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 router.
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 router
Extra arguments	Passes additional arguments to iptables. Should be used with care.

Table 10.8-7: Port Forwarding Configuration for Firewall Zone

10.8.3 Traffic Rules

Network > Firewall > Traffic Rules

Traffic rules allow or restrict access to specific ports or hosts. Rule actions can be configured to accept, drop, or reject traffic.

When configuring rules, 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.

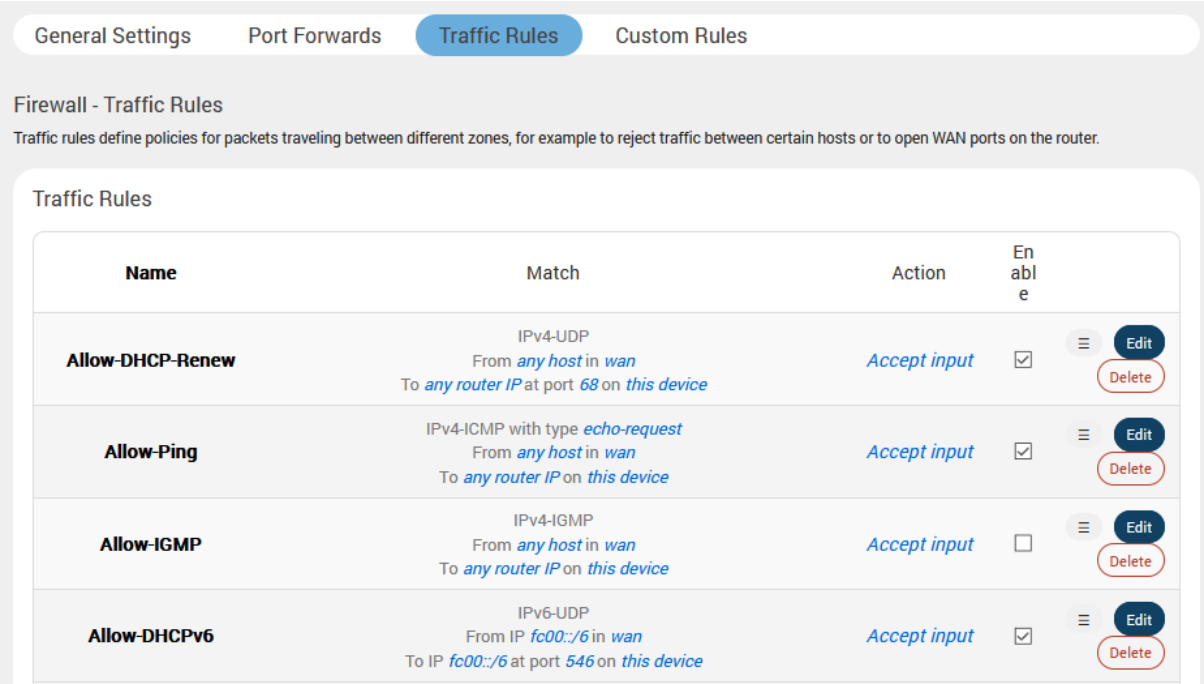


Figure 10.8-8: Firewall Zone Traffic Rules

Parameters	Description
Traffic Rules **These rules define policies for traffic communication between the different zones, primarily used for traffic shaping.**	
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.
Enable	Check to enable the Traffic Rule.
Add	Click to Add a new traffic rule.

Table 10.8-8: Traffic Rule Overview for Firewall Zone

10.8.3.1 Add Traffic Rule

Traffic rules can be used to achieve the following results:

- Block / redirect generic data types for example: ICMP, DHCP requests etc.
- Block certain MAC addresses on the LAN side
- Block communication with one or more public IP addresses
- Block communication with all except one or more IP address
- Open specific ports on WAN side
- DMZ rules and zone creation

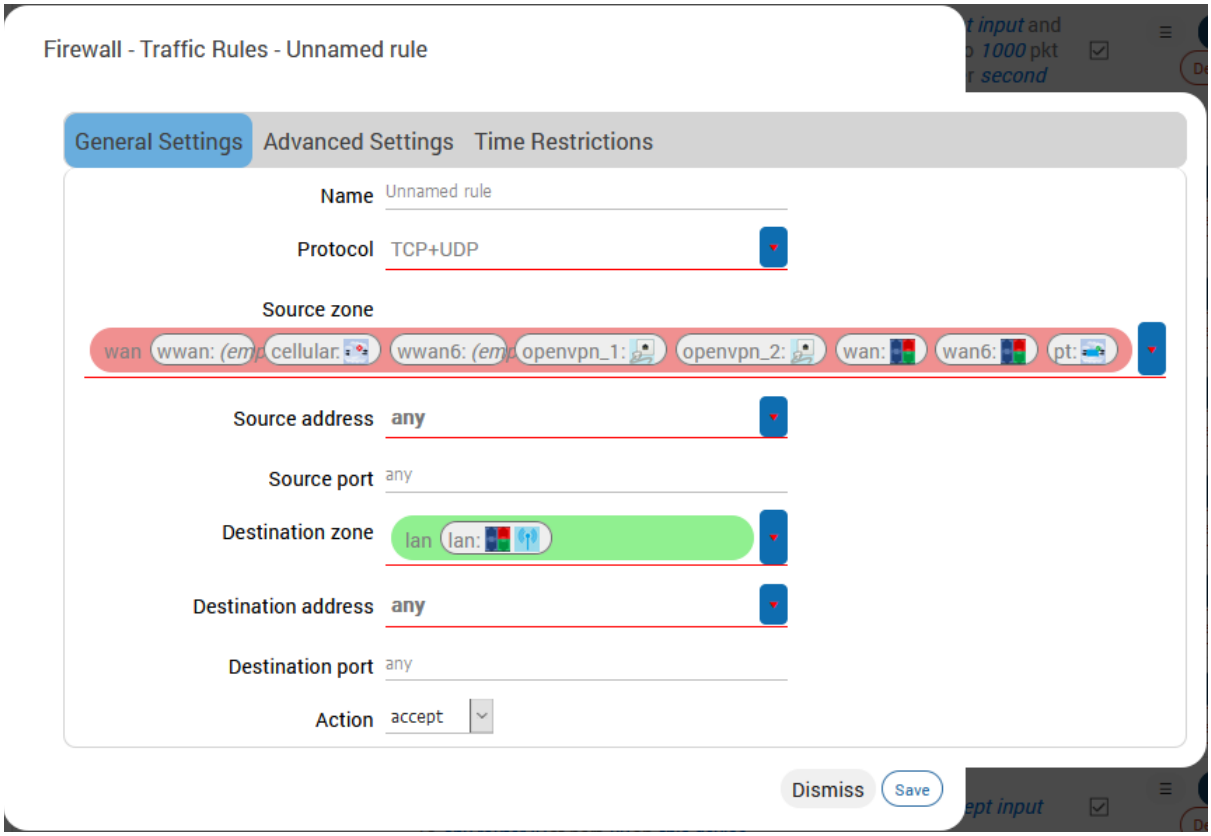


Figure 10.8-9: Firewall Traffic Rules General Configuration

Parameters	Description
General Settings	
Name	Enter the name of the traffic rule.
Protocol	Select the Protocol from the available options. **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

Parameters	Description
Source port	Match incoming traffic from the specified source port
Destination zones	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* *Mark* *Notrack.*
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.
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.

Table 10.8-9: Firewall Traffic Rule Configuration

10.8.4 Custom Rules

Network > Firewall > Custom Rules

The shell script allows you to add customized rules for Firewall. Commands are executed after the firewall is restarted immediately after the default ruleset has been loaded.

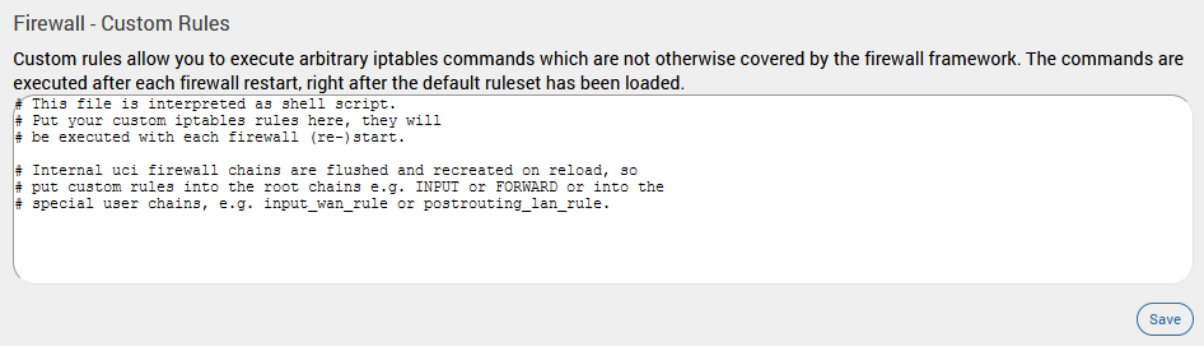


Figure 10.8-10: Firewall Custom Rules Configuration

10.9 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 cut operating costs. The order of Interface priority depends on the metric assigned to the interface.

10.9.1 How it works

Load balancing is determined by the load metric i.e. weight. Each link is assigned a relative weight and the router distributes traffic across links in proportion to the ratio of weights assigned to individual link. This weight determines how much traffic will pass through a particular link relative to the other links.

Administrator can set the metric weight and define how the traffic should be directed to providers to best utilize their bandwidth investments. Weight 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, followed by WWAN and then followed by Cellular.***

Concept of MWAN

Since E series have multiple sources of Internet, one or more sources of Internet could be used at the same time. Using one source of Internet and failing over to another one by defining priorities is called Failover. 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.

When to failover and when to 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 which is essentially the connections is split between the multiple interfaces in the ratio of their weights assigned.

E Series provides a feature called *WAN affinity* where a particular source IP, Destination IP or a data type can be bound to a particular interface. For this, you need to set rules and apply the rules to a particular policy. However you need to first have appropriate members which correspond to physical interfaces in a particular policy.

In summary:

- Members correspond to individual interfaces where you can set metric and weight
- Policy consists of a member or group of members
- Rules are to be applied to a policy

10.9.2 Globals

Network > Load Balancing > Globals

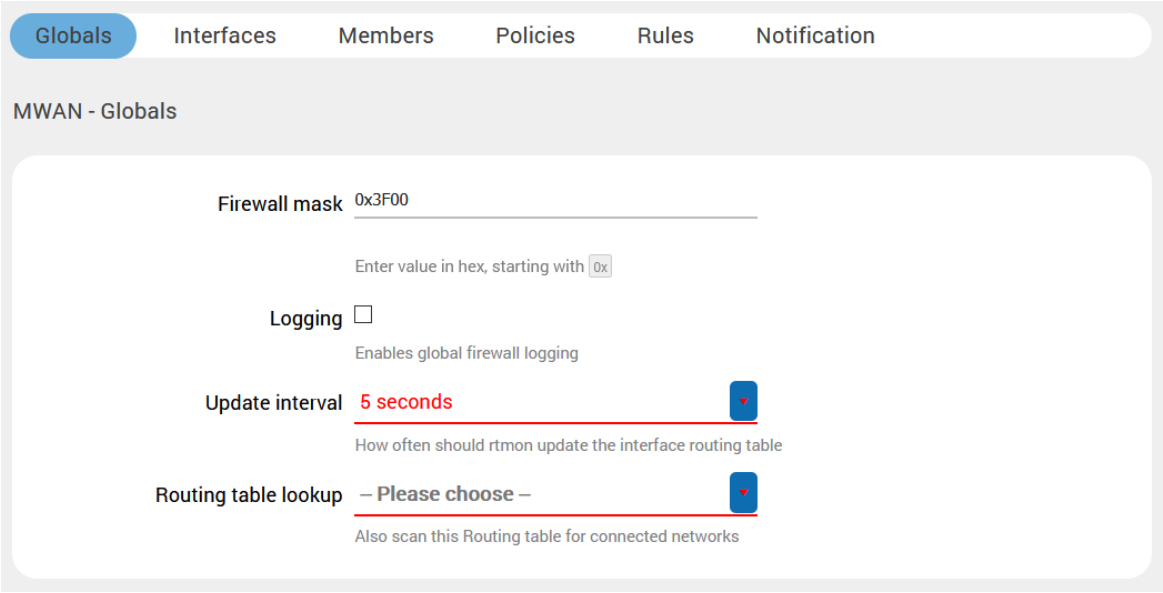


Figure 10.9-1: MWAN Interface Globals Configuration

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

Table 10.9-1: MWAN Interface Globals Configuration

10.9.3 Interfaces

Network > Load Balancing > Interfaces

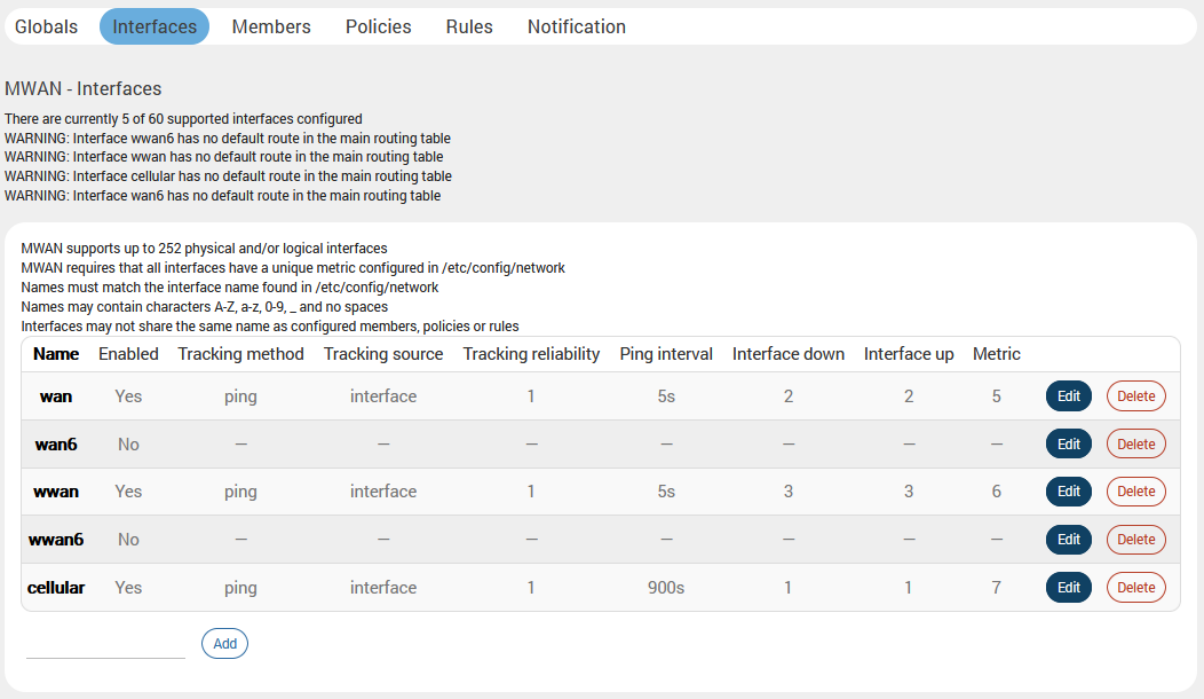


Figure 10.9-2: MWAN Interfaces

Parameters	Description
Interface	Name of the available Interface.
Enabled	Displays the Interface status is enabled or disabled.
Tracking Method	Displays the method used to track the interface.
Tracking Source	Displays the tracking source is address or interface.
Tracking reliability	Displays the number of tracking IP Addresses. The acknowledgement/responses from these tracking IP Addresses are considered to determine the Interface as up/down.
Ping interval	Displays the time in seconds between sending two successive ping packets.
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 from the Advanced Interface Configuration Settings page.
Error	Displays if an error has occurred during the Interface configuration. Error messages are displayed as warnings.

Table 10.9-2: MWAN Interface

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. For more details on load balancing, visit the Lantronix Technical Support website.***

10.9.3.1 Edit Interface

Network > Load Balancing > Interfaces

MWAN Interface Configuration - wan

Enabled ☑

Initial state Online

Expect interface state on up event

Internet Protocol IPv4

Tracking hostname or IP address 8.8.8.8

This hostname or IP address will be pinged to determine if the link is up or down. Leave blank to assume interface is always online

Tracking method ping

Tracking source interface

Tracking reliability 1

Acceptable values: 1-100. This many Tracking IP addresses must respond for the link to be deemed up

Ping count 5

Ping size 56

Max TTL 60

Check link quality ☐

Ping timeout 3 seconds

Ping interval 5 seconds

Failure interval 3 seconds

Ping interval during failure detection

Keep failure interval ☑

Keep ping failure interval during failure state

Recovery interval 3 seconds

Ping interval during failure recovering

Interface down 2

Interface will be deemed down after this many failed ping tests

Interface up 2

Downed interface will be deemed up after this many successful ping tests

Flush conntrack table ☐ ifup (netifd) ☐ ifdown (netifd) ☐ connected (mwan3) ☐ disconnected (mwan3)

Flush global firewall conntrack table on interface events

Metric 5

This displays the metric assigned to this interface in /etc/config/network

Figure 10.9-3: MWAN Interface Edit 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.
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.

Parameters	Description
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.

Table 10.9-3: MWAN Interface Edit Configuration

10.9.4 Members

Network > Load Balancing > Members

Members correspond to individual interfaces where you can set metric and weight.

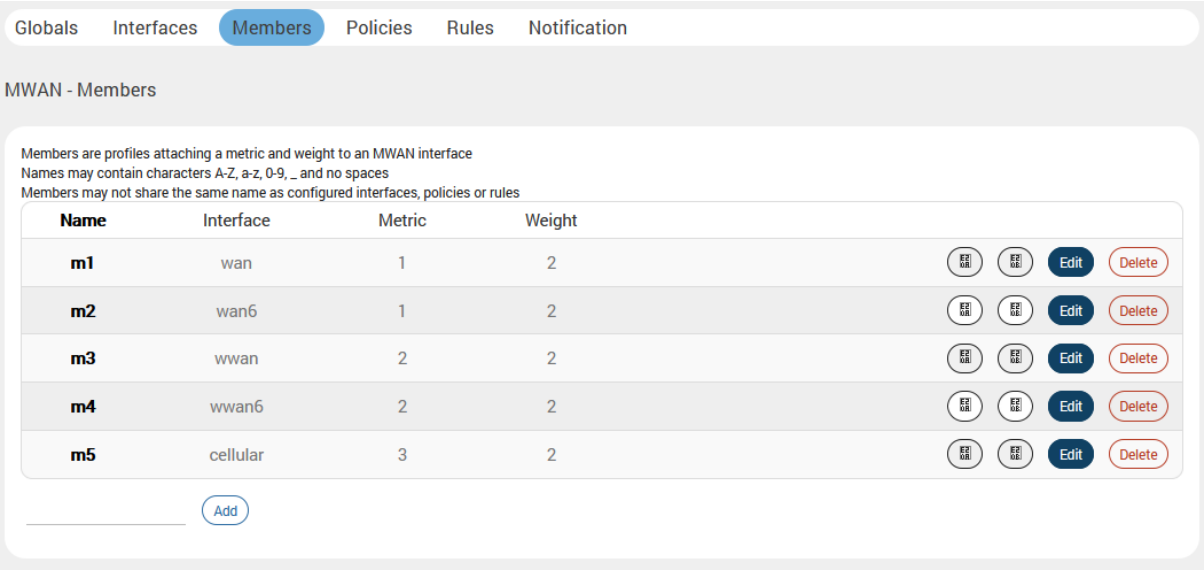


Figure 10.9-4: MWAN Interface Members

Parameters	Description
Member	Displays the Interface member notation number.
Interface	Displays the name of the interface.
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***

Parameters	Description
	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.

Table 10.9-4: MWAN Interface Members

10.9.4.1 Add/Edit Member

Network > Load Balancing > Members

Figure 10.9-5: MWAN Interface 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 metric 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

Table 10.9-5: MWAN Interface Members Configuration

10.9.5 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 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 weights values. Policy can also be configured to use one member and then fail over to another.

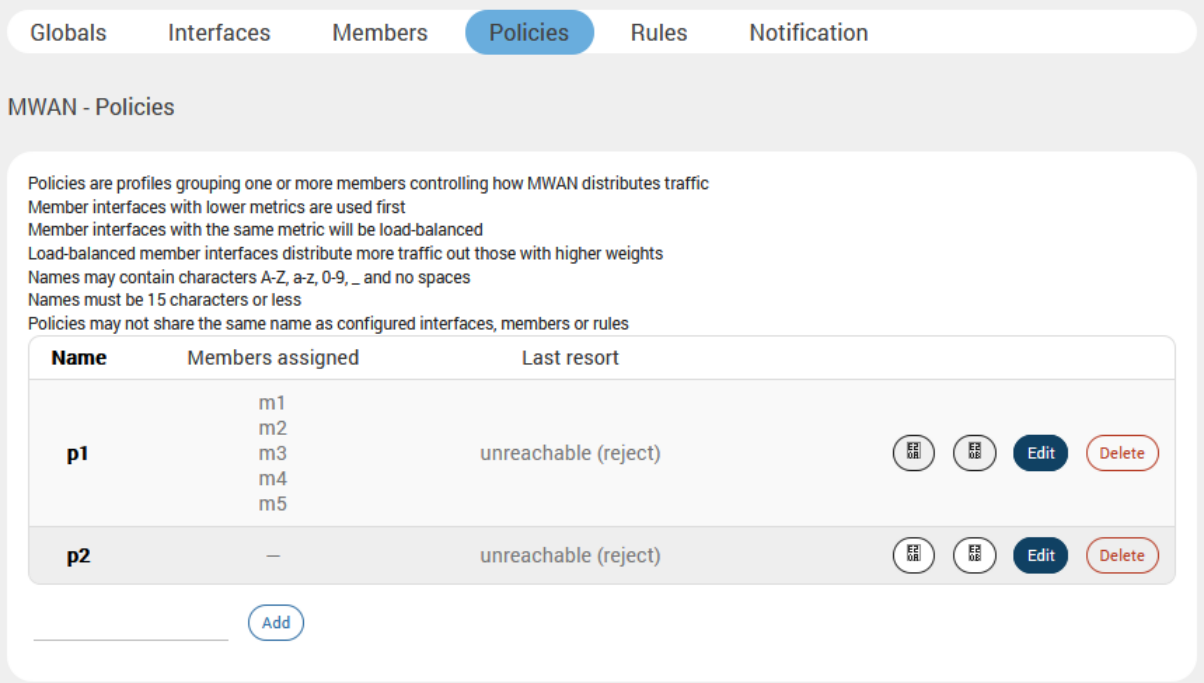


Figure 10.9-6: MWAN Interface Policy

Parameters	Description
Policy	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.
Add	Add a new policy

Table 10.9-6: MWAN Interface Policy

10.9.5.1 Add/Edit Policy

Network > Load Balancing > Policies

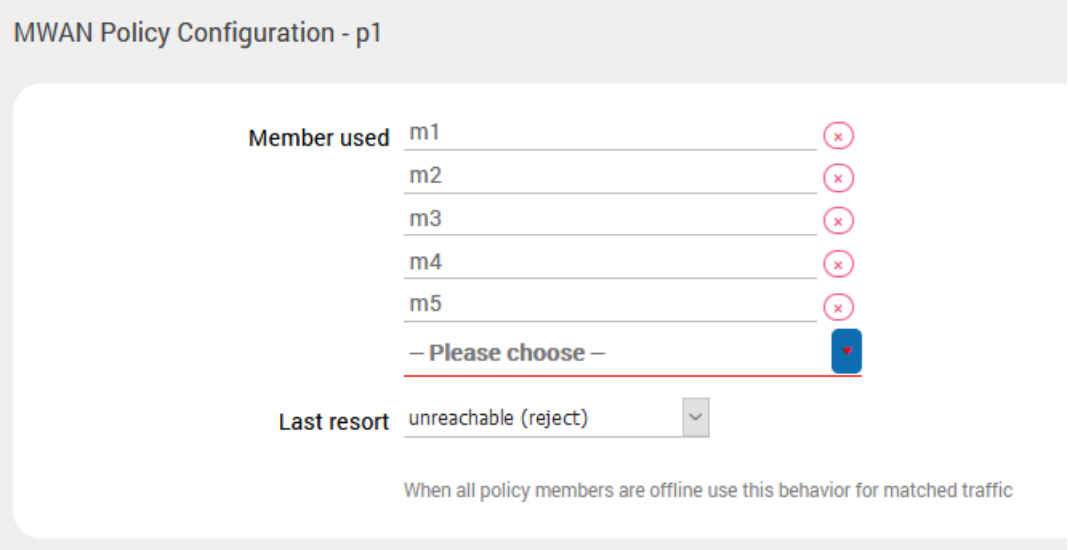


Figure 10.9-7: MWAN Interface Policy Configuration

Parameters	Description
Member used	Select the interface to apply the policy on 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)*

Table 10.9-7: MWAN Interface Policy Configuration

10.9.6 Rules

Network > Load Balancing > Rules

A rule specifies what traffic to match and what policy to assign for that traffic.

The web UI also lists key points to consider when configuring rules as shown in the figure below..

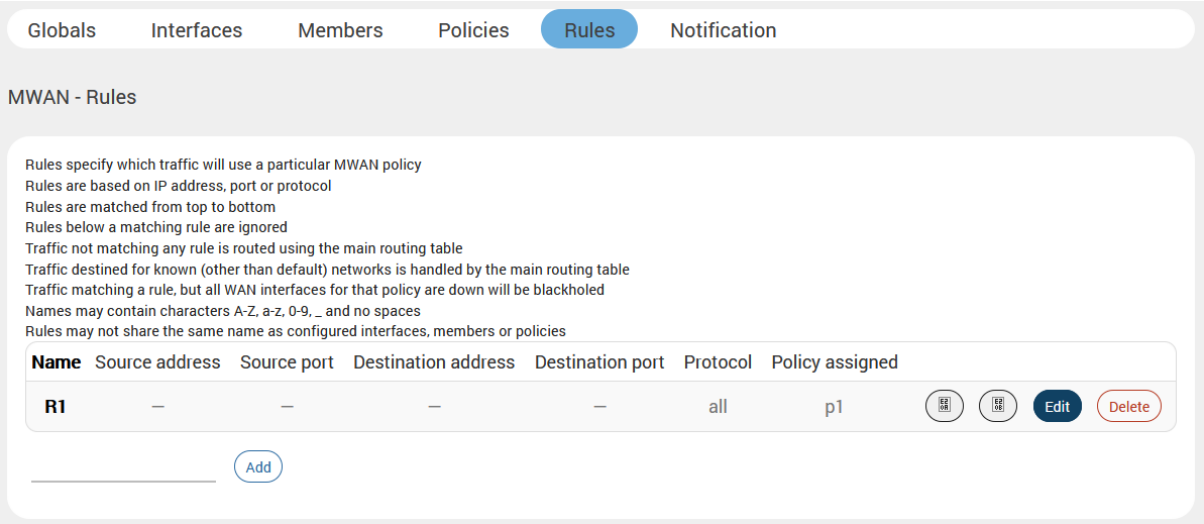


Figure 10.9-8: MWAN Interface Rules

Parameters	Description
Rule	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.
Add	Enter the name of the new rule and click Add. Continue configuring the rule parameters.

Table 10.9-8: MWAN Interface Rules

10.9.6.1 Add/Edit Rule

Network > Load Balancing > Rules

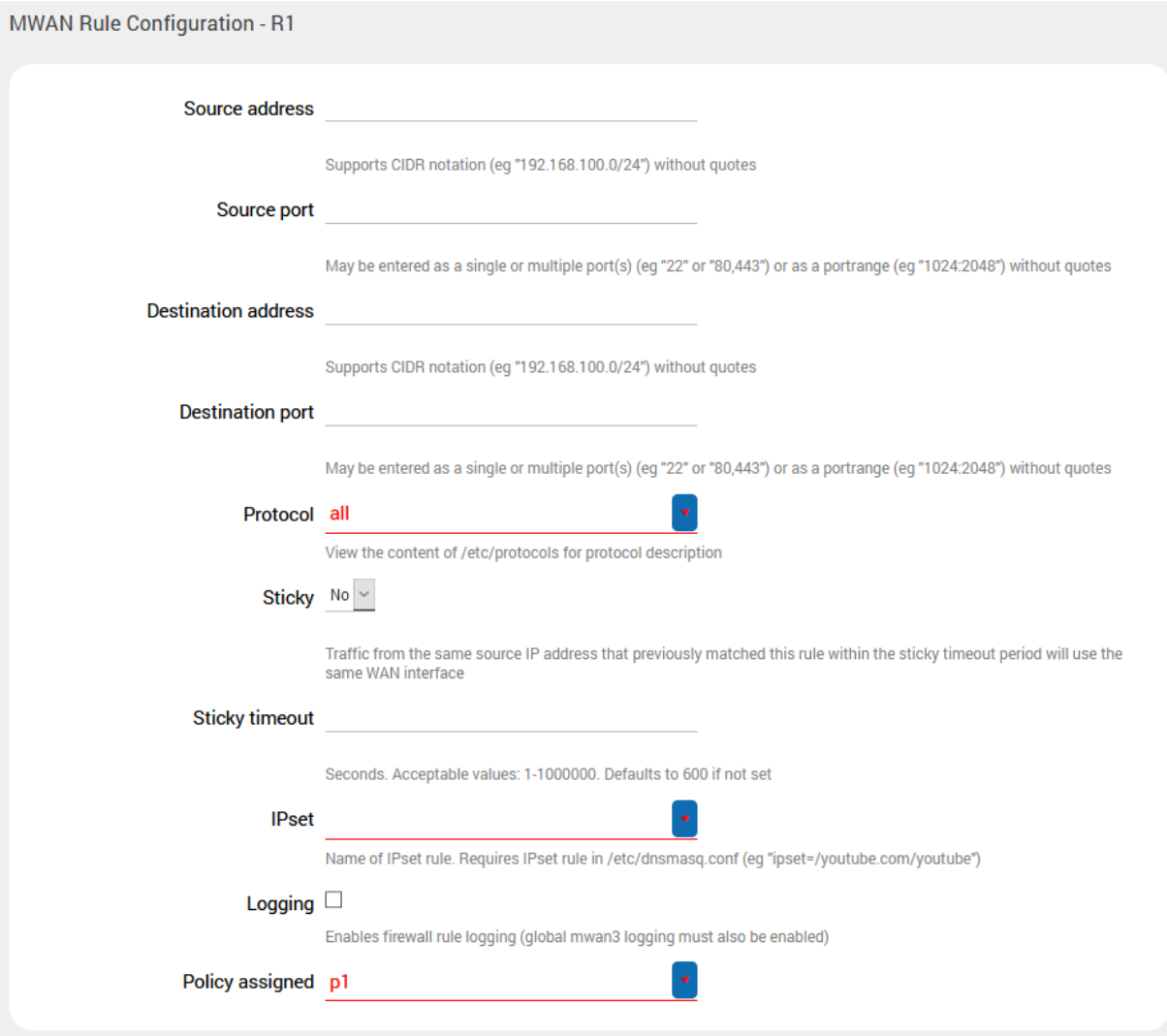


Figure 10.9-9: MWAN Interface Rules Configuration

Parameters	Description
Source address	Enter the Source IP Address.
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.

Parameters	Description
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.

Table 10.9-9: MWAN Interface Rules Configuration

10.9.7 Notification

Network > Load Balancing > Notification

MWAN - Notification

This section allows you to modify the content of "/etc/mwan3.user".
The file is also preserved during sysupgrade.

Notes:
This file is interpreted as a shell script.
The first line of the script must be "#!/bin/sh" without quotes.
Lines beginning with # are comments and are not executed.
Put your custom mwan3 action here, they will
be executed with each netifd hotplug interface event
on interfaces for which mwan3 is enabled.

There are three main environment variables that are passed to this script.

$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")

```
#!/bin/sh
#
# This file is interpreted as shell script.
# Put your custom mwan3 action here, they will
# be executed with each netifd hotplug interface event
# on interfaces for which mwan3 is enabled.
#
# There are three main environment variables that are passed to this script.
#
# $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")
```

Figure 10.9-10: MWAN Notification

11 Percepxion

The E210 and E220 series gateways come integrated with Percepxion cloud platform to allow for the remote management of devices.

11.1 Percepxion Configuration

To view and configure the Percepxion Client, go to:

Percepxion > Client

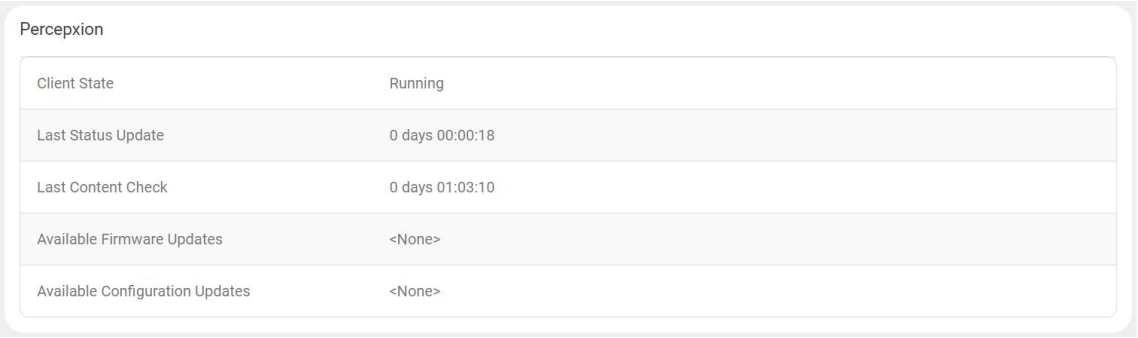


Figure 11.1-1: Percepxion Client Status

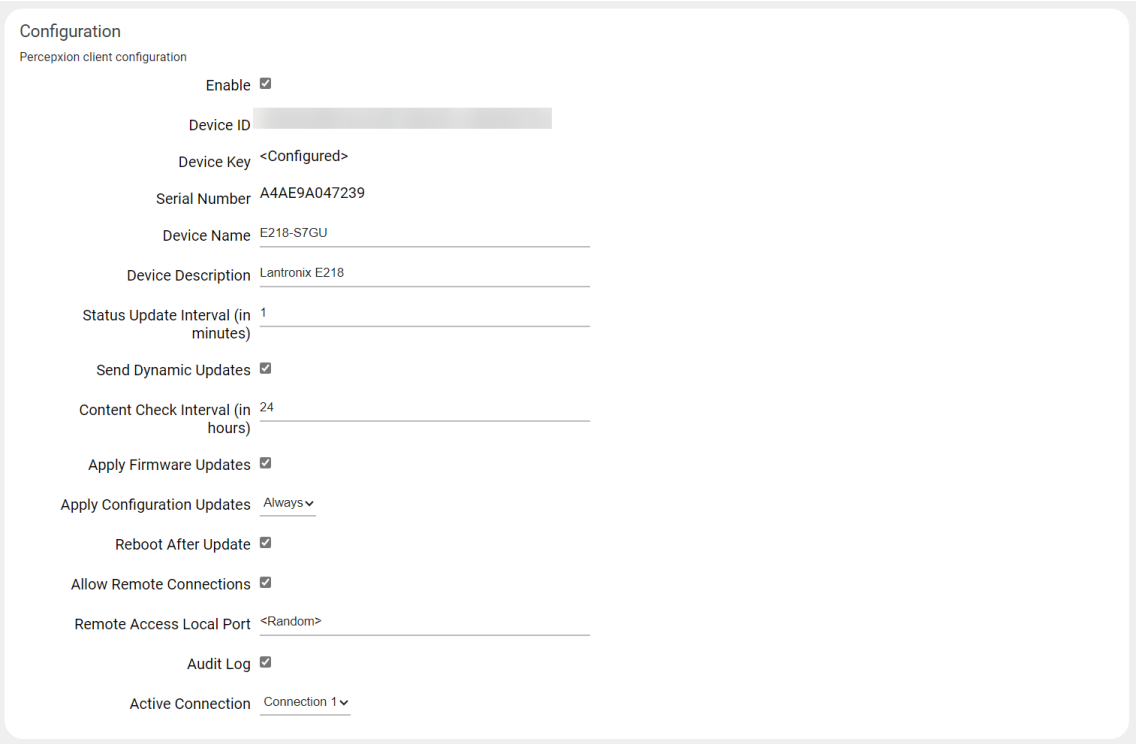


Figure 11.1-2: Percepxion Client Settings

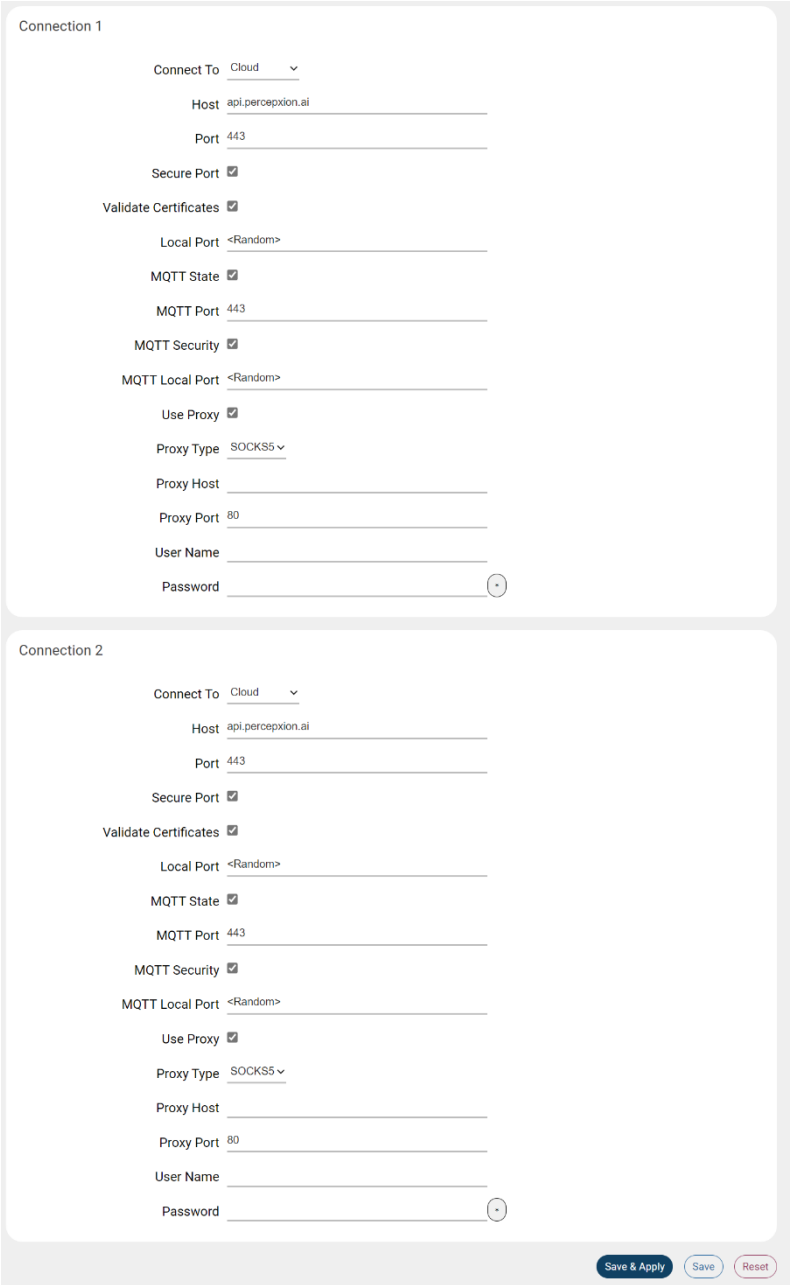


Figure 11.1-3: Percepxion Client Connection1/Connection2 Settings

The below table lists the configuration details of the Percepxion Client settings:

Parameters	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.***
Device Key	Read only. Shows whether the gateway's Device Key has been configured. Device Key may be configured through the Lantronix.

Parameters	Description
	Provisioning Manager.
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	Enable to receive RSSI and Temperature updates.
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 Upgrades	Select to allow firmware updates to be applied via Percepxion. Enabled by default.
Apply Configuration Upgrades	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.
Allow Remote Connections	Select to allow remote connections or clear to disable. Enabled by default.
Remote Access Local Port	Local port for remote access connection.
Audit Log	Enable or disable audit log.
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.
Connection1/Connection2	
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	Enable or disable MQTT.

Parameters	Description
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. They are 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 of the proxy server.

Table 11.1-1: Percepxion Client Settings Configuration

12 Discovery

Network discovery allows your computer to locate other computers and devices on the network. This setting also allows other computers to see your computer. If enabled, the device responds to auto-discovery messages on port 0x77FE.

12.1 Query Port

Discovery>Query Port

This page displays the current query port statistics and the configuration option to enable or disable discovery. Query port is enabled by default.

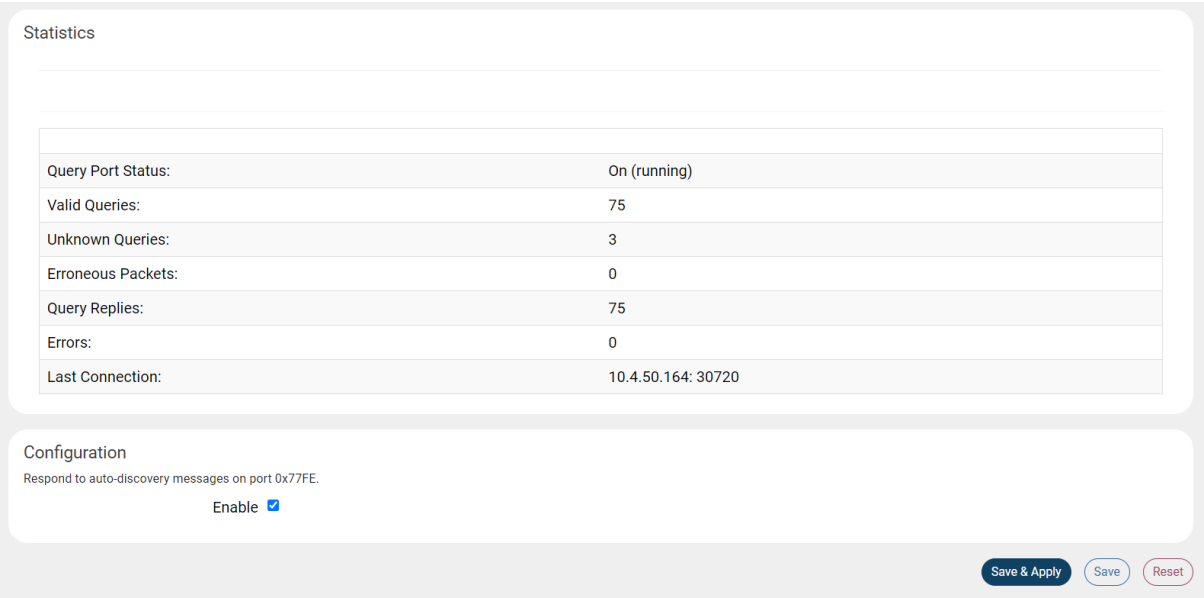


Figure 12.1-1: Discovery Query Port

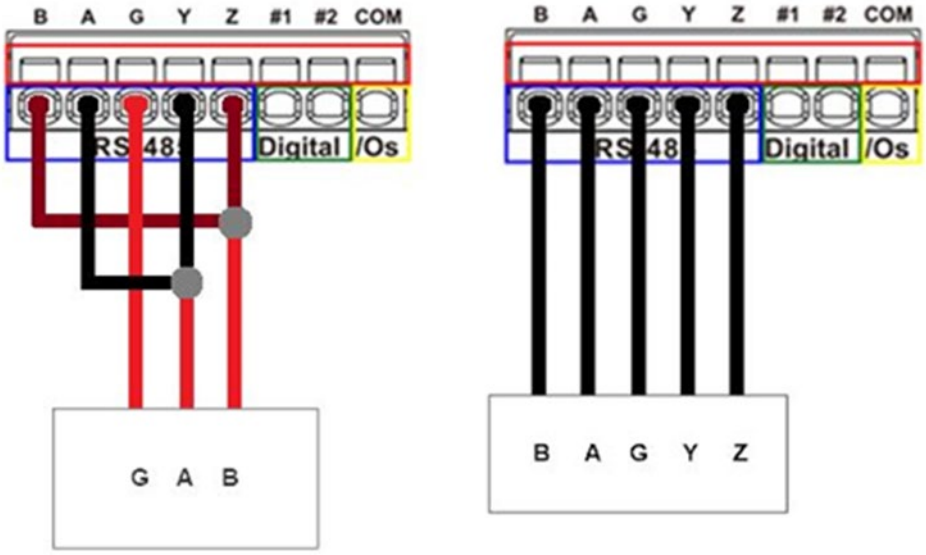
To enable or disable query port discovery:

1. Under Configuration, select **Enable**.
2. Click **Save & Apply**.

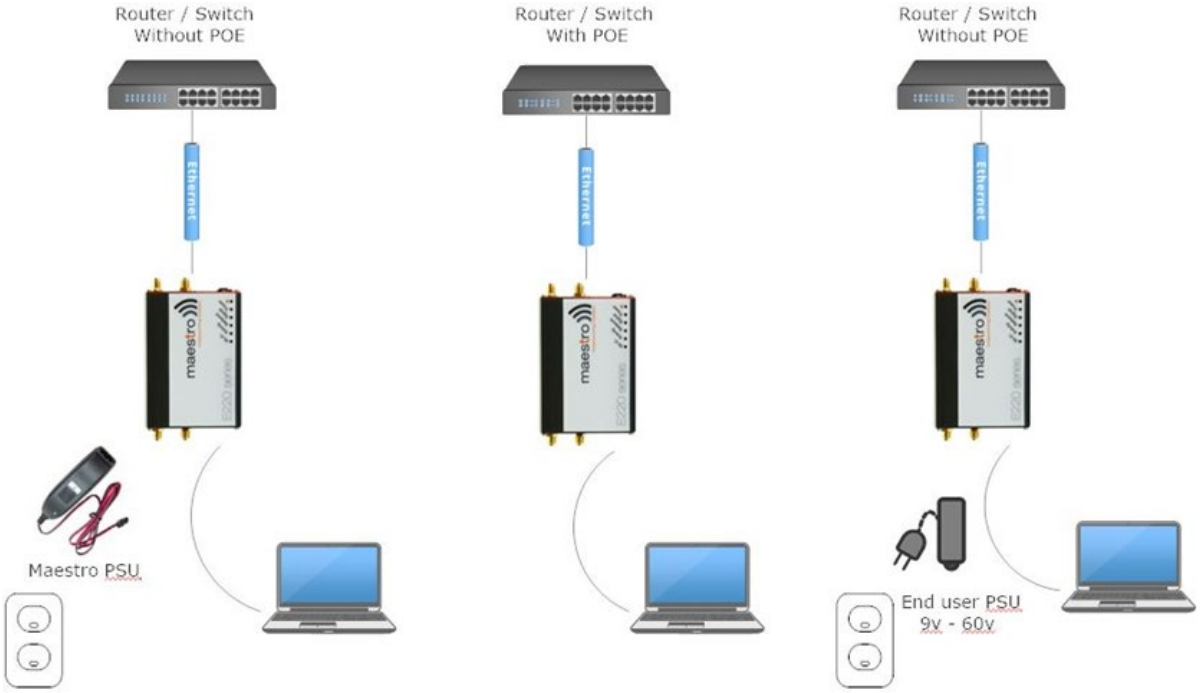
Appendix A. Wiring Diagrams

RS485 Wiring diagram

Half Duplex (Left) RS485 Full Duplex (Right)



Power over Ethernet



Appendix B. LED Behavior

Ethernet Port LEDs

The ethernet port LEDs on the side panels of the E210 and E220 devices indicate link and activity status for WAN and LAN connections.

LED Color	State and Description
Amber LED (Link indicator)	Solid ON When light is on, this LED indicates valid link detection.
Green LED (Activity indicator)	Blinking ON When light is blinking, this LED indicates traffic or data activity on the port.

Top Panel LEDs for E220 Series

The top panel of the E220 devices features 6 LEDs to indicate critical system information.

Name	Color and State		Description
Alert		OFF	No alert, device is running smoothly

Name	Color and State		Description
		Red ON	Hardware fault (high temperature or problem with module), Cellular Module reboot, Linux Kernel booting
Power		OFF	Power off
		Green ON	Power on
Signal		OFF	No signal (CSQ=0 to 5, 97, 98, 99)
		Amber Flashing	Weak signal (CSQ > 6 to 12)
		Amber ON	Strong signal (CSQ >12)
Network		OFF	Not registered on a cellular network.
		Amber Flashing	Registered on a roaming cellular network
		Amber ON	Registered on home cellular network
Activity		OFF	Cellular data service is not connected
		Amber Flashing	Data Transfer over Cellular Network
		Amber ON	Cellular data service is connected
WI-FI		OFF	Wi-Fi network is inactive
		Blue Flashing	Traffic on Wi-Fi network
		Blue ON	Wi-Fi network is up and activated

Top Panel LEDs for E210 Series

The top panel of Lantronix E210 Series Routers features 7 LEDs to indicate critical system information.

Name	Color and State		Description
Alert		OFF	No alert, device is running smoothly
		Red ON	Hardware fault (high temperature or problem with module), Cellular Module reboot, Linux Kernel booting
Power		OFF	Power off
		Green ON	Power on
SIM in use		On	SIM 1
		Flashing	SIM 2
Signal		OFF	No signal (CSQ=0 to 5, 97, 98, 99)
		Amber Flashing	Weak signal (CSQ > 6 to 12)
		Amber ON	Strong signal (CSQ >12)
Network		OFF	Not registered on a cellular network.
		Amber Flashing	Registered on a roaming cellular network
		Amber ON	Registered on home cellular network
Activity		OFF	Cellular data service is not connected

Name	Color and State		Description
		Amber Flashing	Data Transfer over Cellular Network
		Amber ON	Cellular data service is connected
WI-FI		OFF	Wi-Fi network is inactive
		Blue Flashing	Traffic on Wi-Fi network
		Blue ON	Wi-Fi network is up and activated

Appendix C. List of Acronyms

Acronym	Description
2G	2nd Generation
3G	3rd Generation
AES	Advanced Encryption Standard
AP Client	Access Point Client
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 (DHCP) is a standardized networking protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.
DIO	Digital Input/Output
DMZ	In computer security, a DMZ or 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.
DNS	Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network
DynDNS, DDNS	Dynamic DNS (DDNS) 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 digital mobile phone technology that allows improved data transmission rates as a backward-compatible extension of GSM.
GPRS	General packet radio service (GPRS) is a packet oriented mobile data service on the 2G and 3G cellular communication system's global system for mobile communications
GPS	Global Positioning Satellite
GSM	Global system for mobile communications
HT Physical mode	High Throughput Physical Mode
ICMP	Internet Control Message Protocol (ICMP) is one of the main protocols of the Internet Protocol Suite. It is used by network devices, like routers, to send error messages
IGMP	Internet Group Management Protocol is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships

Acronym	Description
IKEv1 and IKEv2	Internet Key Exchange (version 1 or version 2) is an encryption key exchange mode used between two peers.
IP Sec	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
LLTD	Link Layer Topology Discovery is a proprietary Link Layer protocol for network topology discovery and quality of service diagnostics
M2M	Machine to machine
MAC address	Media access control address is a unique identifier assigned to network interfaces for communications on the physical network segment
MD5	MD5 is a message digest algorithm used as a checksum to verify data integrity
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 methodology of modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device for the purpose of remapping one IP address space into another.
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.
PPP	Point to Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PSK	Pre-shared key
QoS	Quality of Service
RF	Radio Frequency

Acronym	Description
Rx	Reception
SCP	Secure Copy Protocol
SHA1/SHA2	Secure Hash Algorithm is an encryption cipher type
SIM	Subscriber identity module
SMS	Short Message Service
SPI	Serial Peripheral Interface
SSH	Secure Shell
SSID	Service set identification
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	Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are security protocols for wireless networks. WPA uses Temporal Key Integrity Protocol (TKIP) for encrypted data transfer and Extensible Authentication Protocol (EAP) for authorizing users. The more secure WPA2 requires using the stronger encryption method Advanced Encryption Standard. (AES).

Appendix D. Running Commands

Commands can be run on the E210 and E220 series gateways 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`.

The following types of commands are available:

- Bash commands
- opkg commands
- UCI commands

Bash Commands

Bash shell is distributed with Busybox which provides a lightweight implementation of common Linux commands.

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 many 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.***

Examples

`ls`

List directory contents

To show current directory commands:

```
# 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

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.

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

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

To show syslogd diagnostic logs:

```
# logread
Oct 11 20:00:16 Lantronix-E228-A4AE9A048423 user.info Eventsms:
TEMPERATURE : 40.00 °Celsius
Oct 11 20:00:16 Lantronix-E228-A4AE9A048423 user.info Eventsms:
CONF_BAND : LTE: [ B2 B4 B5 B13 B66 ]
Oct 11 20:00:16 Lantronix-E228-A4AE9A048423 user.info Eventsms:
REG_BAND : B4
Oct 11 20:00:16 Lantronix-E228-A4AE9A048423 user.info Eventsms:
Operator : 311480
Oct 11 20:00:16 Lantronix-E228-A4AE9A048423 user.info Eventsms:
Operator : Verizon
Oct 11 20:00:16 Lantronix-E228-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 updates.d2sphere.com).

opkg update

Update the packages list

opkg install

Install software package

opkg remove

Remove software package

Example

```
# opkg update
Downloading
https://updates.d2sphere.com/ePack/E21X/ipks/3_18_0_0R9/main/Package
s.gz
Updated list of available packages in /var/opkg-lists/lantronix_core
Downloading
https://updates.d2sphere.com/ePack/E21X/ipks/3_18_0_0R9/main/Package
s.sig
Signature check passed.

# opkg install tcpdump
Installing tcpdump (4.9.3-3) to root...
Downloading
https://updates.d2sphere.com/ePack/E21X/ipks/3_18_0_0R9/main/tcpdump
_4.9.3-3_mipsel_24kc.ipk
Configuring tcpdump.

# opkg remove tcpdump
Removing package tcpdump 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 60***

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 or usage of the UCI commands.

Note:

- ***Some configuration and commands may not be available on the router.***