



ePACK User Manual E210 and E220 Series Devices

Intellectual Property

© 2019-20 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.

7535 Irvine Center Drive, Suite 100
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-453-3995

Technical Support

Online: www.lantronix.com/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

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

Contents

1	About this Guide	8
1.1	Purpose and Audience	8
1.2	Summary of Chapters	8
1.3	Additional Documentation	9
2	Introduction	10
2.1	Product Features	11
2.1.1	E210 Series	11
2.1.2	E220 Series	12
3	Default Configuration	13
3.1	Web Admin Page	13
3.2	Wireless Access Point SSID	13
3.3	Default Interface Configuration	13
4	Web Administration Interface	14
4.1	Web Admin Interface	14
4.2	Logging In	15
4.3	Change Passwords After Initial Login	16
4.4	Logging Out	17
5	Quick Setup	18
5.1	Quick Setup	18
6	Status	20
6.1	Overview	20
6.1.1	Status	20
6.2	Firewall Status	31
6.2.1	IPv4 Firewall	31
6.2.2	IPv6 Firewall	32
6.3	Routes	33
6.4	System Log	35
6.5	Kernel Log	36
6.6	Processes	36
6.7	Realtime Graphs	37
6.7.1	Load	37
6.7.2	Traffic	38
6.7.3	Wireless	39
6.7.4	Connection	40
6.8	Load Balancing	42
6.8.1	Interface	42
6.8.2	Detail	42
6.8.3	Diagnostics	43

6.8.4	Troubleshooting	43
7	System	44
7.1	System	44
7.1.1	General Settings	44
7.1.2	Logging	46
7.1.3	Time Synchronization	48
7.1.4	Language and Style	48
7.2	Administration	50
7.2.1	Router Password	50
7.2.2	SSH Access	51
7.2.3	SSH-Keys	53
7.3	Software	54
7.3.1	Installed and Available Packages	54
7.3.2	OPKG Configuration	55
7.4	Startup	56
7.4.1	Initscripts	56
7.4.2	Local Startup	56
7.5	Scheduled Tasks	57
7.6	LED Configuration	57
7.6.1	Add/Edit LED Configuration	58
7.7	Backup / Flash Firmware	58
7.7.1	Actions	58
7.7.2	Configuration	61
7.8	Custom Commands	62
7.8.1	Dashboard	62
7.8.2	Configure	63
7.9	Reboot	64
8	VPN	65
8.1	IPSec (Internet Protocol Security)	65
8.1.1	Gateway to Gateway	66
8.2	OpenVPN	72
8.2.1	OpenVPN Instances	72
8.2.2	Edit OpenVPN Instance from Template	75
8.2.3	Edit OpenVPN Instance from Configuration File	78
9	Services	79
9.1	Dynamic DNS	80
9.1.1	Basic Settings	80
9.1.2	Advanced Settings	82
9.1.3	Timer Settings	83
9.1.4	Log File Viewer	84
9.2	Agents	85
9.3	SD(HC)/MMC Card	86
9.4	D2sphere	87
9.4.1	D2Sphere Configuration	87

9.5	DOTA	88
9.5.1	Lantronix Server	88
9.5.2	Custom Server	90
9.6	Page Selector	91
9.7	SMS	91
9.7.1	SMS Configuration	91
9.7.2	Ethernet SMS	95
9.7.3	Live Message	97
9.8	Reporting Agent	98
9.8.1	Sending Data	100
9.8.2	Data Format	101
9.9	GPS	103
9.9.1	Sample GPS Frames	106
9.10	Keepalived	112
9.10.1	General	112
9.10.2	Keepalived Global	113
9.10.3	Tracking Scripts	115
9.10.4	Tracking Interfaces	116
9.10.5	Tracking Processes	117
9.10.6	Virtual IP	118
9.10.7	VRRP Instances	119
9.11	Last Gasp	121
9.12	Serial	122
9.12.1	Serial Configuration	122
9.12.2	Serial Data Send Configuration	123
9.13	Service Actions	128
9.14	Events	129
9.14.1	Event Management	129
9.15	uHTTPd	130
9.15.1	General Settings	130
9.15.2	Full Web Server Settings	133
9.15.3	Advanced Settings	135

10 Network

138

10.1	Interfaces	138
10.1.1	Interfaces Overview	139
10.1.2	Interface Status	141
10.1.3	Interface Protocols	142
10.1.4	CELLULAR Interface	153
10.1.5	LAN Interface	155
10.1.6	WAN and WAN6 Interface	158
10.1.7	WWAN and WWAN6 Interface	161
10.1.8	Add Virtual Interface	163
10.2	Wireless	166
10.2.1	Wireless Network Configuration	168
10.3	Switch	176
10.4	DHCP and DNS	178
10.4.1	General Settings	179

10.4.2	Resolv and Host Files	181
10.4.3	TFTP Settings	182
10.4.4	Advanced Settings	183
10.4.5	Static Leases	185
10.5	Hostnames	186
10.6	Static Routes	187
10.6.1	Static IPv4 Routes	187
10.6.2	Static IPv6 Routes	188
10.7	Diagnostics	190
10.8	Firewall	191
10.8.1	General Settings	191
10.8.2	Port Forwards	198
10.8.3	Traffic Rules	201
10.8.4	Custom Rules	204
10.9	Load Balancing	205
10.9.1	How it works	205
10.9.2	Globals	206
10.9.3	Interfaces	207
10.9.4	Members	210
10.9.5	Policies	212
10.9.6	Rules	214
10.9.7	Notification	217

Appendix A. Wiring Diagrams 218

Appendix B. LED Behavior 219

Appendix C. List of Acronyms 223

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 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.

Chapter	Description
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.

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
<i>E210 Series Cellular Router Quick Start Guide</i>	Provides hardware installation instructions, directions to connect the E210 series router, and network IP configuration information.
<i>E220 Series Cellular Router Quick Start Guide</i>	Provides hardware installation instructions, directions to connect the E220 series router, and network IP configuration information.
<i>E210 Series User Guide</i>	Provides E210 series accessories and part number information, product features and hardware description, hardware installation instructions, compliance statements and notices.
<i>E220 Series User Guide</i>	Provides E220 series accessories and part number information, product features and hardware description, hardware installation instructions, compliance statements and notices.
<i>E210 Series Product Brief</i>	Provides E210 series router product overview information and specifications.
<i>E220 Series Product Brief</i>	Provides E220 series router product overview information and specifications.

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		FCS ⁴	ORDER CODE
							COMPLETED IN PROGRESS UNDER CONSIDERATION			
E215	EMEA; South-East Asia; South Asia	3G ²⁷	8/1	2G ^{A1}	8/3	x	EN300328 ETA, TEC		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 ²²	5/8/1	Optional	RCM;		Aug. '18	E214F003S
	EMEA; Asia Pacific		28/20/8/3/1/7	3G ²³ ; 2G ^{A3}	8/1; 8/3		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	LTE cat. 1	13/4	x	N/A	✓	FCC ⁹ , Verizon Wireless		Nov. '18	E214G001S
	The Americas – excl. Verizon Wireless		12/5/4/2	3G ²³	5/4/2		FCC ⁹ , PTCRB, AT&T Wireless; ISED			E214G000S
E218	Brazil; Australia & New Zealand; Thailand	LTE cat. 4	28/5/8/3/1/7	3G ²³ ; 2G ^{A3}	5/8/1; 8/3	Optional	NBTC		Mar. '19	E218F004S
	NTT docomo		19/21/1				-		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	x	N/A	x	Postel		tbd	E213F10ES
E214G	USA & Canada	LTE cat. 1	71/12/13/14/26(5)/66(4)/25(2)				✓	FCC ⁹ , PTCRB; ISED		tbd
	Japan; South Korea		18/5(19)/8/21/3/1/7			JRF, JPA; KC		tbd	E214G10TS	
E218	EMEA; Asia Pacific	LTE cat. 4	28/20/8/3/1/7	3G ²³ ; 2G ^{A3}	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: ^{A1} 85⁶ / 236⁸; or ^{A2} 236⁸ / 236⁸; or ^{A3} 236⁸ / 296 kbps
- 3G: ^{T1} 5.76 / 7.2; or ^{T2} 5.76 / 10¹; or ^{T3} 5.76 / 42² Mbps
- LTE-M1 [NB1]: 375 / 300 [62⁵ / 27²] kbps updated to LTE-M2 [NB2]: 1,000 / 600 [140 / 120] kbps
- LTE cat. 1: 5 / 10 Mbps (FDD); 3¹ / 8⁹⁶ 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 ²⁷	8/1	2G ^{A1}	8/3	*	CE ETA, TEC	Sep. '16	E225FLZS
E225G Mk II	World	3G ²⁷	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 ²³ ; 2G ^{A3}	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 ²⁷	5/8/2/1	2G ^{A1}	5/8/3/2		-	Oct. '16	E225HPLFS
E224	EMEA	LTE cat. 1	20/8/3	2G ^{A3}	8/3	cf. footnote ⁶	CE	Apr. '17	E224HPLZS
	Australia & New Zealand		28/5/8/3	3G ²²	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 ²³	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: ^{A1} 85⁶ / 236⁸; or 236⁸ / ^{A2} 236⁸; or ^{A3} 296 kbps
- 3G: 5⁷⁶ / ^{T1} 7²; or ^{T2} 10¹; or ^{T3} 42² Mbps
- LTE cat. 1: 5 / 10 Mbps (FDD); 3¹ / 8⁹⁶ Mbps (TDD)
- LTE cat. 4: 50 / 150 Mbps (FDD); 35 / 130 Mbps (TDD)

² Ranked by increasing frequencies

- ⁹ 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
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:

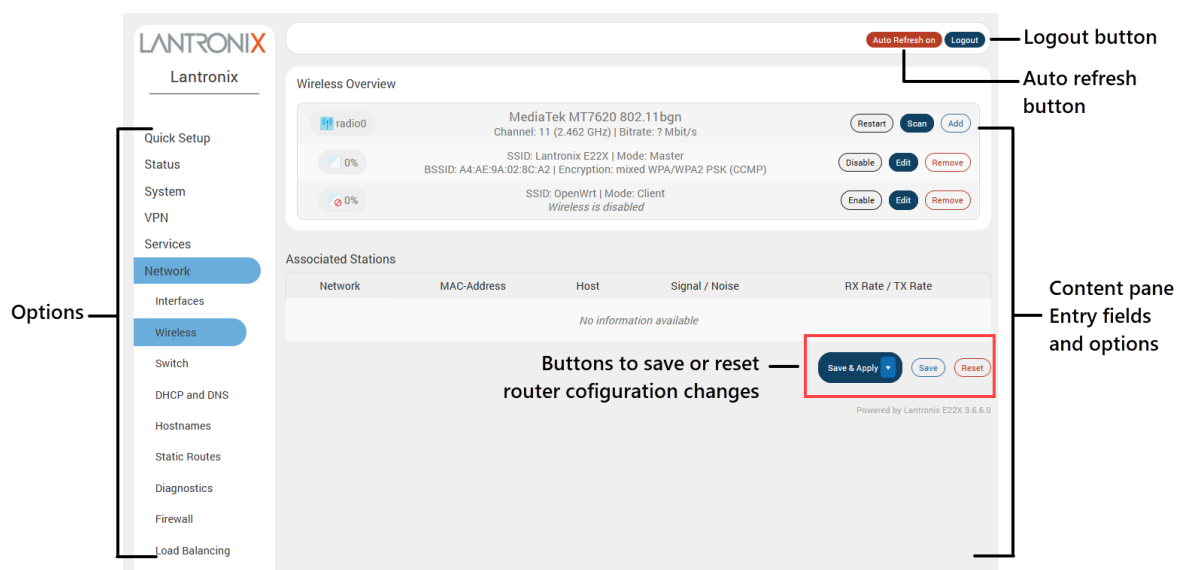


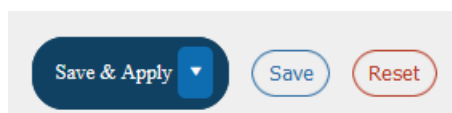
Figure 4.1-1: Web Admin Interface

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:

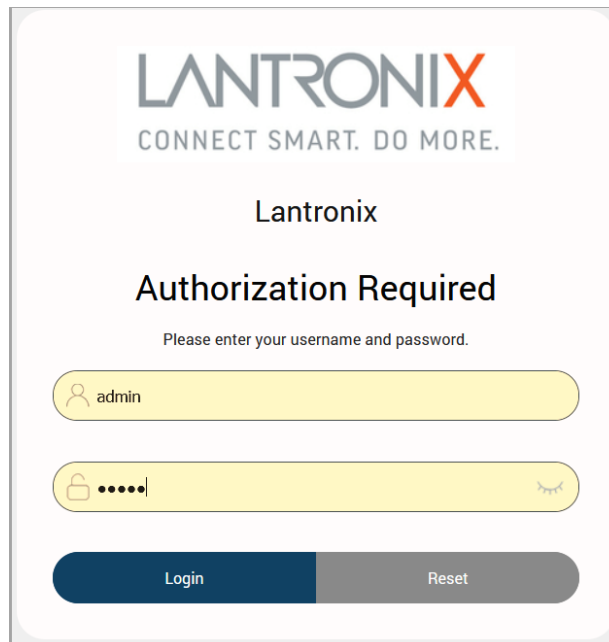
- Ethernet port or Wi-Fi connectivity and Internet service
- Web browser –Google Chrome, Mozilla Firefox, Internet Explorer or Microsoft Edge, Apple Safari (with the latest updates installed)
- DHCP client is enabled on the computer to obtain a valid IP Address from the router with LAN IP address 192.168.1.1.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



The image shows the Lantronix web administration login page. At the top, the Lantronix logo is displayed with the tagline "CONNECT SMART. DO MORE." Below the logo, the text "Lantronix" and "Authorization Required" are centered. A prompt asks the user to "Please enter your username and password." There are two input fields: the first is for the username, containing "admin", and the second is for the password, shown as masked dots. Below the input fields are two buttons: "Login" and "Reset".

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).

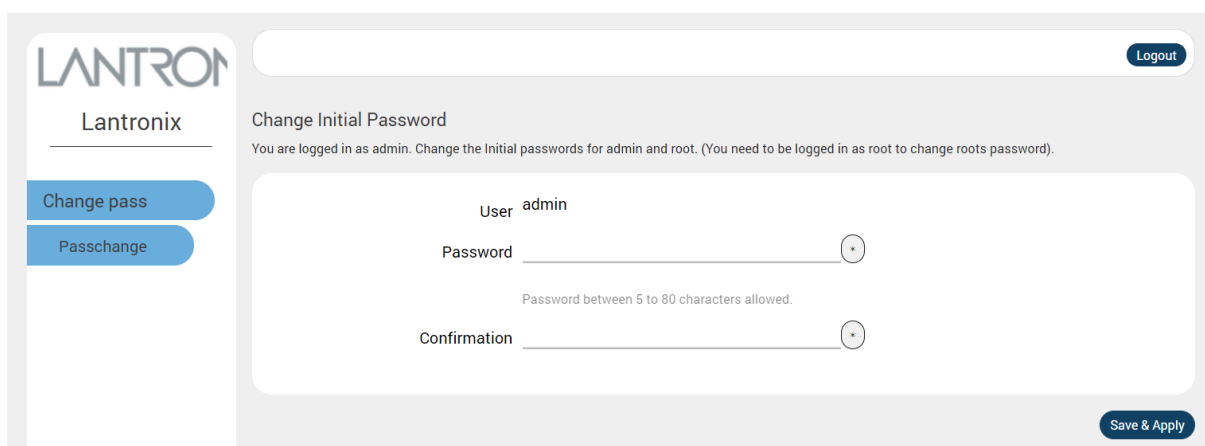
Note

- ***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:



The image shows the "Change Initial Password" page in the Lantronix web interface. The page title is "Change Initial Password" and it includes a sub-header: "You are logged in as admin. Change the Initial passwords for admin and root. (You need to be logged in as root to change roots password)." The page features a sidebar on the left with the Lantronix logo and two buttons: "Change pass" and "Passchange". The main content area has a "User" field set to "admin", a "Password" field, and a "Confirmation" field. A note below the password field states "Password between 5 to 80 characters allowed." There are "Logout" and "Save & Apply" buttons.

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.

Network Setup

Here you can configure the basic aspects of your device like its hostname or the timezone.

Local Area Network (LAN)

IPv4-Address

If this parameter is modified, use "Apply Unchecked" instead of "Save & Apply" to avoid roll back of the configuration

IPv4-Netmask

Wide Area Network (Wired WAN)

Protocol ▼

Manual => Used if you have static IP allocated from ISP.
Automatic => Used if you need to do dhcp with ISP.
PPPoE => Used if you need to do dial-up over ethernet with ISP.

Cellular

SIM settings

APN

PIN

Authentication Type ▼

Enable roaming

Cid

Wireless Network (LAN)

Disable

Mode

SSID

Encryption

Password ⊗

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: <i>Manual</i> - to set a static IP address. If selected, enter the IPv4 address, IPv4 netmask, IPv4 gateway, and DNS server. <i>Automatic</i> – to use DHCP server to acquire the IP address. <i>PPPoE (Point to Point Protocol over Ethernet)</i> . 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](#)
- [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
Model	E228GMKII#078
PID	E228GMKII#078-031103-WP7608-07011811080025
UbootVersion	U-Boot_1.1.3-Aug/13/2018-13:37:51
Architecture	MediaTek MT7620A ver:2 eco:6
Firmware Version	Lantronix E22X 3.5.28.0
Module Firmware	SWI9X07Y_02.28.03.03 000000 jenkins 2019/05/21 03:33:04
Kernel Version	4.14.166
Local Time	2020-09-15 19:18:22
Uptime	5h 17m 8s
Load Average	3.98, 2.80, 2.17
Reboot Cause	Power reset
IMEI	352913090113562

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-xxxxxxxxxxxxx. 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: xxxxxxxxxxxxx. 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 powered from a PSE-POE device over WAN port

Parameters	Description
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 <ul style="list-style-type: none"> <i>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.</i>

Table 6.1-1: System Status Overview

6.1.1.2 Cellular

Status > Overview > Status

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

Cellular	
Cellular Data	DISCONNECTED
Signal Strength	114
Network Status	Registered
Operator Name	T-Mobile
Operator Number	310260
Operator Type	LTE
Roaming Status	HOME
SIM Status	READY
IMSI	310260884373802
Configure BAND	UMTS:B2,B5, LTE:B2,B4,B5,B13,B17,
Registered BAND	1700,MHz,LTE,4
Temperature	45 Celsius
ICCID	8901260882243738025

Figure 6.1-2: 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.

Parameters	Description
	<i>Registered</i> <i>Not Registered</i>
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: <i>Home</i> <i>Roaming</i> <i>N/A</i>
SIM Status	Displays the availability of SIM card in SIM card slot. Error – <i>SIM card is not inserted.</i> Ready – <i>SIM card is inserted.</i>
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 6.1-2: Cellular Status Overview

6.1.1.3 Memory

[Status](#) > [Overview](#) > [Status](#)

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

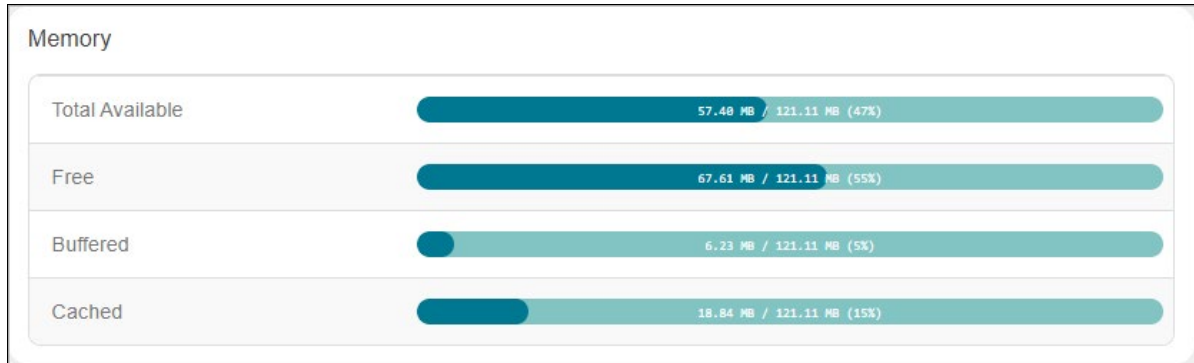


Figure 6.1-3: Memory Status Overview

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 6.1-3: Memory Status Overview

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

Table 6.1-4: E210 and E220 Devices RAM and Flash Size

6.1.1.4 Network

Status > Overview > Status

The Network group provides the IPv4 and IPv6 WAN status. The number of active connections is also displayed.

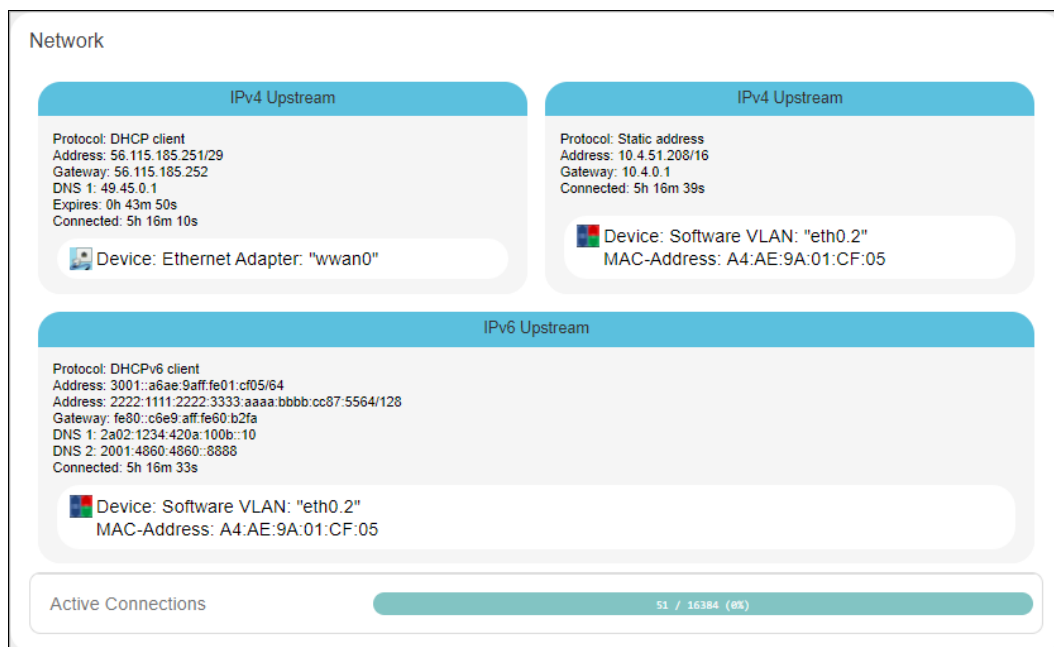


Figure 6.1-4: Network Status Overview

Parameters	Description
WAN	<p>Displays status of fixed-line WAN connection with following details:</p> <p>IP – IP Address of the WAN Interface.</p> <p>Gateway – IP Address of the WAN Interface Gateway.</p> <p>DNS – Two DNS IP Address; Primary DNS Server and Secondary DNS Server.</p> <p>Note</p> <ul style="list-style-type: none"> In case of WAN Access Wi-Fi must be configured in client mode and connected to an Access Point.
Cellular	<p>Displays status of Cellular network data connection with following details:</p> <p>IP – IP Address of the Cellular Interface.</p> <p>Gateway – IP Address of the Cellular Interface Gateway.</p> <p>DNS – Two DNS IP Address; Primary DNS Server and Secondary DNS Server.</p>
WWAN	<p>Displays status of Wi-Fi WWAN connection with following details:</p> <p>IP – IP Address of the WWAN Interface.</p> <p>Gateway – IP Address of the WWAN Interface Gateway.</p> <p>DNS – Two DNS IP Address; Primary DNS Server and Secondary DNS Server.</p>

Table 6.1-5: Network Status Overview

6.1.1.5 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.

Active DHCP Leases			
Hostname	IPv4-Address	MAC-Address	Leasetime remaining
<i>There are no active leases</i>			

Active DHCPv6 Leases			
Host	IPv6-Address	DUID	Leasetime remaining
<i>There are no active leases</i>			

Figure 6.1-5: 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 6.1-6: Active DHCP Leases Status Overview

6.1.1.6 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.

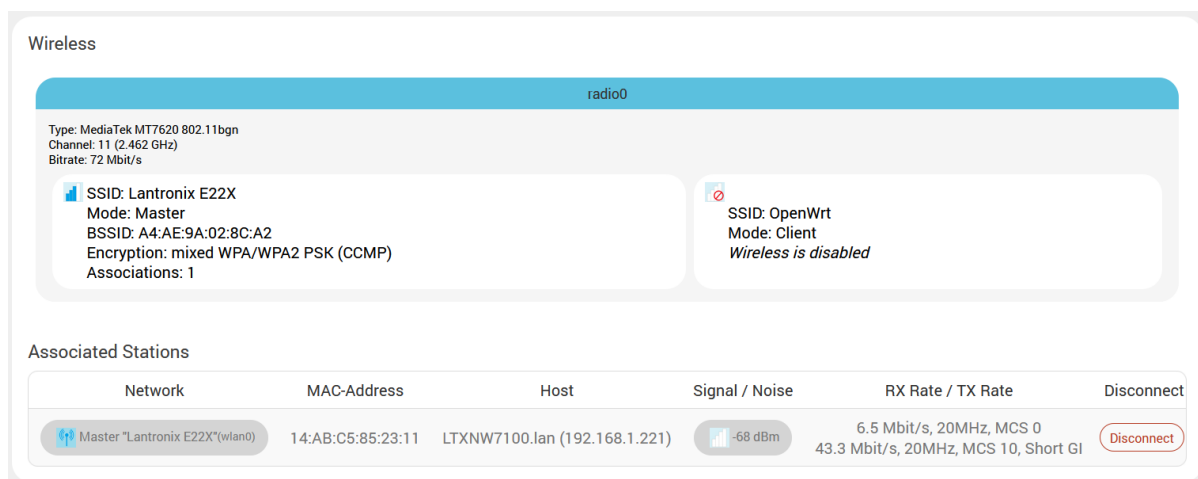


Figure 6.1-6: Wireless Status Overview

Parameters	Description
Connection Name	<p>Displays the name of the connection and the details:</p> <p>Type – The wireless radio chipset</p> <p>Channel – WiFi channel.</p> <p>Bitrate – Data transfer rate</p> <p>SSID –Service Set Identifier (SSID) that uniquely names a Wireless Local Area Network (WLAN)</p> <p>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.</p> <p>Note</p> <ul style="list-style-type: none"> For Wi-Fi WAN (WWAN) operation this should be ‘Client’. <p>BSSID – Displays Basic Service Set Identification (BSSID); 24 bit MAC Address of Wireless device.</p> <p>Encryption – Displays the data encryption method.</p> <p>Associations – Displays the number of associated stations.</p>
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 6.1-7: Wireless Status Overview

6.1.1.7 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.

Digital Input/Output		
Digital Input 1	LOW	●
Digital Input 2	LOW	●
Digital Output 1	OPEN	●
Digital Output 2	OPEN	●

Figure 6.1-7: Status DIO Pins

6.1.1.8 Dynamic DNS

[Status](#) > [Overview](#) > [Status](#)

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

Dynamic DNS				
Configuration	Next Update	Lookup Hostname	Registered IP	Network
myddns_ipv4	Disabled	yourhost.example.com		IPv4 / wan
myddns_ipv6	Disabled	yourhost.example.com		IPv6 / wan6

Figure 6.1-8: Status Dynamic DNS

6.1.1.9 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](#).

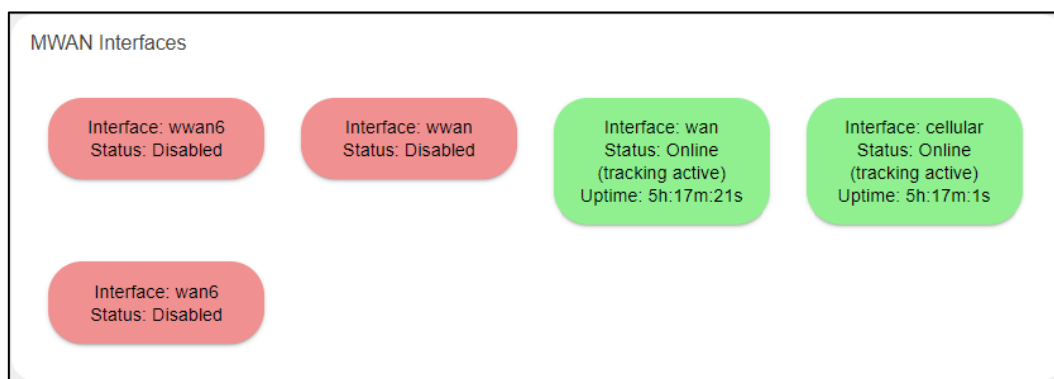


Figure 6.1-9: MWAN interfaces Status Overview

Parameters	Description
Interface	The type of interface. Can be wan, wwan, or cellular. Wan6 or wwan6 indicate IPv6 interfaces.
Status	<p>Shows whether the interface is Online (green), Offline, or Disabled (red).</p> <p>If the status is Online, the following details are displayed:</p> <p><i>tracking active</i> – the interface is being tracked for internet availability by pinging the IP provided in its configuration section.</p> <p><i>tracking off</i> – 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.</p> <p><i>Uptime</i> – the duration in hours, minutes and seconds that the interface has been connected</p> <p>If the status is Offline, the following is displayed:</p> <p><i>Downtime</i> – The time that the interface has been down since the last retry.</p> <p>If the status is Disabled, no details are displayed.</p>

Table 6.1-8: MWAN interfaces Status Overview

6.2 Firewall Status

Status > Firewall Status

6.2.1 IPv4 Firewall

Status > Firewall Status > IPv4 Firewall

Firewall Status

IPv4 Firewall IPv6 Firewall

Table: Filter Hide empty chains Reset Counters Restart Firewall

Chain *INPUT* (Policy: *ACCEPT*, 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
22.16 K	2.35 MB	ACCEPT	all	lo	*	0.0.0.0/0	0.0.0.0/0	-	-
113.27 K	12.93 MB	input_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom input rule chain
66.30 K	8.93 MB	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-
2.31 K	120.12 KB	syn_flood	tcp	*	*	0.0.0.0/0	0.0.0.0/0	tcp flags:0x17/0x02	-
0	0 B	zone_lan_input	all	br-lan	*	0.0.0.0/0	0.0.0.0/0	-	-
46.97 K	4.00 MB	zone_wan_input	all	eth0.2	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_input	all	tun0	*	0.0.0.0/0	0.0.0.0/0	-	-
0	0 B	zone_wan_input	all	tun1	*	0.0.0.0/0	0.0.0.0/0	-	-
3	120 B	zone_wan_input	all	wwan0	*	0.0.0.0/0	0.0.0.0/0	-	-

Chain *FORWARD* (Policy: *ACCEPT*, 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	forwarding_rule	all	*	*	0.0.0.0/0	0.0.0.0/0	-	Custom forwarding rule chain
0	0 B	ACCEPT	all	*	*	0.0.0.0/0	0.0.0.0/0	ctstate RELATED,ESTABLISHED	-

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
Out	Output Interface
Source	Displays the source IPv4 Address.

Parameters	Description
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

Firewall Status

IPv4 Firewall IPv6 Firewall

Table: Filter Show empty chains Reset Counters Restart Firewall

Chain *INPUT* (Policy: ACCEPT, 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	ACCEPT	all	lo	*	::/0	::/0	-	-
9.73 K	789.03 KB	input_rule	all	*	*	::/0	::/0	-	Custom input rule chain
0	0 B	ACCEPT	all	*	*	::/0	::/0	ctstate RELATED,ESTABLISHED	-
0	0 B	syn_flood	tcp	*	*	::/0	::/0	tcp flags:0x17/0x02	-
0	0 B	zone_lan_input	all	br-lan	*	::/0	::/0	-	-
9.73 K	789.03 KB	zone_wan_input	all	eth0.2	*	::/0	::/0	-	-
0	0 B	zone_wan_input	all	tun0	*	::/0	::/0	-	-
0	0 B	zone_wan_input	all	tun1	*	::/0	::/0	-	-
0	0 B	zone_wan_input	all	wwan0	*	::/0	::/0	-	-

Chain *FORWARD* (Policy: ACCEPT, 0 Packets, 0 B Traffic)

Pkts.	Traffic	Target	Prot.	In	Out	Source	Destination	Options	Comment
0	0 B	forwarding_rule	all	*	*	::/0	::/0	-	Custom forwarding rule chain
0	0 B	ACCEPT	all	*	*	::/0	::/0	ctstate RELATED,ESTABLISHED	-

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.
Target	Displays the target.
Prot.	Displays the name of all the protocols configured in the Firewall Rule.
In	Input Interface
Out	Output Interface

Parameters	Description
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.

Parameters	Description
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](#).

```
System Log
Tue Sep 15 22:33:38 2020 user.info Eventsms: BAND : All supported bands
Tue Sep 15 22:33:38 2020 user.info Eventsms: CCID : 89918540400406933297
Tue Sep 15 22:33:38 2020 user.info Eventsms: IMEI : 352913090113562
Tue Sep 15 22:33:38 2020 user.info Eventsms: Retries to check 5
Tue Sep 15 22:33:38 2020 user.info Eventsms: Reset forced retry 0
Tue Sep 15 22:33:38 2020 user.info Eventsms: CSQ : 26
Tue Sep 15 22:33:38 2020 user.info Eventsms: CESQ : -61 dBm
Tue Sep 15 22:33:38 2020 user.info Eventsms: Registration : 1
Tue Sep 15 22:33:38 2020 user.info Eventsms: IMSI : 405854091816644
Tue Sep 15 22:33:38 2020 user.info Eventsms: CPIN : READY
Tue Sep 15 22:33:38 2020 user.info Eventsms: Operator : 405854
Tue Sep 15 22:33:38 2020 user.info Eventsms: Operator : Jio 4G Jio 4G
Tue Sep 15 22:33:38 2020 user.info Eventsms: OperatorType : LTE
```

Figure 6.4-1: System Logs

6.5 Kernel Log

Status > Kernel log

This log displays the Linux kernel log events.

```
Kernel Log
[ 0.000000] Linux version 4.14.166 (amathur@build-slave-03) (gcc version 7.5.0 (OpenWrt GCC 7.5.0 r0+1-f6f8aae)) #0 Mon Sep 7 07:31:49 2020
[ 0.000000] Board has DDR2
[ 0.000000] Analog PMU set to hw control
[ 0.000000] Digital PMU set to hw control
[ 0.000000] SoC Type: MediaTek MT7620A ver:2 eco:6
[ 0.000000] bootconsole [early0] enabled
[ 0.000000] CPU0 revision is: 00019650 (MIPS 24Kec)
[ 0.000000] MIPS: machine is Lantronix E22X
[ 0.000000] Determined physical RAM map:
[ 0.000000] memory: 08000000 @ 00000000 (usable)
[ 0.000000] Initrd not found or empty - disabling initrd
[ 0.000000] Primary instruction cache 64kB, VIPT, 4-way, linesize 32 bytes.
[ 0.000000] Primary data cache 32kB, 4-way, PIPT, no aliases, linesize 32 bytes
[ 0.000000] Zone ranges:
[ 0.000000]   Normal [mem 0x0000000000000000-0x0000000007fffffff]
[ 0.000000] Movable zone start for each node
[ 0.000000] Early memory node ranges
[ 0.000000]   node 0: [mem 0x0000000000000000-0x0000000007fffffff]
[ 0.000000] Initmem setup node 0 [mem 0x0000000000000000-0x0000000007fffffff]
[ 0.000000] On node 0 totalpages: 32768
[ 0.000000] free_area_init_node: node 0, pgdat 8056dea0, node_mem_map 81000040
[ 0.000000]   Normal: 32768 pages used for memmap
```

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.

Processes					
This list gives an overview over currently running system processes and their status.					
PID	Owner	Command	CPU usage (%)	Memory usage (%)	Actions
1	root	/sbin/procd	0%	1%	Hang Up Terminate Kill
2	root	[kthreadd]	0%	0%	Hang Up Terminate Kill
7	root	[ksoftirqd/0]	0%	0%	Hang Up Terminate Kill
8	root	[oom_reaper]	0%	0%	Hang Up Terminate Kill

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, displayed as a percentage.
Hang up	Sends a hang up signal to terminate the process.

Parameters	Description
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.

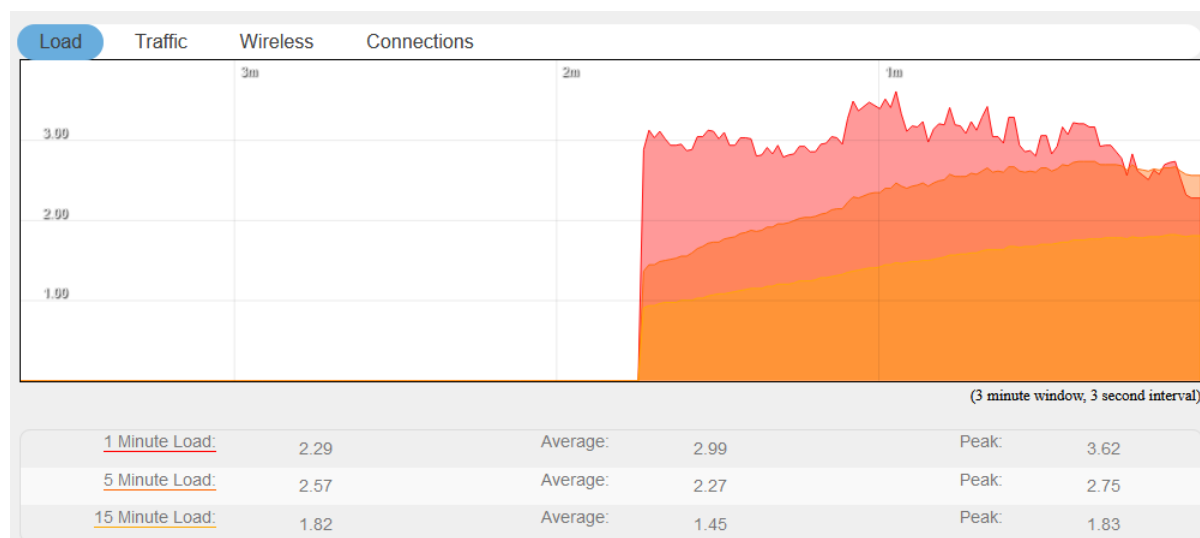


Figure 6.7-1: Real Time Load Graph

Parameters	Description
Load	<p>Graph shows the periodic average CPU load on the Router.</p> <p>Details</p> <p><i>X axis – Time Interval (1 minute)</i></p> <p><i>Y axis – CPU Load (Percentage)</i></p>

Parameters	Description
	Legends <i>Red – 1 Minute Load</i> <i>Orange – 5 Minute Load</i> <i>Yellow – 15 Minute Load</i>

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:

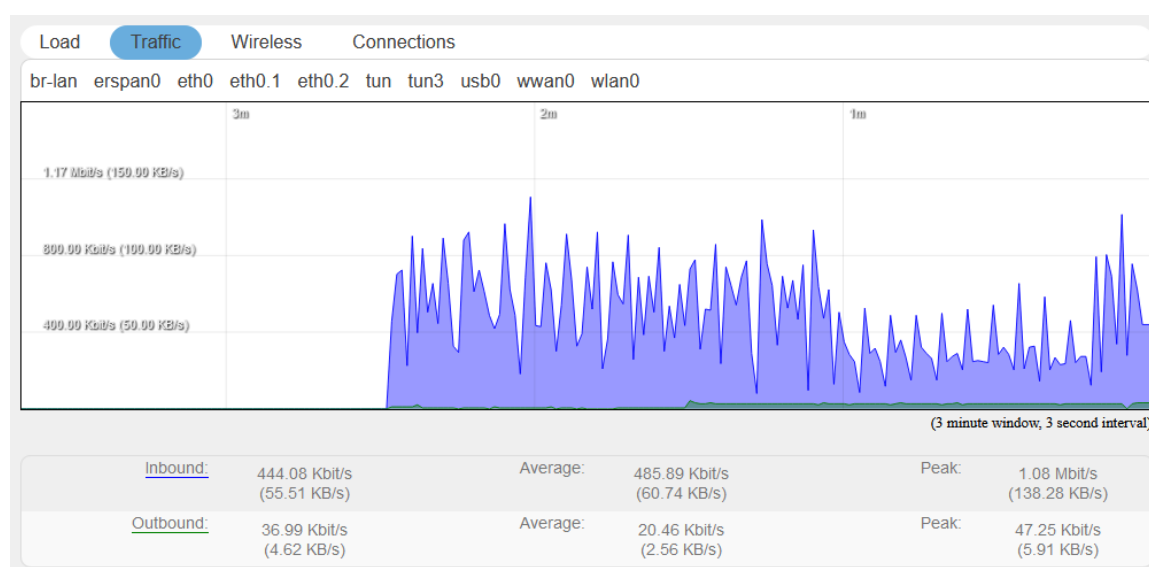


Figure 6.7-2: Status Realtime traffic for eth0

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.

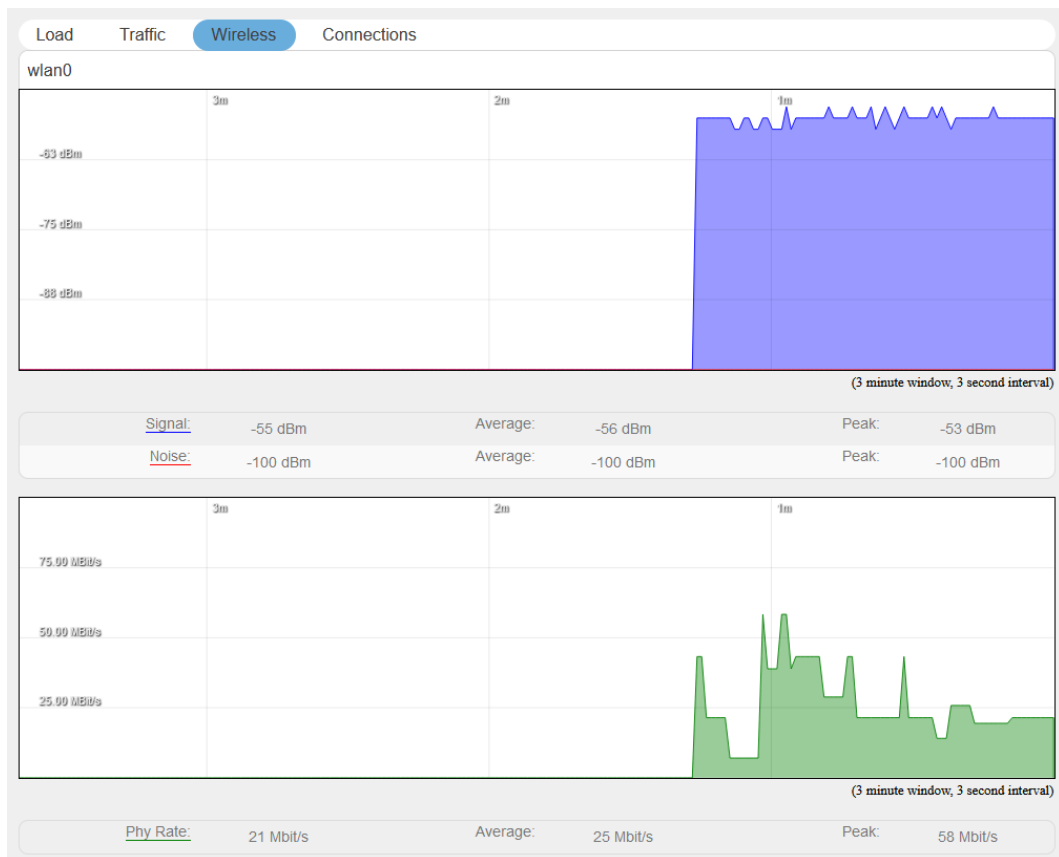


Figure 6.7-3: Real Time Wireless Traffic Graph

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

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.

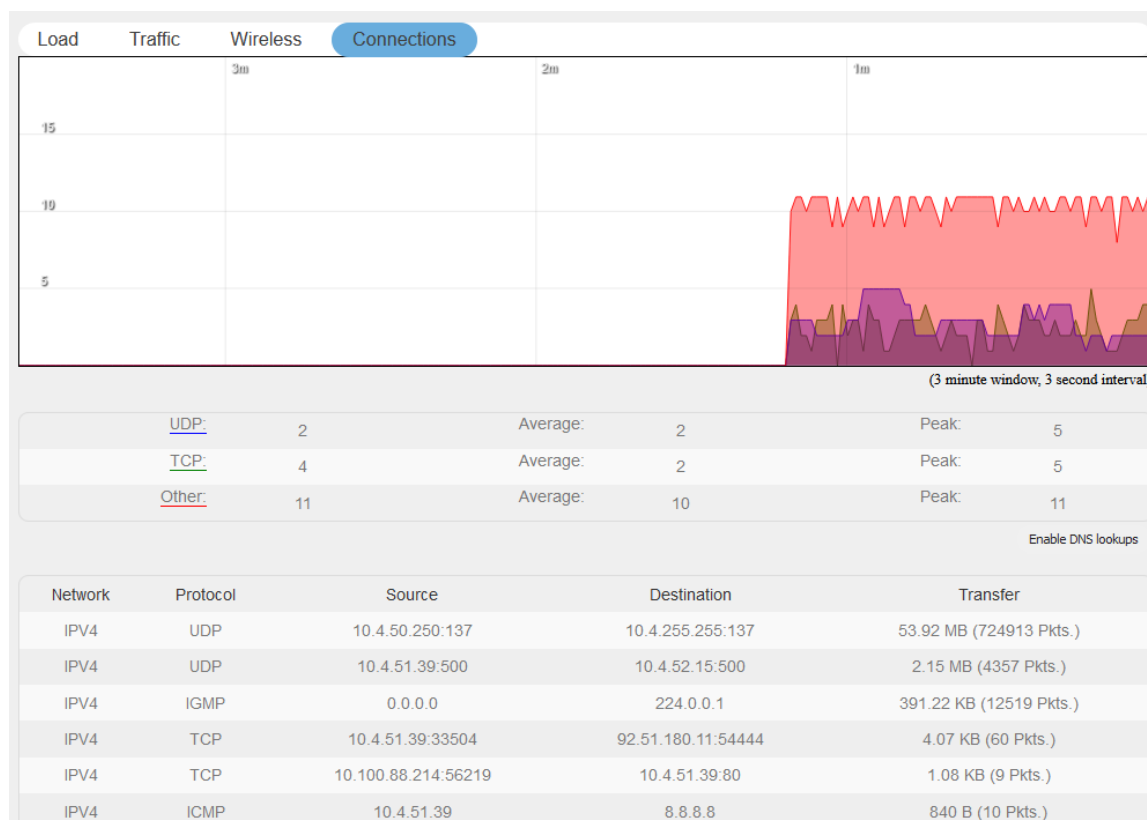


Figure 6.7-4: Real Time Connection Traffic Graph

Parameters	Description
Protocol	<p>Graph shows the periodic average of data transfer using specific protocols on the Router using the active connections in real time.</p> <p>Details</p> <p><i>X axis – Time Interval (1 minute)</i></p> <p><i>Y axis – Number of Active Connections</i></p> <p>Legends</p> <p><i>Blue – UDP</i></p> <p><i>Green – TCP</i></p> <p><i>Red – Other Protocols</i></p>
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.

Parameters	Description
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.

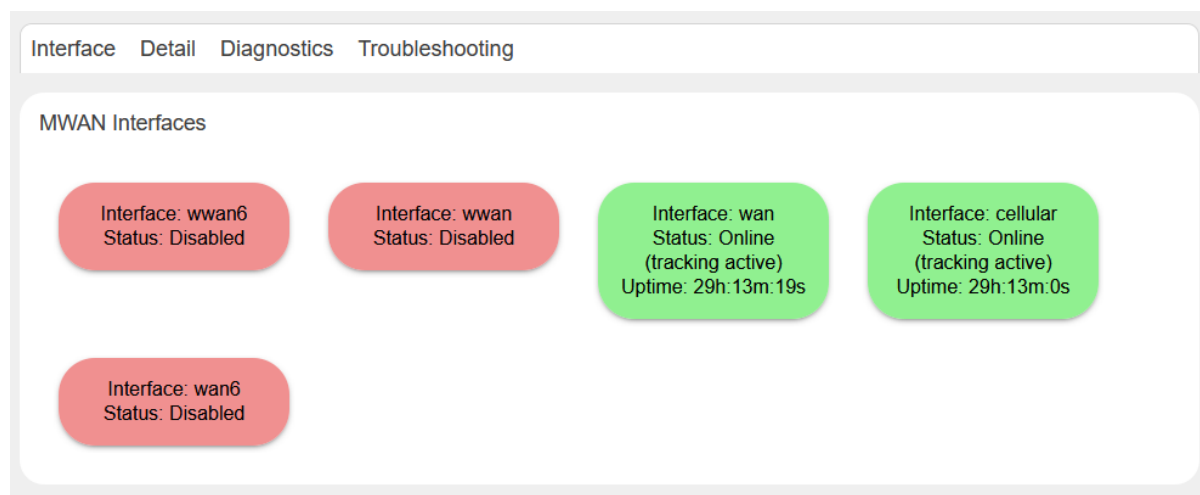


Figure 6.8-1: MWAN Interface Status

6.8.2 Detail

[Status](#) > [Load Balancing](#) > [Detail](#)

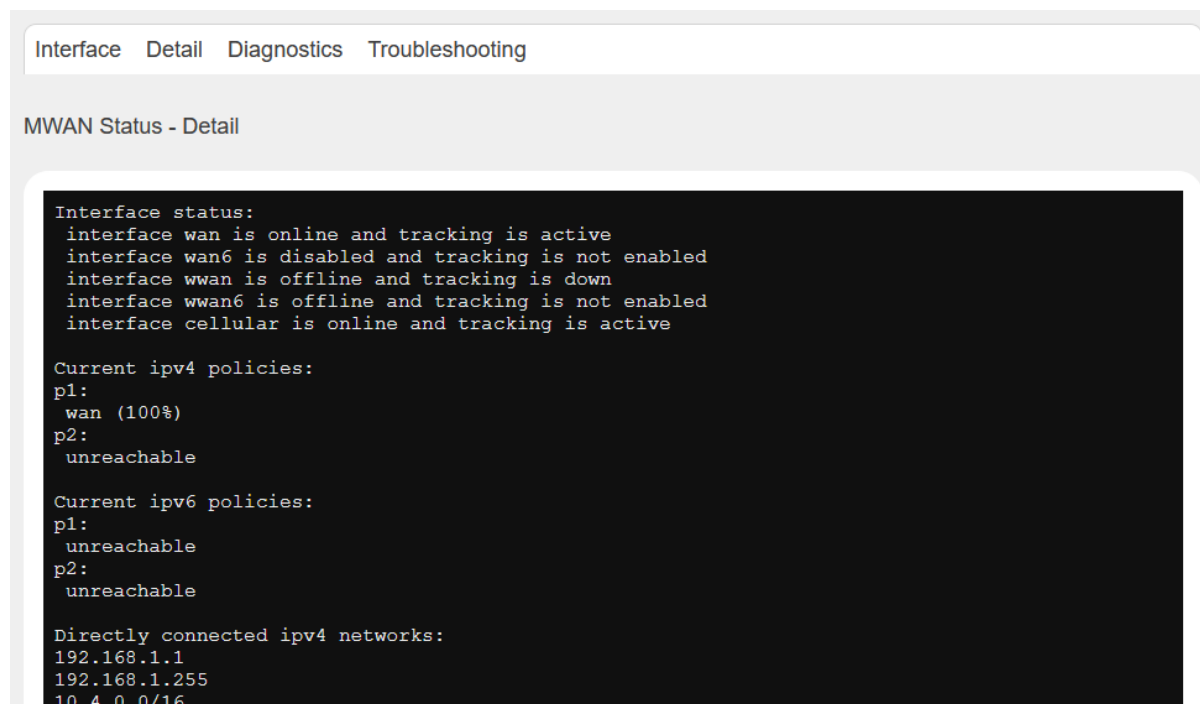


Figure 6.8-2: MWAN Status Detail

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.

```

Command:
ping -I 'eth0.2' -c 5 -W 1 '10.4.0.1' 2>&1

Result:
PING 10.4.0.1 (10.4.0.1): 56 data bytes
64 bytes from 10.4.0.1: seq=0 ttl=254 time=5.440 ms
64 bytes from 10.4.0.1: seq=1 ttl=254 time=2.340 ms
64 bytes from 10.4.0.1: seq=2 ttl=254 time=2.240 ms
64 bytes from 10.4.0.1: seq=3 ttl=254 time=4.080 ms
64 bytes from 10.4.0.1: seq=4 ttl=254 time=1.960 ms

--- 10.4.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.960/3.212/5.440 ms

```

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.

```

Software-Version
-----
OpenWrt - Lantronix E22X 3.5.28.0 r0+1-fd6b947
LuCI - git-20.251.20731-ae09bfa

Output of "ip a show"
-----
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default
    link/ether a4:ae:9a:01:cf:04 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::a6ae:9aff:fe01:cf04/64 scope link
        valid_lft forever preferred_lft forever

```

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

Parameters	Description
	<p>server.</p> <p>Note</p> <ul style="list-style-type: none"> <i>The displayed time is dependent on the configuration of your local computer that is being used as an NTP server.</i>
Router Time	Displays the current router time according to the configured time zone.
Hostname	<p>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.</p> <p>The configured Hostname appears on the Status > Overview page.</p>
Timezone	<p>Select time zone according to the geographical region in which router is deployed.</p> <p>The default time zone is UTC.</p>

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. UDP server is used to store the system logs The default port is 514.
External system log server	UDP or TCP

Parameters	Description
protocol	
Log output level	<p>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.</p> <p>Debug – Logs will be used by The E2xx series router software developer for debugging the router application. These logs are not useful during operations.</p> <p>Info – These logs provide normal operational information messages that are used for general purposes like reporting.</p> <p>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.</p> <p>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.</p> <p>Error – Displays the logs indicating an error condition.</p> <p>Note</p> <ul style="list-style-type: none"> For help with log errors, please contact Lantronix Technical Support. <p>Critical – Indicates failure in secondary system and must be corrected immediately.</p> <p>Alert – Problems which should be corrected immediately.</p> <p>Emergency – System is Unusable.</p>
Cron log level	<p>Select the minimum level for cron messages to be logged to syslog.</p> <p>Debug – Helps you debug cron process which has failed during runtime.</p> <p>Normal – Normal informational messages</p> <p>Warning – Indicates some issues can happen or error could be generated in cron process.</p> <p>Note</p> <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none"> • 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 <ul style="list-style-type: none">• <i>Auto refresh can be turned on or off using the Auto Refresh button on the UI.</i>

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. <i>Unspecified – If this option is selected, SSH listens on all interfaces.</i>
Port	Provide listening port of the Dropbear instance. Default port is 22.
Password Authentication	Select to allow authentication using SSH password. The default option is disabled.

Parameters	Description
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**.

Router Password SSH Access **SSH-Keys**

SSH-Keys

Public keys allow for the passwordless SSH logins with a higher security compared to the use of plain passwords. In order to upload a new key to the device, paste an OpenSSH compatible public key line or drag a `.pub` file into the input field.

d2sphere@d2sphere.com
 RSA, 8176 Bit
 AAAAB3NzaC1yc2EAAAADAQABAAQD/y1Jx...
 cTZCnDpVF0cPHt13SQh4o9
 /pldotliyQ==

app@android
 RSA, 2048 Bit
 AAAAB3NzaC1yc2EAAAADAQABAAQ4h...
 euu6C1nS5cUFDss4qDM3N4+E3k1iF+NIX3

Paste or drag SSH key fil 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.

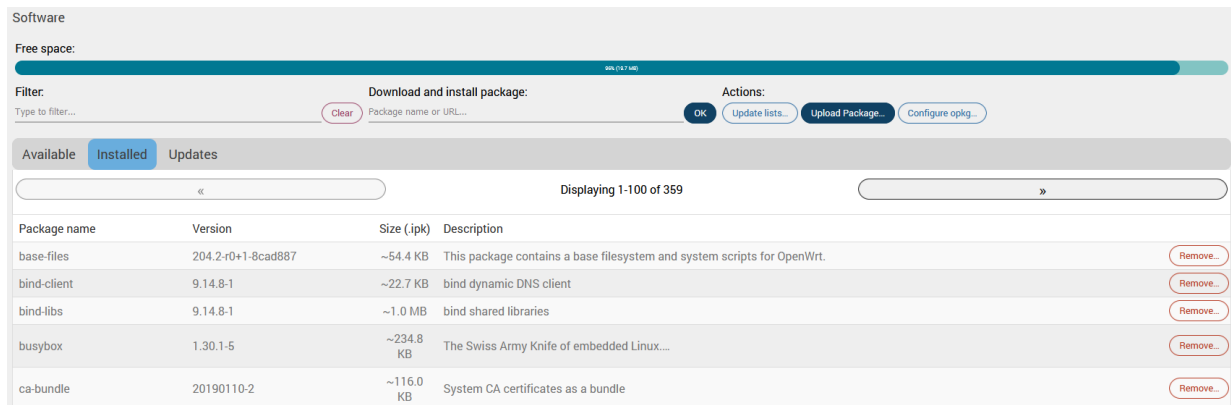


Figure 7.3-1: Installed Software Packages

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.
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.

OPKG Configuration

Below is a listing of the various configuration files used by `opkg`. Use `opkg.conf` for global settings and `customfeeds.conf` for custom repository entries. The configuration in the other files may be changed but is usually not preserved by `sysupgrade`.

```

opkg.conf
dest root /
dest ram /tmp
lists_dir ext /var/opkg-lists
option overlay_root /overlay
option check_signature

opkg/customfeeds.conf
# add your custom package feeds here
#
# src/gz example_feed_name http://www.example.com/path/to/files

opkg/distfeeds.conf
src/gz lantronix_core http://updates.d2sphere.com/ePack/E22X/ipks/3_6_6_0/main

```

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.

Start priority	Initscript	Enable/Disable	Start	Restart	Stop
00	urngd	Enabled	Start	Restart	Stop
10	boot	Enabled	Start	Restart	Stop
10	system	Enabled	Start	Restart	Stop
11	sysctl	Enabled	Start	Restart	Stop

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.

This is the content of /etc/rc.local. Insert your own commands here (in front of 'exit 0') to execute them at the end of the boot process.

```
# Put your custom commands here that should be executed once
# the system init finished. By default this file does nothing.

exit 0
```

Save

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.

Scheduled Tasks

This is the system crontab in which scheduled tasks can be defined.
 Note: you need to manually restart the cron service if the crontab file was empty before editing.

```
* * * * * /usr/sbin/d2sphere/d2sphere_client.sh &
```

Save

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](#).

LED Configuration

Customizes the behaviour of the device LEDs if possible.
 WARNING: Do not change this unless you know what you are doing.

Name	LED Name	Default state	Trigger	
power	e22x-power	On	none	⋮ Edit Delete
wlan	e22x-wwanactivity	Off	netdev	⋮ Edit Delete
lan	e22x-lanactivity	Off	netdev	⋮ Edit Delete
wan	e22x-wanactivity	Off	netdev	⋮ Edit Delete
activity	e22x-activity	Off	netdev	⋮ Edit Delete

Add LED action

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	<p>Displays the trigger event that will toggle the LED state.</p> <p><i>Default-on – defaulton. deprecated, use default = ON and trigger = None instead.</i></p> <p><i>Network Activity triggers – netdev. The LED flashes with link status and/or send and receive activity (trigger mode) on the configured interface (device).</i></p> <p><i>None – none. LED is always in default state (off). Can be used to set the LED to always On</i></p> <p><i>WiFi Activity triggers – Options with "phy" prefix. The LED flashes on events in the physical interface rather than in the software network interface.</i></p> <p><i>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).</i></p> <p><i>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.</i></p> <p><i>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.</i></p>

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 be 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

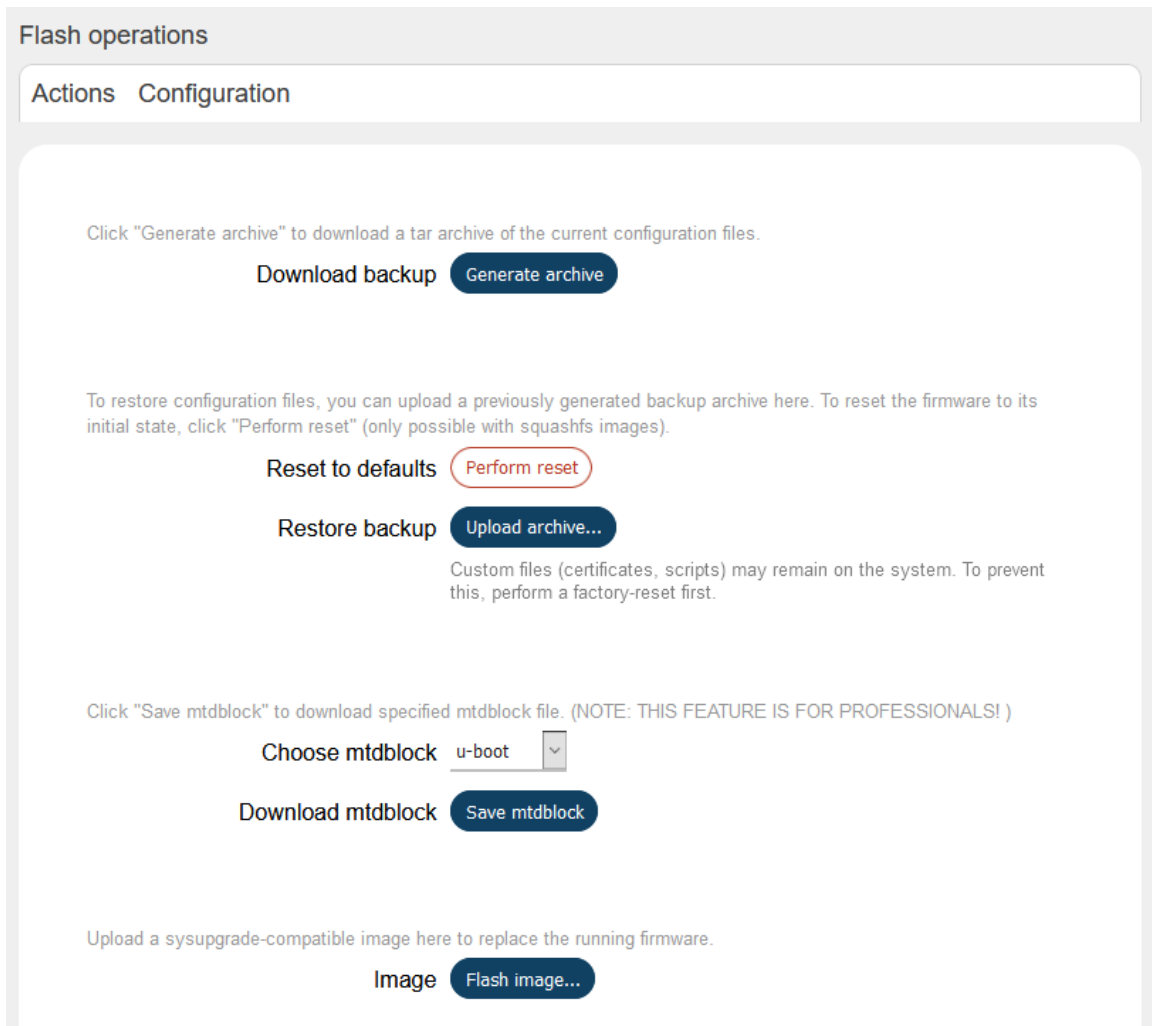


Figure 7.7-1: Backup Restore and Flash Firmware

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. <ul style="list-style-type: none"> • 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.

Parameters	Description
Flash image	
Image	<p>Click Flash image button to upload a sysupgrade compatible image for replacing the running firmware.</p> <p>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.</p> <p>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.</p> <p>Avoid the "Keep settings" option when upgrading from version 2.x to 3.x or downgrading from 3.x to 2.x.</p>

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.

This is a list of shell glob patterns for matching files and directories to include during sysupgrade. Modified files in /etc/config/ and certain other configurations are automatically preserved.

Show current backup file list [Open list...](#)

```
## 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
```

[Save](#)

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. You can also download or display the output.



Figure 7.8-1: Custom Command Dashboard

Parameter	Description
Run	Execute the command
Download	Download the custom command as a text file to the local drive.
Link	Access links to download or display the results.

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.

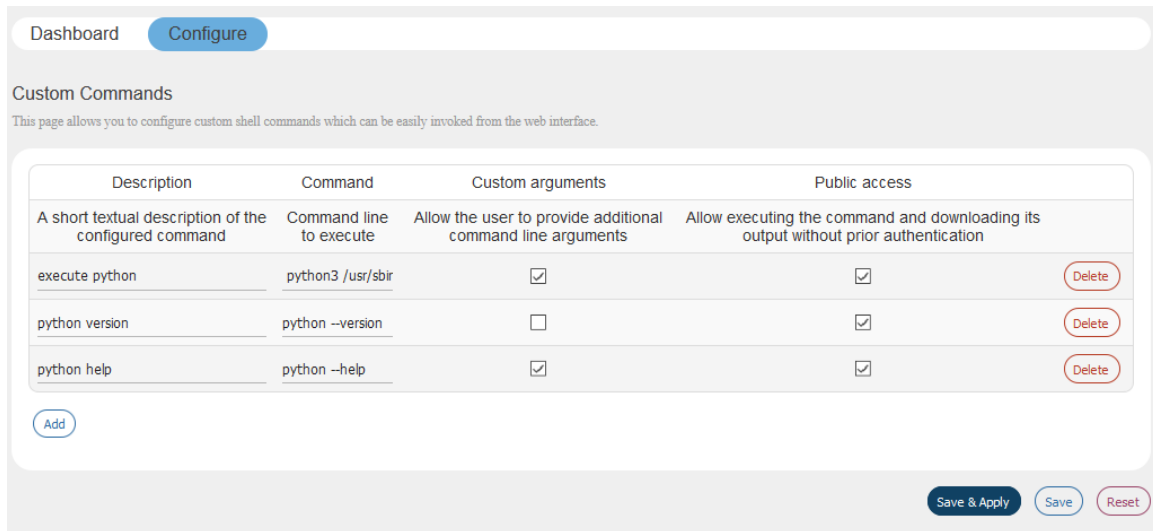


Figure 7.8-2: Custom Commands Configuration

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.**

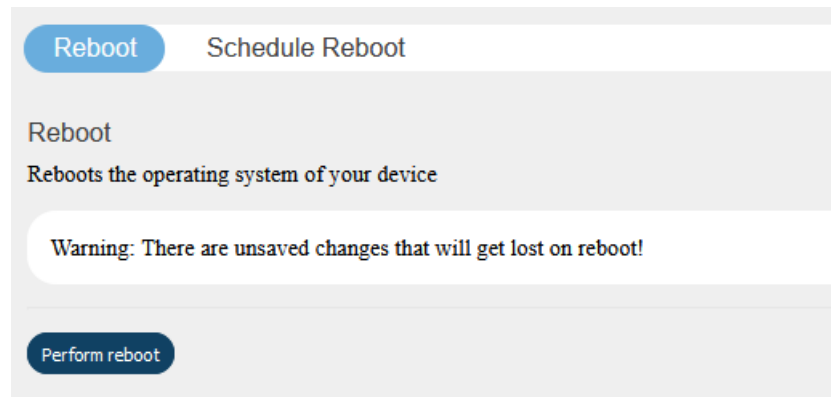


Figure 7.9-1: System Reboot

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.

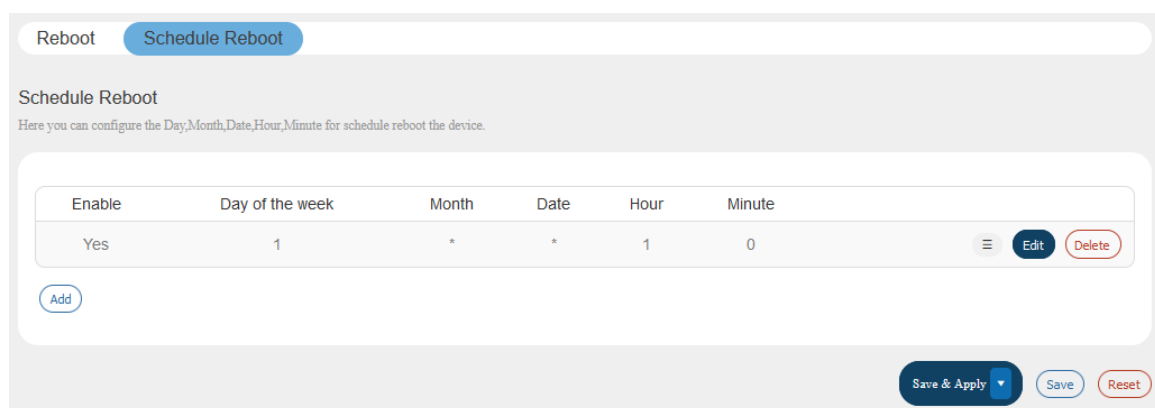


Figure 7.9-2: Schedule Reboot

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.

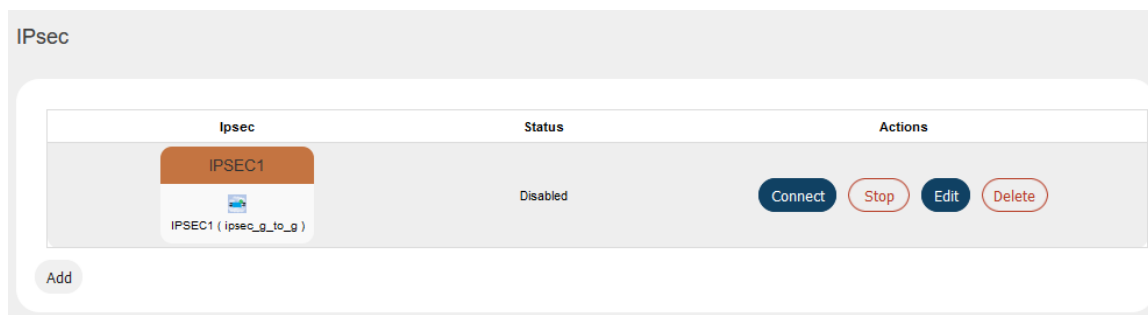


Figure 8.1-1: IPsec VPN Instance

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

[Back to Overview](#) »

General Settings

Advanced Settings

Profile Name

ProtoType

Enable

Remote IPSEC Gateway

Remote Address

Remote ID

Method

Route

Interface

Local Address

Local ID

Key Mode

Preshared-Key

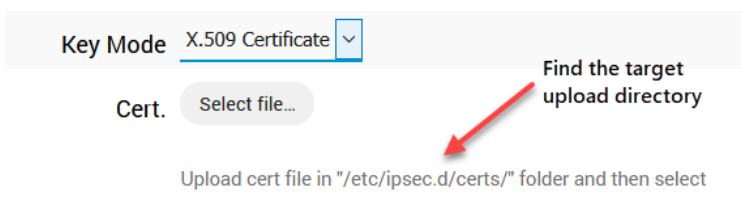
Single hop IP for watchdog.

Monitor interface ping failure.

[Save](#)

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

Parameters	Description
	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.
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. <i>Static – indicates that you will specify the interface to be used to establish the tunnel</i> <i>Auto – uses the interface that is active from the Load Balancer (MWAN) policies</i>
Route	Available if Static is selected in Method field. Select the interface used to configure IPSec: <i>Wan</i> <i>Wifi</i> <i>Cellular</i>
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.
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: <i>Pre shared Key</i> <i>X.509 certificate</i>
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.
Cert. Key CA Cert.	<p>These fields are available if X.509 Certificate is selected in the Key Mode field. The certificate files must be uploaded to the directory listed in the field.</p>  <p>Upload cert file in "/etc/ipsec.d/certs/" folder and then select</p> <p>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.</p>








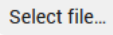
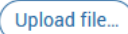

Parameters	Description
	<p>Cert. </p> <p>(root)</p> <p> bin 2020-10-11 20:44:13 </p> <p> dev 2020-10-20 05:48:58 </p> <p> etc  Click "etc" to select the folder 2020-10-17 08:14:10</p> <p>Navigate to the "ipsec.d" and "certs" folders in the same way. In the "certs" folder, click Upload file... and select the cert file to be uploaded.</p> <p>Key Mode <input type="text" value="X.509 Certificate"/></p> <p>Cert. </p> <p>(root) » etc » ipsec.d » certs <i>No entries in this directory</i></p> <p> </p> <p>Upload cert file in "/etc/ipsec.d/certs/" folder and then select</p> <p>Repeat this procedure with the Key and CA Cert files.</p>
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. <i>Main</i> <i>Aggressive</i>
Key Exchange	Select the mode of encryption key exchange between two communicating peers: <i>IKEV1</i> <i>IKEV2</i> <i>The default mode of Internet Key Exchange is IKEV1.</i>
IKE Encryption	Select the cipher type to use for the internet key exchange (IKE): <i>Any</i> <i>AES</i> <i>AES-128</i>

Parameters	Description
	<p>AES-192 AES-256 3DES DES</p> <p>The cipher type "Any" is the default IKE Encryption.</p>
IKE Hash	<p>The IKE hash is used for authentication of packets for the key exchange.</p> <p>Select the IKE Hash type to use for VPN connection:</p> <p>Any MD5 SHA1 SHA2 256 SHA2 384 SHA2 512</p> <p>The hash type "Any" is the default IKE hash.</p>
IKE DH Group	<p>Select the desired Diffie-Hellman group to use:</p> <p>Any Group 1 (768) Group 2 (1024) Group 5 (1536) Group 14 (2048) Group 15 (3072) Group 16 (4096) Group 17 (6144) Group 18 (8192)</p> <p>Higher groups are more secure but also require longer to generate key.</p> <p>The group "Any" is selected by default.</p>
IPSec Encryption	<p>Select the type of IPSec encryption for VPN connection:</p> <p>Any AES AES-128 AES-192 AES-256 3DES DES</p> <p>The cipher type "Any" is the default IPSec Encryption.</p>
IPSec Hash	<p>The IPSec hash is used for authentication of packets for the key exchange.</p> <p>Select the IPSec Hash type to use for VPN connection:</p> <p>Any MD5 SHA1 SHA2 256 SHA2-384 SHA2-512</p> <p>The hash type "Any" is the default IPSec hash.</p>

Parameters	Description
DH Group	<p>Select the desired Diffie-Hellman group to use:</p> <ul style="list-style-type: none"> <i>Any</i> <i>Group 1 (768)</i> <i>Group 2 (1024)</i> <i>Group 5 (1536)</i> <i>Group 14 (2048)</i> <i>Group 15 (3072)</i> <i>Group 16 (4096)</i> <i>Group 17 (6144)</i> <i>Group 18 (8192)</i> <p>Higher groups are more secure but also require longer to generate the key.</p> <p>The group “Any” is selected by default.</p>
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.

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](#).**

OpenVPN

Profile Name	Status
 (tap)	RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)
 (tun1)	RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)

OpenVPN instances

Below is a list of configured OpenVPN instances and their current state

Name	Enabled	Started	Start/Stop	Port	Protocol	Tunnel	
openvpn_1	<input type="checkbox"/>	no	start	-	-	tap	Edit Delete

Template based configuration

Instance name Simple server configuration for a routed point-to-point VPN Add

OVPN configuration file upload

Instance name Browse... No file selected. Upload

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: <ul style="list-style-type: none"> 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.
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

Parameters	Description
	<p>adding the instance, you can edit its configuration.</p> <p>Instance name – select the OpenVPN instance</p> <p>Select template – select the client or server template to use as the basis for the instance.</p> <p>Click Add to add the instance.</p> <p>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</p>
OVPN configuration file upload	<p>Create a VPN instance using a configuration file. Select the OpenVPN instance name and then click Browse to locate the configuration file.</p> <p>Click Upload to upload the selected file and create the configuration for the OpenVPN instance..</p> <p>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.</p>

Table 8.2-1: OpenVPN Service Configuration

8.2.2 Edit OpenVPN Instance from Template

[Overview](#) » Instance "openvpn_1"

[Switch to advanced configuration](#) »

verb 3

Set output verbosity

nobind

Do not bind to local address and port

comp_lzo yes

Use fast LZO compression

client

Configure client mode

remote vpnserver.example.org

Remote host name or ip address

ca ca.crt (File not accessible)

Certificate authority

dh dh1024.pem (File not accessible)

Diffie Hellman parameters

cert my_client.crt (File not accessible)

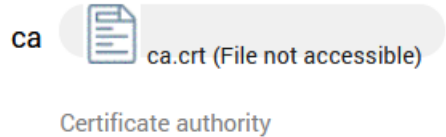
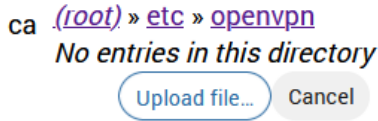
Local certificate

key my_client.key (File not accessible)

Local private key

-- Additional Field --

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_izo	Select Yes to use fast Izo 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	<p>Upload the Certificate authority file.</p> <p>The certificate and key files are uploaded to the /etc/openvpn/ folder on the router using the web interface.</p> <p>For example, to upload the CA cert file:</p> <p>Click the icon next to "ca" to display the directory structure of the router.</p>  <p>Navigate to and click "etc" to select the "etc" folder.</p> <p>Next, navigate to and select the "openvpn" folder.</p> <p>Under /etc/openvpn/, click Upload file... and select the file to be uploaded.</p>  <p>Certificate authority</p> <p>Repeat this procedure with the other certificate and key files.</p>

Parameters	Description
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.

[Overview](#) » Instance "openvpn_2"

Section to modify the OVPN config file (/etc/openvpn/openvpn_2.ovpn)

```
client
dev tun
remote-cert-tls server
cipher aes-256-cbc
pull
nobind
reneg-sec 0
resolv-retry infinite
verb 3
persist-key
persist-tun
remote pool-1.prd.us.losangeles.ovpn.com 443
proto tcp

auth-user-pass

key-direction 1
<ca>
-----BEGIN CERTIFICATE-----
MIIEFTCCA2WgAwIBAgIJAK2alWqpLj1/MA0GCSqGSIb3DQEBBQUAMIGFMQswCQYD
```

Section to add an optional 'auth-user-pass' file with your credentials (/etc/openvpn/openvpn_2.auth)

```
username
password
```

Save

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](#)
- [D2Sphere](#)
- [DOTA](#)
- [Page Selector](#)
- [SMS](#)
- [Reporting Agent](#)
- [GPS](#)
- [Keepalived](#)
- [Last Gasp](#)
- [Serial](#)
- [Service Actions](#)
- [Events](#)
- [uHTTPd](#)

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

Details for: myddns_ipv4

Configure here the details for selected Dynamic DNS service.

Basic Settings | Advanced Settings | Timer Settings | Log File Viewer

Enabled

If this service section is disabled it could not be started.
Neither from LuCI interface nor from console

Lookup Hostname

Hostname/FQDN to validate, if IP update happen or necessary

IP address version IPv4-Address IPv6-Address

Defines which IP address 'IPv4/IPv6' is send to the DDNS provider

DDNS Service provider [IPv4]

Domain

Replaces [DOMAIN] in Update-URL

Username

Replaces [USERNAME] in Update-URL (URL-encoded)

Password

Replaces [PASSWORD] in Update-URL (URL-encoded)

Use HTTP Secure

Enable secure communication with DDNS provider

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

Configure here the details for selected Dynamic DNS service.

Basic Settings **Advanced Settings** Timer Settings Log File Viewer

IP address source [IPv4] Network

Defines the source to read systems IPv4-Address from, that will be send to the DDNS provider

Network [IPv4] wan

Defines the network to read systems IPv4-Address from

Force IP Version

OPTIONAL: Force the usage of pure IPv4/IPv6 only communication.

DNS-Server mydns.lan

OPTIONAL: Use non-default DNS-Server to detect 'Registered IP'.
Format: IP or FQDN

PROXY-Server user:password@myproxy.lan:8080

OPTIONAL: Proxy-Server for detection and updates.
Format: [user:password@]proxyhost:port
IPv6 address must be given in square brackets: [2001:db8::1]:8080

Log to syslog Notice

Writes log messages to syslog. Critical Errors will always be written to syslog.

Log to file

Writes detailed messages to log file. File will be truncated automatically.
File: "/var/log/ddns/myddns_ipv4.log"

Figure 9.1-2: Dynamic DNS Advanced Configuration

Parameters	Description
IP address source [IPv4/IPv6]	<p>Select the IP Address source: Network, Interface, URL, or Script and enter the appropriate configuration details.</p> <p>Network <i>Network (IPv4) - Select the software Interface name to read systems IPv4 address from.</i></p> <p>Interface <i>Interface - Select the physical network interface from the available options</i></p> <p>URL <i>URL to detect - Enter the URL to read systems IP address from. The source IP Address by default is URL.</i></p>

Parameters	Description
	<p><i>Event Network (IPv4) – network on which the ddns updater scripts will be run</i></p> <p><i>Bind Network – leave as "default" or select the network to use for communication</i></p> <p>Script</p> <p><i>Script - Enter the script path and file name.</i></p> <p><i>Event Network (IPv4) – network on which the ddns updater scripts will be run</i></p>
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: <i>No logging, Info, Notice, Warning, Error.</i> 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

Configure here the details for selected Dynamic DNS service.

Basic Settings Advanced Settings **Timer Settings** Log File Viewer

Check Interval 10 minutes minutes
Interval to check for changed IP
Values below 5 minutes == 300 seconds are not supported

Force Interval 72 hours hours
Interval to force updates send to DDNS Provider
Setting this parameter to 0 will force the script to only run once
Values lower 'Check Interval' except '0' are not supported

Error Retry Counter 0
On Error the script will stop execution after given number of retries
The default setting of '0' will retry infinite.

Error Retry Interval 60 seconds seconds
On Error the script will retry the failed action after given time

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.

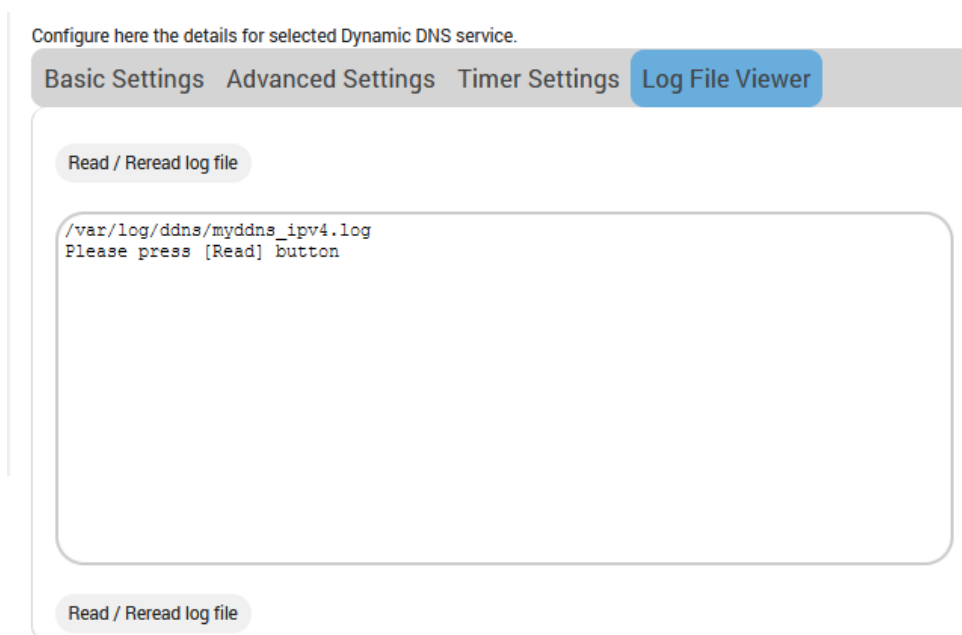


Figure 9.1-4: Dynamic DNS Log File Viewer

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: <i>MWAS – Lantronix Wireless Acquisition System</i>
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. <i>Backup WAN IP/URL - Enter the IP Address of backup M2M Gateway.</i> <i>Backup WAN Port - Enter the Port number of backup M2M Gateway.</i>

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.

SD(HC) / MMC card

Delete

MMC device _____

Mount point _____

Generally /tmp/NAME

Auto mount

Options _____

see mount -help for available options for -o. Comma seperated if more than one options

Add

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 D2sphere

Services > D2Sphere

Lantronix D2Sphere™ allows you to perform remote firmware updates for the E210 and E220 series devices. D2Sphere is a complete IoT platform to monitor, administrate, and operate devices over-the-air. To learn more about D2Sphere and to register for an account, please visit <https://www.d2sphere.com>.

9.4.1 D2Sphere Configuration

D2Sphere Configuration

Make sure to visit www.d2sphere.com to learn our features list and register a free account. If you do not have a custom account please use our live server.

Enable

IP/URL
default: live.d2sphere.com; device IMEI must be registered under your D2Sphere account prior to being

Port
default: 54444

Reporting Time (in minutes)
from 1 to 267840

Name

Description

Contact

Location

Latitude

Longitude

Figure 9.4-1: D2Sphere Configuration

Parameters	Description
Enable	Select the box to enable or disable management using D2Sphere management server.
IP/URL	Enter the IP address or URL provided while registering your device in the D2Sphere server.
Port	Enter the D2Sphere listening port provided while registering your device in the D2Sphere server. Default port is 54444.
Reporting Time (in minutes)	Enter the reporting interval (in minutes) value between 1 and 267840. Default value is 1440 minutes.

Parameters	Description
Name	Enter D2Sphere administrator contact name
Description	Enter D2Sphere administrator description.
Contact	Enter contact details such as mobile phone number.
Location	Enter contact location details such as street address.
Latitude	Enter server GPS coordinates in decimal degree format.
Longitude	Enter server GPS coordinates in decimal degree format.

Figure 9.4-2: D2Sphere Configuration

9.5 DOTA

Services > DOTA

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

9.5.1 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. The Lantronix server is configured at Services > D2Sphere.

Figure 9.5-1. 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

Parameters	Description
	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 9.5-1: DOTA for Lantronix Server

9.5.2 Custom Server

Services > Dota > Custom Server

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

The screenshot displays the 'Custom Server Setting' page. At the top, there are two tabs: 'Lantronix Server' and 'Custom Server', with 'Custom Server' being the active tab. Below the tabs, the page title is 'Custom Server Setting'. Underneath, it says 'Download Over The Air From Custom Server' and features a blue 'Update now' button. A log box shows two entries: 'Sat Sep 26 01:48:16 IST 2020 No new version. You have the latest.' and 'Sat Sep 26 01:48:15 IST 2020 Checking http://updates.d2sphere.com/ePack/E210/released/'. Below the log, there are several configuration fields: 'Protocol' is a dropdown menu set to 'HTTP'; 'URL/IP' is a text input field with a note below it stating 'URL/IP includes http/https'; 'Filename' is a text input field; 'Username' is a text input field with 'admin' entered; 'Password' is a text input field with a toggle icon on the right; 'Timeout in Minutes' is a text input field with '10' entered; and 'Retries' is a text input field with '3' entered. A note below the 'Retries' field states: 'The process will abort after the configured amount of time and retry again for configured number of retries. Default is 10 minutes if kept empty.' and 'Number of retries to check/download the file from server. Default is 3 if kept empty.'

Figure 9.5-2. Download over the Air (DOTA) for Custom Server Configuration

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

Parameters	Description
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 9.5-2: 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 9.7-2 for syntax details.**

9.6 Page Selector

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

9.7 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.

9.7.1 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: +9198xxxxxxx

Figure 9.7-1: SMS Configuration

Parameters	Description
SMS Configuration	
Enable	Enable remote SMS configuration.
AT Enable	Enable remote AT commands using SMS
SMS Administrator	<p>Displays up to four Administrators configured to receive the diagnostics information of the router via SMS after an SMS command is sent.</p> <p>Note</p> <ul style="list-style-type: none"> If no number is configured then the router will accept SMS from any number. <p>For each administrator to be configured, enter the mobile number with country code.</p> <p>The format of mobile number must be: +<countrycode><phonenumber> with a preceding special character "plus (+)". Example: +9198xxxxxxx</p>

Table 9.7-1: SMS Service Configuration

SMS AT Commands

The following figure shows the supported SMS command syntax.

List of Commands		
No.	Command name	Command
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>
6	LAN Ping	AT+LANPING=<IPA>
7	WWAN Ping	AT+WWANPING=<IPA>
8	CELL Ping	AT+CELLPING=<IPA>
9	Enable Remote access	AT+REMACC=<1/0>
10	Hardware information	AT+HWI?
11	Software information	AT+SWI?
12	Start Stop VPN	AT+VPN=<VPN Type>,<VPN Name>,<start/stop>
13	Install/Update IPK	AT+IPKDOTA=<Name of IPK file>,<install/upgrade/remove/autoremove>
14	Lan Settings	AT+IPLAN=<IPv4 address>,<SubnetMask>
15	Dota Custom Settings	AT+DOTASETTINGS=<HTTP/HTTPS>,<Server URL>,<File name>,<Username>,<Password>,<Timeout>,<Retry>
16	OPKG Configuration Settings	AT+OPKGSETTINGS=<Server URL>
17	Manage Digital Output	AT#OUT=<GP01/GP02>,<OPEN/CLOSE>
18	AT Command	AT#ATCMD='<AT command string>','<Timeout>
19	Dota Action	AT+DOTA=<C/M>,<update/check>[,<released/beta/development>,<filename>]
20	Cellular Settings	AT+IPGPRS=<1>,<Apn>,<Username>,<Password>,<Auth-Type>,<Data-Roam>

Figure 9.7-2: 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: <i>IPA- IP address of the WAN interface to ping.</i>
6	LAN Ping	AT+LANPING=<IPA> Parameter: <i>IPA – IP address of the LAN interface to ping</i>
7	WWAN Ping	AT+WWANPING=<IPA> Parameter: <i>IPA- IP address of the WAN interface to ping.</i>
8	CELL Ping	AT+CELLPING=<IPA> Parameter:

#	Name	Command Syntax
		<i>IPA- IP address of the WAN interface to ping.</i>
9	Enable Remote Access	AT+REMACC=<1/0> Parameter: <i>1/0 – Set 1 to enable, set 0 to disable remote access</i>
10	Hardware Information	AT+HWI?
11	Software Information	AT+SWI?
12	Start/Stop VPN	AT+VPN=<VPN Type>,<VPN Name>,<start/stop> Parameters: <i>VPN type – Openvpn or ipsec</i> <i>VPN name – VPN instance name</i> <i>Start/stop – action to start or stop the vpn</i>
13	Install/Update IPK	AT+IPKDOTA=<Name of IPK file>,<install/upgrade/remove/autoremove> Parameters: <i>Name of IPK file – IPK file name that OPKG will install, upgrade, or remove.</i> <i>install/upgrade/remove/autoremove – action that OPKG will run</i>
14	Lan Settings	AT+IPLAN=<IPv4 address>,<SubnetMask> Parameters: <i>IPv4 address – The IP address of the LAN interface</i> <i>Subnet mask – Subnet mask of the LAN IP address</i>
15	Dota Custom Settings	AT+DOTASETTINGS=<HTTP/HTTPS>,<Server URL>,<File name>,<Username>,<Password>,<Timeout>,<Retry> Parameters: <i>HTTP/HTTPS – protocol of the custom server</i> <i>Server URL – server URL, must include http: or https:</i> <i>File name – name of the file to be accessed for the update</i> <i>Username – server user name</i> <i>Password – server password</i> <i>Timeout – period of time to wait for the download to complete (minutes)</i> <i>Retry Parameters – number of retry attempts to check and download the file from the server.</i>
16	OPKG Configuration Settings	AT+OPKGSETTINGS=<Server URL> Parameter: <i>Server URL – Enter the URL of the</i>
17	Manage Digital Output	AT#OUT=<GPO1/GPO2>,<OPEN/CLOSE> Parameters: <i>GPO1/GPO2 – the pin to be configured</i> <i>OPEN/CLOSE – Set OPEN for low, or CLOSE for high.</i>
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: <i>AT command string – AT command such as AT+CSQ (signal quality) or AT+CREG? (to check the registration status of GSM module).</i>

#	Name	Command Syntax
		<p><i>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.</i></p> <p><i>Example: AT#ATCMD=AT+CSQ,5 - to check signal strength</i></p>
19	DOTA Action	<p>AT+DOTA=<C/M>,<update/check>[,<released/beta/development>,<filename>]</p> <p>Parameters:</p> <p><i>C/M – C for custom server, M for D2Sphere</i></p> <p><i>update/check – whether to update the router with the specified filename or to check for available updates</i></p> <p><i>released/beta/development – the release channel on the D2Sphere server to use for the update/check</i></p> <p><i>filename – filename of the package to use for the update</i></p>
20	Cellular Settings	<p>AT+IPGPRS=<1>,<Apn>,<Username>,<Password>,<Auth-Type>,<Data-Roam></p> <p>Parameters:</p> <p><i>1 or 1/2 – SIM slot number. 1 slot is supported on E22x models. 2 slots are supported on E21x models only.</i></p> <p><i>Apn – access point name provided by the cellular network provider</i></p> <p><i>Username – username if auth type is pap, chap, or pap/chap</i></p> <p><i>Password – password if auth type is pap, chap, or pap/chap</i></p> <p><i>Auth-type – none, pap, pap/chap, or chap (the auth-type parameter is case sensitive, must be all lowercase)</i></p> <p><i>Data-Roam – Enter 0 for disabled or 1 for enabled</i></p>

Table 9.7-2: SMS AT Command Syntax

9.7.2 Ethernet SMS

Services > SMS > Ethernet SMS

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

Figure 9.7-3: 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 9.7-3: 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

9.7.3 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.

SMS Configuration Ethernet SMS **Live Message**

Live Message
Ethernet SMS should be enabled to use this feature

SEND SMS:
Mobile Number: #91xxxxxxxxxx **SendSms**
Message Area:
Up to 159 Character

READ SMS:
1 **ReadSms**

DELETE SMS:
1 **DeleteSms**

Figure 9.7-4: 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.

9.8 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 9.8-1. 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. <ul style="list-style-type: none"> • Status • Uptime • IP

Parameters	Description
	<ul style="list-style-type: none"> Data usage
WAN Parameters	
	Select to enable individual WAN settings. <ul style="list-style-type: none"> Status Uptime IP Gateway DNS Data usage
Cellular Parameters	
	Select to enable individual Cellular settings. <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> Status Uptime IP Gateway DNS Data usage Wifi Client Info
GPS Parameters	
	Select to enable individual GPS settings. <ul style="list-style-type: none"> Time Latitude Longitude Altitude

Table 9.8-1: Reporting Agent Configuration

9.8.1 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.

Device Info

Reporting Agents

Enable Data Send

Protocol

Starting string of the frame

Less than 20 characters

Ending string of the frame

Less than 20 characters

IP1/URL1

Port1

TCP Timeout

TCP user timeout is between 10 to 900 Sec.[Used to switch between Main to Backup IP when main IP fails & Backup to Main IP when Backup IP fails]

Backup

If selected and data sending failed on primary Ip then backup ip will be used.If backup ip failed then again primary ip will be used. There will be 3 such tries

Send Interval in Second

Figure 9.8-2 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.
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.

Parameters	Description
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. <i>IP2/URL2</i> <i>Port2</i> 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 9.8-2: Reporting Agent Data Send Configuration

9.8.2 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=#
```

9.9 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.

GPS

GPS Enable

Parameter	Value
Time (GMT)	21:15:40
Latitude (degree.mmss)	17.446750
N/S Indicator	N
Longitude (degree.mmss)	78.375098
E/W Indicator	E
Position Fix Indicator	1
Number of Satellites Used	6
HDOP	1.400000
Altitude (in meters)	617.100000
Status	A
Speed	0.000000
Course of Ground	43.500000

Protocol

Enable Data Send

Figure 9.9-1 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.

Protocol

Enable Data Send

Protocol TCP

IP1/URL1 0.0.0.0

Port1 0-65535

Backup

If selected and data sending failed on primary Ip then backup ip will be used. If backup ip failed then again primary ip will be used. There will be 3 such tries

Polling Interval(In Seconds)

Sending Interval(In Seconds)

Figure 9.9-2 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. <i>0 – Fix not available or invalid</i> <i>1 – GPS SPS Mode, fix valid</i> <i>2 – Differential GPS, SPS Mode, fix valid</i> <i>3 to 5 – Not supported</i> <i>6 – Dead Reckoning Mode, fix valid</i>
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
Speed	Speed over ground in knots
Course of Ground	Track, or intended direction of travel
Protocol	

Parameters	Description
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. <i>IP2 – Enter the backup IP Address.</i> <i>Port2 – Enter the backup Port Number.</i>
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 9.9-1: GPS Service Configuration

9.9.1 Sample GPS Frames

9.9.1.1 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 9.9-2: 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.

9.9.1.2 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 hhmmss.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 <i>0 – Fix not available or invalid</i> <i>1 – GPS SPS Mode, fix valid</i> <i>2 – Differential GPS, SPS Mode, fix valid</i> <i>3 to 5 – Not supported</i> <i>6 – Dead Reckoning Mode, fix valid</i> 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 Separation	Geoid-to-ellipsoid separation. Ellipsoid altitude = MSL Altitude + Geoid Separation Example – -64.0 meters
Units	Example – M meters
Age of Diff.Corr.	Null fields when DGPS is not used. ⁴ The units is sec.
Diff. Ref.Station ID	-
Checksum	*42
<CR><LF>	End of message termination

Table 9.9-3: GGA Data Format

9.9.1.3 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 <i>A – Autonomous</i> <i>D – DGPS</i> <i>E – DR</i> <i>N – Output Data Not Valid</i> <i>R – Course Position^{(2) (3) (4)}</i> <i>S – Simulator</i> Example – A
Checksum	*20
<CR><LF>	End of message termination

Table 9.9-4: 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.

9.9.1.4 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 <i>A</i> – Autonomous <i>D</i> – DGPS <i>E</i> – DR <i>N</i> – Output Data Not Valid <i>R</i> – Course Position ⁽³⁾ ⁽⁴⁾ ⁽⁵⁾ <i>S</i> – Simulator Example – A
Checksum	*1E
<CR><LF>	End of message termination

Table 9.9-5: 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.

9.9.1.5 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 9.9-6: 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.

9.10 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).

9.10.1 General

Services > Keepalived > General

Figure 9.10-1 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 9.10-1: Keepalived General Configuration

9.10.2 Keepalived Global

Services > Keepalived > Keepalived Global

This provides general settings for the Keepalived service.

Keepalived Global

Global settings for Keppalived configuration.

Vrrp startup delay _____
Delay in seconds for starting vrrp.

Global Router Id/name Jd5wM07j
Global Routerid, unique for each device in a pool.

Keepalived config file Select file...
Upload keepalived.conf file in /etc/keepalived/ folder to avoid other settings except 'All scripts uploaded in Tracking Scripts and in user notify settings under VRRP Instances, Name of the script should match with the config file settings'.

Remove configuration for Keepalived Remove configuration for Keepalived
This permanently deletes the configuration.

User root
Default user for scripts execution.

Enable Script Security
To avoid running scripts changed by non-root user in runtime.

Enable dynamic interfaces
Allows keepalived to work with interfaces that may be deleted and restored.

Dynamic interfaces None ▼
Set Dynamic interfaces option for keepalived.

Figure 9.10-2: 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 loaded in Tracking Scripts, and the User Notify settings in VRRP Instances.

Parameters	Description
	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 9.10-2: Keepalived Global Configuration

9.10.3 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.

Tracking Scripts

These scripts will pass or fail the router increasing/decreasing their weight or changing the state to FAULT.

[Delete](#)

Name of trackscript block

Please enter the name even if using conf file.

Script [Select file...](#)

Upload to /usr/sbin/ folder and script name should start with 'keepalived_' and end with '.sh' string. Script should have #!/bin/sh as its first line.

Remove script [Remove script](#)

This permanently deletes the scripts.

TrackScript interval

Interval in seconds for trackscript to run.

Weight

Priority to be increase or decrease by if trackscript pass or fail. +ve will increase, -ve will decrease. range (-253 to 253). Ignore if we want to fail the router in case of script failure.

TrackScript pass count

Required number of successe count for OK transition.

TrackScript fail count

Required number of fail count for NOK transition

[Add](#)

Figure 9.10-3: 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".
Remove script	Click to remove the tracking script.

Parameters	Description
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 9.10-3: Keepalived Tracking Scripts Configuration

9.10.4 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 9.10-4: Keepalived Tracking Interfaces Configuration

Parameters	Description
Tracking Interfaces	
Name of interface block	Enter the name of the tracking interface block

Parameters	Description
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 9.10-4: Keepalived Tracking Interfaces Configuration

9.10.5 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.**

Tracking Processes

These processes will be monitored for running state which will pass or fail the router.

Delete

Name of process block

Process

Name of the process to monitor running state for changing the state of router.

Weight

Priority to be increase or decrease by if process above is not running. +ve will increase, -ve will decrease. range (-253 to 253). Ignore if we want to fail the router in case of process not running.

Add

Figure 9.10-5: 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

Parameters	Description
	means that the router will fail in case of the interface not running.

Table 9.10-5: Keepalived Tracking Processes Configuration

9.10.6 Virtual IP

Services > Keepalived > Virtual IP

Configure the Virtual IP address for the VRRP instance.

Virtual IP

Add virtual IPs here which has to used by VRRP instance.

[Delete](#)

Name of address block

Provide name to this block.

Virtual ipaddress

Virtual IP address to use

Physical device

Device to use for virtual ip

Scope of the virtual ip

Prefer global

[Add](#)

Figure 9.10-6: 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 9.10-6: Keepalived Virtual IP Configuration

9.10.7 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.

VRRP Instances

Add VRRP instances here which keepalived needs to use.

Delete

General Settings
Advanced Settings
User Notify Settings

Enable

Name of instance
Add name of the VRRP instance block.

Virtual Router ID
Should be same between virtual routers of same network.

Interface to look for v
Select interface which needs to monitored for switching.

Virtual Router Priority
< 1-255 > Highest priority will be Master.

Delay
Delay between advertisement.

Debug v
Debug level between 0-4.

Initial Virtual Router State. v

Enable Authentication
Enable password authentication for accessing vrrpd

Add

Figure 9.10-7: 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 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 9.10-7: Keepalived VRRP Instances Configuration

9.11 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 9.11-1 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 9.11-1: Last Gasp Configuration (E220 series devices only)

9.12 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](#).

9.12.1 Serial Configuration

The Serial configuration parameters such as baud rate must be configured for the data connection to the serial port. The serial communication mode can be Transparent or Modbus RTU to Modbus TCP mode.

Serial Configuration

Path

Is baudrate custom

Baud Rate

Data bit

Parity

Stop bit

Timeout in Seconds

For this timeout Inter-byte timeout will be [Timeout / 20]

Mode

Data Send Configuration

Enable

Figure 9.12-1: 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: <i>Odd</i> <i>Even</i> <i>None</i> The default is None.
Stop bit	Select the number of stop bits: <i>1</i> <i>2</i> 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 <i>Transparent mode of communication does not alter any data structure before or during the data communication.</i> Modbus RTU to Modbus TCP: <i>This mode converts the Modbus RTU data to/from RS485 to Modbus TCP before transmitting over TCP network.</i>

Table 9.12-1: Serial Configuration

9.12.2 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 either via TCP or UDP 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 [9.12.2.3 Data Send Configuration for FTP](#).

9.12.2.1 TCP Server Mode Configuration

Data Send Configuration

Enable

Protocol TCP

Mode Server

Type External

Internal: Listen on LAN. External: Listen on WAN/Wifi/Cellular auto fallback

Port 4000

Figure 9.12-2: Data Send Configuration – Server Mode on WAN Interface

Data Send Configuration

Enable

Protocol TCP

Mode Server

Type Internal

Internal: Listen on LAN. External: Listen on WAN/Wifi/Cellular auto fallback

IP 192.168.80.1 (Lantronix.lan)

Port 4000

Figure 9.12-3: Data Send Configuration – Server Mode on LAN Interface

Parameters	Description
Enable	Select the box to enable sending serial data
Protocol	Select the protocol. <i>For TCP, select TCP.</i> <i>For FTP transport, select FTP.</i>
Mode	Select the serial operating mode.
	Note:

Parameters	Description
	<ul style="list-style-type: none"> • Server mode operation requires a public IP address on the external interface (WAN). <p>For TCP server mode, select Server. For TCP client mode, select Client</p>
Type	<p>This setting is available if TCP Protocol and Server Mode settings are selected.</p> <p>Select External to listen for network connections on the WAN interface. Select Internal to listen for network connections on the LAN interface.</p>
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 9.12-2: Data Send Configuration - Server Mode

9.12.2.2 TCP Client Mode Configuration

Data Send Configuration

Enable

Protocol

Mode

IP

Port

Backup Server Enable
Valid on for persistent connection

Backup IP

Backup Port

Socket Timeout Enable
For persistent connection keep the checkbox unchecked

Figure 9.12-4: Data Send Configuration – Client Mode

Parameters	Description
Enable	Select the box to enable sending serial data
Protocol	Select the protocol. <i>For TCP, select TCP.</i> <i>For FTP transport, select FTP.</i>
Mode	Select the serial operating mode. <i>For TCP server mode, select Server.</i> <i>For TCP client mode, select Client</i>
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 9.12-3: Data Send Configuration - Client Mode

9.12.2.3 Data Send Configuration for FTP

Data Send Configuration

Enable

Protocol FTP

File Name

IMEI
Append IMEI in the file name.

Date Format YYYYMMDDHHMMSS
Append date in the file name.

FTP Server Address

FTP Server Port

User Name

Password *

Directory Path

Figure 9.12-5: Data Send Configuration FTP Protocol

Parameters	Description
Enable	Select the box to enable sending serial data.
Protocol	Select the protocol. <i>For TCP, select TCP.</i> <i>For FTP transport, select FTP.</i>
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 9.12-4: Data Send Configuration FTP Protocol

9.13 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.**

Service	Actions					
agents	Start	Stop	Reload	Restart	Enable	Disable
boot	Start	Stop	Reload	Restart	Enable	Disable
bootcount	Start	Stop	Reload	Restart	Enable	Disable
cellular_monitor	Start	Stop	Reload	Restart	Enable	Disable
cron	Start	Stop	Reload	Restart	Enable	Disable

Figure 9.13-1: Service Actions

9.14 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.

9.14.1 Event Management

Services > Events

Event Management

Enable

Event	Action	Mobile Number	Text
DI1_H	SMS	919820168224	alert

Events: Digital Input # 2 has voltage
 Action: Close digital Output # 1
 Mobile Number / VPN type: +91xxxxxxxxxx
 Text / VPN Name: _____

Figure 9.14-1: 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. <i>Close/Open digital Output # 1/2 – to close or open the digital pin</i> <i>Start VPN – start VPN</i> <i>Stop VPN – stop VPN</i> <i>SMS – to send the event details using the SMS.</i> <i>Switch Digital Output – Change the state of Digital Output</i> <i>Reboot – To reboot the router.</i>
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 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 9.14-1: Event Service Configuration

9.15 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.

9.15.1 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.

MAIN

General Settings
Full Web Server Settings
Advanced Settings

HTTP listeners (address:port) ✕

0.0.0.0:80 ✕

[::]:80 ✕

_____ +

Bind to specific interface:port (by specifying interface address)

HTTPS listener (address:port) ✕

0.0.0.0:443 ✕

[::]:443 ✕

_____ +

Bind to specific interface:port (by specifying interface address)

Redirect all HTTP to HTTPS

Ignore private IPs on public interface

Prevent access from private (RFC1918) IPs on an interface if it has a public IP address

HTTPS Certificate (DER Encoded) /etc/uhttpd.crt (939 B)

HTTPS Private Key (DER Encoded) /etc/uhttpd.key (1.70 KB)

Remove old certificate and key Remove old certificate and key

uHTTPd will generate a new self-signed certificate using the configuration shown below.

Remove configuration for certificate and key Remove configuration for certificate and key

This permanently deletes the cert, key, and configuration to use same.

1 Add

Figure 9.15-1: uHTTPd Service General Settings Configuration

uHTTPd Self-signed Certificate Parameters

Valid for # of Days

Length of key in bits

Server Hostname

a.k.a CommonName

Country

State

Location

Figure 9.15-2: 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
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.

Parameters	Description
	Default: Lantronix
Country	Country of the certificate issuer
State	State of the certificate issuer
Location	Location/city of the certificate issuer

Table 9.15-1: uHTTPd Service General Configuration

9.15.2 Full Web Server Settings

Services > uHTTPd > Full Web Server Settings

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

MAIN

General Settings **Full Web Server Settings** Advanced Settings

For settings primarily geared to serving more than the web UI

Index page(s) +
 E.g specify with index.html and index.php when using PHP

CGI filetype handler +
 Interpreter to associate with file endings ('suffix=handler', e.g. '.php=/usr/bin/php-cgi')

Do not follow symlinks outside document root

Do not generate directory listings

Aliases +
 (/old/path=/new/path) or (just /old/path which becomes /cgi-prefix/old/path)

Realm for Basic Auth

Config file (e.g. for credentials for Basic Auth)
 Will not use HTTP authentication if not present

404 Error
 Virtual URL or CGI script to display on status '404 Not Found'. Must begin with '/'

Add

Figure 9.15-3: 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.
Do not generate directory listings	If selected the http/https server will not generate directory listings.

Parameters	Description
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 9.15-2: uHTTPd Service Full Web Server Configuration

9.15.3 Advanced Settings

Services > uHTTPd > Advanced Settings

MAIN

General Settings Full Web Server Settings **Advanced Settings**

Settings which are either rarely needed or which affect serving the WebUI

Document root	/www
Base directory for files to be served	
Path prefix for CGI scripts	/cgi-bin
CGI is disabled if not present.	
Virtual path prefix for Lua scripts	/cgi-bin/luci=/usr/lib/lua/luci/cgi/uhttpd.l
Full real path to handler for Lua scripts	
Embedded Lua interpreter is disabled if not present.	
Virtual path prefix for ubus via JSON-RPC integration	
ubus integration is disabled if not present	
Override path for ubus socket	
Enable JSON-RPC Cross-Origin Resource Support	<input type="checkbox"/>
Disable JSON-RPC authorization via ubus session API	<input type="checkbox"/>
Maximum wait time for Lua, CGI, or ubus execution	60
Maximum wait time for network activity	30
Connection reuse	20
TCP Keepalive	1
Maximum number of connections	100
Maximum number of script requests	6
Maximum wait time for rpc timeout in seconds per requests	55

[Add](#)

Figure 9.15-4: 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 requests	Enter the maximum wait time for RPC timeout in seconds. Default: 55
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

Parameters	Description
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 9.15-3: uHTTPd Service Advanced Configuration

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.

The screenshot shows the 'Interfaces Overview' page with the following data:

Interface	Protocol	Status	Configuration	Actions
cellular-cellular	Cellular	Active	RX: 0 B (0 Pkts.) TX: 0 B (0 Pkts.)	Restart, Stop, Edit, Delete
br-lan	Static address	Active	Uptime: 1h 42m 10s MAC: A4:AE:9A:02:8C:A3 RX: 0 B (0 Pkts.) TX: 43.57 KB (333 Pkts.) IPv4: 192.168.1.1/24 IPv6: fd18:b939:4517::1/60	Restart, Stop, Edit, Delete
eth0.2	Static address	Active	Uptime: 1h 42m 9s MAC: A4:AE:9A:02:8C:A4 RX: 99.25 MB (301219 Pkts.) TX: 5.65 MB (19910 Pkts.) IPv4: 172.19.216.12/16	Restart, Stop, Edit, Delete
eth0.2	DHCPv6 client	Active	Uptime: 1h 42m 6s MAC: A4:AE:9A:02:8C:A4 RX: 99.25 MB (301219 Pkts.) TX: 5.65 MB (19910 Pkts.) IPv6: 2001:db80:ac13:d91e:a6ae:9aff:fe02:8ca4/64	Restart, Stop, Edit, Delete
Not present	DHCP client	Not present	Error. Network device is not present	Restart, Stop, Edit, Delete
Not present	DHCPv6 client	Not present	Error. Network device is not present	Restart, Stop, Edit, Delete

At the bottom of the interface list, there is a button labeled 'Add new interface...'.

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 <ul style="list-style-type: none"> When Wi-Fi is configured as Client, Interface WWAN will become active.
Status	Displays the status of the interface. See Section 10.1.2 .
Actions	Select the action to be taken for the interface. Restart – Connects the interface or reconnects the already

Parameters	Description
	<p><i>started interface.</i></p> <p>Stop – Stops the interface.</p> <p>Edit – Allows you to edit the interface settings.</p> <p>Detete – Deletes the interface.</p> <p>Note</p> <ul style="list-style-type: none"> • 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	<p>Select this box to enable or clear the box to disable the Network Watchdog.</p> <p>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.</p> <p>By default, the network watchdog is in enabled mode.</p>
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

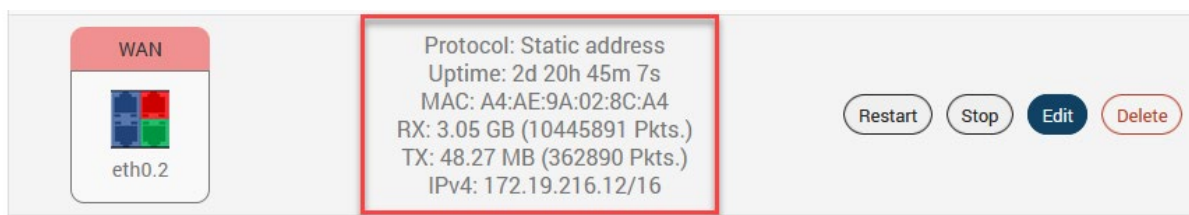


Figure 10.1-2: WAN Interface Status

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 →	LAN	WAN	WWAN	Cellular
Protocols ↓				
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 10.1-2 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	<i>Enter the IPv4 Address for Gateway.</i>
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	<p>Select the IPv6 assignment length.</p> <p>Available Options</p> <ul style="list-style-type: none"> • 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. <p>IPv6 assignment length is disabled by default.</p> <p>If assignment length is disabled, enter the following:</p> <p>IPv6 address - Enter the IPv6 Address.</p> <p>IPv6 gateway - Enter the IPv6 Address for Gateway.</p> <p>IPv6 routed prefix - Enter the public prefix to direct the client distribution to the router.</p> <p>If assignment length is 60, 64, or custom, enter the following:</p> <p>IPv6 assignment hint -Enter hexacimal subprefix ID for this instance to assign prefix parts.</p> <p>IPv6 suffix - Enter the IPv6 suffix.</p>
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

Parameters	Description
	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. Note <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> 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.

Parameters	Description
Lease time	<p>Remaining time until which the device can use the DHCP server leased IP Address.</p> <p>Note</p> <ul style="list-style-type: none"> <i>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.</i>
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	<p>Define additional DHCP options</p> <p>Example</p> <ul style="list-style-type: none"> <i>"6,192.168.2.1, 192.168.2.2" which advertises different DNS servers to clients.</i>
DHCP > IPv6 Settings	
Router Advertisement-Service	Select the Router Advertisement-Service mode; disabled, server mode, relay mode, hybrid mode.
DHCPv6-Service	Select the DHCPv6-Service mode; disabled, server mode, relay mode, hybrid mode.
NDP-Proxy	Select the NDP mode; disabled, server mode, relay mode, hybrid mode.
DHCPv6-Mode	<p>Select the DHCPv6-Service mode:</p> <p><i>Stateless</i></p> <p><i>Stateful</i></p> <p><i>Stateless + Stateful</i></p> <p>Stateful only</p>
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 MTU size
Physical Settings	
Bridge Interfaces	Click to enable creating a bridge over multiple interfaces. Enable STP – Check to enable the Spanning Tree Protocol over the bridge. Enable IGMP snooping – Check to enable IGMP snooping on the bridge.

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

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: <i>Unspecified</i> <i>Automatic (default)</i> <i>disabled – use if you want single IPv6 address for the AP without a subnet for routing</i> <i>48, 52, 56, 60, 64 –hinted prefix length</i> <i>custom – enter custom prefix length</i>
Advanced Settings	
Use builtin IPv6 -management	Allows to use the built in IPv6 management configuration.
Force link	Select this option to assign interface properties regardless of the link being active or not. If not selected, items are assigned only after the link has become active. Default is not selected.
Use default gateway	Click to configure a default gateway route. None of the gateway routes are configured by default.
Custom delegated IPv6 prefix	Enter the custom IPv6 prefix to be used.
Use DNS server advertised by peer	Allows advertising the DNS server address. Use DNS server advertised by peer for WAN interface is checked by default. If unchecked, the advertised DNS server addresses are ignored.
Client ID to send when requesting DHCP	Enter the Client ID that shall be sent when requesting DHCP.

Parameters	Description
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 <ul style="list-style-type: none"> • 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.

Parameters	Description
	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 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 <i>modem</i>
Bring up on boot	Allows the interface to be live after every reboot. Bring up on boot is checked by default.
Cellular Module	Displays the Cellular module
Modem device	Displays the cellular modem device

Parameters	Description
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 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)	
APN	Enter the Access Point Name provided by the cellular network operator.
PIN	Enter the PIN of the SIM card
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.
Modem device	Displays the modem device
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
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	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. 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	

Parameters	Description
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)	
APN	Enter the Access Point Name provided by the cellular network operator.
PIN	Enter the PIN of the SIM card
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 10.1-8: 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**.

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

Interfaces » CELLULAR

General Settings Advanced Settings Firewall Settings **Sim1 Settings** Sim2 Settings

APN

PIN

Authentication Type

Enable roaming

Figure 10.1-3: Cellular Interface dual SIM Configuration (E214 shown)

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**.

Interfaces » LAN

General Settings | Advanced Settings | Physical Settings | Firewall Settings

DHCP Server

Status Device: br-lan
 Uptime: 2d 18h 6m 43s
 MAC: A4:AE:9A:01:D0:F9
 RX: 68.34 MB (467784 Pkts.)
 TX: 88.98 MB (77919 Pkts.)
 IPv4: 192.168.10.1/24
 IPv6: fd07:c055:2cc0::1/60

Protocol Static address ▾

Bring up on boot

IPv4 address 192.168.10.1

IPv4 netmask 255.255.255.0

IPv4 gateway _____

IPv4 broadcast 192.168.10.255

Use custom DNS servers _____

IPv6 assignment length 60
 Assign a part of given length of every public IPv6-prefix to this interface

IPv6 assignment hint 0
 Assign prefix parts using this hexadecimal subprefix ID for this interface.

IPv6 suffix ::1
 Optional. Allowed values: 'eui64', 'random', fixed value like '::1' or '::1:2'.
 When IPv6 prefix (like 'a:b:c:d::') is received from a delegating server, use
 the suffix (like '::1') to form the IPv6 address ('a:b:c:d::1') for the interface.

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**.


Interfaces » WAN


General Settings Advanced Settings Physical Settings Firewall Settings DHCP Server

Status  Device: eth0.2
Uptime: 2d 16h 57m 6s
MAC: A4:AE:9A:01:D0:FA
RX: 8.57 GB (21998505 Pkts.)
TX: 80.62 MB (521763 Pkts.)
IPv4: 10.4.52.144/16

Protocol Static address 


Bring up on boot


IPv4 address 10.4.52.144 


IPv4 netmask 255.255.0.0 

IPv4 gateway 10.4.0.1

IPv4 broadcast 10.4.255.255

Use custom DNS servers 

IPv6 assignment length disabled 
Assign a part of given length of every public IPv6-prefix to this interface

IPv6 address Add IPv6 address... 

IPv6 gateway

IPv6 routed prefix
Public prefix routed to this device for distribution to clients.

IPv6 suffix ::1
Optional. Allowed values: 'eui64', 'random', fixed value like '::1' or '::1:2'. When IPv6 pr received from a delegating server, use the suffix (like '::1') to form the IPv6 address (' interface.

Dismiss Save

Figure 10.1-4: 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**.

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 10.1-5: Add New Interface

Protocol	Parameters
GRE	GRE point-to-point tunnel over IPv4 General Settings <i>Bring up on boot – Start the interface when the device is booted. Selected by default.</i> <i>Enable GRE tunnel – Enable GRE on the interface.</i> <i>GRE Server Address – Enter the WAN IP address or domain name of the remote GRE server.</i> <i>Local Address – Enter the WAN IP address of the router</i>

Protocol	Parameters
	<p>Local Tunnel Address – Enter the local IP address of the router on the GRE tunnel</p> <p>Remote Tunnel Address – Enter the remote IP address on the GRE tunnel</p> <p>Keepalive Interval (in minutes) – The amount of time before sending a keepalive probe packet to check the connection</p> <p>Keepalive Retries – The number of unanswered echo requests before considering the peer dead</p> <p>Interface – Enter the interface to bind to GRE. GRE cannot move from one interface to another. It must be bound to a particular interface.</p> <p>Advanced Settings</p> <p>Use builtin IPv6 management - Allows to use the built in IPv6 management configuration</p> <p>Force link - Select this option to assign interface properties regardless of the link being active or not.</p> <p>If not selected, items are assigned only after the link has become active. This is the default.</p> <p>Firewall Settings</p> <p>Select the WAN zone as the firewall zone.</p>
L2TP	<p>PPP over L2TP pseudowire tunnel</p> <p>General Settings</p> <p>Bring up on boot – Start the interface when the device is booted. Selected by default.</p> <p>L2TP Server – Enter the public IP address of the VPN server for L2TP connection</p> <p>PAP/CHAP username – Enter the PAP/CHAP username. The default password is admin.</p> <p>PAP/CHAP password – Enter the PAP/CHAP password.</p> <p>Advanced Settings</p> <p>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.</p> <p><i>Keepalive Requests is similar to LCP echo failure threshold.</i></p> <p><i>Checkup Interval is similar to Inactivity timeout.</i></p> <p>L2TP does not include fields for <i>LCP echo interval</i> or <i>Host-Uniq tag content</i>.</p> <p>Firewall Settings</p> <p>Select the WAN zone as the firewall zone.</p>
PPP	<p>PPP protocol for dialup modem connections</p> <p>General Settings</p> <p>Modem device – Select the modem device from the list.</p> <p>PAP/CHAP username – Enter the PAP/CHAP username. The default password is admin.</p> <p>PAP/CHAP password – Enter the PAP/CHAP password.</p> <p>Advanced settings</p> <p>Advanced settings are similar to those of PPPoE. See Section 10.1.3.6 for a description of the configuration.</p> <p>Firewall Settings</p> <p>Select the WAN zone as the firewall zone.</p>

Protocol	Parameters
PPtP	<p>Point to Point Tunneling Protocol (PPtP) VPN</p> <p>General Settings</p> <p>VPN Server – Enter the public IP Address or DNS name of the remote VPN Server for the PPTP connection.</p> <p>PAP/CHAP username – Enter the PAP/CHAP username.</p> <p>PAP/CHAP password – Enter the PAP/CHAP password. The default password is admin.</p> <p>Interface – Select the interface that the device will use to initiate the PPTP connection.</p> <p><i>Unspecified</i> – use the active interface to make the connection.</p> <p>Advanced Settings</p> <p>Advanced settings are similar to those of PPPoE. See Section 10.1.3.6 for a description of the configuration.</p> <p>One additional setting is described below:</p> <p>Use mppe – Select to enable encryption if this setting is enabled on the remote server.</p> <p>Firewall Settings</p> <p>Select the WAN zone as the firewall zone.</p> <p>Note:</p> <ul style="list-style-type: none"> 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.

Wireless Overview

radio0
MediaTek MT7620 802.11bgn
Channel: 11 (2.462 GHz) | Bitrate: ? Mbit/s

0%
SSID: Lantronix E22X | Mode: Master
BSSID: A4:AE:9A:02:8C:A2 | Encryption: mixed WPA/WPA2 PSK (CCMP)

0%
SSID: OpenWrt | Mode: Client
Wireless is disabled

Associated Stations

Network	MAC-Address	Host	Signal / Noise	RX Rate / TX Rate
No information available				

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.

Parameters	Description
	<p>Mode – Displays the mode of WLAN interface like Access Point Mode or Client Mode.</p> <p>BSSID – Displays Basic Service Set Identification (BSSID); 24 bit MAC Address of Wireless Access Point.</p> <p>Encryption – Displays the data encryption method.</p> <p>Channel – Wi-Fi channel</p> <p>Tx-Power – Transfer power limit</p> <p>Signal Strength – Displays the signal strength in percentage</p> <p>Bitrate – Data transfer rate</p> <p>Country – country code</p>
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

The screenshot shows the 'General Setup' tab of the wireless configuration interface. It includes a status box with a signal strength indicator at 0% and various parameters: Mode: Master, SSID: Lantronix E22X, BSSID: A4:AE:9A:02:8C:A3, Encryption: mixed WPA/WPA2 PSK (CCMP), Channel: 7 (2.442 GHz), Tx-Power: 20 dBm, Signal: 0 dBm | Noise: 0 dBm, and Bitrate: 0.0 Mbit/s | Country: 00. Below this, there is a toggle for 'Wireless network is enabled' with a 'Disable' button. Further down, there are dropdown menus for 'Mode' (set to N), 'Channel' (set to 11 (2462 Mhz)), and 'Width' (set to 20 MHz). At the bottom, there is a dropdown for 'Maximum transmit power' (set to driver default) and a note: '- Current power: 20 dBm'. A descriptive note at the bottom states: 'Specifies the maximum transmit power the wireless radio may use. Depending on regulatory requirements and wireless usage, the actual transmit power may be reduced by the driver.'

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

Parameters	Description
Status	<p>Displays the following details:</p> <ul style="list-style-type: none"> 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 Signal/Noise – Displays the signal strength and noise in dBm Bitrate/Country – Displays the bit rate and country code

Parameters	Description
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

General Setup
Advanced Settings

Country Code ▼

Allow legacy 802.11b rates

Distance Optimization

Distance to farthest network member in meters.

Fragmentation Threshold

RTS/CTS Threshold

Force 40MHz mode

Always use 40MHz channels even if the secondary channel overlaps. Using this option does not comply with IEEE 802.11n-2009!

Beacon Interval

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

Parameters	Description
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 <ul style="list-style-type: none"> <i>In case of access point setting, it is recommended not to use RTS/CTS threshold.</i>
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

General Setup
Wireless Security
MAC-Filter
Advanced Settings

Mode Access Point v

ESSID Lantronix E22X

Network lan:

Choose the network(s) you want to attach to this wireless interface or fill out the *create* field to define a new network.

Hide ESSID

WMM Mode

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

Parameters	Description
Mode	Select the Wi-Fi Interface mode. Available Options <i>Access Point</i> – router will act as an access point (master mode) <i>Client</i> - router will act as a wireless client <i>Ad-Hoc</i> – point to point connection between two stations without an intermediary <i>802.11s</i> – used for mesh networking <i>Pseudo Ad-Hoc (ahdemo)</i> – variant of ad-hoc mode that provides a point to point connection between two stations without an intermediary <i>Monitor</i> – client mode setting where wireless interface will listen to all traffic, not just its own. <i>Access Point (WDS)</i> – used for bridging two routers as WDS access points wirelessly to extend the Wi-Fi network. WDS with WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK Mixed Mode encryption modes are supported. <i>Client (WDS)</i> - WDS client mode allows a router to connect to a WDS access point. The default mode is Access Point.
Mode: All modes except 802.11s	
ESSID	Displays the device name assigned to the router. The default name is <i>Lantronix E22X</i> for E220 series routers or <i>Lantronix E21X</i> 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.

Parameters	Description
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	<p>This field is displayed for Access Point and Access Point (WDS) only.</p> <p>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.</p> <div style="border: 1px solid black; background-color: #f4a460; padding: 5px;"> <p>Note</p> <ul style="list-style-type: none"> • 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. </div> <p>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.</p>
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.

General Setup
Wireless Security
MAC-Filter
Advanced Settings

Encryption WPA-PSK/WPA2-PSK Mixed Mode (medium security) ▾

Cipher auto ▾

Key
●●●●●●●●
*

802.11r Fast Transition

Enables fast roaming among access points that belong to the same Mobility Domain

802.11w Management Frame Protection Disabled ▾

Requires the 'full' version of wpa2/hostapd and support from the wifi driver (as of Jan 2019: ath9k, ath10k, mwlwifi and mt76)

Enable key reinstallation (KRACK) countermeasures

Complicates key reinstallation attacks on the client side by disabling retransmission of EAPOL-Key frames that are used to install keys. This workaround might cause interoperability issues and reduced robustness of key negotiation especially in environments with heavy traffic load.

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 <i>No Encryption</i> <i>WPA-PSK/WPA2-PSK Mixed mode</i> <i>WPA2-PSK</i> <i>WPA-PSK</i> <i>WEP Shared Key</i> <i>WEP Open System</i> 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.
Cipher	For all encryption modes except No Encryption. Select the cipher suitable to the Router.

Parameters	Description
	Available Options <i>Auto</i> <i>Force CCMP (AES)</i> <i>Force TKIP</i> <i>Force TKIP and CCMP (AES)</i> 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.

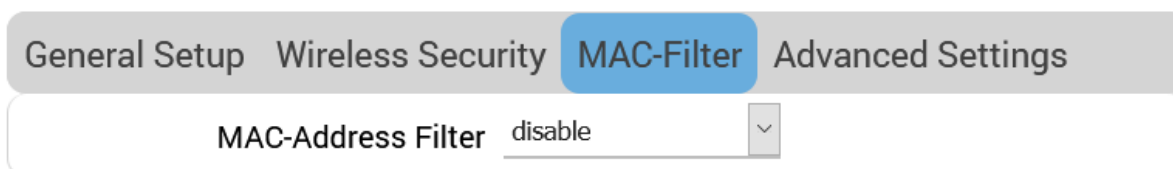


Figure 10.2-6: Wireless Interface MAC-Filter Configuration (Access Point mode)

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

General Setup
Wireless Security
MAC-Filter
Advanced Settings

Isolate Clients

Prevents client-to-client communication

Interface name

Override default interface name

Short Preamble

DTIM Interval

Delivery Traffic Indication Message Interval

Time interval for rekeying GTK

sec

Disable Inactivity Polling

Station inactivity limit

sec

Maximum allowed Listen Interval

Disassociate On Low Acknowledgement

Allow AP mode to disconnect STAs based on low ACK condition

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. Clear the box to disable.
RSSI threshold for joining	This setting appears in 802.11s mode only.

Parameters	Description
	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](#).

Switch

The network ports on this device can be combined to several [VLANs](#) in which computers can communicate directly with each other. [VLANs](#) are often used to separate different network segments. Often there is by default one Uplink port for a connection to the next greater network like the internet and other ports for a local network. **WARNING:** Do not change this unless advised by support or have strong knowledge of this device.

Enable VLAN functionality

VLANs on "mt7620" (mt7620)

VLAN ID	CPU (eth0)	LAN 1	LAN 2	LAN 3	LAN 4	WAN	
Port status:	 1000baseT full-duplex	 no link	 100baseT full-duplex	 no link	 no link	 100baseT full-duplex	
1	tagged <input type="checkbox"/>	untagged <input type="checkbox"/>	untagged <input type="checkbox"/>	untagged <input type="checkbox"/>	untagged <input type="checkbox"/>	off <input type="checkbox"/>	Delete
2	tagged <input type="checkbox"/>	off <input type="checkbox"/>	off <input type="checkbox"/>	off <input type="checkbox"/>	off <input type="checkbox"/>	untagged <input type="checkbox"/>	Delete

[Add VLAN](#)

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

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

Domain required
 Don't forward [DNS](#)-Requests without [DNS](#)-Name

Authoritative
 This is the only [DHCP](#) in the local network

Local server
 Local domain specification. Names matching this domain are never forwarded and are resolved from DHCP or hosts files only

Local domain
 Local domain suffix appended to DHCP names and hosts file entries

Log queries
 Write received DNS requests to syslog

DNS forwardings +
 List of [DNS](#) servers to forward requests to

Rebind protection
 Discard upstream RFC1918 responses

Allow localhost
 Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL services

Domain whitelist +
 List of domains to allow RFC1918 responses for

Local Service Only
 Limit DNS service to subnets interfaces on which we are serving DNS.

Non-wildcard
 Bind dynamically to interfaces rather than wildcard address (recommended as linux default)

Listen Interfaces +
 Limit listening to these interfaces, and loopback.

Exclude interfaces +
 Prevent listening on these interfaces.

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.

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

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

Use
 Read to configure the [DHCP-Server](#)

Leasefile
 file where given [DHCP](#)-leases will be stored

Ignore resolve file

Ignore

Additional Hosts files

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

Parameters	Description
Use /etc/ethers	Check to use <code>/etc/ethers</code> 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.

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

Enable TFTP server

TFTP server root
Root directory for files served via TFTP

Network boot image
Filename of the boot image advertised to clients

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

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

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served. Use the *Add* Button to add a new lease entry. The *MAC-Address* identifies the host, the *IPv4-Address* specifies the fixed address to use, and the *Hostname* is assigned as a symbolic name to the requesting host. The optional *Lease time* can be used to set non-standard host-specific lease time, e.g. 12h, 3d or infinite.

Hostname	MAC-Address	IPv4-Address	Lease time	DUID	IPv6-Suffix (hex)
<i>This section contains no values yet</i>					

Add

Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
<i>There are no active leases</i>			

Active DHCPv6 Leases

Host	IPv6-Address	DUID	Leasetime remaining
<i>There are no active leases</i>			

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 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

Parameters	Description
	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

Hostnames

Hostname _____

IP address unspecified ▼

Dismiss Save

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

The screenshot shows a configuration window titled 'Routes'. It has two tabs: 'General Settings' (selected) and 'Advanced Settings'. Under 'General Settings', there are four input fields: 'Interface' with a dropdown menu showing 'cellular', 'Target' with a red underline and a hint 'Host-IP or Network', 'IPv4-Netmask' with the value '255.255.255.255' and a hint 'if target is a network', and 'IPv4-Gateway' which is currently empty. At the bottom right of the window are 'Dismiss' and 'Save' buttons.

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.
Route type	Select the route type. Available options: <i>unicast</i> – route entry describes real paths to the destinations

Parameters	Description
	<p>covered by the route prefix</p> <p>local – destinations are assigned by this host. Packets are looped back and delivered locally.</p> <p>broadcast – destinations are broadcast addresses. Packets are sent as link broadcasts.</p> <p>multicast – special type used for multicast routing.</p> <p>unreachable – these destinations are unreachable</p> <p>prohibit – these destinations are unreachable.</p> <p>blackhole – these destinations are unreachable. Packets are discarded silently. Local senders get an ENVAL error.</p> <p>anycast – these destinations are anycast addresses assigned to this host.</p>
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 IPv4 Routes

Routes

General Settings Advanced Settings

Interface

Target

IPv6-Address or Network (CIDR)

IPv6-Gateway

Dismiss Save

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: <i>unicast</i> – route entry describes real paths to the destinations covered by the route prefix <i>local</i> – destinations are assigned by this host. Packets are looped back and delivered locally. <i>broadcast</i> – destinations are broadcast addresses. Packets are sent as link broadcasts. <i>multicast</i> – special type used for multicast routing. <i>unreachable</i> – these destinations are unreachable <i>prohibit</i> – these destinations are unreachable. <i>blackhole</i> – these destinations are unreachable. Packets are discarded silently. Local senders get an ENVAL error. <i>anycast</i> – 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

Diagnostics

Network Utilities

172.19.216.2 updates.d2sphere.com updates.d2sphere.com

IPv4 Ping IPv4 Traceroute Nslookup

```

PING 172.19.216.2 (172.19.216.2): 56 data bytes
64 bytes from 172.19.216.2: seq=0 ttl=62 time=220.960 ms
64 bytes from 172.19.216.2: seq=1 ttl=62 time=221.680 ms
64 bytes from 172.19.216.2: seq=2 ttl=62 time=220.700 ms
64 bytes from 172.19.216.2: seq=3 ttl=62 time=220.320 ms
64 bytes from 172.19.216.2: seq=4 ttl=62 time=222.400 ms

— 172.19.216.2 ping statistics —
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 220.320/221.212/222.400 ms

```

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)

General Settings
Port Forwards
Traffic Rules
Custom Rules

Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

Enable SYN-flood protection

Drop invalid packets

Input accept ▼

Output accept ▼

Forward accept ▼

Experimental feature. Not fully compatible with QoS/SQM.

Software flow offloading

Software based offloading for routing/NAT

Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	
<div style="display: flex; align-items: center; gap: 5px;"> <div style="background-color: #28a745; border-radius: 10px; padding: 2px 5px;">lan</div> <div style="font-size: 0.8em;">⇒</div> <div style="background-color: #dc3545; border-radius: 10px; padding: 2px 5px;">wan</div> </div>	accept ▼	accept ▼	accept ▼	<input type="checkbox"/>	≡ Edit Delete
<div style="display: flex; align-items: center; gap: 5px;"> <div style="background-color: #dc3545; border-radius: 10px; padding: 2px 5px;">wan</div> <div style="font-size: 0.8em;">⇒</div> <div style="background-color: #28a745; border-radius: 10px; padding: 2px 5px;">lan</div> </div>	reject ▼	accept ▼	accept ▼	<input checked="" type="checkbox"/>	≡ Edit Delete

Add

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 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.

Parameters	Description
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

Firewall - Zone Settings

General Settings | Advanced Settings | Contrack Settings

Extra iptables arguments

This section defines common properties of "this new zone". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are members of this zone.

Name Unnamed zone

Input accept

Output accept

Forward accept

Masquerading

MSS clamping

Covered networks unspecified

The options below control the forwarding policies between this zone (this new zone) and other zones. *Destination zones* cover forwarded traffic originating from this new zone. *Source zones* match forwarded traffic from other zones targeted at this new zone. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Allow forward to *destination* zones: unspecified

Allow forward from *source* zones: unspecified

Dismiss Save

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

Firewall - Zone Settings

General Settings **Advanced Settings** Contrack Settings

Extra iptables arguments

The options below control the forwarding policies between this zone (this new zone) and other zones. *Destination zones* cover forwarded traffic originating from this new zone. *Source zones* match forwarded traffic from other zones targeted at this new zone. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

Covered devices unspecified ▼
Use this option to classify zone traffic by raw, non-uci managed network devices.

Covered subnets
Use this option to classify zone traffic by source or destination subnet instead of networks or devices.

Restrict to address family IPv4 and IPv6 ▼

Restrict Masquerading to given source subnets +

Restrict Masquerading to given destination subnets +

Enable logging on this zone

Dismiss Save

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

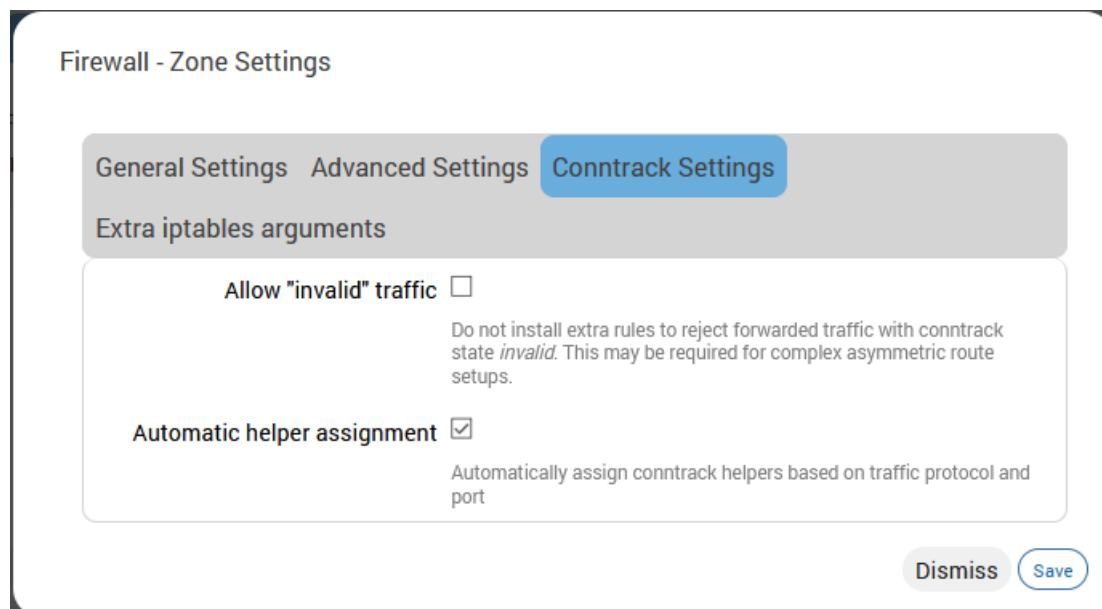


Figure 10.8-4: Firewall Conntrack Configuration

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

Firewall - Zone Settings

General Settings Advanced Settings Contrack Settings

Extra iptables arguments

Passing raw iptables arguments to source and destination traffic classification rules allows to match packets based on other criteria than interfaces or subnets. These options should be used with extreme care as invalid values could render the firewall ruleset broken, completely exposing all services.

Extra source arguments

Additional raw *iptables* arguments to classify zone source traffic, e.g. `-p tcp --sport 443` to only match inbound HTTPS traffic.

Extra destination arguments

Additional raw *iptables* arguments to classify zone destination traffic, e.g. `-p tcp --dport 443` to only match outbound HTTPS traffic.

Dismiss Save

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. .

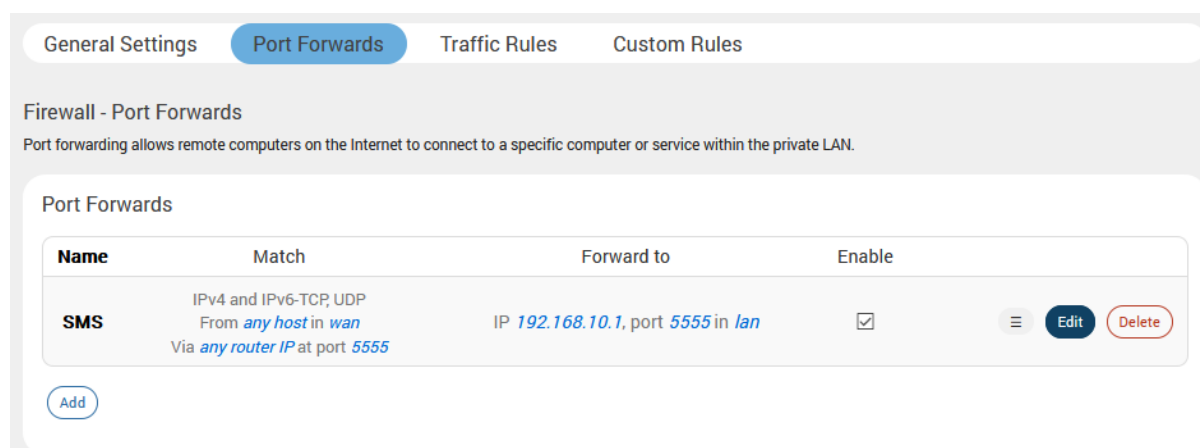


Figure 10.8-6: Firewall Port Forwards

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: <i>TCP</i> <i>TCP + UDP</i> <i>UDP</i> <i>ICMP</i> <i>unspecified</i> <i>custom</i>
Source Zone	Specify the traffic source zone. This must refer to one of the firewall zones, usually WAN.
External Port	Enter the WAN port of the external network.

Parameters	Description
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.

The screenshot shows the 'Firewall - Traffic Rules' configuration page. It features a navigation bar with 'General Settings', 'Port Forwards', 'Traffic Rules' (selected), and 'Custom Rules'. Below the navigation bar, there is a title 'Firewall - Traffic Rules' and a brief description: 'Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.' The main content area is titled 'Traffic Rules' and contains a table with the following data:

Name	Match	Action	Enable
Allow-DHCP-Renew	IPv4-UDP From <i>any host</i> in <i>wan</i> To <i>any router IP</i> at port <i>68</i> on <i>this device</i>	Accept input	<input checked="" type="checkbox"/>
Allow-Ping	IPv4-ICMP with type <i>echo-request</i> From <i>any host</i> in <i>wan</i> To <i>any router IP</i> on <i>this device</i>	Accept input	<input checked="" type="checkbox"/>
Allow-IGMP	IPv4-IGMP From <i>any host</i> in <i>wan</i> To <i>any router IP</i> on <i>this device</i>	Accept input	<input type="checkbox"/>
Allow-DHCPv6	IPv6-UDP From IP <i>fc00::/6</i> in <i>wan</i> To IP <i>fc00::/6</i> at port <i>546</i> on <i>this device</i>	Accept input	<input checked="" type="checkbox"/>

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

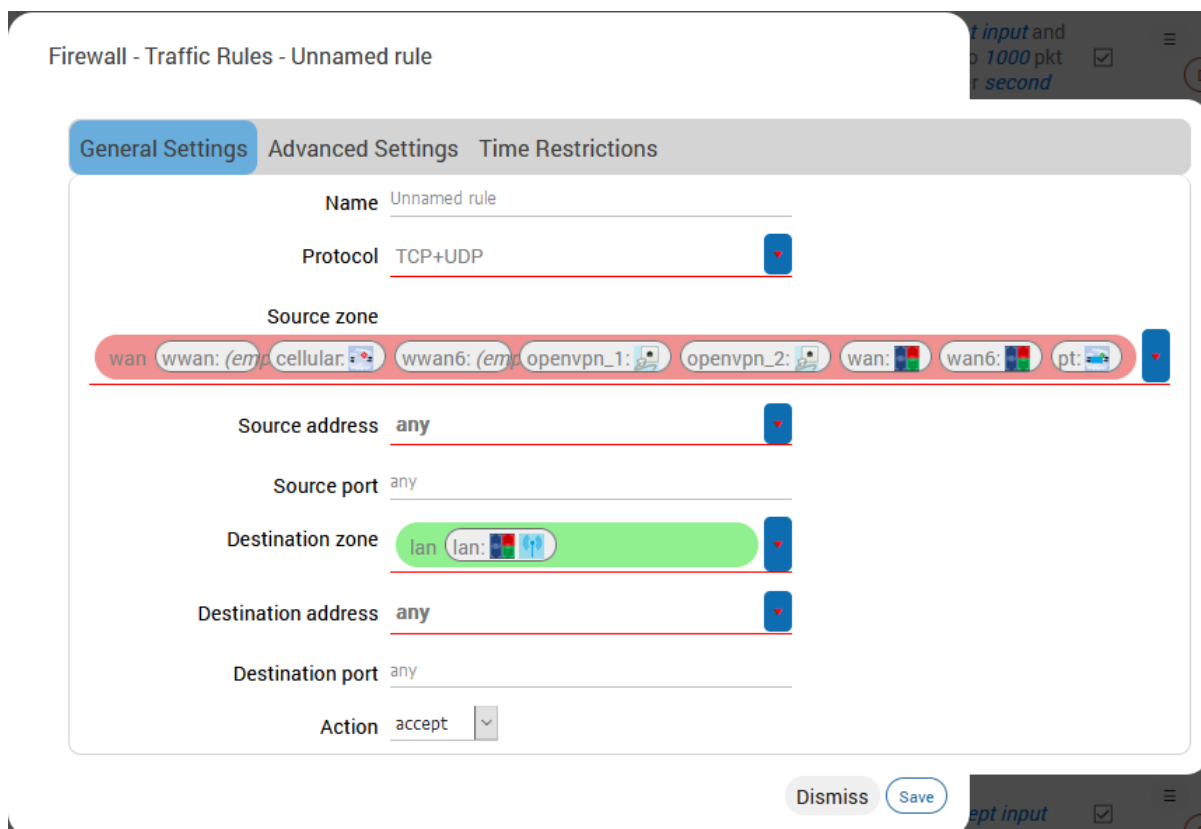


Figure 10.8-9: Firewall Traffic Rules General Configuration

Parameters	Description
General Settings	
Name	Enter the name of the traffic rule.
Protocol	Select the Protocol from the available options. Available Options <i>TCP</i> – Allows only TCP traffic to the open port <i>UDP</i> – Allows only UDP traffic to the open port <i>TCP+UDP</i> – Allows both TCP and UDP traffic to the open port
Source zone	Select the traffic source zone. This is usually WAN zone.
Source address	Match incoming traffic from the specified source IP address
Source port	Match incoming traffic from the specified source port
Destination zones	Select the destination firewall zone. If specified the rule applies to

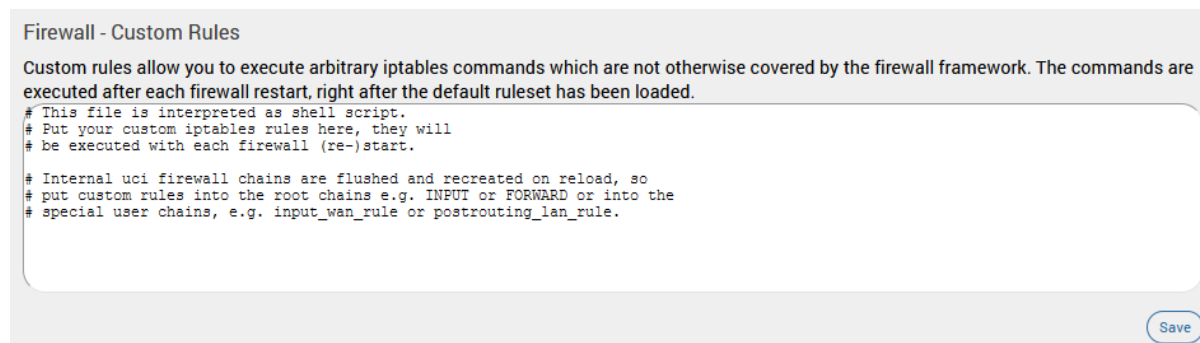
Parameters	Description
	forwarded traffic, otherwise it is treated as an input rule.
Destination address	Match incoming traffic directed to the specified destination IP address. If no destination zone is specified, the rule is treated as an input rule.
Destination port	Match incoming traffic directed to the specified destination port.
Action	Sets the target parameter to indicate the firewall action. Options include: <i>Accept</i> <i>Reject</i> <i>Drop</i> <i>Mark</i> <i>Notrack</i> .
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.



Firewall - Custom Rules

Custom rules allow you to execute arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default ruleset has been loaded.

```
# This file is interpreted as shell script.
# Put your custom iptables rules here, they will
# be executed with each firewall (re-)start.

# Internal uci firewall chains are flushed and recreated on reload, so
# put custom rules into the root chains e.g. INPUT or FORWARD or into the
# special user chains, e.g. input_wan_rule or postrouting_lan_rule.
```

Save

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

Globals **Interfaces** Members Policies Rules Notification

MWAN - Interfaces

There are currently 5 of 60 supported interfaces configured
 WARNING: Interface wwan6 has no default route in the main routing table
 WARNING: Interface wwan has no default route in the main routing table
 WARNING: Interface cellular has no default route in the main routing table
 WARNING: Interface wan6 has no default route in the main routing table

MWAN supports up to 252 physical and/or logical interfaces
 MWAN requires that all interfaces have a unique metric configured in /etc/config/network
 Names must match the interface name found in /etc/config/network
 Names may contain characters A-Z, a-z, 0-9, _ and no spaces
 Interfaces may not share the same name as configured members, policies or rules

Name	Enabled	Tracking method	Tracking source	Tracking reliability	Ping interval	Interface down	Interface up	Metric		
wan	Yes	ping	interface	1	5s	2	2	5	Edit	Delete
wan6	No	—	—	—	—	—	—	—	Edit	Delete
wwan	Yes	ping	interface	1	5s	3	3	6	Edit	Delete
wwan6	No	—	—	—	—	—	—	—	Edit	Delete
cellular	Yes	ping	interface	1	900s	1	1	7	Edit	Delete

[Add](#)

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.
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.

Members are profiles attaching a metric and weight to an MWAN interface
Names may contain characters A-Z, a-z, 0-9, _ and no spaces
Members may not share the same name as configured interfaces, policies or rules

Name	Interface	Metric	Weight	
m1	wan	1	2	Edit Delete
m2	wan6	1	2	Edit Delete
m3	wwan	2	2	Edit Delete
m4	wwan6	2	2	Edit Delete
m5	cellular	3	2	Edit Delete

[Add](#)

Figure 10.9-4: MWAN Interface Members


Parameters	Description
Member	Displays the Interface member notation number.
Interface	Displays the name of the interface.
Metric	<p>Displays the metric assigned to the interface.</p> <p>The interface with the lowest metric has the highest priority and all data is always routed through it.</p> <p>Note</p> <ul style="list-style-type: none"> <i>If two or more interfaces have same metric configured and that metric is lowest compared to other interfaces, then the data/load is balanced and data/load is distributed among the two interfaces in the ratio of the respective weight.</i>
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

MWAN Member Configuration - m1

Interface wan 

Metric 1

Acceptable values: 1-256. Defaults to 1 if not set

Weight 2

Acceptable values: 1-1000. Defaults to 1 if not set

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.

Policies are profiles grouping one or more members controlling how MWAN distributes traffic
 Member interfaces with lower metrics are used first
 Member interfaces with the same metric will be load-balanced
 Load-balanced member interfaces distribute more traffic out those with higher weights
 Names may contain characters A-Z, a-z, 0-9, _ and no spaces
 Names must be 15 characters or less
 Policies may not share the same name as configured interfaces, members or rules

Name	Members assigned	Last resort	
p1	m1 m2 m3 m4 m5	unreachable (reject)	
p2	—	unreachable (reject)	

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

MWAN Policy Configuration - p1

Member used	m1	<input type="button" value="x"/>
	m2	<input type="button" value="x"/>
	m3	<input type="button" value="x"/>
	m4	<input type="button" value="x"/>
	m5	<input type="button" value="x"/>
	– Please choose –	<input type="button" value="v"/>

Last resort

When all policy members are offline use this behavior for matched traffic

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: <i>unreachable (reject)</i> <i>blackhole (drop)</i> <i>default (use main routing table)</i>

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..

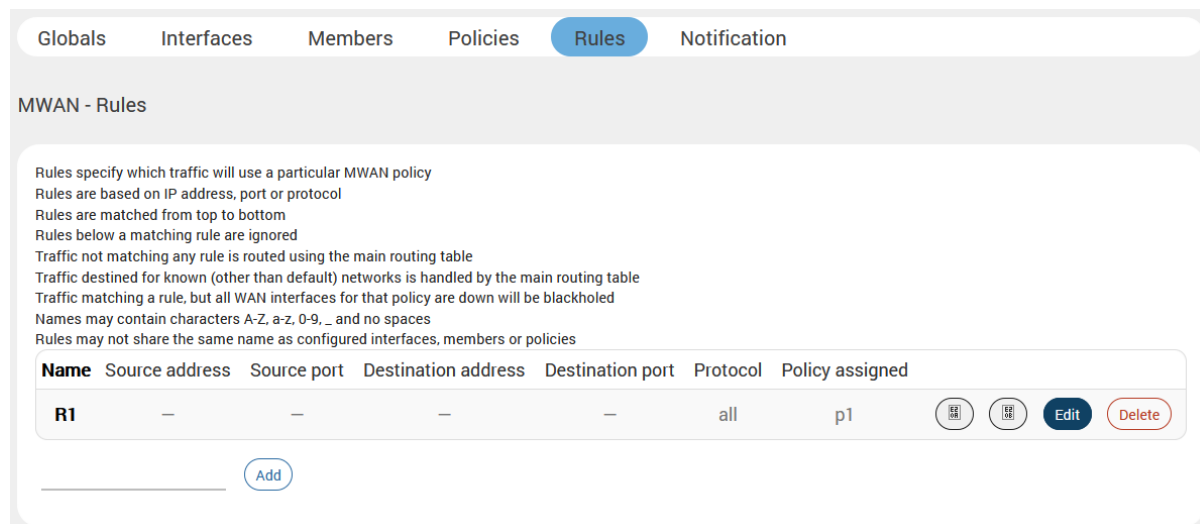


Figure 10.9-8: Mwan Interface Rules

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


MWAN Rule Configuration - R1


Source address _____
Supports CIDR notation (eg "192.168.100.0/24") without quotes

Source port _____
May be entered as a single or multiple port(s) (eg "22" or "80,443") or as a portrange (eg "1024:2048") without quotes


Destination address _____
Supports CIDR notation (eg "192.168.100.0/24") without quotes

Destination port _____
May be entered as a single or multiple port(s) (eg "22" or "80,443") or as a portrange (eg "1024:2048") without quotes

Protocol **all** 
View the content of /etc/protocols for protocol description

Sticky **No** 
Traffic from the same source IP address that previously matched this rule within the sticky timeout period will use the same WAN interface

Sticky timeout _____
Seconds. Acceptable values: 1-1000000. Defaults to 600 if not set

IPset _____ 
Name of IPset rule. Requires IPset rule in /etc/dnsmasq.conf (eg "ipset=/youtube.com/youtube")

Logging
Enables firewall rule logging (global mwan3 logging must also be enabled)


Policy assigned **p1** 

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.
Sticky timeout	Enter the stickiness timeout value in seconds. If no value is entered, this defaults to 600.

Parameters	Description
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")

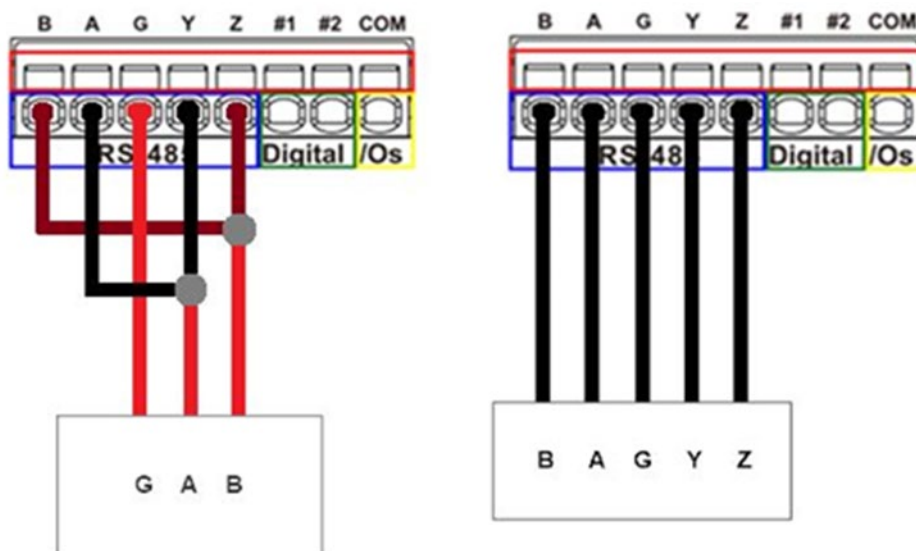
```
#!/bin/sh
#
# This file is interpreted as shell script.
# Put your custom mwan3 action here, they will
# be executed with each netifd hotplug interface event
# on interfaces for which mwan3 is enabled.
#
# There are three main environment variables that are passed to this script.
#
# $ACTION
# <ifup>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

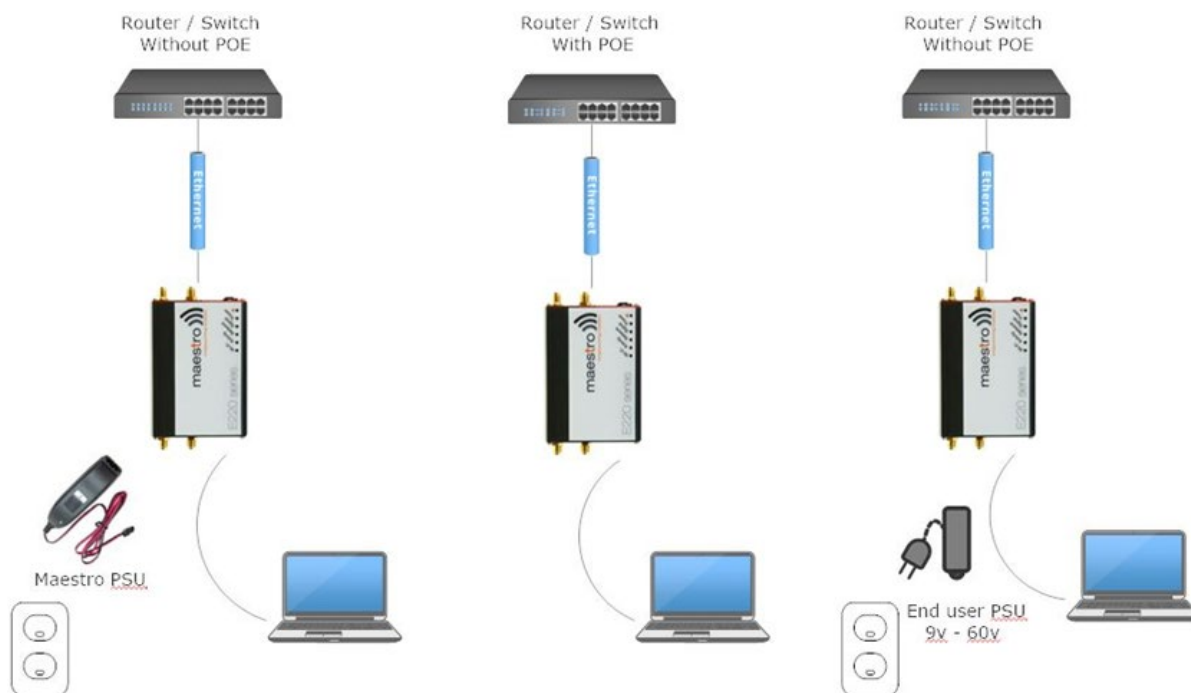
Appendix A. Wiring Diagrams

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
		Red ON	Hardware fault (high temperature or problem with module), Cellular Module reboot, Linux Kernel booting






Name	Color and State		Description
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
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

Acronym	Description
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
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

Acronym	Description
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).