ePACK User Manual
E210 and E220 Series Devices

Part Number PMD-00018
Revision B January 2020

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

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

Table of Contents

1. Overview 7

2. Prerequisite 9

3. Default Configuration 10

3.1 Web Admin Page 10

3.2 Wi-Fi enabled, with WPA/WPA2 TKIP key 10

3.3 Default Basic Configuration 10

4. LED Behavior 11

5. Logon Procedure 14

6. Common Icons and Buttons 15

7. Quick Setup 16

7.1 Quick Setup 16

7.2 Network Setup 17

8. Status 19

8.1 Overview 19

8.1.1 Status 19

8.2 Firewall 31

8.2.1 IPv4 Firewall 31

8.2.2 IPv6 Firewall 33

8.3 Routes 35

8.4 System Logs 37

8.5 Realtime Graphs 38

8.5.1 Wireless 38

8.5.2 Load 40

8.5.3 Traffic 41

8.5.4 Connection 46

9. System 48

9.1 Systems 48

9.1.1 General Settings 48

9.1.2 Logging 50

9.1.3 Language and Style 52

9.2 Administration 53

9.2.1 Router Password 53

9.2.2 SSH Access 54

9.3 Software 56

9.3.1 Actions 56
9.3.2 Configuration 59
9.4 Backup / Flash Firmware 60
9.4.1 Flash Operation 60
9.5 Reboot 63

10. Network 64

10.1 Interfaces 64
10.1.1 Interface Overview 69
10.1.2 3G (Only for E205) 73
10.1.3 CELLDHCP (Only for E206) 78
10.1.4 CELLULAR 82
10.1.5 WAN 86
10.1.6 LAN 91
10.1.7 WWAN 100
10.2 Load Balancing 105
10.2.1 Overview 106
10.2.2 Configuration 108
10.2.3 Advanced Settings 120
10.3 Wi-Fi 125
10.3.1 Add 127
10.4 DHCP and DNS 135
10.4.1 General Settings 136
10.4.2 Resolv and Host file 138
10.4.3 TFTP Settings 139
10.4.4 Advanced Settings 140
10.5 Hostnames 142
10.6 Whitelist / Blacklist 143
10.7 Static Routes 144
10.8 Diagnostics 145
10.9 Firewall 146
10.9.1 General Setting 146
10.9.2 Port Forwarding 151
10.9.3 Traffic Rules 152
10.9.4 Custom Rules 155

11. Services 156

11.1 VPN 157
11.1.1 PPTP 158
11.1.2 IPSec (Internet Protocol Security) 162
11.1.3 L2TP 173

11.1.4 GRE 176
11.1.5 OpenVPN 178
11.2 Agents 180
11.3 SMS 182
11.3.1 SMS Configuration 182
11.3.2 Ethernet SMS 184
11.4 DOTA 186
11.5 Serial 188
11.6 Content Filtering 190
11.7 Reporting Agent 192
11.7.1 LAN 192
11.7.2 WAN 192
11.7.3 Cellular 194
11.7.4 Wi-Fi 195
11.7.5 GPS 196
11.7.6 Sending Data 196
11.7.7 Data Sending Format 197
11.8 GPS 199
11.9 Events 207
11.10 Dynamic DNS 208

12. Wiring Diagrams 211

12.1 RS485 Wiring diagram: 211
12.2 Power over Ethernet 211

13. List of Acronym 212

1. Overview

With high-speed cellular (3G and beyond), WAN, LAN and Wi-Fi connectivity, the Lantronix's e-series of routers are highly versatile, reliable and rugged router 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:

- Lantronix E228
- Lantronix E225LITE#02
- Lantronix E225LITE
- Lantronix E224
- Lantronix E215#02
- Lantronix E214
- Lantronix E218
- Lantronix E205XT02
- Lantronix E205XT04
- Lantronix E206XT

The below table mentions the various available SKUs:

E220 Series

Model name	Territories or Operator(s)	Cellular type	Bands	Fallback mode(s)	Bands	GNSS	Planned certifications	FCS (*)	Order code
E225 Lite	EMEA, [most of] Asia Pacific	3G [a]	1/8	2G	3/8	×	RED, GCF		E225LITE#02
E224	EMEA	LTE cat. 1	3/8/20			same as E228's			E224#38K##38
	Asia Pacific		3/5/8/28	3G [b]	1/5/8		RCM, NCC		E224#358S#158
E225	EMEA, [most of] Asia Pacific	3G [a]	1/8	2G	3/8		RED, GCF		E225#02
	World		1/2/5/8		2/3/5/8		JPA, JRF, NBTC		E225
E228 Mk II	EMEA	LTE cat. 4	1/3/7/8/20/28	3G [c]; 2G	1/8; 3/8	IZat™ gen. 8C gpsOne	RED, GCF	Apr. '18	E228MKII#02
	Asia Pacific		1/3/5/7/8/28	3G [c]	1/5/8		RCM, KCC, NCC	May '18	E228MKII#04
	China, India		1/3/5 TDD 40/41**	3G [c]; 2G	1/8; 3/8		CCC, NAL, SRRC	Sep. '18	E228MKII#078
E228	AT&T Wireless, Rogers *User-configurable to* Verizon Wireless		2/4/5/17 4/13	3G [c] ×	2/5 N/A	Concurrent GPS, Galileo and either GLONASS (factory setting) or Beidou	IC, FCC, PTCRB, AT&T Wireless, Verizon Wireless		E228#245DH#25
	Asia Pacific		3/7/28	×	N/A		RCM, NCC		E228#37S
	NTT docomo		1/19/21				JPA, JRF		E228#1JL
	KDDI		1/11/18						E228#1BI
	South Korea		1/3/5/7				KCC		E228#1357

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

Uplink / Downlink maximum data rates – 3G: 5.76 / [a] 7.2; or [b] 10.1; or [c] 42.2 Mbps First customer shipment*

– LTE cat. 1: 5 / 10 Mbps (FDD); 3.1 / 8.96 Mbps (TDD)
– LTE cat. 4: 50 / 150 Mbps (FDD); 35 / 130 Mbps (TDD)

*** TDD B41 contains TDD B38*

E210 Series

Model name	Territories or Operator(s)	Cellular type	Bands	Fall back mode(s)	Bands	GNSS	Planned certifications	FCS (*)	Order code
E213	World	2-mode LTE-M1 / NB-IoT	1/2/3**/4/ 8/12***/13/ 20/26****/28	2G	2/3/5/8	same as E214G's	*TBD*	Apr. '18	E213
E214	EMEA	LTE cat. 1	1/3/7/8/20/28	3G [c]; 2G	1/8; 3/8	×	RED, GCF		E214#02
	Asia Pacific		3**/5/8/28	3G [b]	1/5/8		RCM, NCC		E214#358S#158
	China, India		1/3/5 TDD 40/41	3G [c]; 2G	1/8; 3/8	same as E214G's	CCC, NAL, SRRC	Sep. '18	E214#078
E214G	Verizon Wireless		4/13	×	N/A	IZat™ gen. 8C gpsOne	FCC, Verizon Wireless	Apr. '18	E214G#01
	AT&T Wireless, T-Mobile USA, Sprint		2/4/5/12***	3G [c]	2/4/5		IC, FCC, PTCRB, AT&T Wireless		E214G#00
E215	EMEA, [most of] Asia Pacific	3G [a]	1/8	2G	3/8	×	RED, GCF		E215#02
E216	Israel, Australia & New Zealand, NTT docomo, Thailand	3G [b]	1/5/8	×	N/A		NBTC, Postel		E216
E218	NTT docomo	LTE cat. 4	1/19/21				JPA, JRF		E218#1JL
	KDDI		1/11/18						E218#1BI

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

Uplink / Downlink maximum data rates – 3G: 5.76 / [(a)] 7.2; or [(b)] 10.1; or [(c)] 42.2 Mbps
– NB-IoT: 62.5 / 27.2 kbps; LTE-M1: 375 / 375 kbps
– LTE cat. 1: 5 / 10 Mbps (FDD); 3.1 / 8.96 Mbps (TDD)
– LTE cat. 4: 50 / 150 Mbps (FDD); 35 / 130 Mbps (TDD)

** First customer shipment*
*** B3 contains Japan's B9 *** B12 contains B17*
***** B26 contains (i) KDDI's B18; and (ii) NorAm's B5 which contains NTT docomo's B19 which contains Japan's B6*

Note

- ***Except when explicitly mentioned, all the screenshots in this user guide are taken from a Lantronix E225 unit.***

2. Prerequisite

Before continuing with the installation of your E2XX Series router, 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 such as Internet Explorer 10+ or Google Chrome 30+, Mozilla Firefox 20+ or Apple Safari 4+ to access the Lantronix Web Admin Console
- DHCP client enabled in the computer to obtain a valid IP Address from router.

A. How to Enable DHCP in Windows?

- Navigate to **Start > Control Panel > Network and Sharing Centre > Click the existing Connection > Network Connection Status dialog box appears > click Properties > Double click Internet Protocol Version 4 (TCP/IPv4) > Internet Protocol Version 4 (TCP/IPv4) Properties dialog box appears > Under tab General**, select following options:
    a. Obtain an IP address automatically
    b. Obtain DNS server address automatically

3. Default Configuration

Note

- ***All the Username and Password are case sensitive.***

3.1 Web Admin Page

Parameters	Details
IP Address (LAN)	192.168.1.1
Username	admin
Password	Admin

Table 3.1-1: Default Web Admin Page Credentials

3.2 Wi-Fi enabled, with WPA/WPA2 TKIP key

Parameter	Details
SSID	Maestro E200
WPA Key	W1rele$$

Table 3.2-1: Default Wi-Fi Credentials (WPA/WPA TKIP)

3.3 Default Basic Configuration

- WAN (Ethernet) Connection – Automatic (DHCP client)
- LAN (Ethernet) Active DHCP with starting IP Address: 192.168.1.100 with pool of 100 clients.
- WAN as priority source of Internet with Cellular backup
- Cellular default Access Point Name (APN) is "**internet**" and no PAP / CHAP Authentication
- Wi-Fi is on with SSID Maestro EXX as an access point

4. LED Behavior

- Ethernet port (WAN and LAN)
  - **Amber LED (Link Indicator) –** When ON indicates the valid link detection (10/100Mbps).
  - **Green LED (Activity indicator) –** When On (Blinking) indicates traffic/data activity on the port.

- Other LEDs – For E200 and E220 Series

Figure 3.3-1: Front Panel

The top panel of Lantronix E200 and E220 Series Routers features 6 LEDs on the front to indicate critical system information.

Name	Colour 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
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)

Name	Colour and State		Description
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

Table 3.3-1: LED States and Description

- Other LEDs – For E210 Series
  The top panel of Lantronix E200 and E220 Series Routers features 7 LEDs on the front to indicate critical system information.

Name	Colour 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

Name	Colour and State		Description
			(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

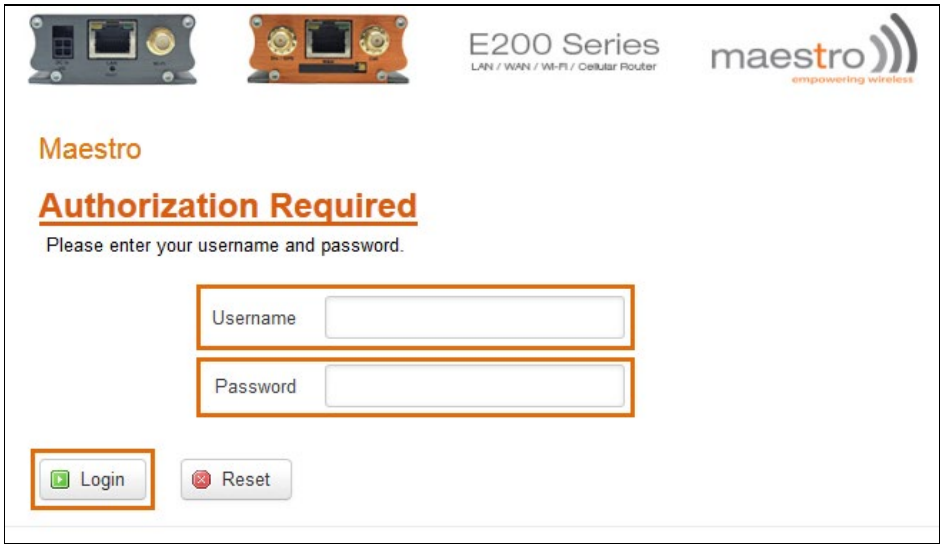
Table 3.3-2: LED States and Description

5. Logon Procedure

Open a Web browser on the computer, and enter the LAN IP Address http://192.168.1.1 of the Lantronix Router in browser's URL box. A dialog box appears prompting the user to enter Username and Password.

Note

- ***The default LAN IP Address of Lantronix Router is 192.168.1.1.***
- ***DHCP must be enabled on the computer to access Lantronix Router with LAN IP Address 192.168.1.1. For more information refer How to Enable DHCP?***



Screen 5-1: Login Page

Parameters	Description
Username	Enter the Username **admin**.
Password	Enter the Password. If you are logging on for the first time after the installation, please use the default password **admin.** ***Note*** • ***We strongly recommend you to change your login password.***
Login Button	Logs on to Router's GUI. Click **Login Button.**
Reset Button	Click **Reset Button** to discard the provided password and re-type the Username and Password.

Table 3.3-1: Login Page

6. Common Icons and Buttons

- **Save** Save – Saves the new/modified configuration.

  Note

  - ***All saved configuration will be lost on Router reboot, if they are not saved and applied.***

- **Save & Apply** Save & Apply – Saves the new/modified configuration and loading the configuration into the Router.

- **Reset** Reset – Discards the unsaved configuration. This allows the user to provide the configuration details again on the GUI page.

- **Add** – Add a field.

- **Delete** – Delete a field.

- **Reveal/Hide Password** – Click to reveal and verify the password. Click it again to hide the password and secure it.

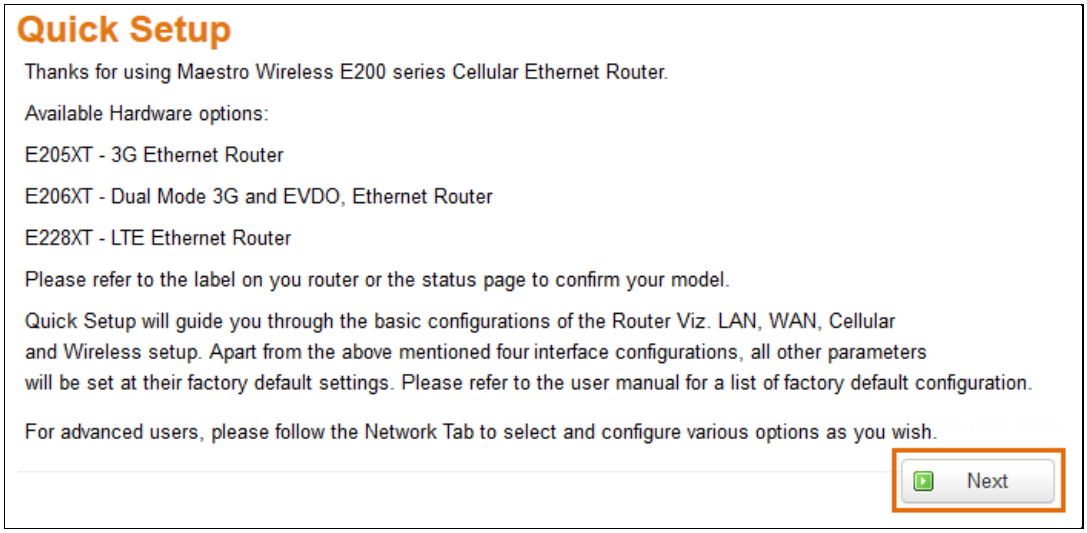
7. Quick Setup

7.1 Quick Setup

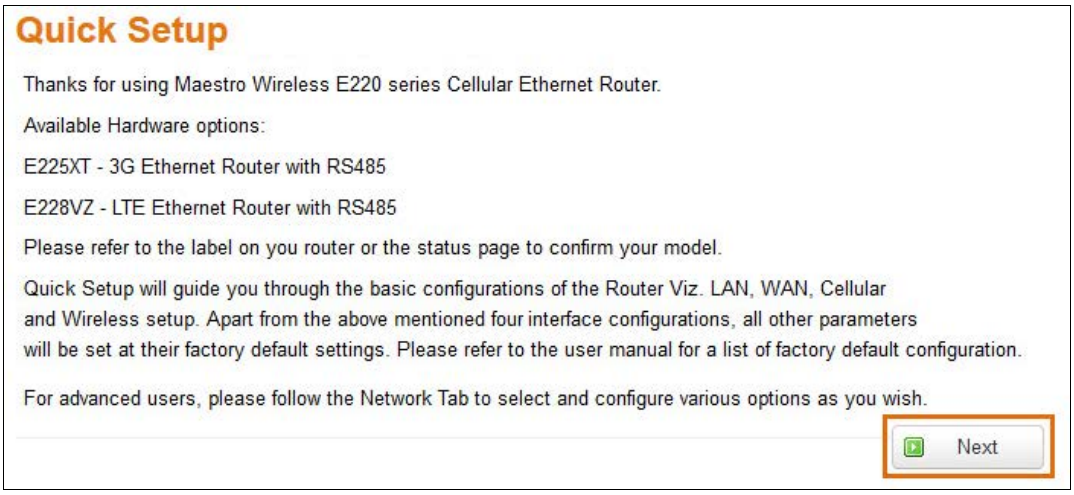
Quick Setup > Quick Setup

Quick Setup page will guide the administrator through the steps required to configure the basic parameters needed for the router to come up and start running.

> ***Note***
>
> - ***Alternately, an administrator can go to Network Settings and import and load a predefined settings file.***



Screen 7-1a: E200 Router Information

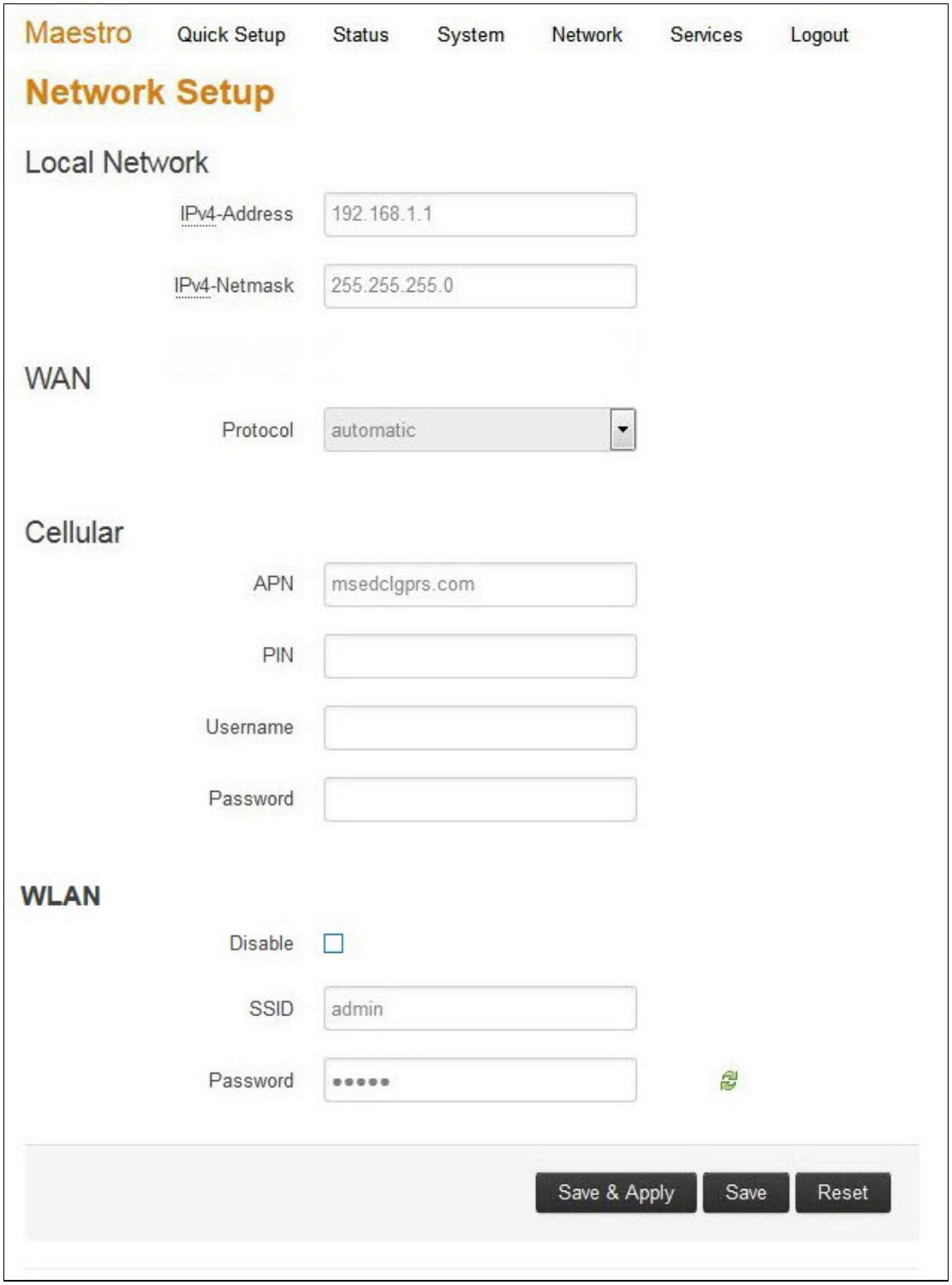


Screen 7-2b: E200 Router Information

7.2 Network Setup

Quick Setup > Quick Setup > Network Setup

Basic network parameters for LAN, WAN, Cellular and Wi-Fi can be configured from the Network Setup page.



Screen 7-2: Quick Start Network Configuration

Parameters	Description
Local Network	
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
WAN	
Protocol	Select the WAN protocol from the available options: **Available Options** • Manual • Automatic • PPPoE (Point to Point Protocol over Ethernet) The default WAN protocol is selected as Automatic.
Cellular	
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.
Username	Enter the login name. The default Username for Lantronix E200 Router is **admin**. The default Username for Lantronix E220 Router is **Maestro E220**.
Password	Enter the password.
WLAN	
Disable	By default, Wi-Fi interface is in enable mode. Check to disable the Wi-Fi interface if you do not want to use it.
SSID	Service Set Identifier (SSID) is a sequence of characters which uniquely names a wireless local area network (WLAN). The default SSID is Maestro E200.
Password	The default password is W1rele$$.

Table 7.2-1: Quick Start Network Configuration

8. Status

Status provides a summary view all the vital configurations of your Lantronix Router such as routing information, firewall details, traffic statistics including real-time graphs.

- Overview
- Firewall
- Routes
- System Logs
- Real-Time Graphs

8.1 Overview

Status > Overview

Overview page provides a quick and bird-eye overview of all the important parameters of your Lantronix router that requires special attention.

8.1.1 Status

Status > Overview > Status

Status Overview page outlines the setting details of basic sub-modules that must be configured for the Router. Status Overview uses tables to display information. The Status page provides information about:

- System
- Cellular
- Memory
- Network
- MWAN Interface Live Status
- DHCP Leases
- DHCPv6 Leases
- Wireless
- Associated Stations

A. System

Status > Overview > Status

The System group provides the Router make and software related information.

System

Hostname	Maestro
Model	MAESTRO E225
PID	E225-071102-HL8548-07011608300030
Firmware Version	Maestro E220 2.2.0 RC5
PoE	Not in use
Kernel Version	3.10.49
Local Time	Mon Dec 19 11:48:37 2016
Uptime	0h 49m 30s
IMEI	359515051941502

Screen 8-1A System Status Overview

Parameters	Description
Hostname	Name assigned to the router for addressing purposes.
Model	Model number of the router that is deployed. Example – Lantronix E225
PID	Display 35 characters long, unique Product Identification number (PID). Consider an example of PID E225-071102-HL8548-xxxxxxxxxxxxxx. It is composed of: • 4 characters SKU: E225 • **6 characters UID:** 071102 (WAN, GNSS, Wi-Fi, 2x LAN, SIM) • 6 character Module Name: HL8548 • 14 characters Serial Number: • xxxxxxxxxxxxxx. Comprises of HW/PCB version (01 to 99), Lot number (01 to 99), Production date (YYMMDD), Unit number (4 digits). •
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
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.

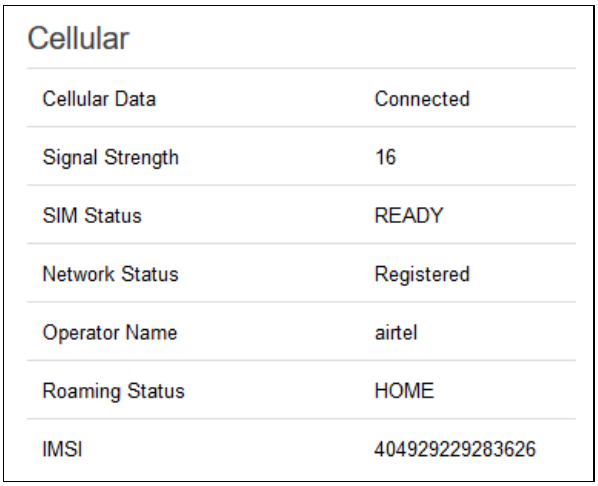
Parameters	Description
Up Time	Displays the time for which the router is up and running since last power ON. The format is hh:mm:ss. The time is displayed in 24 hour clock format.
Last Reboot Cause	Displays the last reboot event time and cause for the Router
IMEI/MEID **(MEID is only available in CDMA / 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 numbers to identify GSM or UMTS mobile devices. It is used to prevent call initiation from a misplaced or stolen GSM or UTMS device, even if someone swaps out the device's SIM card. A MEID number (Mobile Equipment Identifier) is used to identify a cell phone that utilizes the CDMA technology for wireless service. ***Note*** • ***We recommend you record the IMEI or MEID number and secure it, so that it can be quickly accessed in the event of theft or loss of the router.***

Table 8.1-A: System Status Overview

B. Cellular

Status > Overview > Status

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



Cellular

Cellular Data	Connected
Signal Strength	16
SIM Status	READY
Network Status	Registered
Operator Name	airtel
Roaming Status	HOME
IMSI	404929229283626

Screen 8-1B: Cellular Status Overview

Parameters	Description
Cellular Data	Displays the status of the Cellular data. **Status** • **ERROR –** SIM Card is not available in the Router or cellular connectivity malfunction. • **Connected –** SIM card is active, and is connected for data communication. • **Disconnected –** SIM card is inactive and there is no data communication.
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.***
SIM Status	Displays the availability of SIM card in SIM card slot. • **Error –** SIM card is not inserted. • **Ready –** SIM card is inserted.
Network Status	The registration status of the router on the current cellular network.
Operator Name	Name of the current cellular operator in use.
Roaming Status	The roaming status of the router: • Home • Roaming
IMSI	Displays the IMSI Number. In case of UMTS, it is read from the SIM

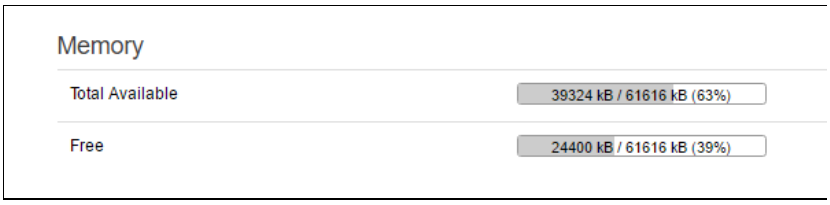
Parameters	Description
	card. An International Subscriber Identity (IMSI) is 15 digit unique Mobile number associated with cellular network and used to acquire the details of the mobile for identifying the user of a cellular network.
ESN (Only for CDMA / EVDO Routers)	Displays the ESN number of cellular module. It must be subscribed for a Verizon account (EVDO).
Revision (Only for CDMA / EVDO Routers)	Displays the Firmware revision number of the cellular module.
Cellular Module Info (Only for E206)	Displays the critical parameters from the cellular module.

Table 8.1-B: Cellular Status Overview

C. Memory

Status > Overview > Status

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



Screen 8.1-C: 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. Grey highlight and the percentage value display the amount of used memory.
Free	Free RAM memory. Grey highlight and the percentage value display the amount of used memory.

Table 8.1-C1: Memory Status Overview

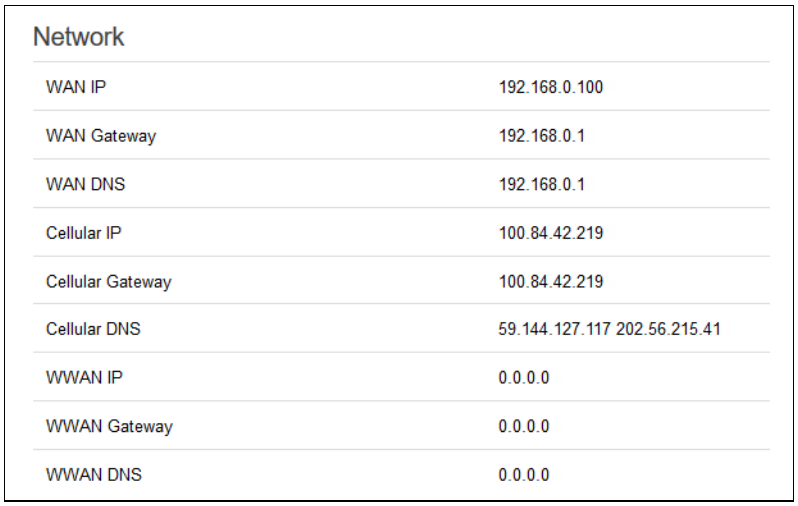
Model	RAM size	Flash size
E205XT02	32MB	32MB
E206XT	32MB	32MB
E220LITE	64MB	32MB
E220	128MB	64MB
E210	128MB	32MB

Table 8.1-C2: Memory Status Overview

D. Network

Status > Overview > Status

The Network group provides the status of IPv4and IPv6 WAN status



Network

WAN IP	192.168.0.100
WAN Gateway	192.168.0.1
WAN DNS	192.168.0.1
Cellular IP	100.84.42.219
Cellular Gateway	100.84.42.219
Cellular DNS	59.144.127.117 202.56.215.41
WWAN IP	0.0.0.0
WWAN Gateway	0.0.0.0
WWAN DNS	0.0.0.0

Screen 8-1D: Network Status Overview

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

Table 8.1-D: Network Status Overview

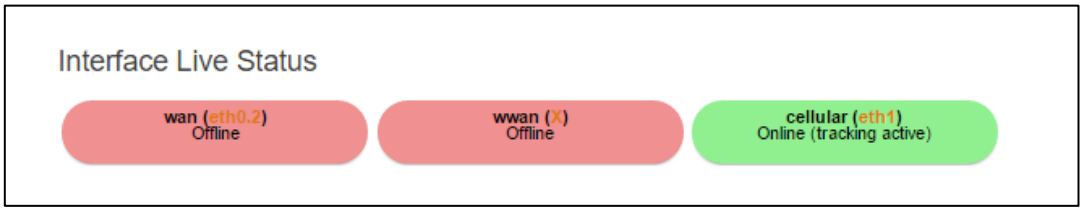
E. MWAN Interface Live Status

Status > Overview > Status

Lantronix routers E200 and E220 series have multiple sources of Internet and can switch seamlessly between them. The below screenshot shows 3 sources of Internet which is WAN (Wired Ethernet), WWAN (Wi-Fi when used as a WAN instead of LAN which is the default configuration) and Cellular.

MWAN Interface provides a birds-eye view of all the available and connected WAN options. In the example figure below, the interfaces marked in Green are live and connected while the ones in red are currently offline.

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



Screen 8-1E: MWAN Interface Live Status

Parameters	Description
Multiple WAN Interface Live Status **Indicates the current status of the interferes – WAN, WWAN, 3G**	
Offline	The interfaces that are not connected to network are marked in RED.
Online	The interfaces that are connected to the network are marked in GREEN. **Status** • **Tracking off –** The interface will not track the availability of the other active interface. • **Tracking active –** The interface will track the availability of the other active interface.

Table 8.1-E: MWAN Interface Live Status

F. DHCP 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.

DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
ASUS-PC	192.168.1.164	40:16:7e:43:85:5a	11h 58m 28s
android-2519158a6ea7ac7e	192.168.1.167	c0:ee:fb:31:1c:d1	11h 51m 1s

Screen 8-1F: DHCP Lease 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 by the router's 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	The remaining time for which the device can use the DHCP server leased IPv4 Address.

Table 8.1-F: DHCP Lease Status Overview

G. DHCPv6 Leases

Status > Overview > Status

Displays the information about the machines connected to router using DHCPv6 lease. This includes IPv4 as well as IPv6 connections.

DHCPv6 Leases

Hostname	IPv6-Address	DUID	Leasetime remaining
Lenovo-PC	fd8c:fd94:3919::294/128	000100011be53cc268f7281265a0	11h 59m 35s

Screen 8-1G: DHCPv6 Lease Status Overview

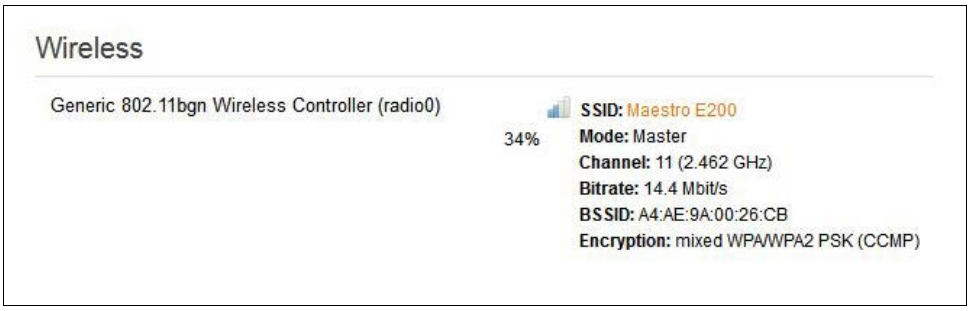
Parameters	Description
Host Name	Name of the device (laptop, mobile, etc.) that is connected to the router and has been leased an IPv6 Address by the router's DHCPv6 server.
IPv6 Address	IPv6 Address assigned to the device connected to the router.
DUID	DUID (Device Unique Identifier) of the device connected to the router
Leasetime remaining	The remaining time for which the device can use the DHCPv6 sever leased IPv6 Address.

Table 8.1-G:DHCPv6 Lease Status Overview

H. Wireless

Status > Overview > Status

The Wireless Group provides the detail information of the Wi-Fi network used by the router.



Screen 8-1H: Wireless Status Overview

Parameters	Description
Connection Name	Displays the name of the connection and the details: **SSID –** A Service Set Identifier (SSID) is a public identifier of 32 characters that uniquely names a Wireless Local Area Network (WLAN) **Mode –** Displays whether the WLAN interface is currently configured as an Access Point 'Master' or as a Client of a higher order Wi-Fi network. ***Note*** • ***For Wi-Fi WAN operation this should be 'Client'.*** • **Channel –** Wireless Local Area Network channel. • **Bitrate –** Data transfer rate • **BSSID –** Displays Basic Service Set Identification (BSSID); 24 bit MAC Address of Wireless device. • **Encryption –** Displays the data encryption method. • **Signal Strength –** Displays the signal strength in percentage.

Table 8.1-H: Wireless Status Overview

I. Associated Stations

Status > Overview > Status

The Associated Stations group enlists the computers and/or devices that are connected to the router over Wi-Fi.

> ***Note***
>
> - ***Associated Station details are available only when router is configured as Master (access point).***

Associated Stations

	MAC-Address	Network	Signal	Noise	RX Rate	TX Rate
	C0:EE:FB:31:1C:D1	Master "Maestro E200"	-86 dBm	0 dBm	6.0 Mbit/s, MCS 0, 20MHz	14.4 Mbit/s, MCS 1, 20MHz

Screen 8-1I: Associated Stations Status Overview

Parameters	Description
Associated Stations	
MAC Address	MAC Address of the computers and/or devices that are connected to the router.
Network	Mode and Name of the network to which the device is connected.
Signal	Signal strength in dBm
Noise	Noise in dBm
RX Rate	Data transfer rate at which the data is received.
TX Rate	Data transfer rate at which the data is transmitted. • Modulation and Coding Scheme (MCS) 1, • High Throughput (HT) 20 Mhz

Table 8.1-I: Associated Stations Status Overview

8.2 Firewall

Status > Firewall

8.2.1 IPv4 Firewall

Status > Firewall > IPv4 Firewall

Firewall Status

IPv4 Firewall | IPv6 Firewall

Actions

- Reset Counters
- Restart Firewall

Table: Filter

Chain *INPUT* (Policy: *ACCEPT*, Packets: 0, Traffic: 0.00 B)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	7155	625.75 KB	delegate_input	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Table: NAT

Chain *PREROUTING* (Policy: *ACCEPT*, Packets: 10993, Traffic: 1.78 MB)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	10993	1.78 MB	delegate_prerouting	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Table: Mangle

Chain *PREROUTING* (Policy: *ACCEPT*, Packets: 103552, Traffic: 39.43 MB)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	275808	119.01 MB	mwan3_hook	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-
2	103552	39.43 MB	fwmark	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Table: Raw

Chain *PREROUTING* (Policy: *ACCEPT*, Packets: 103553, Traffic: 39.43 MB)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	103553	39.43 MB	delegate_notrack	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

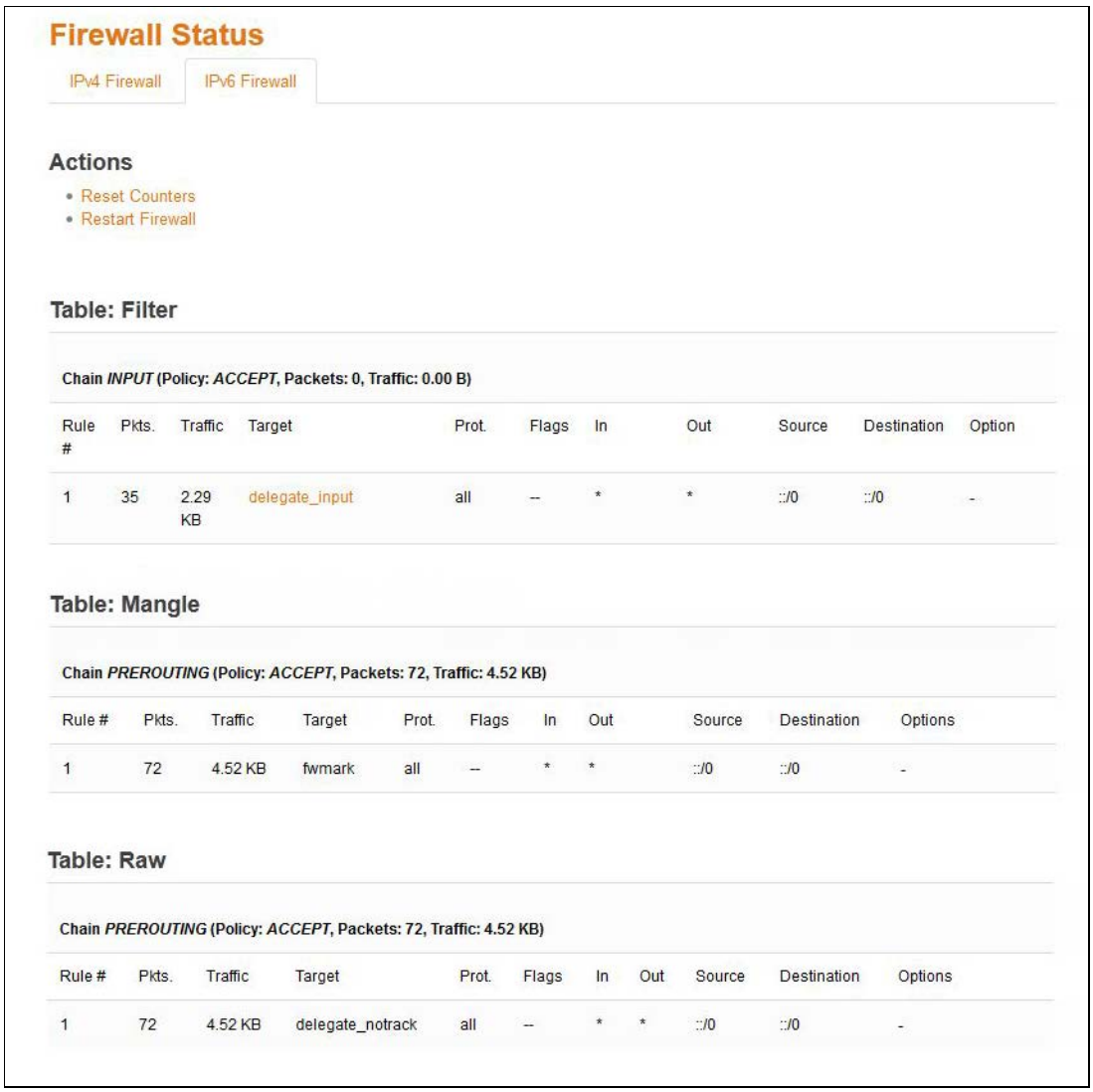
Screen 8.2.1: IPv4 Firewall Status

Parameters	Description
Reset Counters	Click to rest counters Packets and Traffic.
Reset Firewall	Click to reload the existing Firewall configuration of every interface.
Rule #	Displays the serial number of Firewall Rule.
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.
Destination	Displays the destination IPv4 Address.

Table 8.2-1: IPv4 Firewall Status

8.2.2 IPv6 Firewall

Status > Firewall > IPv6 Firewall



Screen 8.2.2 IPv6 Firewall Status

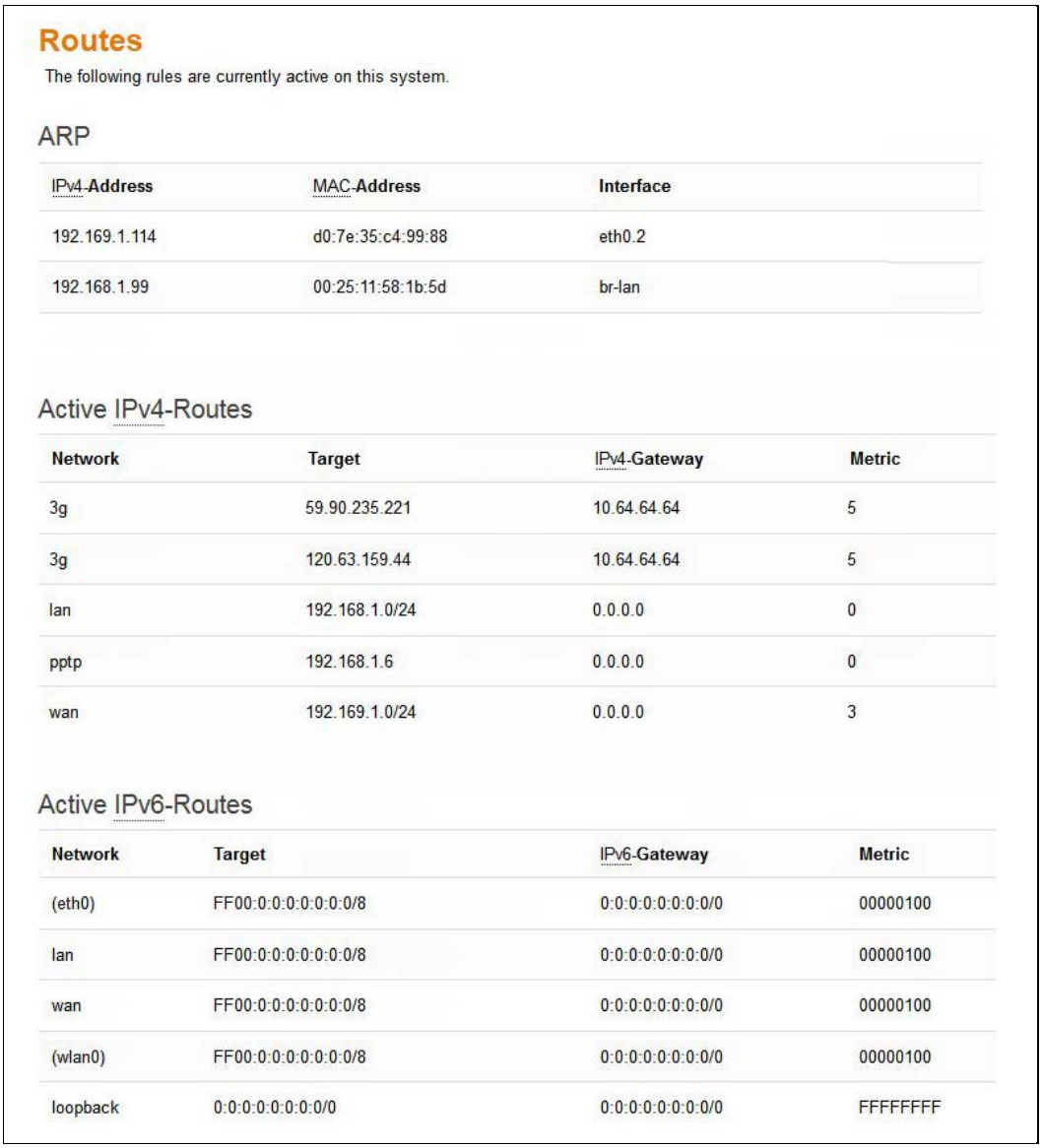
Parameters	Description
Reset Counters	Click to rest counters Packets and Traffic.
Reset Firewall	Click to reload the existing Firewall configuration of every interface.
Rule #	Displays the serial number of Firewall Rule.
Pkts	Displays the number of accepted packets.
Traffic	Displays the amount of traffic 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
Source	Displays the source IPv6 Address.

Parameters	Description
Destination	Displays the destination IPv6 Address.
Options	Displays the destination IPv4 Address.

Table 8.2-2: IPv6 Firewall Status

8.3 Routes

Status > Routes



Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address	Interface
192.169.1.114	d0:7e:35:c4:99:88	eth0.2
192.168.1.99	00:25:11:58:1b:5d	br-lan

Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric
3g	59.90.235.221	10.64.64.64	5
3g	120.63.159.44	10.64.64.64	5
lan	192.168.1.0/24	0.0.0.0	0
pptp	192.168.1.6	0.0.0.0	0
wan	192.169.1.0/24	0.0.0.0	3

Active IPv6-Routes

Network	Target	IPv6-Gateway	Metric
(eth0)	FF00:0:0:0:0:0:0:0/8	0:0:0:0:0:0:0:0/0	00000100
lan	FF00:0:0:0:0:0:0:0/8	0:0:0:0:0:0:0:0/0	00000100
wan	FF00:0:0:0:0:0:0:0/8	0:0:0:0:0:0:0:0/0	00000100
(wlan0)	FF00:0:0:0:0:0:0:0/8	0:0:0:0:0:0:0:0/0	00000100
loopback	0:0:0:0:0:0:0:0/0	0:0:0:0:0:0:0:0/0	FFFFFFFF

Screen 8-3: Routes Status

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

Active IPv6 Routes – Displays the active IPv6 network route information.	
Network	Displays the network Type used by the active IPv4 routes.
Target	Displays the destination IPv6 Address.
IPv6 Gateway	Displays the IPv6 Address Gateway used for traffic routing.
Metric	Displays the metric assigned to Interface.

Table 8.3-1: Routes Status

8.4 System Logs

Status > System Logs

The E2xx series router provides 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 E2xx series router can either store logs locally or send logs to external syslog servers for storage and archival purposes.

The E2xx series router can log many different network activities and traffic including:

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

The E2xx series router supports a single syslog servers for remote logging and it can be configured from **System > System > Logging**.

The E2xx series router can either store logs locally or send to the Syslog UDP servers.

Screen 8-2: System Logs

8.5 Realtime Graphs

Status > Realtime Graphs

Use Real-Time Graph to view Router related activities for different time intervals.

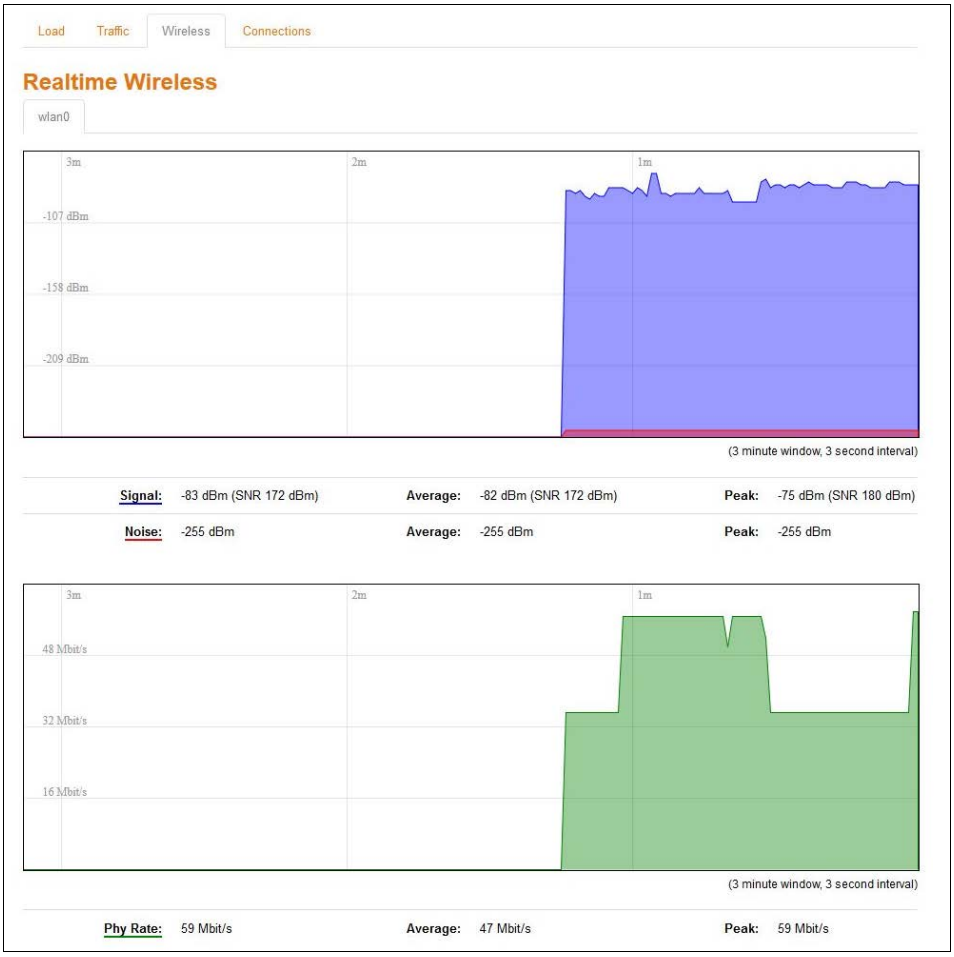
The period wise graph will display the following graphs for the selected period: Load Average, Interface Traffic information (LAN, WAN, Tunnel, Wi-Fi), Wireless usage Information and Connection detailed information.

8.5.1 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, shows the average and peak Signal and Noise and Physical data rates individually.



Screen 8-3: Real Time Wireless Traffic Graph

Parameters	Description
WLAN Interface	
Signal	Graph shows the periodic average of Signal and Noise on the Router.

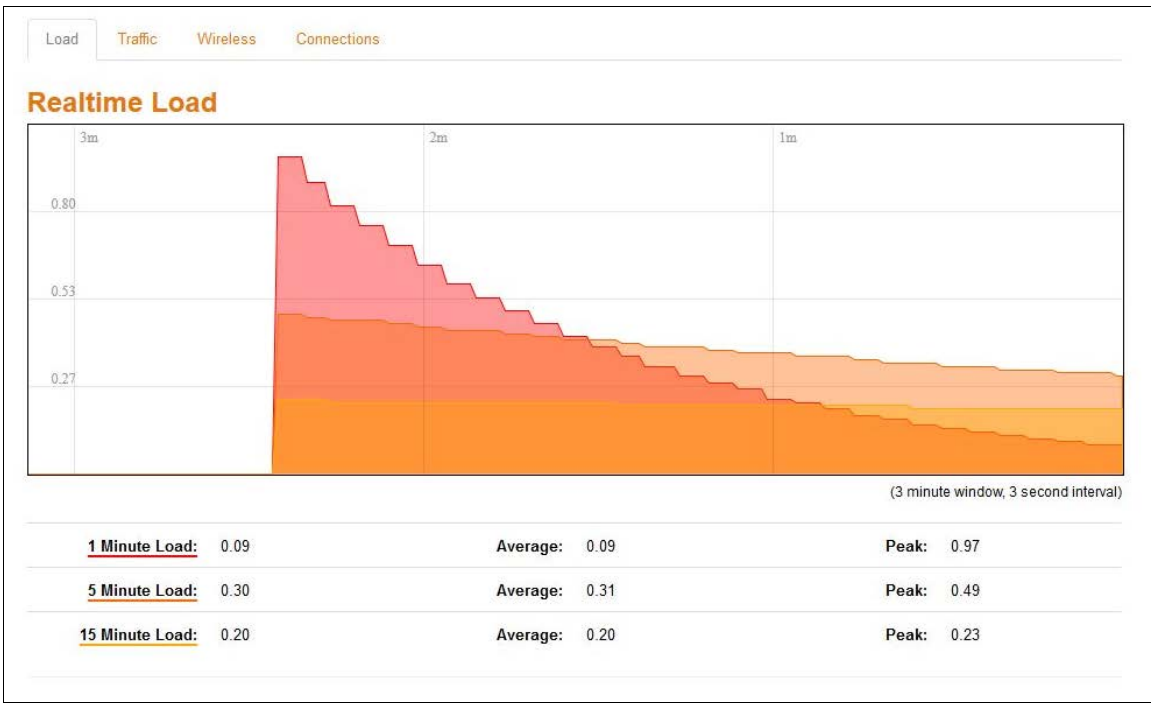
Parameters	Description
	Details • X axis – Time Interval (1 minute) • Y axis – Data Rate (Mbit/s) **Legends** • Blue – Signal • Red – Noise • Green – Physical Rate

Table 8.5-1: Real Time Wireless Traffic Graph

8.5.2 Load

Status Realtime Graphs > Load

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



Screen 8-4: Real Time Load Graph

Parameters	Description
Load	Graph shows the periodic average CPU load on the Router. **Details** • X axis – Time Interval (1 minute) • Y axis – CPU Load (Percentage) **Legends** • Red – 1 Minute Load • Orange – 5 Minute Load • Yellow – 15 Minute Load

Table 8.5-2: Real Time Load Graph

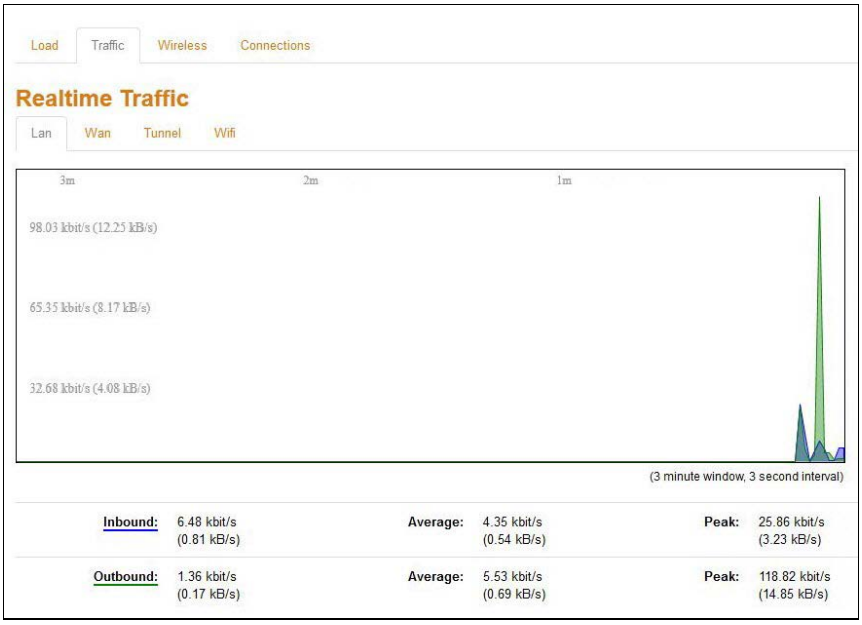
8.5.3 Traffic

Status > Realtime Graphs > Traffic

Traffic indicates the WAN side incoming and outgoing traffic. Traffic Graphs displays combined graph of Upload and Download data transfer. Colors differentiate upload and download data traffic. In addition, shows the average and peak data transfer for upload and download individually.

A. LAN

Graph shows past three minutes average LAN traffic and peak LAN traffic on the router.



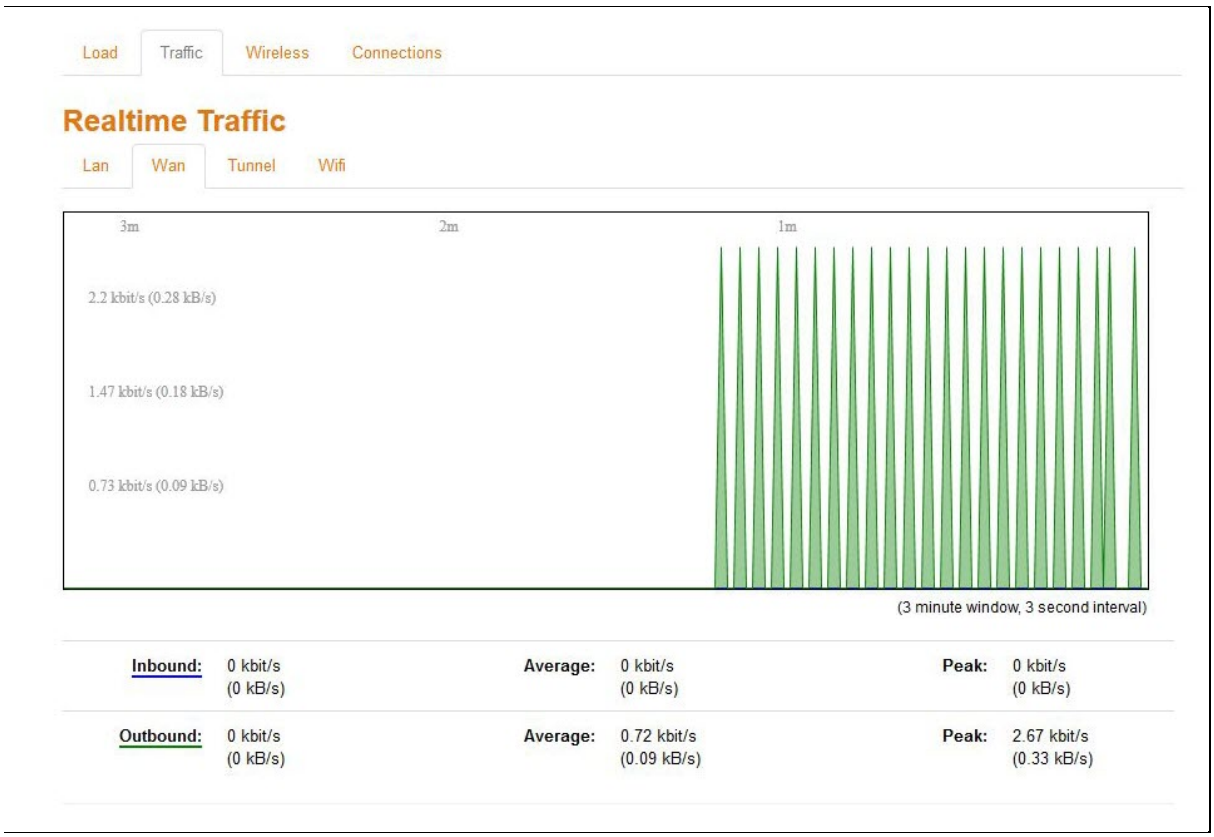
Screen 8-5: Real Time LAN Traffic Graph

Parameters	Description
Traffic (Inbound / Outbound)	Graph shows the periodic average LAN Traffic on the Router. **Details** • X axis – Time Interval (1 minute) • Y axis – LAN Traffic (kB/s) **Legends** • Blue – Inbound Traffic • Green – Outbound Traffic

Table 8.5-3: Real Time LAN Traffic Graph

B. WAN

Graph shows past three minutes average WAN and Cellular traffic and peak WAN and Cellular traffic on the router.



Screen 8-6: Real Time WAN Traffic Graph

Parameters	Description
Traffic (Inbound / Outbound)	Graph shows the periodic average WAN and Cellular Traffic on the Router. **Details** • X axis – Time Interval (1 minute) • Y axis – WAN and Cellular Traffic (kB/s) **Legends** • Blue – Inbound Traffic • Green – Outbound Traffic

Table 8.5-4: Real Time WAN Traffic Graph

C. Cellular

Graph shows past two minutes average Cellular traffic and peak Cellular traffic on the router.

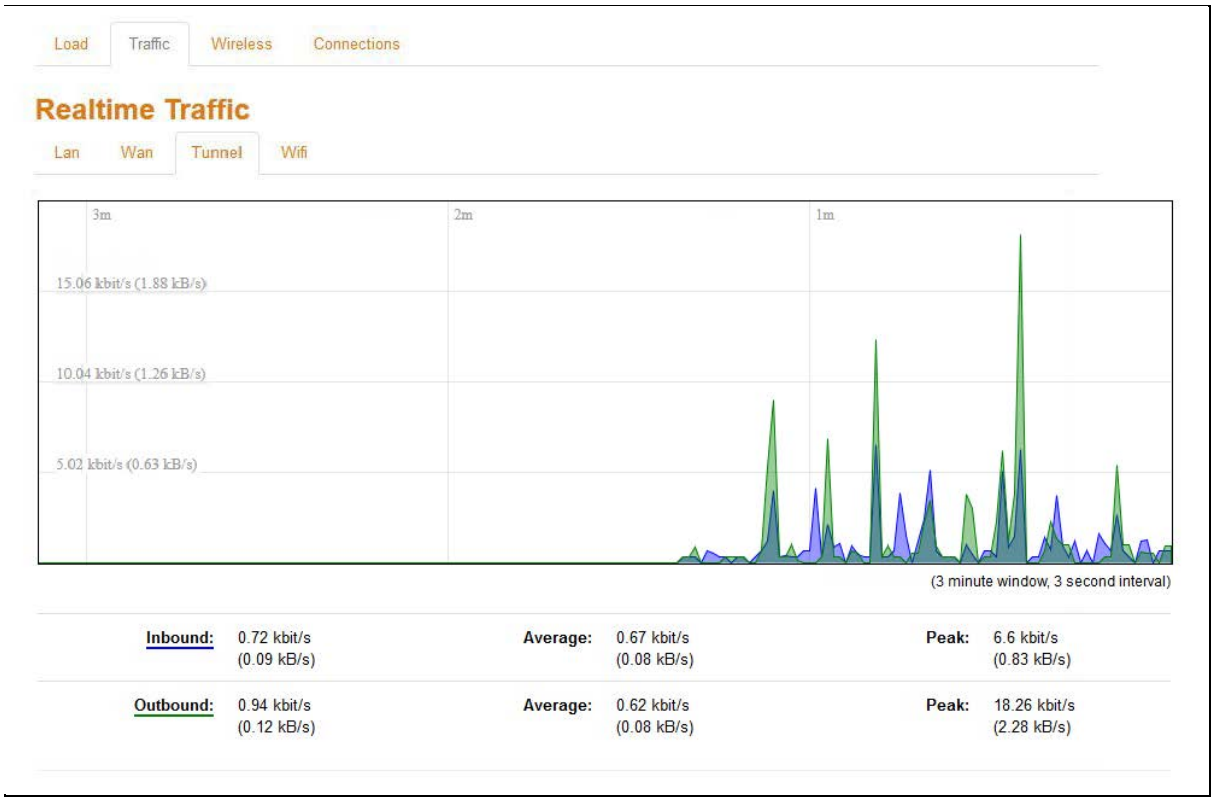
Screen 8-7: Real Time Cellular Traffic Graph

Parameters	Description
Traffic (Inbound / Outbound)	Graph shows the periodic average Cellular Traffic on the Router. **Details** • X axis – Time Interval (1 minute) • Y axis – Tunnel Traffic (kB/s) **Legends** • Blue – Inbound Traffic • Green – Outbound Traffic

Table 8.5-5: Real Time Cellular Traffic Graph

D. Tunnel

Graph shows past three minutes average Tunnel traffic and peak Tunnel traffic on the router.



Screen 8-8: Real Time Tunnel Traffic Graph

Parameters	Description
Traffic (Inbound / Outbound)	Graph shows the periodic average Tunnel Traffic on the Router. **Details** • X axis – Time Interval (1 minute) • Y axis – Tunnel Traffic (kB/s) **Legends** • Blue – Inbound Traffic • Green – Outbound Traffic

Table 8.5-6: Real Time Tunnel Traffic Graph

E. Wi-Fi

Graph shows past three minutes average Wi-Fi traffic and peak Wi-Fi traffic on the router.

Screen 8-9: Real Time Wi-Fi Traffic Graph

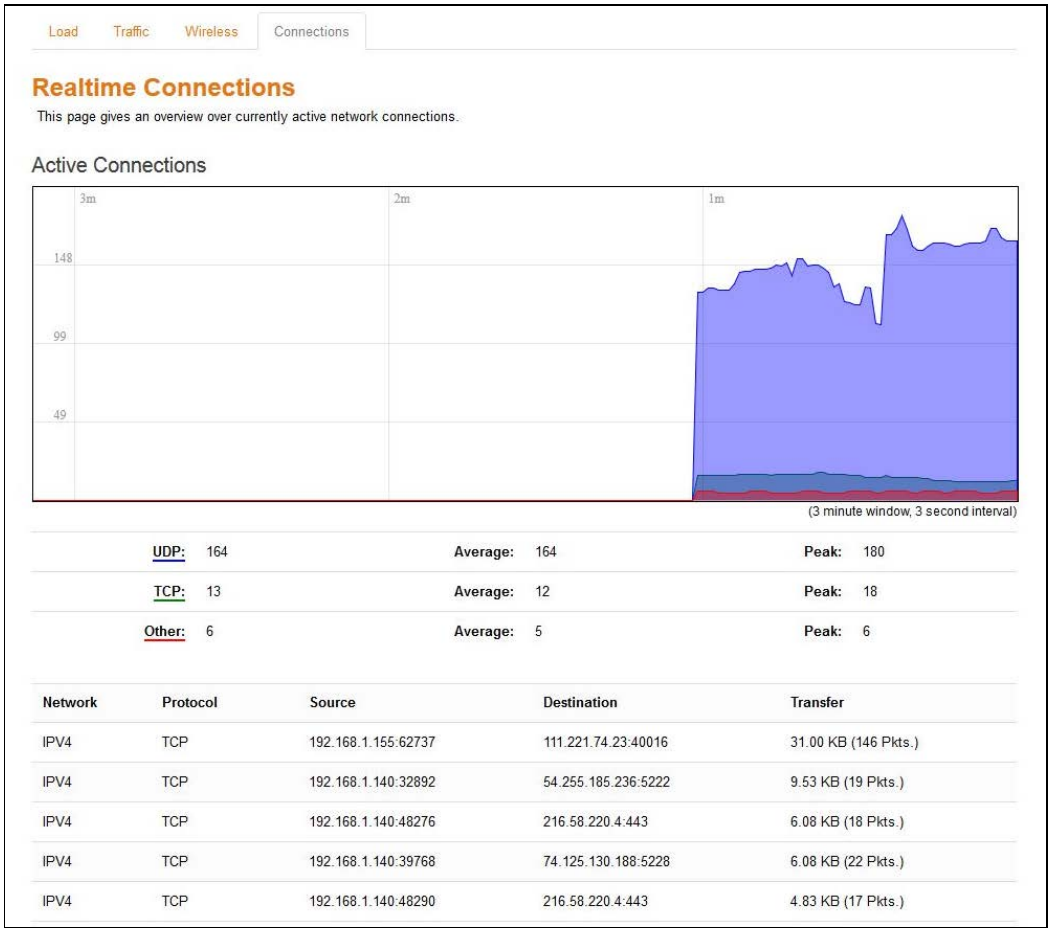
Parameters	Description
Traffic (Inbound / Outbound)	Graph shows the periodic average Wi-Fi Traffic on the Router. **Details** • X axis – Time Interval (1 minute) • Y axis – Wi-Fi Traffic (kB/s) **Legends** • Blue – Inbound Traffic • Green – Outbound Traffic

Table 8.5-7: Real Time Wi-Fi Traffic Graph

8.5.4 Connection

Status > Realtime Graphs > Connection

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



Screen 8-10: Real Time Connection Traffic Graph

Parameters	Description
Protocol	Graph shows the periodic average of data transfer using specific protocols on the Router using the active connections in real time. **Details** • X axis – Time Interval (1 minute) • Y axis – Number of Active Connections **Legends** • Blue – UDP • Green – TCP • Red – Other Protocols
Network	Network connection type, IPv4 or IPv6.
Protocol	Name of the protocol used for routing data.
Source	Source IP Address and port number of an active connection.
Destination	Destination IP Address and port number of an active connection.

Parameters	Description
Transfer	Displays the total data transferred using the specific network connection.

Table 8.5-8: Real Time Connection Traffic Graph

9. System

System allows configuration and administration of router for secure local and remote management. It also provides the basic system settings, time management, language settings, Software packages updates, firmware updates and reboot schedules of the Router.

- System
- Administration
- Software
- Backup / Flash Firmware
- Reboot

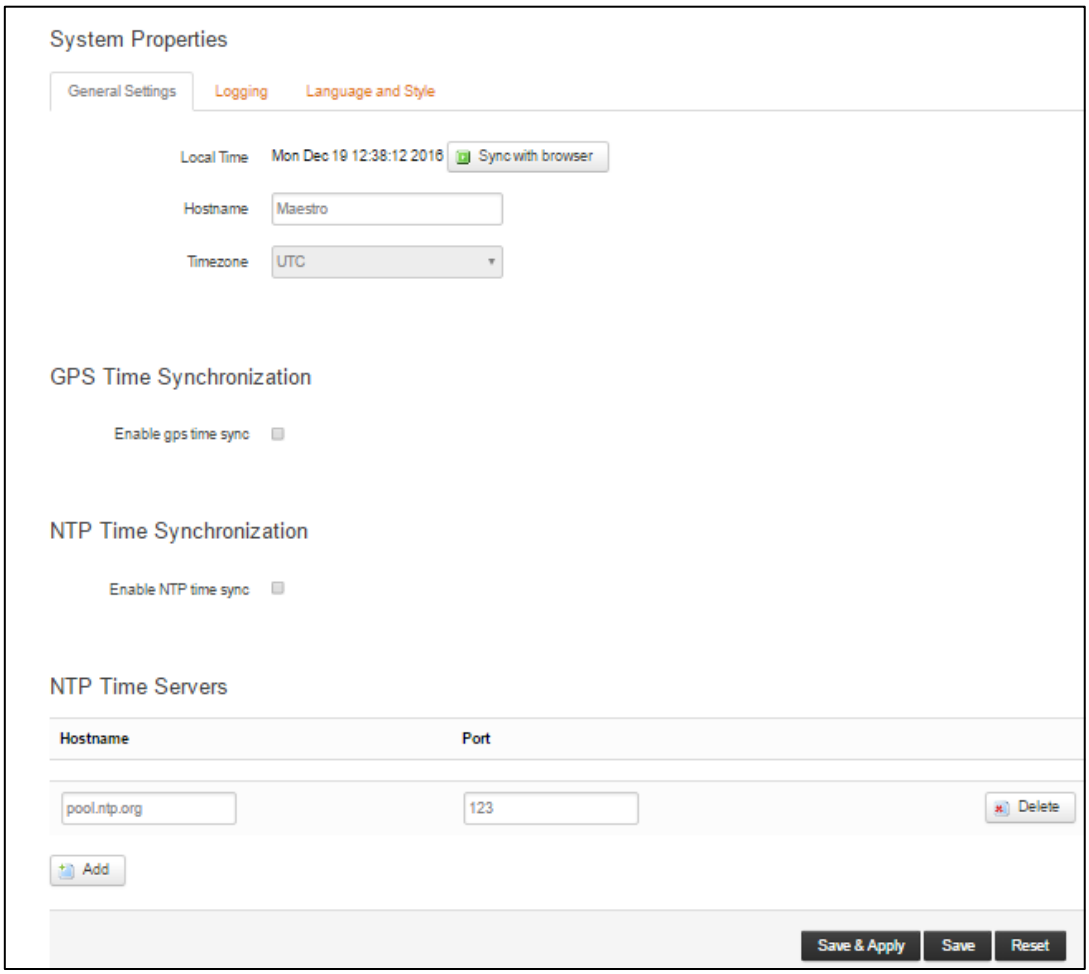
9.1 Systems

System > System

9.1.1 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 also happen at a precise time.



Screen 9-1: System General Settings

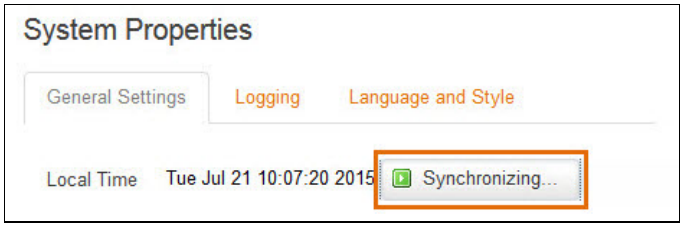
Parameters	Description
Local Time	Current router time. Click “Sync with browser” button to synchronize router clock with the local computer browser.  ***Note*** • ***The displayed time is dependent on the configuration of your local computer that is being used as NTP server.***
Hostname	Enter the Hostname. The configured Hostname appears on the **Status > Overview page**.
Timezone	Select time zone according to the geographical region in which Router is deployed.
Time Synchronization	
GPS Time sync	For The E2xx series router models which support GPS functionality, you can sync the time with GPS. ***Note*** • ***GPS Antenna will be needed for GPS time sync***
NTP time sync	Enable if you want Router to get time from an NTP server. ***Note*** • ***If NTP Server is activated, the Router will update time every 60 minutes from the NTP Servers.*** • ***Enabling NTP Client consumes data.***
Provide NTP Server	Click to use the router as a NTP server and port details

Table 9.1-1: System General Settings

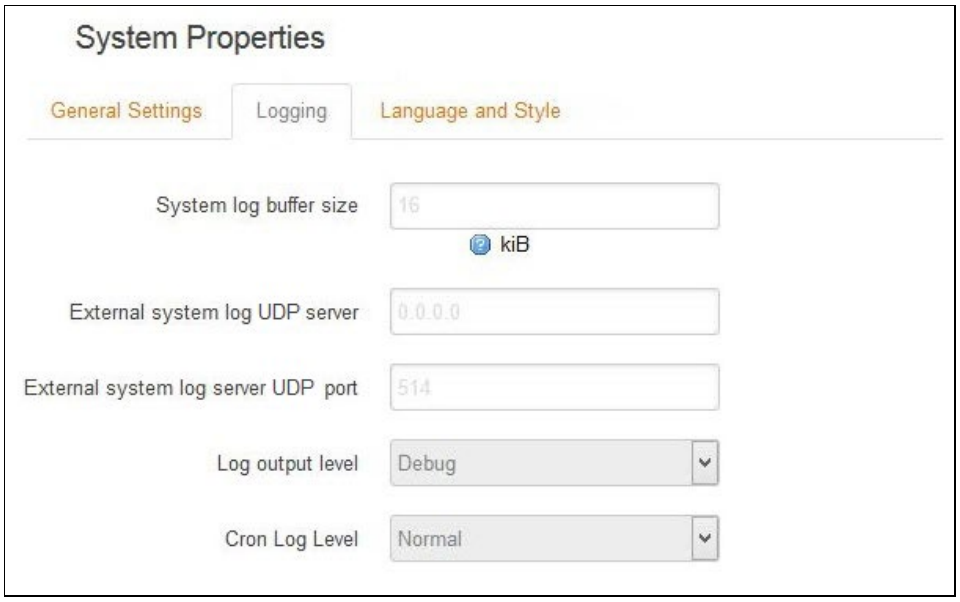
9.1.2 Logging

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 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.



Screen 9-2: Syslog Configurations

Parameters	Description
System log buffer size	Enter the size of the buffer in Kilobytes (KB) to save logs and stus information details. The default System Log Buffer size is 16 KB.
External system log UDP server	Enter the IP Address of an External UDP 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 UDP	Enter the Port number of an External UDP server system.

Parameters	Description
server port	UDP server is used to store the system logs The default Port number of external log server is 514.
Log output level	Select the Log output level to serve for one of the following purpose: • **Debug –** Logs will be used by The E2xx series router software developer for debugging the router application. These logs are not useful during operations. • **Info –** These logs provide normal operational information messages that are used for general purposes like reporting. • **Notice –** Provides alerts for peculiar events that are not an error. These logs help to identify potential issues. Since these logs do not indicate errors, immediate action may/may not be necessary. • **Warning –** A warning messages is displayed for a potential issue, indicating to take an action. An error may occur if no action is taken against the warning issued. • **Error –** Displays the logs indicating an error condition. ***Note*** ***For help with log errors, please contact Lantronix Technical Support.*** • **Critical –** Indicates failure in secondary system and must be corrected immediately. • **Alert –** Problems which should be corrected immediately. • **Emergency –** System is Unusable.
Cron log level	Select the criticality level of output. • **Debug –** Helps you debug cron process which has failed during runtime. • **Normal –** Normal informational messages • **Warning –** Indicates some issues can happen or error could be generated in cron process. ***Note*** • ***For help with Cron log warning messages, please contact Lantronix Technical Support.***

Table 9.1-2: Syslog Configurations

9.1.3 Language and Style

System > System > Language and Style

Screen 9-3: Language and Style Configurations

Parameters	Description
Language	Select preferred language as English. Default value is auto.
Design	Select Bootstrap design of the user interface. Default design selected is bootstrap.

Table 9.1-3: Language and Style Configurations

9.2 Administration

System > Administration

The Administration page allows configuration of the general settings in Router. Various ports and login security can be configured using Administration submenu.

9.2.1 Router Password

System > Administration > Router Password

The Router is shipped with the default – username & password credentials set as “admin”. This administrator is always authenticated locally i.e. by Router itself. We recommend that you change the password for this username immediately after deployment.

Screen 9-4: Router Credential Configurations

Parameters	Description
Password	Specify the new administrator password. Click to reset the password and re-type.
Confirmation	Confirm the new administrator password. Click to reset the password and re-type.

Table 9.2-1: Router Credential Configurations

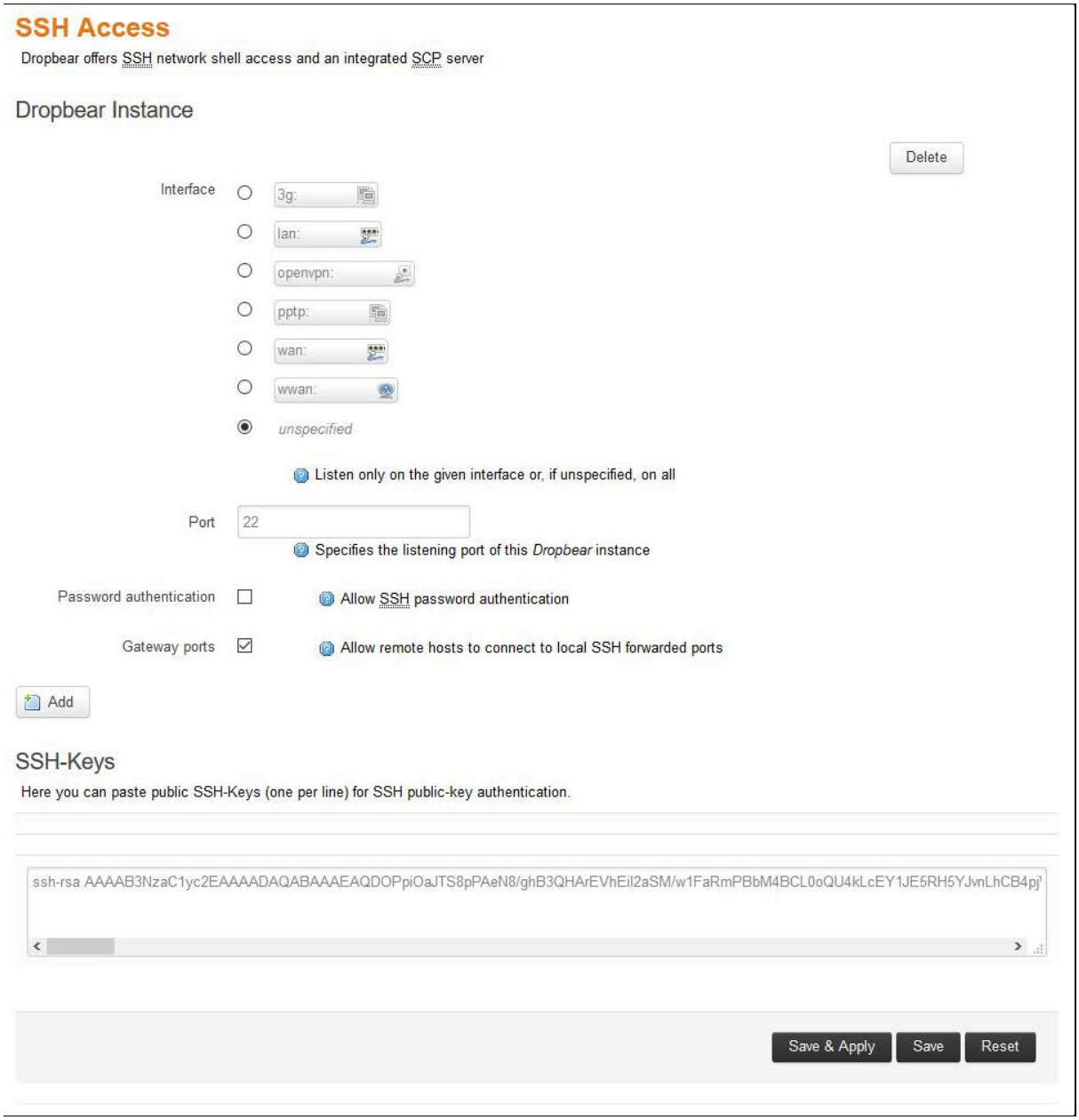
9.2.2 SSH Access

System > Administration > SSH Access

The E series integrate Dropbear which offers SSH network shell access and an integrated SCP (Secure Copy Protocol) server.

You can also set parameters for Dropbear Instance for SSH Access and you can paste 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 SH access from 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.



Screen 9-5: SSH Access Configurations

Parameters	Description
Dropbear Instance	
Interface	Select the interface. SSH listens only on the selected interface. ***Note*** • ***Interface options celldhcp and cellular is available only in E206.*** If unspecified option is selected it listens to all the interfaces.
Port	Provide listening port of the Dropbear instance. Default port is 22.
Password Authentication	Select to allow authentication using SSH password. By default it is disabled.
Gateway ports	Select to allow remote hosts to connect to local SSH forwarded ports.
Add	Click Add button to add an Interface.
Delete	Click Delete button to delete the Interface
SSH Keys **Public SSH keys can be provided one per line for authenticating with SSH public-key.** ***Note*** • *Public SSH keys are provided by default. They are configured by default on Port 22. SSH are by default disabled WAN access. You can either enable Port 22 from the Web interface or using the SMS.*	

Table 9.2-2: SSH Access Configurations

9.3 Software

System > Software

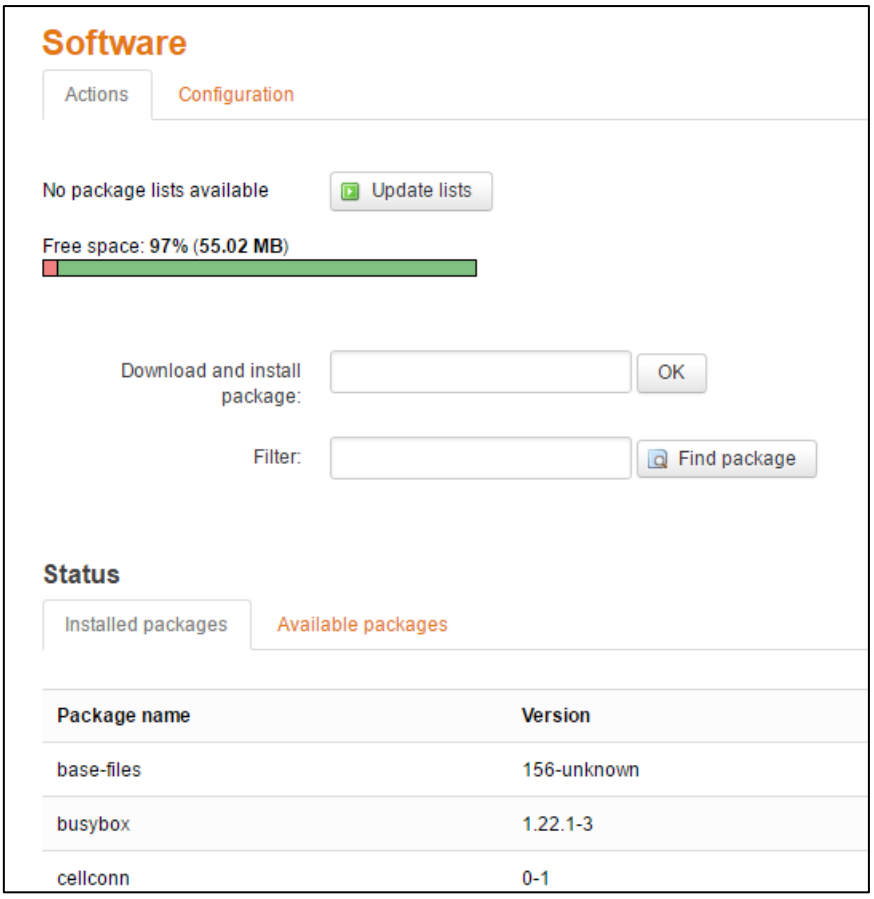
Software page give you access to the list of installed as well as available software package or filter installed on your router. In addition, E Series router allows the user to install their developed application packages and 3rd party packages. For information about installing your own or third-party application packages, please contact Lantronix Technical Support.

Lantronix has its own list of packages which would be downloaded from D2Sphere. For details on D2Sphere, please contact your regional Lantronix Sales office.

9.3.1 Actions

System > Software > Actions

A. Installed



Screen 9-6: Software Installation and Installed Package Details

Parameters	Description
Update lists	Click to update the package list from the package repository servers.
Free space	Indicates the free space and used space on flash memory. **Legends**

Parameters	Description
	• Red – Used space • Green – Free space
Download and install package	Enter the **exact name** of the package to be downloaded from package repository servers and install it. Click OK initialize installation.
Filter	Enter the **keyword** of the required package and click Find Package to search it from package repository servers.
Find package	Click Find package button to search the package.
Status – Installed Package	
Package name	Displays the name of installed package.
Version	Displays the version of installed package.

Table 9.3-1: Software Installation and Installed Package Details

B. Available Packages

Screen 9-7: Software Packages Available for Installation

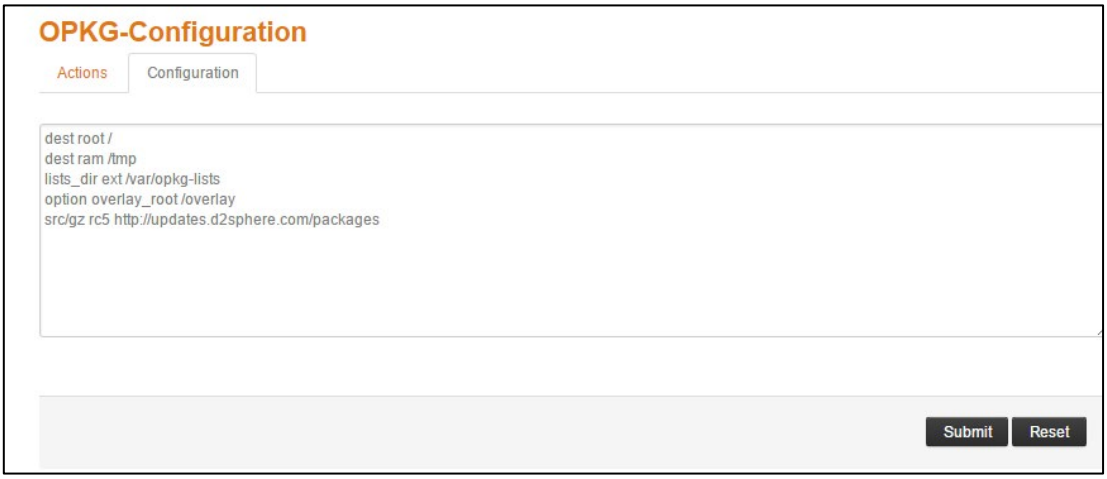
Parameters	Description
Install	Click Install against respective Package to install it.
Package name	Displays the name of package.
Version	Displays the version of package.
Description	Displays the description of package.

Table 9.3-2: Software Packages Available for Installation

9.3.2 Configuration

System > Software > Configuration

This configuration page provides the path to the router as to where it should go and update the packages. All Lantronix packages would be updated from D2Sphere.com however you can add your own http servers where you wish to upload your packages.



Screen 9-8: Software Configuration - OPKG

9.4 Backup / Flash Firmware

System > Backup / Flash Firmware

Backups are required in order to keep the working configuration data. This backup file can also be used to configure other Routers for same settings, instead of configuring each of them for every parameter.

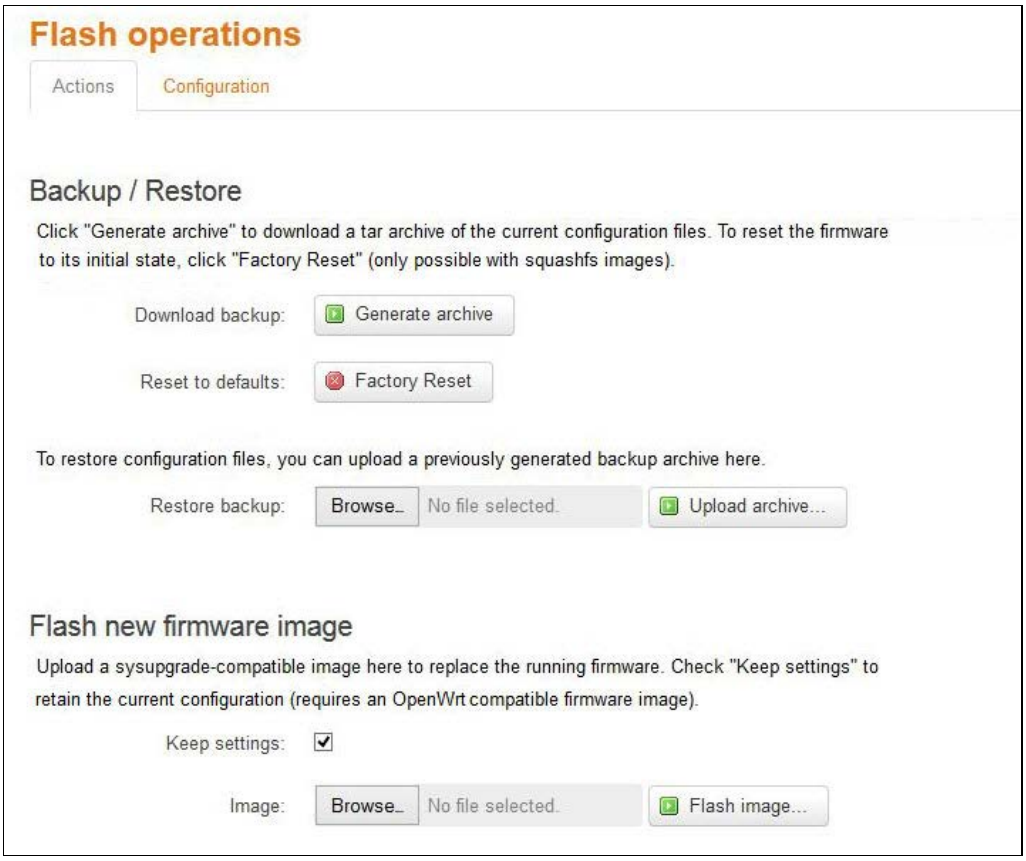
Backup consists of all the policies and all other user related information. Once the backup is taken, you need to upload the file for restoring the backup.

> ***Note***
>
> - ***Restoring older configuration leads to the loss of current configuration.***

9.4.1 Flash Operation

System > Backup / Flash Firmware > Flash Operation

A. Actions



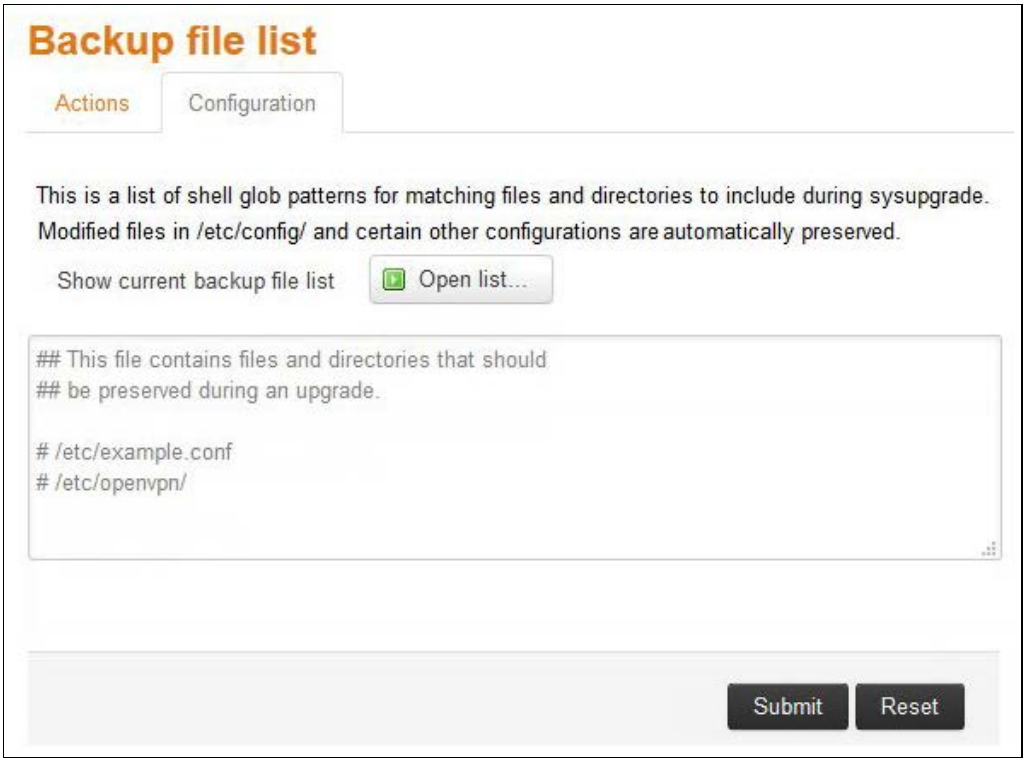
Screen 9-9: Backup - Restore and Flash Operations

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 Factory Reset button to reset the firmware to its default

Parameters	Description
	configurations. ***Note*** • ***This valid only with squashfs images.***
Restore backup	Click browse to select the configuration file to restore backup. OR Click “Upload archive” button to upload a previously generated backup archive.
Flash new firmware image	
Keep settings	Select to retain the current configuration even after the new firmware re-flash. ***Known Behavior*** • ***Some of the configurations (like GUI Webpage details) may not get updated until a factory reboot.***
Image	Click “Flash image” button to upload a sysupgrade compatible image for replacing the running firmware. When the binary image is loaded (.bin file), there is a file integrity check which is done via the use of md5 algorithm. We recommend you to md5 value with the one given along with the binary file..

Table 9.4-1: Backup - Restore and Flash Operations

B. Configurations



Screen 9-10: Backup File Configurations

Parameters	Description
Open list	Click to open the list of files and directories that should be preserved during an upgrade.

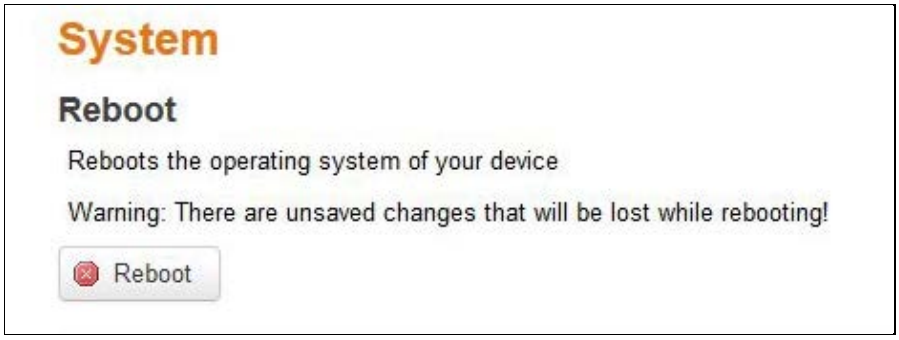
Table 9.4-2: Backup File Configurations

9.5 Reboot

System > Reboot

Router will be rebooted and will reload the configuration.

> ***Note***
>
> - ***The unsaved configuration will be lost if you opt for this option.***

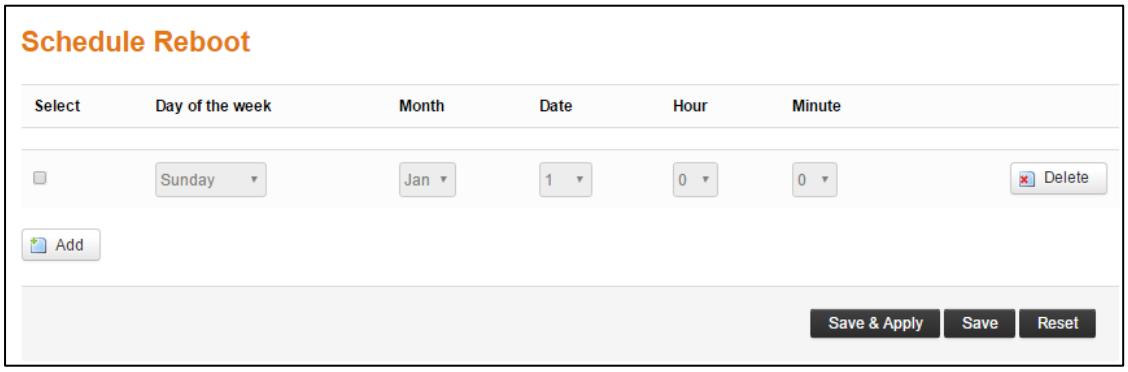


Screen 9-11: System Reboot

System > Schedule Reboot

Router will be rebooted periodically as per the schedule set and will reload the configuration. You can set a reboot schedule on the basis of

- Time of the day
- Weekly at a particular time
- Monthly on a particular date and time



Screen 9-12: Schedule Reboot

10. Network

E Series Router's user-friendly software is very flexible and provides the administrator several options to customize the Network configurations adhering to the organization's requirements. To configure the Network parameters, following sub-sections are made available:

- Interfaces
- Load Balancing
- Wi-Fi
- DHCP and DNS
- Hostnames
- Whitelist / Blacklist
- Static Routes
- Diagnostics
- Firewall

10.1 Interfaces

Network > Interface

Interface sub-module provides the overview of the interface configuration that includes the network configuration and interface status. It further allows configuring and updating the each interface for general setups like selecting the protocol; advanced settings like gateway configurations, DNS settings, DHCP configurations; firewall settings like assigning firewall zone to the Interface.

- Interface Overview
- CELLDHCP (Only for E206)
- CELLULAR
- WAN
- LAN
- WWAN

A. Interface Status

The Interface Status parameter displays the following details associated to interface:

- **Uptime** – Displays the time for which the Interface is up and active since last interface connection/reconnection. The format is hh:mm:ss. The time is displayed in 24 hour clock format.

  Note

  - ***Uptime is displayed for LAN, WAN, Cellular and WWAN 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.

  Note

  - ***IPv4 is displayed for LAN, 3G and WAN Interfaces.***

- **IPv6 –** Displays IPv6 Address of the Interface.

  Note

  - ***IPv6 is displayed for LAN, 3G and WAN Interfaces.***

B. Interface Protocols

The **Protocol configuration** on the Interface General Settings page allows configuring the protocol with respect to the router model number. The available protocol options are as below and please make sure that you select an appropriate protocol as mentioned in the table below for the selected interface.

Interface→ / Protocols↓	LAN	WAN	WWAN	Cellular	CELLDHCP (E206)
Static Address	✓	✓	✗	✗	✗
DHCP Client	✗	✓	✓	✗	✓
PPPoE	✗	✓	✗	✗	✗
PPPoATM	✗	✓	✗	✗	✗
UMTS / GPRS	✗	✗	✗	✓	✗
CELLULAR **(E206)**	✗	✗	✗	✓	✗

Note

- ***For E206 only, the cellular interface is separated between two interfaces: CELLDHCP and "CELLULAR". CELLDHCP is managing local connection with cellular module inside the router.***

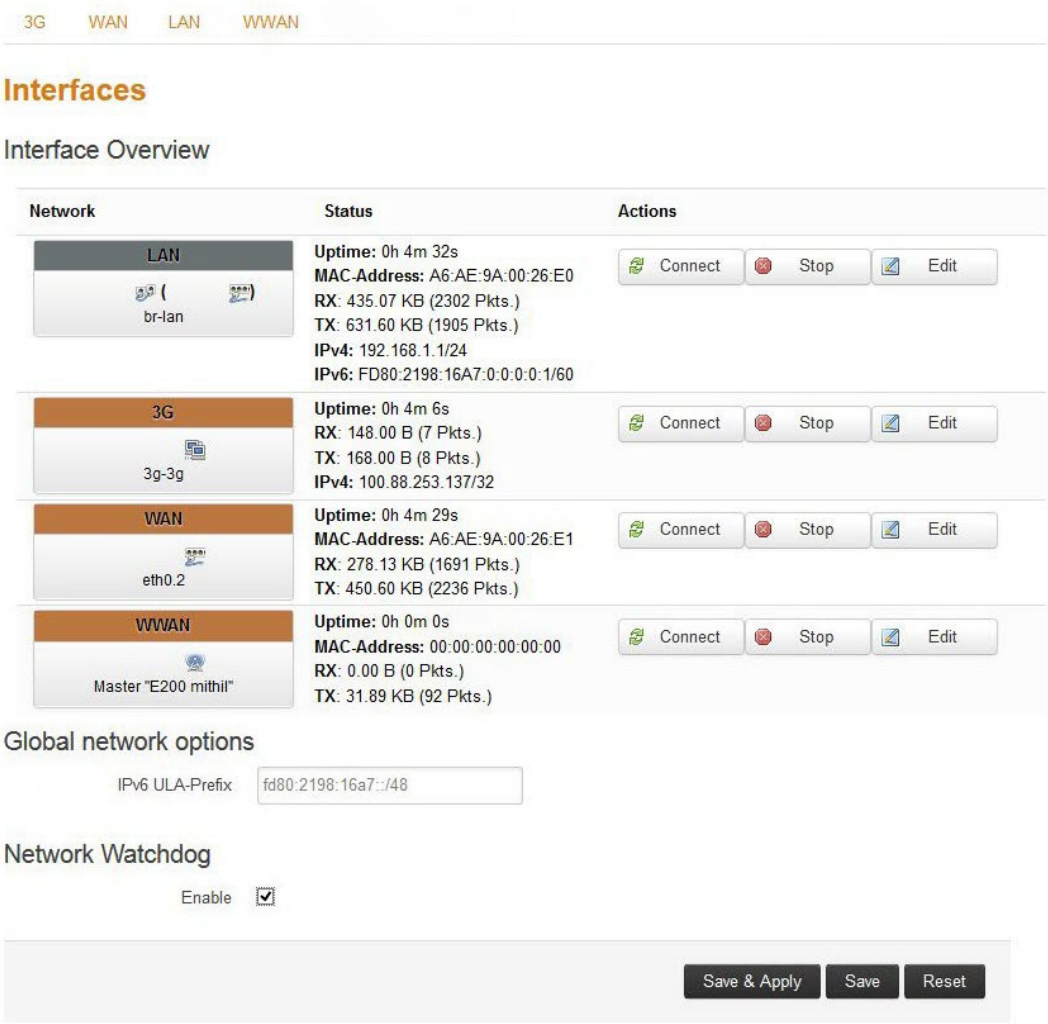
Parameters	Description
Static address	• **IPv4 address –** Enter the IPv4 Address. This IP Address must be used to access the Router. The default IP Address is 198.162.1.1 for LAN. • **IPv4 Netmask –** Select the IPv4 Netmask. • **IPv4 Gateway –** Enter the IPv4 Address for Gateway. In case of LAN, if you do not provide any Gateway IP Address, by default it will take the same IP Address as that of the IPv4 LAN IP Address (192.168.1.1). For WAN, enter the IP Address of WAN gateway. • **IPv4 broadcast –** Enter the IPv4 Address for broadcast. • **Use Custom DNS servers –** Click to add custom DNS servers. • **IPv6 assignment length –** Select the IPv6 assignment length. Available Options • **64 –** Assign a part of the given length of public IPv6-prefix to this interface. • **disabled** • **--custom-- –** Assign a part of the given length of public IPv6-prefix to this interface. IPv6 assignment length is disabled by default. • **IPv6 address -** Enter the IPv6 Address. • **IPv6 gateway -** Enter the IPv6 Address for Gateway.

Parameters	Description
	• **IPv6 routed prefix -** Enter the public prefix direct the client distribution to the router. • **DHCP Server (Only for LAN)** - Provide static details for configuring DHCP Server. • **General Setup** a. **Ignore interface –** DHCP is disabled when Ignore interface is checked. • **IPv6 Settings** a. **Router Advertisement-Service –** Select the Router Advertisement-Service mode; disabled, server mode, relay mode, hybrid mode. b. **DHCPv6-Service –** Select the DHCPv6-Service mode; disabled, server mode, relay mode, hybrid mode. c. **NDP-Proxy –** Select the Router Advertisement-Service mode; disabled, relay mode, hybrid mode. d. **Announced DNS servers –** Add the DNS servers. e. **Announced DNS domains –** Add the DNS domains.
DHCP Client	Enter the Hostname to be sent to a DHCP server when requesting for IP Address.
PPPoE	• **PAP/CHAP username –** Enter the PAP/CHAP username. Click to reset the password. The default password is admin. • **PAP/CHAP password –** Enter the PAP/CHAP password. • **Access Concentrator –** Enter the access concentrator name. • **Service Name –** Enter the service name. ***Note*** • ***Access Concentrator name and Service Name gets auto populated from PPPoE Access Point Router if they are not explicitly provided***
PPPoATM	• **Protocol support is not installed –** Click Install package "ppp-mod-pppoa" to install the protocol support. • **PPPoA Encapsulation –** Select the PPPoA encapsulation method; VC-Mux and LLC. • **ATM device number –** Enter the ATM device number. • The default ATM device number is 0. • **ATM Virtual Channel Identifier (VCI) –** Enter ATM Virtual Channel Identifier (VCI) number. • The default VCI number is 35. • **ATM Virtual Path Identifier (VPI) –** Enter ATM Virtual Path Identifier (VPI) number. • The default VPI number is 8.

Parameters	Description
	• **PAP/CHAP username –** Enter the PAP/CHAP username. • **PaP/CHAP password –** Enter the PAP/CHAP password.
UMTS/GPRS	• **Protocol –** Select the protocol with respect to the router model number. • **Service Type –** Select the type of service from the available. You can select if you want 2G only, 3G only, 3G with 2G fallback, 4G only and 4G with 3G or 2G fallback. Please note that this selections largely depends on the Router Model. • **APN –** Enter the APN provided by your network operator. • **PIN –** Enter the SIM PIN if any. • **Username –** Enter the Username for APN access if exists. • **Password –** Enter the Password Username for APN access if exists. • **Authentication –** Enter the type of authentication that your cellular operator provided for PPP negotiation from PAP/CHAP/No Authentication
CELLULAR **(E206)**	• **Priority –** Select the service from the available options that are AT&T, GenericGSM, GenericCDMA, Sprint and Verizon. • **Delay –** Enter the delay in second/minutes for the Cellular Module to reboot post the selection of the service from parameter Priority. • **APN –** Enter the APN provided by your network operator. • **PIN –** Enter the SIM PIN if any • **Username –** Enter the Username. • **Password –** Enter the Password.

10.1.1 Interface Overview

Network > Interface > Interface Overview



Screen 10-1: Interface Overview

Parameters	Description
Interface Overview	
Network	Displays the all the configured Network Interfaces. The pre-configured interfaces for the router are • LAN • CELLDHCP (Only for E206) • CELLULAR (Only for E206) • WAN • WWAN ***Note*** • ***Default Interfaces LAN, Cellular, WAN, WWAN cannot be deleted.*** • ***When Wi-Fi is configured as Client, Interface WWAN will become active.***

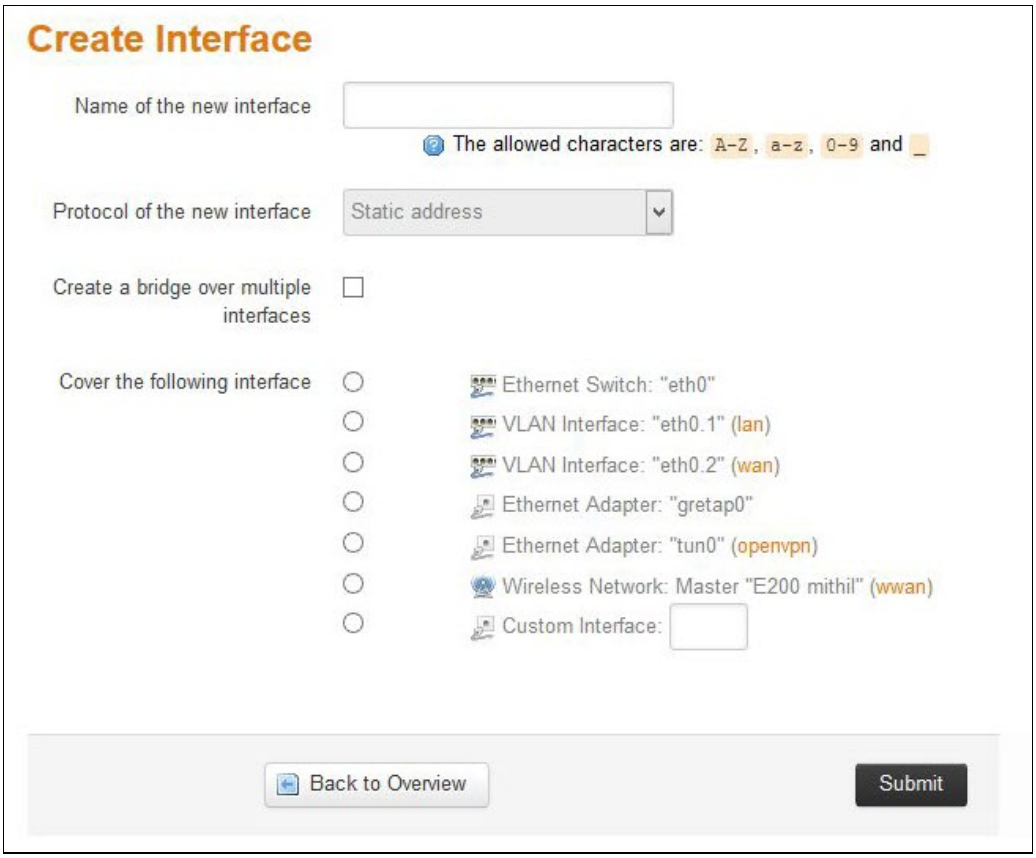
Parameters	Description
Status	Displays the following Interface details: • Uptime • MAC-Address • RX • TX • IPv4 • IPv6
Actions	Select the action to be taken for the Interface. • **Connect –** Connects the interface or reconnects the already connected interface • **Stop –** Stops the Interface • **Edit –** Click to edit the Interface.
Add VPN Interface	Click to add and configure the virtual interfaces. ***Note*** • ***Adding a Virtual Interface may require complex configuration modifications in load balancer settings. For more details, please visit Lantronix Technical Support.***
Global Network Options	
IPv6 ULA-Prefix	Displays the IPv6 ULA-Prefix
Network Watchdog	
Enable	Click to enable Network Watchdog. Watchdog keeps a check on the connectivity of all WAN interfaces. In absence of the connectivity resulting in Network down, the router resets itself. By default, the network watchdog is in disable mode.

Table 10.1-1: Interface Overview

A. Add VPN Interface

Note

- ***Adding a Virtual Interface may require complex configuration modifications in load balancer settings. For more details, please visit [Lantronix Technical Support](#).***



Screen 10-2: Configure VPN Interface

Parameters	Description
Name of the new interface	Enter the name of the new VPN Interface. The name must include only alpha numeric characters and special character underscore (_).
Protocol of the new interface	Select the protocol of the new Interface from the available options: • Static address • DHCP Client • Unmanaged • PPtP • PPPoE • UMTS/GPRS (Only for E205) • CELLULAR (Only for E206)
Create a bridge over multiple interface	Click to enable creating a bridge over multiple interfaces.
Cover the following interfaces	Select the interface to be configured.

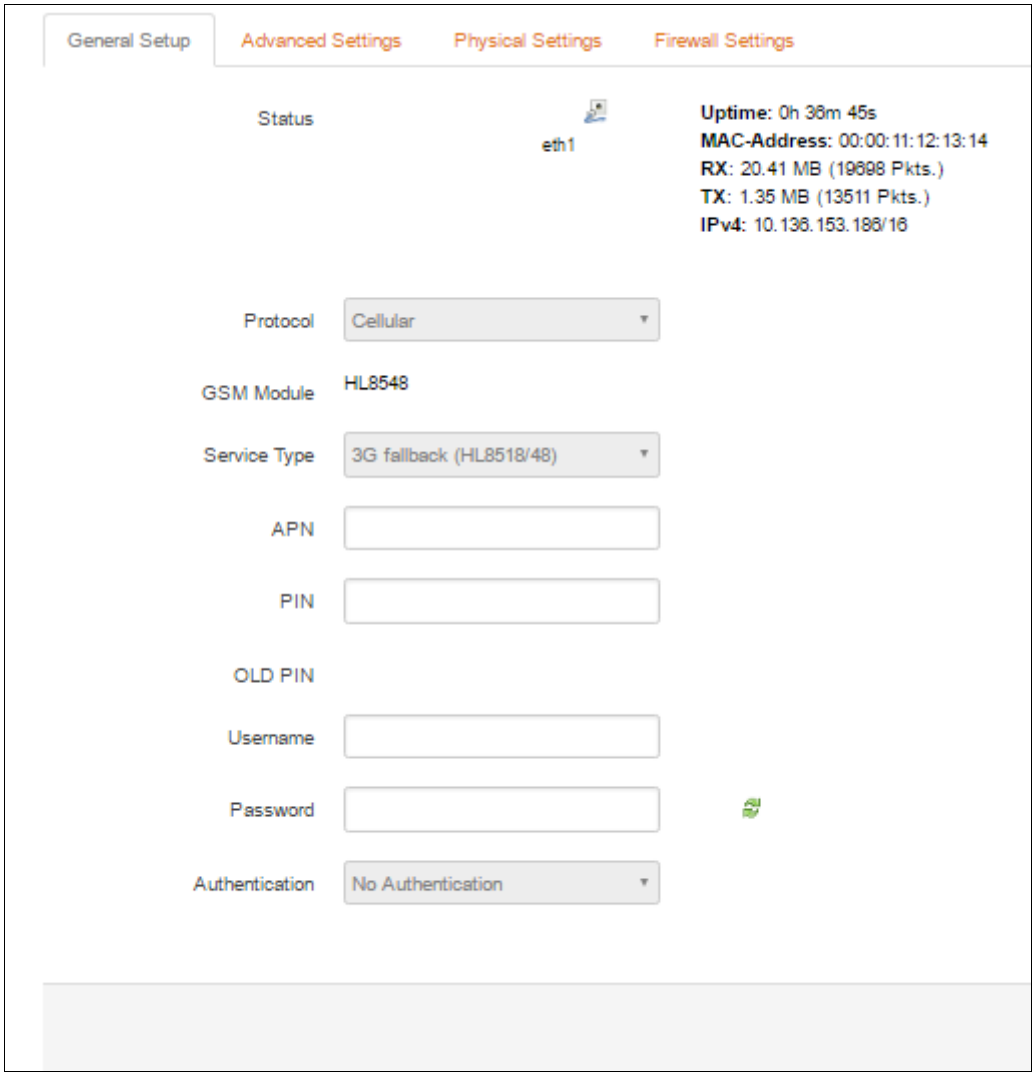
Parameters	Description
	Select more than one interface, if a parameter creating a bridge over multiple interfaces is enabled.
Back to Overview	Click to return to Interface Overview page.

Table 10.1-2: Configure VPN Interface

10.1.2 3G (Only for E205)

Network > Interface > 3G

A. General Setup



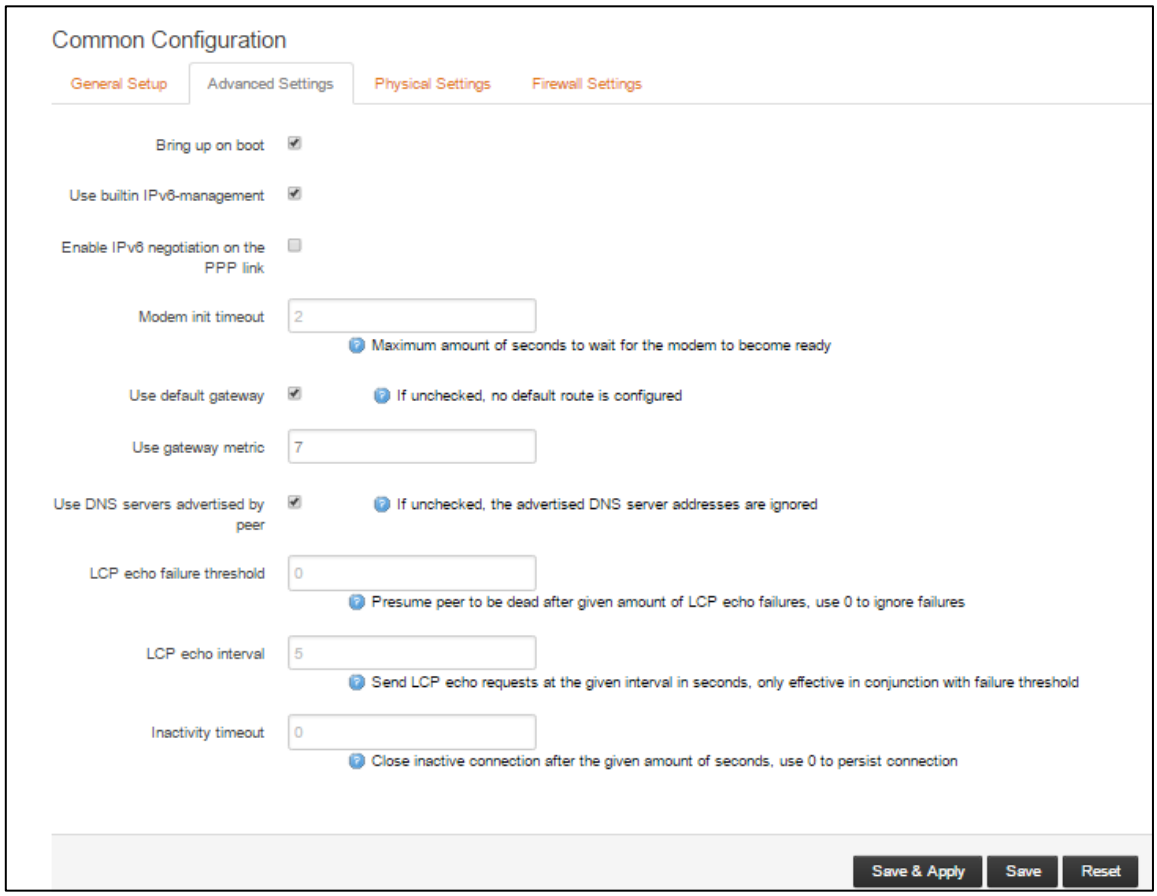
Screen 10-3: General Configurations for 3G Interface

Parameters	Description
Status	Enter the following Interface details: • Uptime • RX • TX • IPv4
Protocol	Select the protocol with respect to the router model number. ***Note*** • ***Be absolutely sure that to select protocol*** ***i. E205 - UMTS/GPRS*** ***ii. E206 - UMTS/GPRS or EVDO***

Parameters	Description
	• ***DO NOT select any other protocol.***
Service Type	Select the type of service from the available: • **2G only –** The router connects only to 2G network. • **3G only –** The router connects only to 3G/UMTS network. • **3G fallback –** The router connects to 3G network whenever available and fails over to 2G in absence of a 3G network. • **4G only –** The router will connect only to 4G network • **4G fallback –** The router connects to 4G network whenever available and fails over to 3G/2G in absence of a 4G network. •
APN	Enter the APN provided by your network operator.
PIN	Enter the SIM PIN if any.
Old Pin	Displays the previously set SIM PIN if any
PAP/CHAP Username	Enter the Username for the Data connection if any.
PAP/CHAP Password	Enter the Password for the Data connection if any. Click to reveal and verify the password. Click it again to hide the password and secure it.
Authentication	Select the authentication type followed by your network operator from PAP/CHAP/No Authentication

Table 10.1-3: General Configurations for 3G Interface

B. Advanced Settings



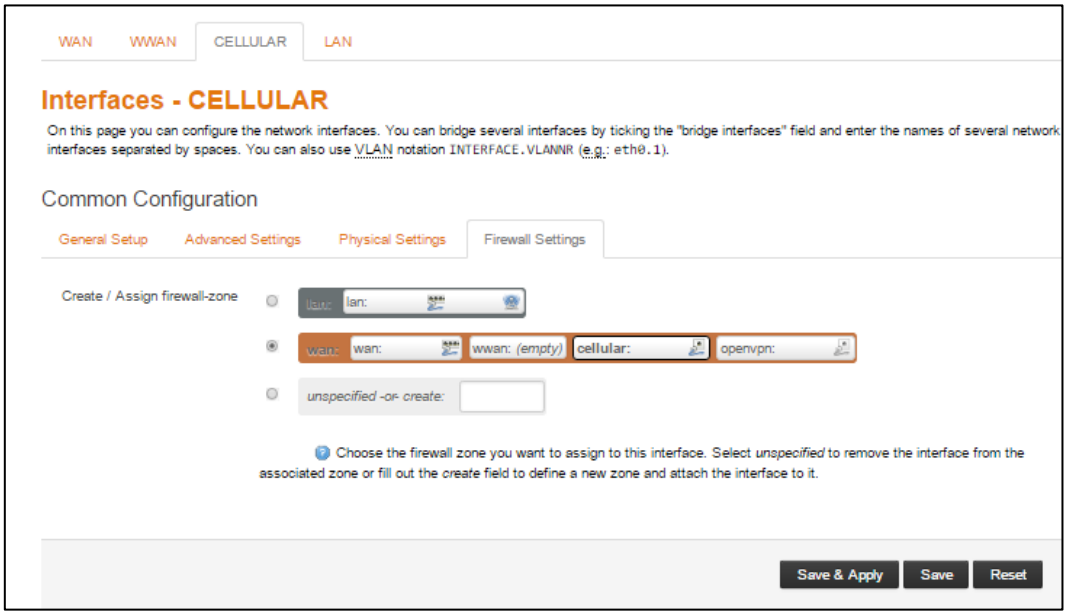
Screen 10-4: Advanced Configurations for Cellular Interface

Parameters	Description
Bring up on boot	Allows the Cellular interface to be live after every reboot. Bring up on boot for Cellular interface is checked by default.
Use builtin IPv6 –management	Allows to use the built in IPv6 management configuration.
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 7.
Use DNS server advertised by peer	Allows the router to advertise the DNS server address. Use DNS server advertised by peer for Cellular interface is checked by default.

Parameters	Description
LCP echo failure threshold	Presume peer to be dead after configured LCP echo failures. Use 0 to ignore failures
LCP echo interval	This is time the router should wait before sending an echo request to check whether the link is alive or not. The LCP echo interval by default is 20 seconds.
Inactivity timeout	The Router will wait for the LCP echo request response for the LCP Echo interval defined after every attempt. It declares LCP link as closed if it does not receive response after this defined period of attempts Use 0 seconds to persist the connection.

Table 10.1-4: Advanced Configurations for 3G Interface

C. Firewall Settings



Screen 10-5: Firewall Configuration for 3G

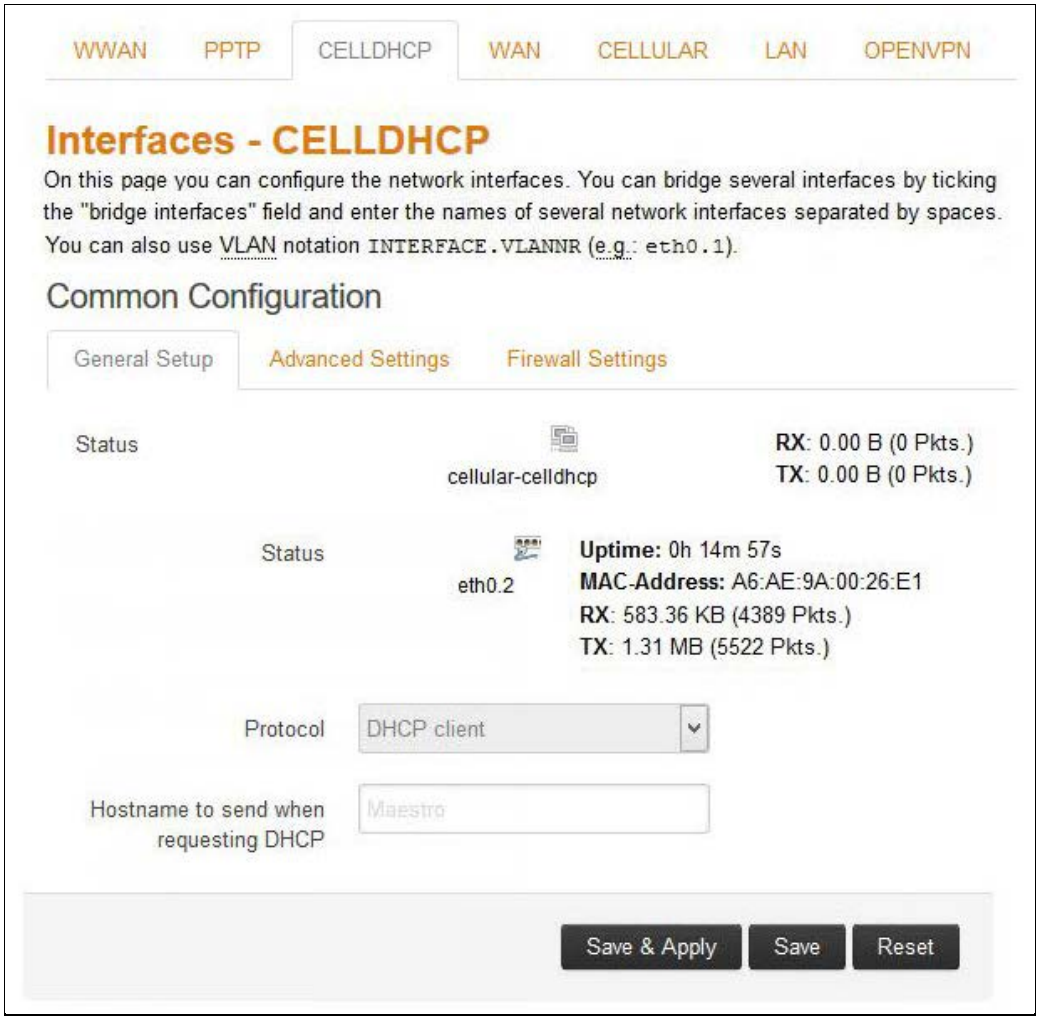
Parameters	Description
Create/Assign firewall -zone	Select the firewall zone to be assigned to the interface. Select **unspecified – or – create** to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box and click Save & Apply button. By default, there are two Firewall Zones, LAN and WAN. ***Note*** • ***Every interface must be assigned to a Firewall Zone.*** • ***Failure to assign an interface to a Firewall Zone will render the interface inactive.***

Table 10.1-5: Firewall Configuration for 3G

10.1.3 CELLDHCP (Only for E206)

Network > Interface > CELLDHCP

A. General Setup

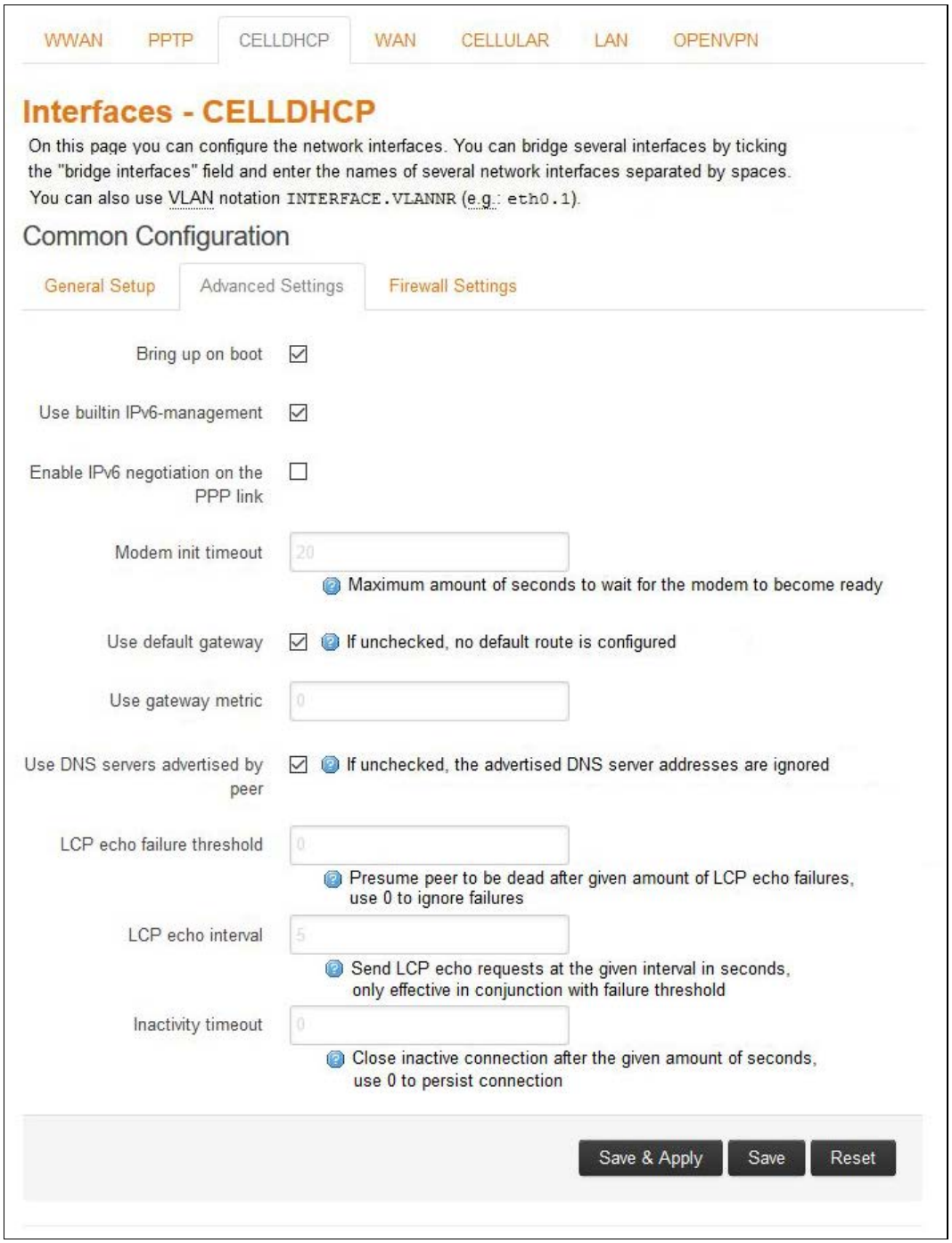


Screen 10-6: General Configuration of CELLDHCP Interface

Parameters	Description
Status	Enter the following Interface details • RX • TX
Protocol	Select the protocol with respect to the router model number. To update the CELLULAR protocol, select the protocol and click Switch Protocol button. The default protocol is CELLULAR.

Table 10.1-6: General Configuration of CELLDHCP Interface

B. Advanced Settings



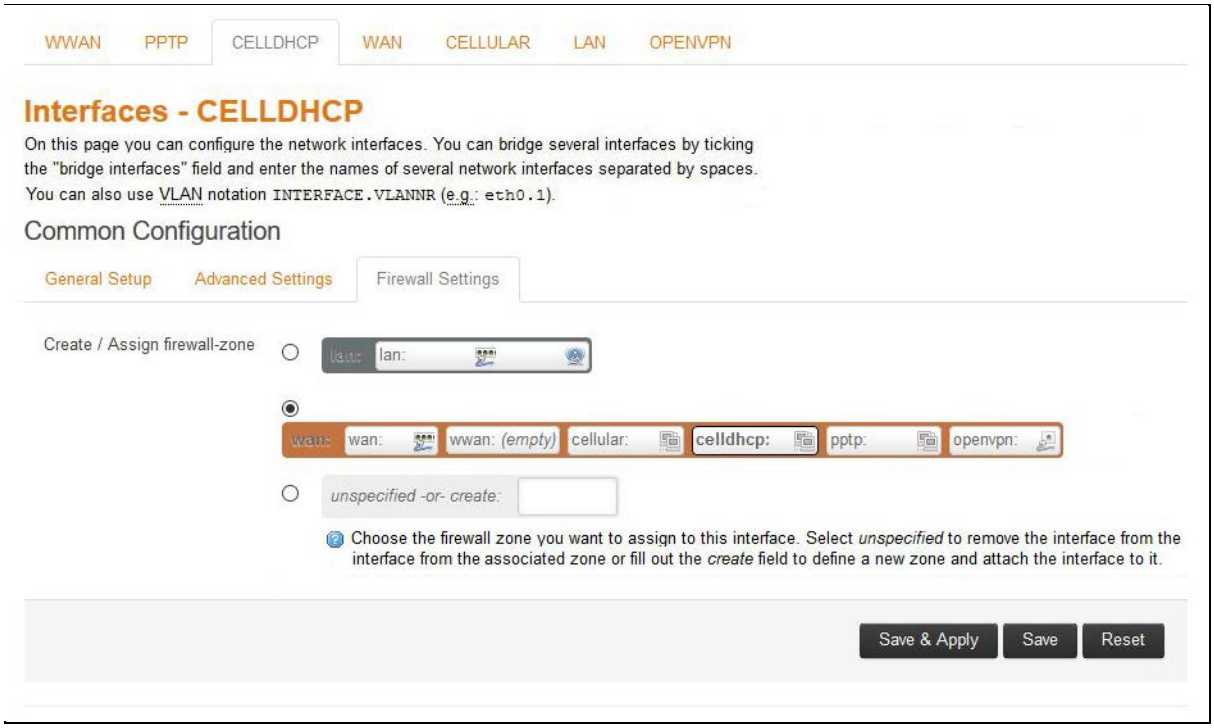
Screen 10-7: Advance Configuration of CELLDHCP Interface

Parameters	Description
Bring up on boot	Allows the 3G interface to be live after every reboot. Bring up on boot for 3G interface is checked by default.
Use builtin IPv6 -management	Allows to use the built in IPv6 management configuration.
Enable IPv6 negotiation on	Click to enable IPv6 negotiation on PPP link.

Parameters	Description
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 1.
Use DNS server advertised by peer	Allows the router to advertise the DNS server address. Use DNS server advertised by peer for 3G interface is checked by default.
LCP echo failure threshold	Presume peer to be dead after configured LCP echo failures. Use 0 to ignore failures.
LCP echo interval	This is time the router should wait before sending an echo request to check whether the link is alive or not. The LCP echo interval by default is 20 seconds.
Inactivity timeout	The Router will wait for the LCP echo request response for the LCP Echo interval defined after every attempt. It declares LCP link as closed if it does not receive response after this defined period of attempts Use 0 seconds to persist the connection.

Table 10.1-7: Advance Configuration of CELLDHCP Interface

C. Firewall Settings



Screen 10-8: Firewall Configuration of CELLDHCP Interface

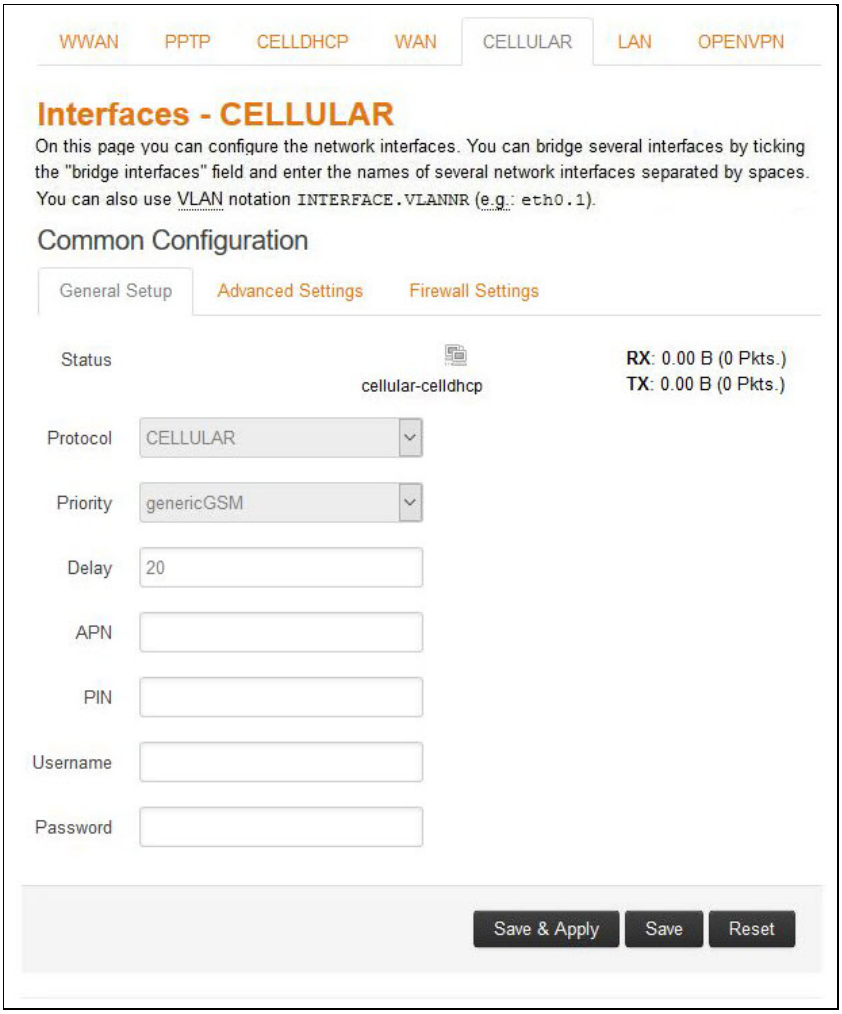
Parameters	Description
Create/Assign firewall –zone	Select the firewall zone to be assigned to the interface. Select unspecified – or – create to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box and click Save & Apply button.

Table 10.1-8: Firewall Configuration of CELLDHCP Interface

10.1.4 CELLULAR

Network > Interface > CELLULAR

A. General Setup

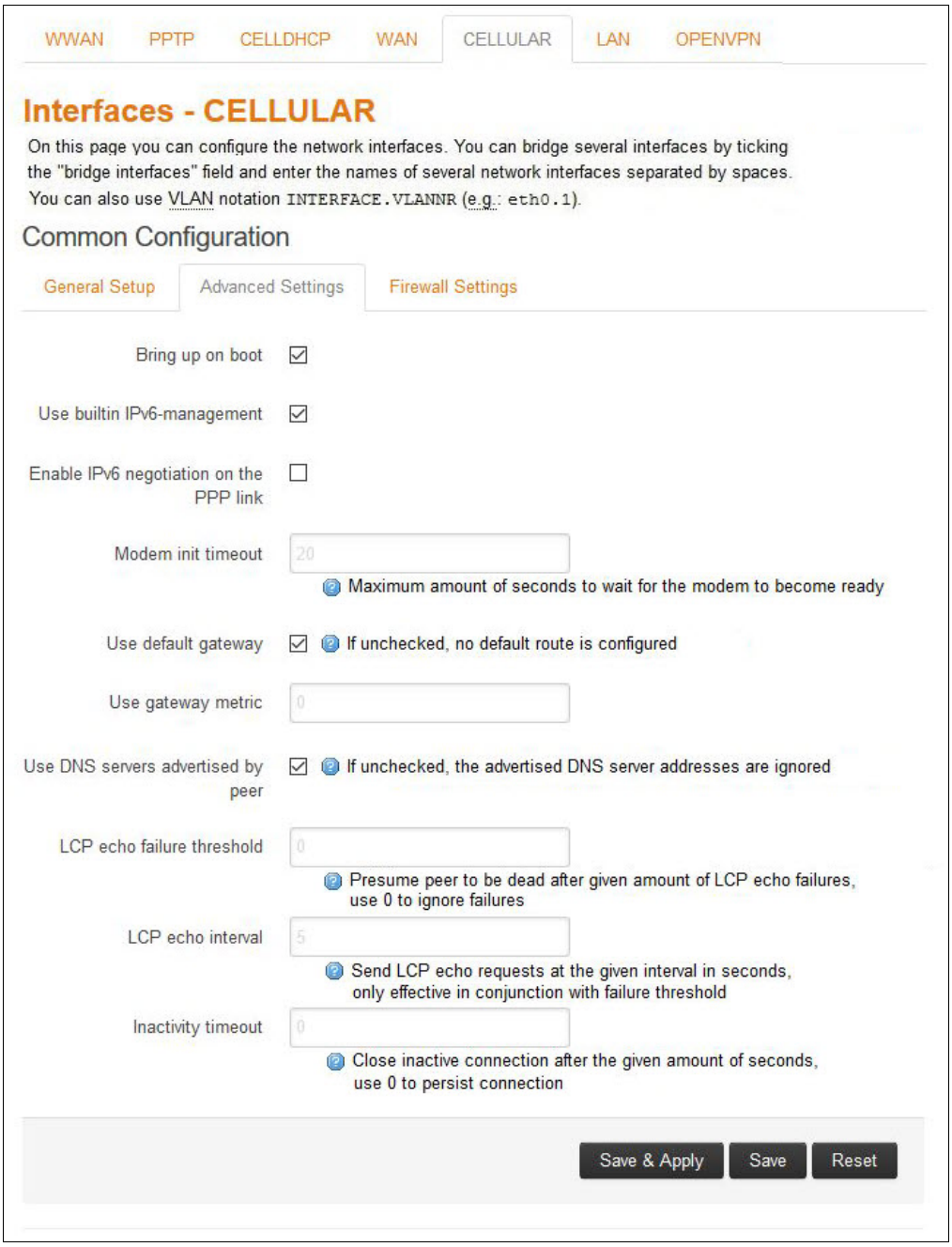


Screen 10-9: General Configuration of CELLULAR Interface

Parameters	Description
Status	Enter the following Interface details • RX • TX
Protocol	Select the protocol with respect to the router model number. To update the CELLULAR protocol, select the protocol and click Switch Protocol button. The default protocol is CELLULAR.

Table 10.1-9: General Configuration of CELLULAR Interface

B. Advanced Settings



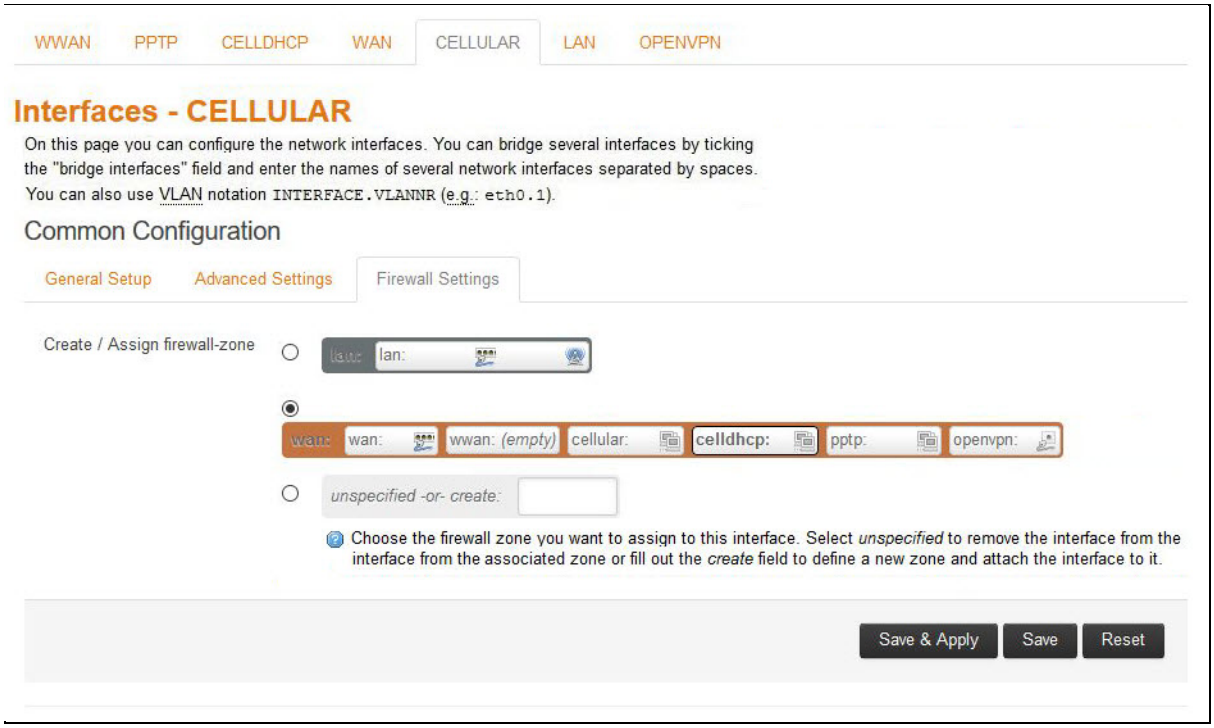
Screen 10-10: Advance Configuration of CELLULAR Interface

Parameters	Description
Bring up on boot	Allows the 3G interface to be live after every reboot. Bring up on boot for 3G interface is checked by default.
Use builtin IPv6 -management	Allows to use the built in IPv6 management configuration.
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

Parameters	Description
	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 server advertised by peer	Allows the router to advertise the DNS server address. Use DNS server advertised by peer for 3G interface is checked by default.
LCP echo failure threshold	Presume peer to be dead after configured LCP echo failures. Use 0 to ignore failures.
LCP echo interval	This is time the router should wait before sending an echo request to check whether the link is alive or not. The LCP echo interval by default is 20 seconds.
Inactivity timeout	The Router will wait for the LCP echo request response for the LCP Echo interval defined after every attempt. It declares LCP link as closed if it does not receive response after this defined period of attempts Use 0 seconds to persist the connection.

Table 10.1-10: Advance Configuration of CELLULAR Interface

C. Firewall Settings



Screen 10-11: Firewall Configuration of CELLULAR Interface

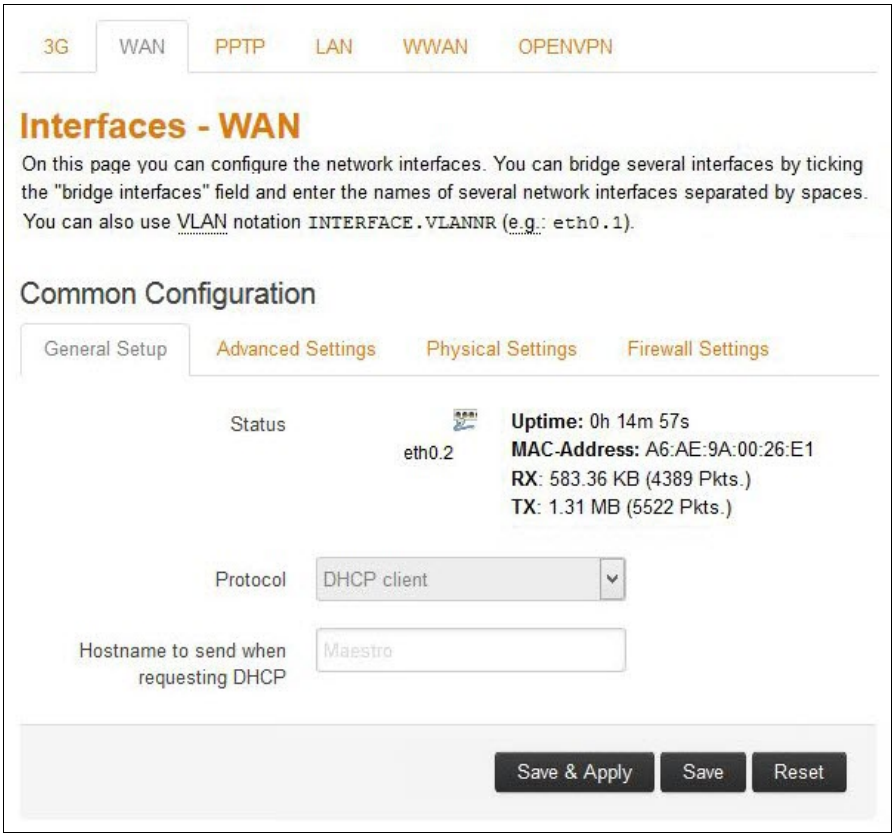
Parameters	Description
Create/Assign firewall -zone	Select the firewall zone to be assigned to the interface. Select unspecified – or – create to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box and click Save & Apply button.

Table 10.1-11: Firewall Configuration of CELLULAR Interface

10.1.5 WAN

Network > Interface > WAN

A. General Setup

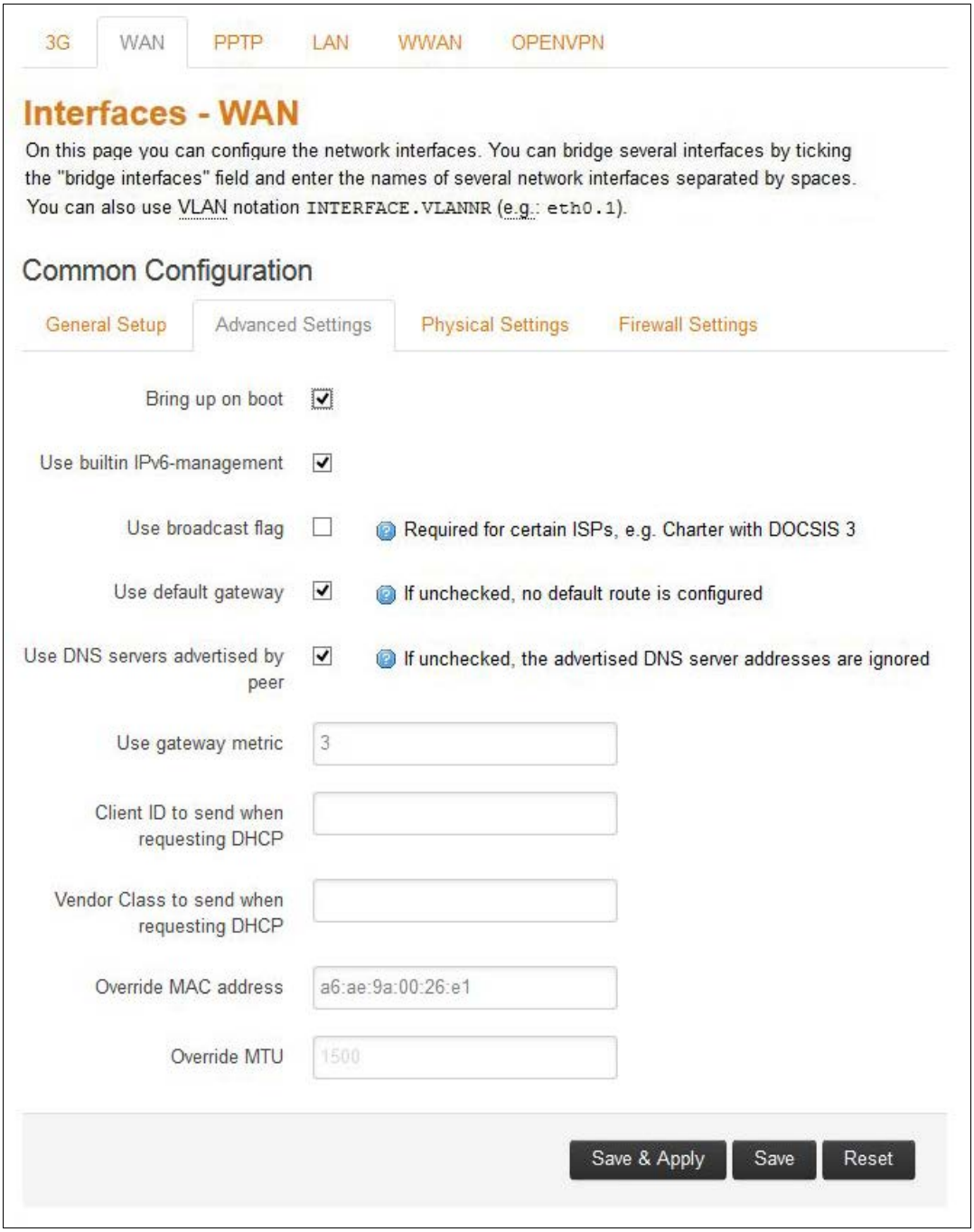


Screen 10-12: General Configurations for WAN Interface

Parameters	Description
Status	Enter the following Interface details: • Uptime • MAC–Address • RX • TX • IPv4
Protocol	Select the protocol with respect to the router model number. To update the WAN protocol, select the protocol and click Switch Protocol button. DHCP client is the default protocol.

Table 10.1-12: General Configurations for WAN Interface

B. Advanced Settings



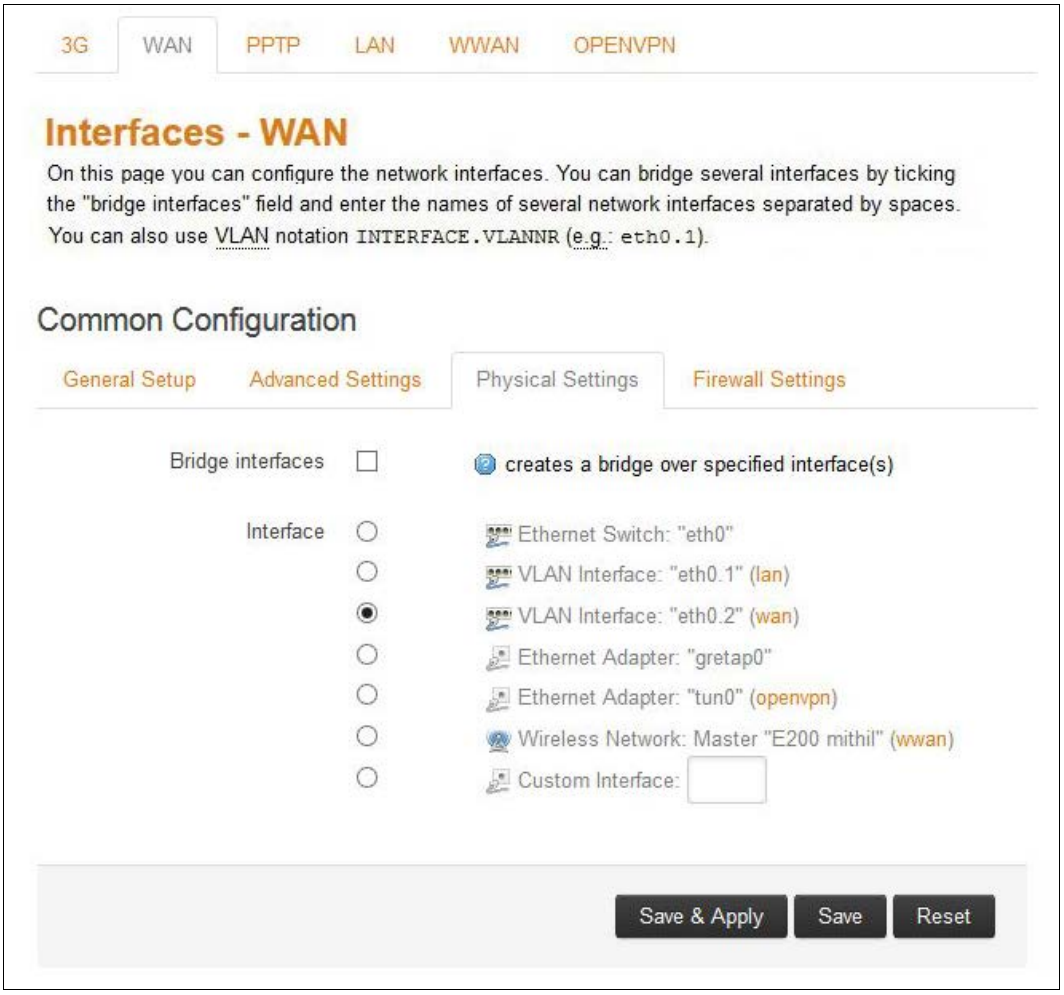
Screen 10-13: Advanced Configurations of WAN Interface

Parameters	Description
Bring up on boot	Allows the WAN interface to be live after every reboot. Bring up on boot for WAN interface is checked by default.
Use builtin IPv6 -management	Allows to use the built in IPv6 management configuration.
Use broadcast flag	Check to use the broadcast flag. This flag is generally used by the ISP's.

Parameters	Description
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. It ensures a separate routing entry for the respective interface in the main routing table. The default metric is 3.
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.
Overrride MTU	Click to override the default MTU value (Maximum Transmission Unit) The default MTU is 1500.

Table 10.1-13: Advanced Configurations of WAN Interface

C. Physical Settings

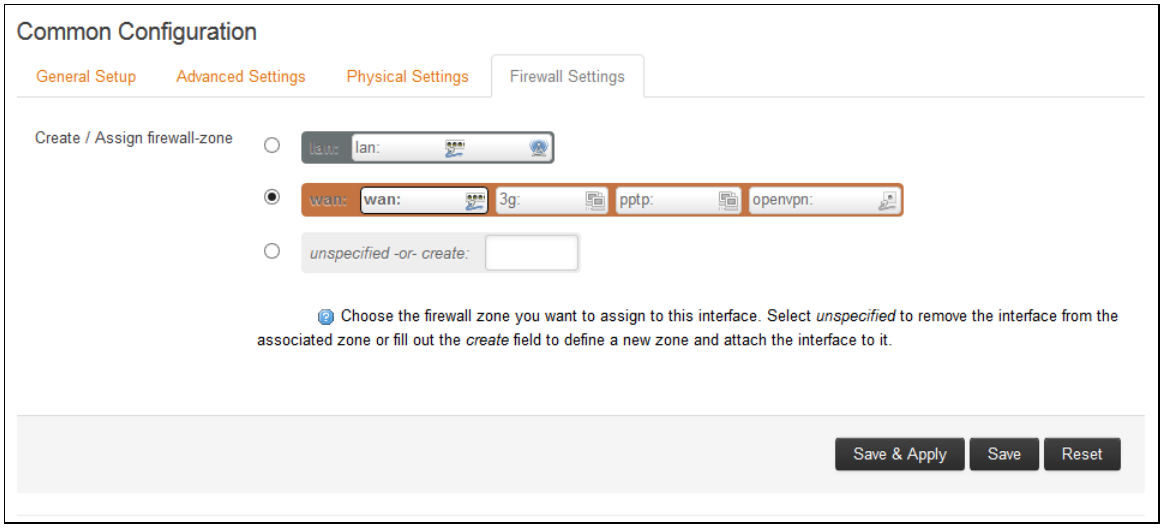


Screen 10-14: Physical Configurations for WAN interface

Parameters	Description
Bridge Interfaces	Click to enable creating a bridge over multiple interfaces. **Enable STP** – Check to enable the Spanning Tree Protocol over the bridge.
Interface	Select the interface to be configured. Select more than one interface, if parameter creating a bridge over multiple interfaces is enabled.

Table 10.1-14: Physical Configurations for WAN interface

D. Firewall Settings



Screen 10-15: Firewall Configurations for WAN Interface

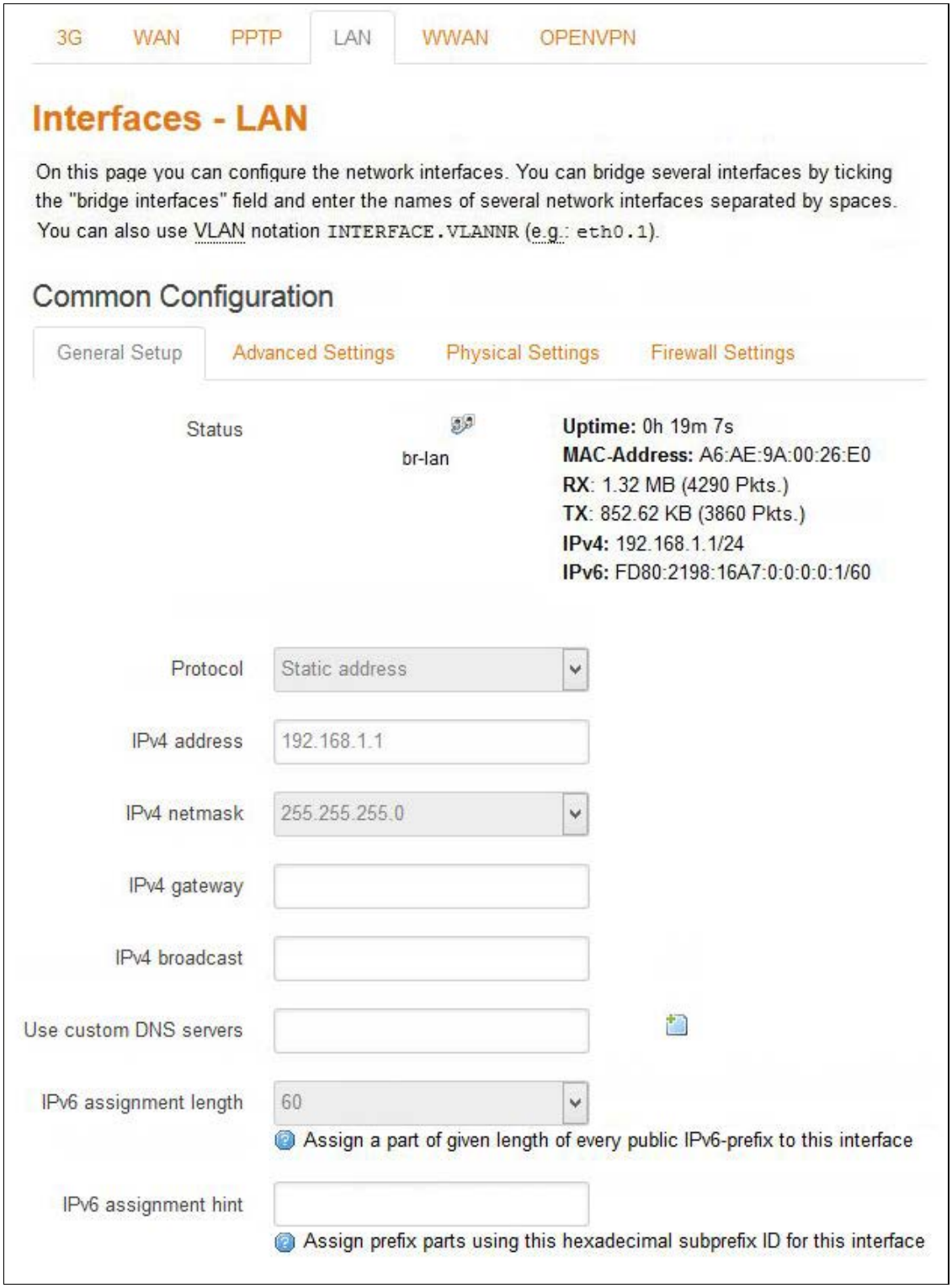
Parameters	Description
Create/Assign firewall -zone	Select the firewall zone to be assigned to the interface. Select **unspecified – or – create** to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box and click Save & Apply button.

Table 10.1-15: Firewall Configurations for WAN Interface

10.1.6 LAN

Network > Interface > LAN

A. General Setup

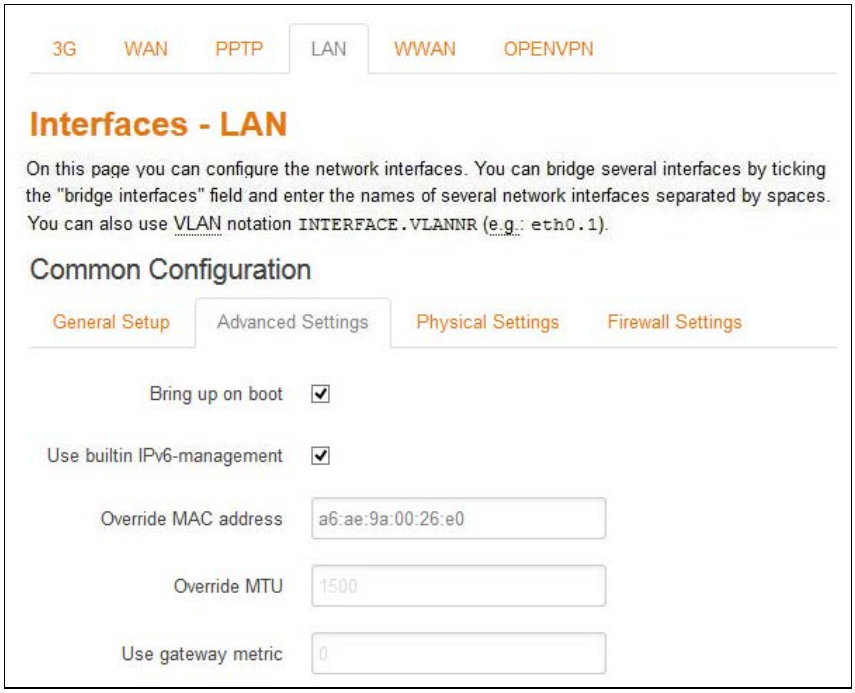


Screen 10-16: General Configurations of LAN Interface

Parameters	Description
Status	Displays the following Interface details: • Uptime • MAC–Address • RX • TX • IPv4 • IPv6
Protocol	Select the protocol with respect to the router model number. To update the WAN protocol, select the protocol and click Switch Protocol button. Static Address is the default protocol.

Table 10.1-16: General Configurations of LAN Interface

B. Advanced Settings

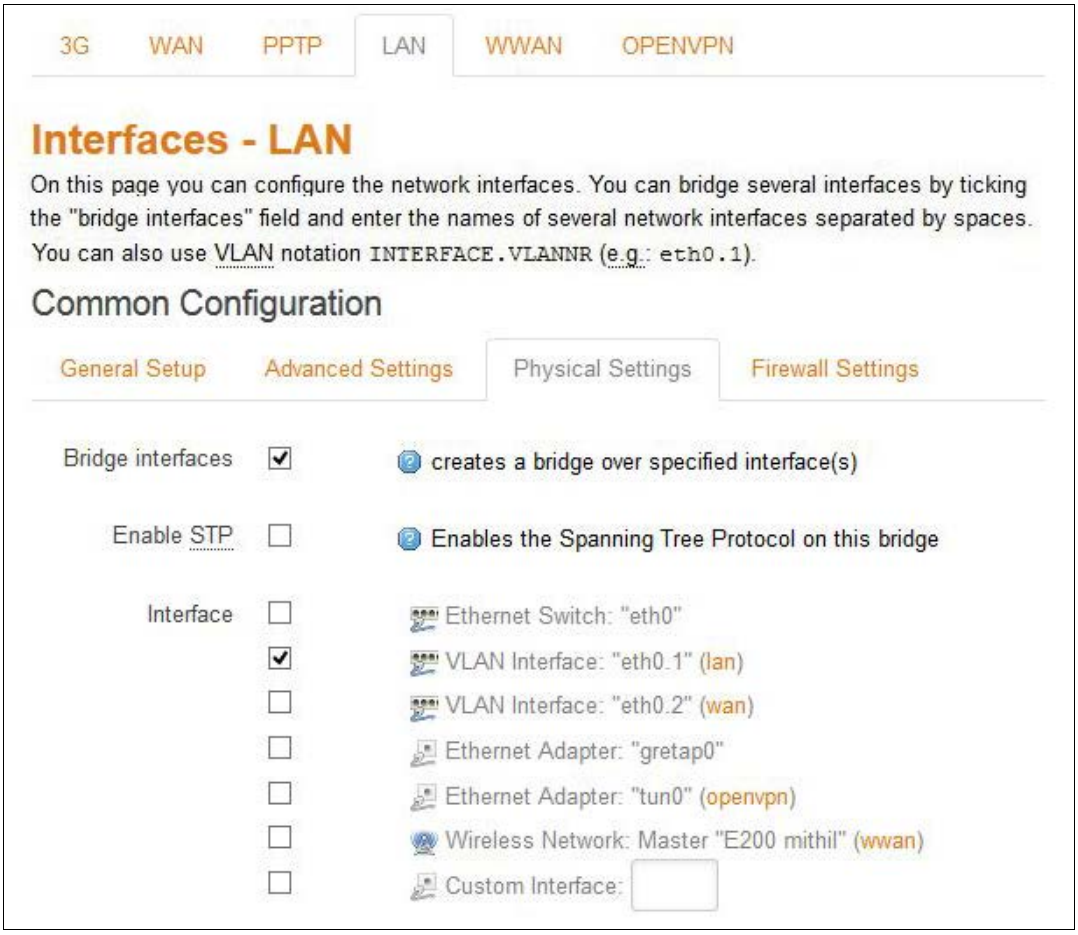


Screen 10-17: Advanced Settings for LAN Interface

Parameters	Description
Bring up on boot	Allows the WAN interface to be live after every reboot. Bring up on boot for WAN interface is checked by default.
Use builtin IPv6 -management	Allows to use the built in IPv6 management configuration.
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.
Overrride MTU	Click to override the default MTU value (Maximum Transmission Unit) The default MTU is 1500.
Use gateway metric	Enter the gateway metric. The default metric is 0.

Table 10.1-17: Advanced Settings for LAN Interface

C. Physical Settings

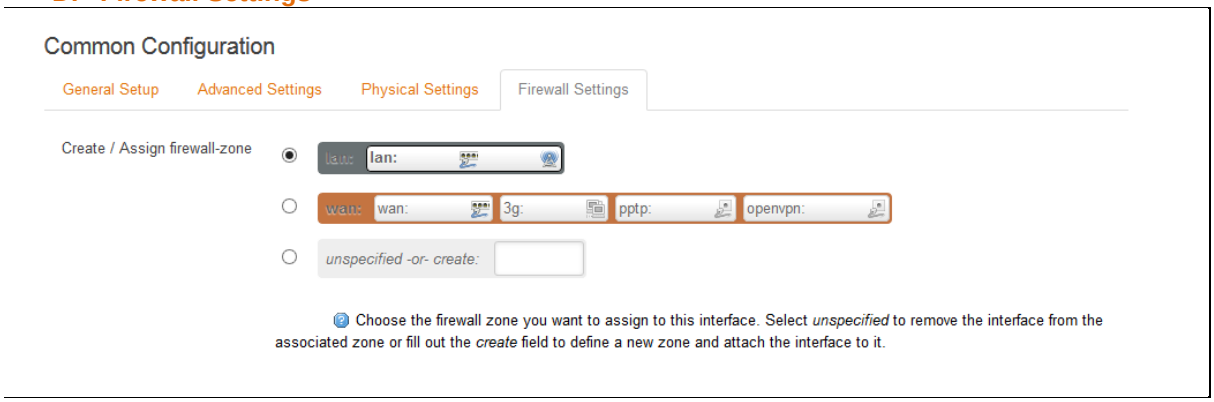


Screen 10-18: Physical Configurations of LAN Interface

Parameters	Description
Bridge Interfaces	Click to enable creating a bridge over multiple interfaces. **Enable STP** – Check to enable the Spanning Tree Protocol over the bridge.
Interface	Select the interface to be configured. Select more than one interface if parameter creating a bridge over multiple interfaces is enabled.

Table 10.1-18: Physical Configurations of LAN Interface

D. Firewall Settings



Screen 10-19: Firewall Configurations of LAN Interface

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.

Table 10.1-19: Firewall Configurations of LAN Interface

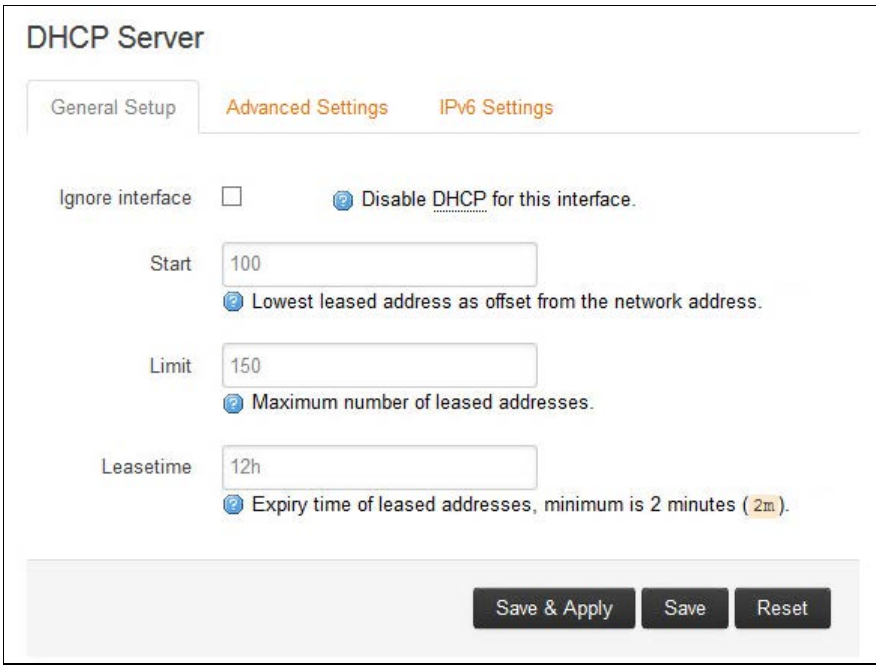
E. DHCP Server

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.

a. General Setup

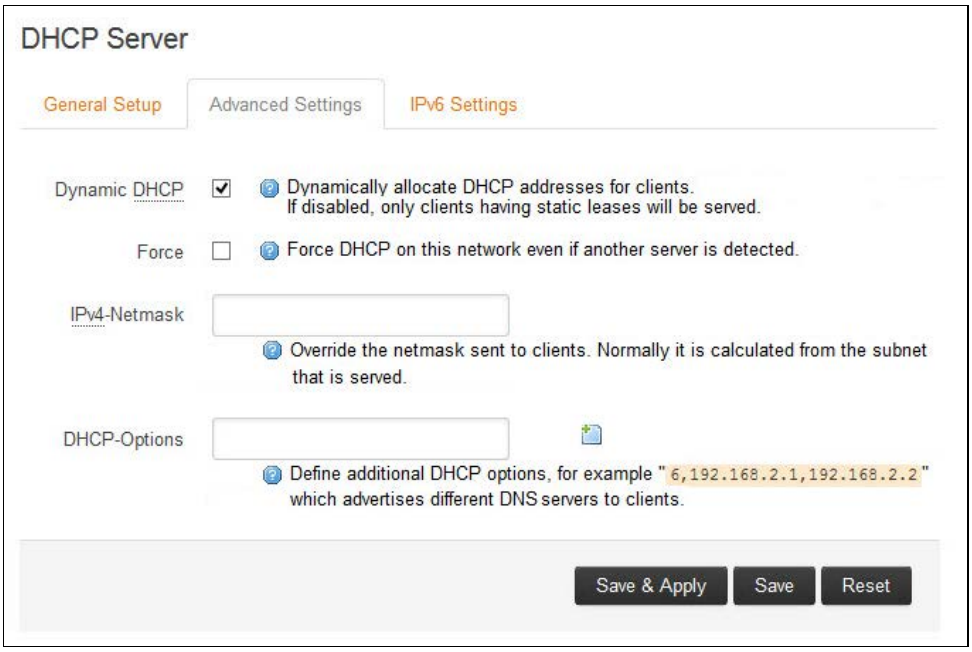


Screen 10-20: General Configurations for DHCP Server

Parameters	Description
Ignore Interface	Check to disable the DHCP interface. ***Note*** • ***If DHCP is disabled for this interface, all the LAN devices connected to the router should have a static LAN IP configured.***
Start	Lowest leased address as offset from the network address. **Example –** if your LAN IP address is 192.168.1.1 and the parameter Start is configured as 100, then the starting IP Address of the leased IP Address range is 192.168.1.100
Limit	Maximum number of leased addresses that can be configured. Example – if your LAN IP Address is 192.168.1.1, the parameter Start is configured as 100, and parameter Limit is configured as 150, then a total of 150 devices are configured. Thus the leased IP Address range is 192.168.1.100 to 192.168.1.249.
Leasetime	Remaining time until which the device can use the DHCP server leased IP Address. ***Note*** • ***IP address allocated by the router will disappear from the Wi-Fi / Overview / Associates stations list only after individual lease time for each IP expires.***

Table 10.1-20: General Configurations for DHCP Server

b. Advanced Settings

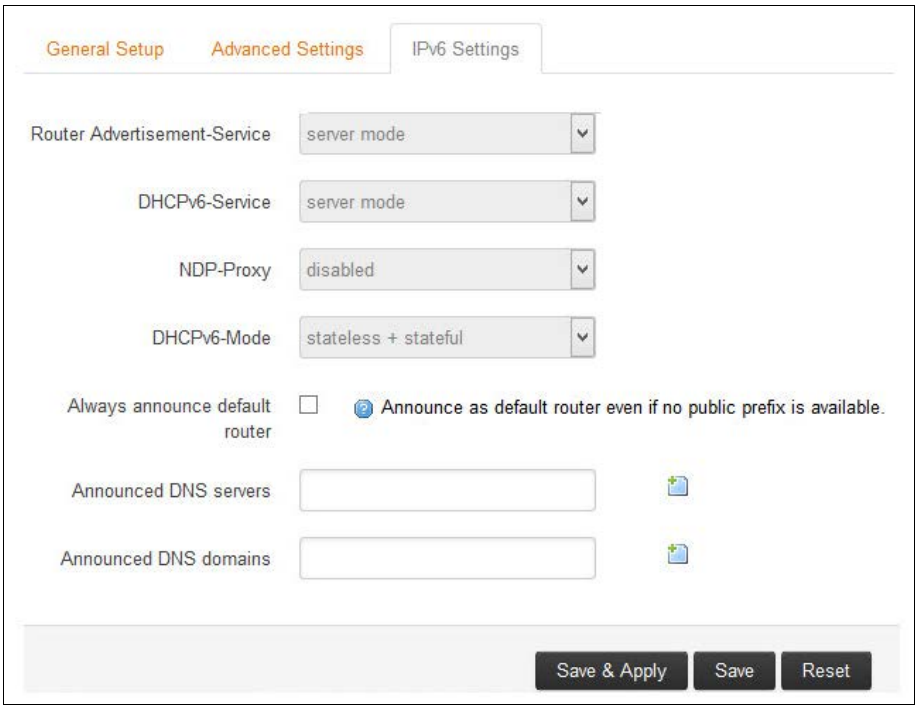


Screen 10-21: Advance Configurations for DHCP Server

Parameters	Description
Dynamic DHCP	Check to allocate DHCP IP addresses dynamically to the clients. When unchecked, service will be provided only to the clients having the static IP Address.
Force	Check to override the current configured Server and use DHCP server.
IPv4-Netmask	Enter the IPv4 netmask. This netmask will override the netmask used by the clients. In normal scenario netmask is calculated from the subnet.
DHCP-Options	Define additional DHCP options, **Example –** "6,192.168.2.1, 192.168.2.2" which advertises different DNS servers to clients.

Table 10.1-21: Advance Configurations for DHCP Server

c. IPv6 Settings



Screen 10-22: IPv6 Configuration of DHCP Server

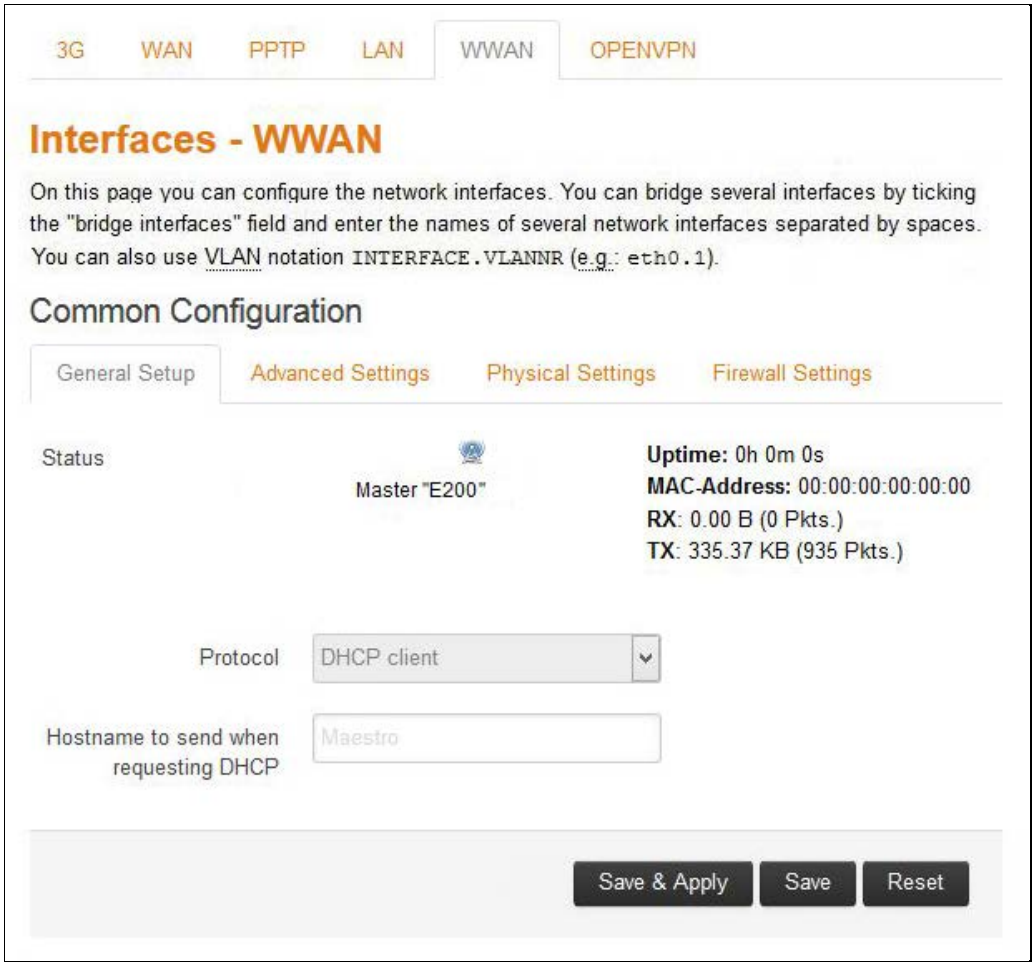
Parameters	Description
Router Advertisement-Service	Select the Router Advertisement-Service mode; disabled, server mode, relay mode, hybrid mode.
DHCPv6-Service	Select the DHCPv6-Service mode; disabled, server mode, relay mode, hybrid mode.
NDP-Proxy	Select the NDP mode; disabled, server mode, relay mode, hybrid mode.
DHCPv6-Mode	Select the DHCPv6-Service mode: • Stateless • Stateful • Stateless + Stateful • Stateful only
Always announce default router	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 10.1-22: IPv6 Configuration of DHCP Server

10.1.7 WWAN

Network > Interface > WWAN

A. General Setup

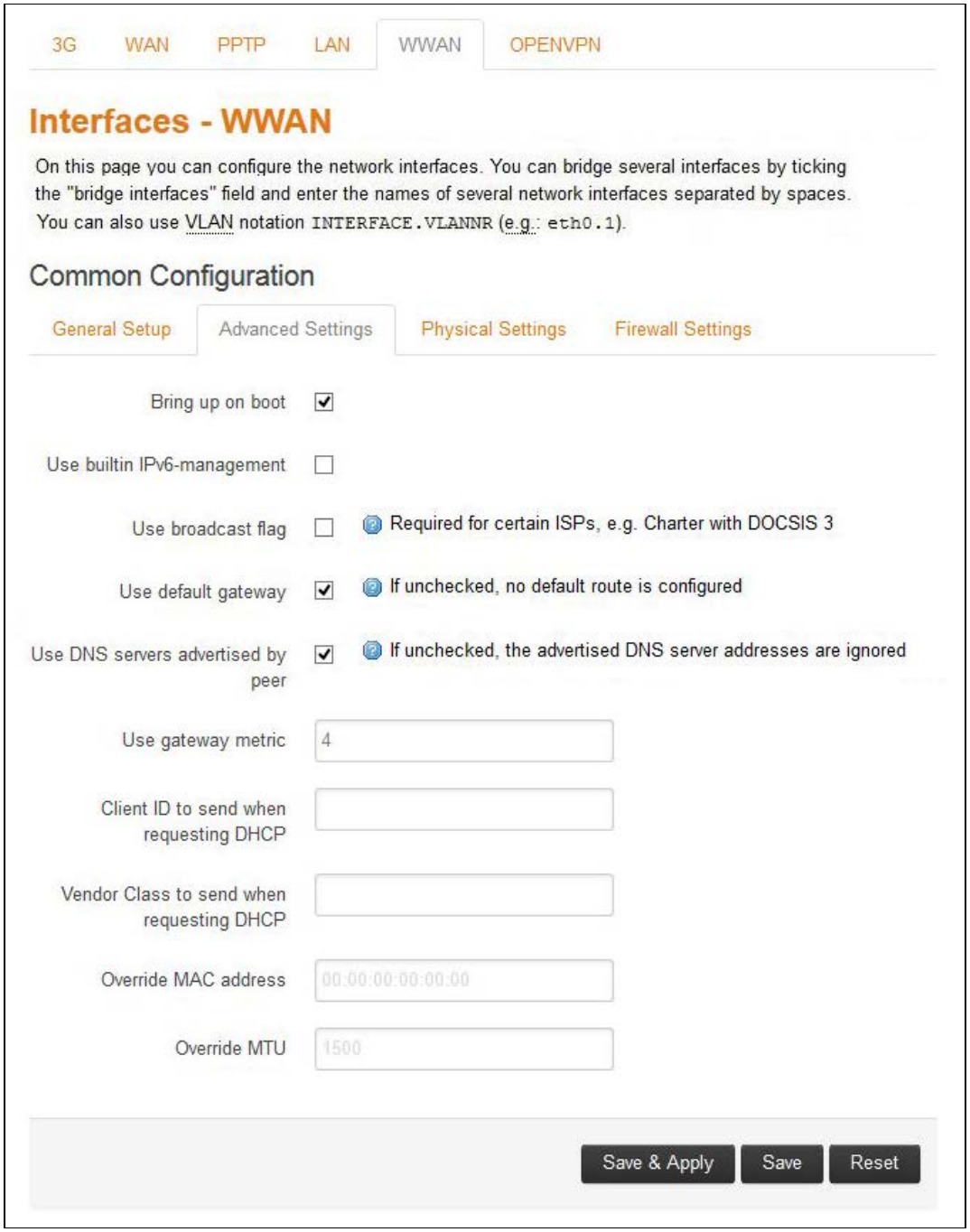


Screen 10-23: General Configuration for WWAN Interface

Parameters	Description
Status	Enter the following Interface details: • Uptime • MAC–Address • RX • TX • IPv4
Protocol	Select the protocol with respect to the router model number. To update the WAN protocol, select the protocol and click Switch Protocol button. DHCP client is the default protocol. ***Note*** • ***We recommend to select either DHCP or Static Address, PPPoE or PPPoATM***

Table 10.1-23: General Configuration for WWAN Interface

B. Advanced Settings



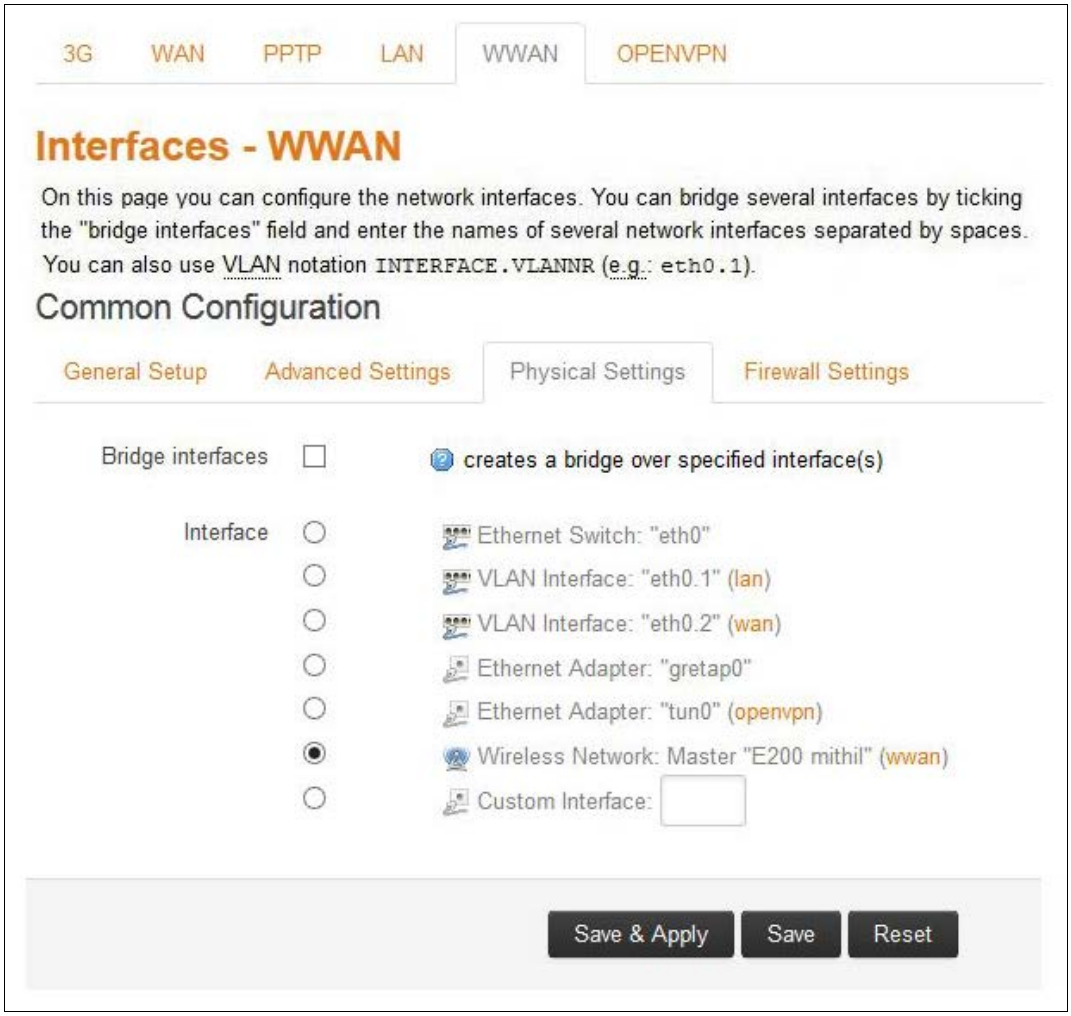
Screen 10-24: Advanced Configuration for WWAN Interface

Parameters	Description
Bring up on boot	Allows the WAN interface to be live after every reboot. Bring up on boot for WAN interface is checked by default.
Use builtin IPv6 -management	Allows to use the built in IPv6 management configuration.
Use broadcast flag	Check to use the broadcast flag. This flag is generally used by the ISP's.

Parameters	Description
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.
Overrride MTU	Click to override the default MTU value (Maximum Transmission Unit) The default MTU is 1500.

Table 10.1-24: Advanced Configuration for WWAN Interface

C. Physical Settings

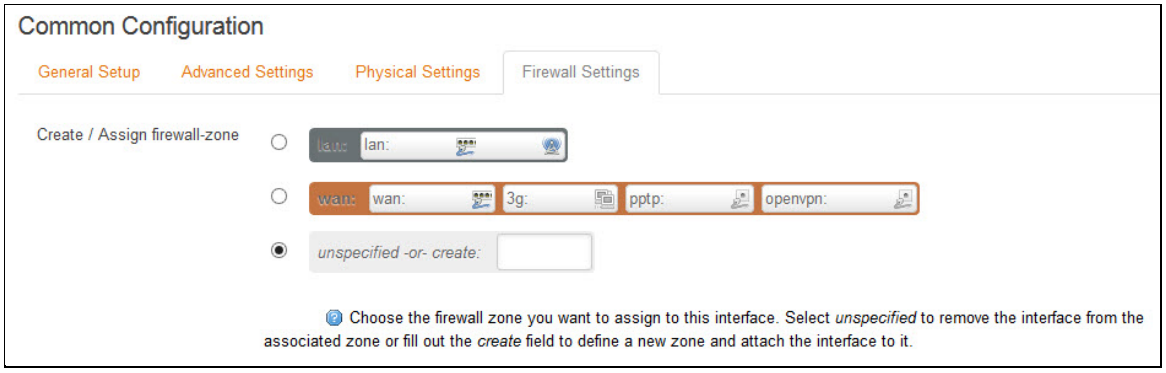


Screen 10-25: Physical Configuration for WWAN Interface

Parameters	Description
Bridge Interfaces	Click to enable creating a bridge over multiple interfaces. **Enable STP** – Check to enable the Spanning Tree Protocol over the bridge.
Interface	Select the interface to be configured. Select more than one interface if parameter creating a bridge over multiple interfaces is enabled.

Table 10.1-25: Physical Configuration for WWAN Interface

D. Firewall Settings



Screen 10-26: Firewall Configuration for WWAN Interface

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.

Table 10.1-26: Firewall Configuration for WWAN Interface

10.2 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.

a. How it works

Load balancing is determined by the load metric i.e. weight. Each link is assigned a relative weight and 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 link.

Administrator can set 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)

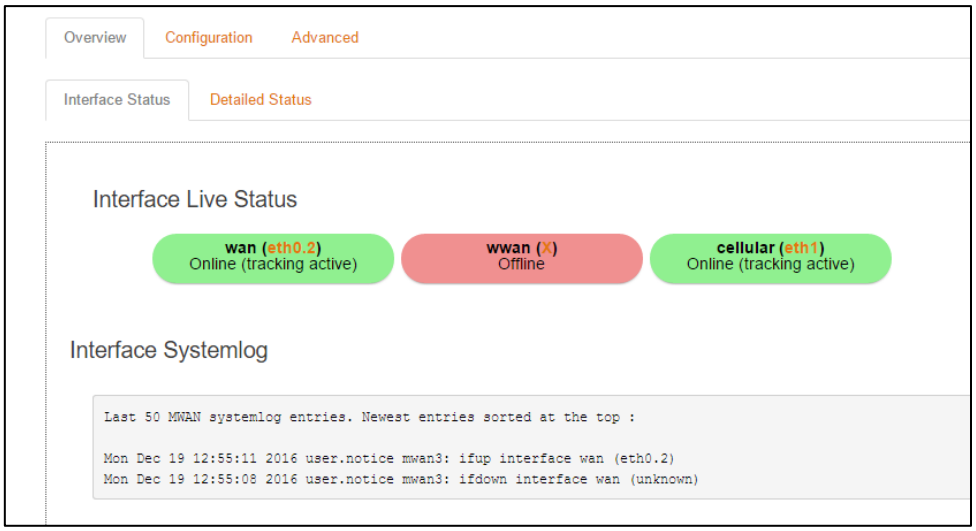
Note

- ***The default configuration of load balancer is in Failover Mode with the highest priority given to WAN, followed by WWAN and followed by Cellular.***

10.2.1 Overview

Network > Load Balancing > Overview

A. Interface Status

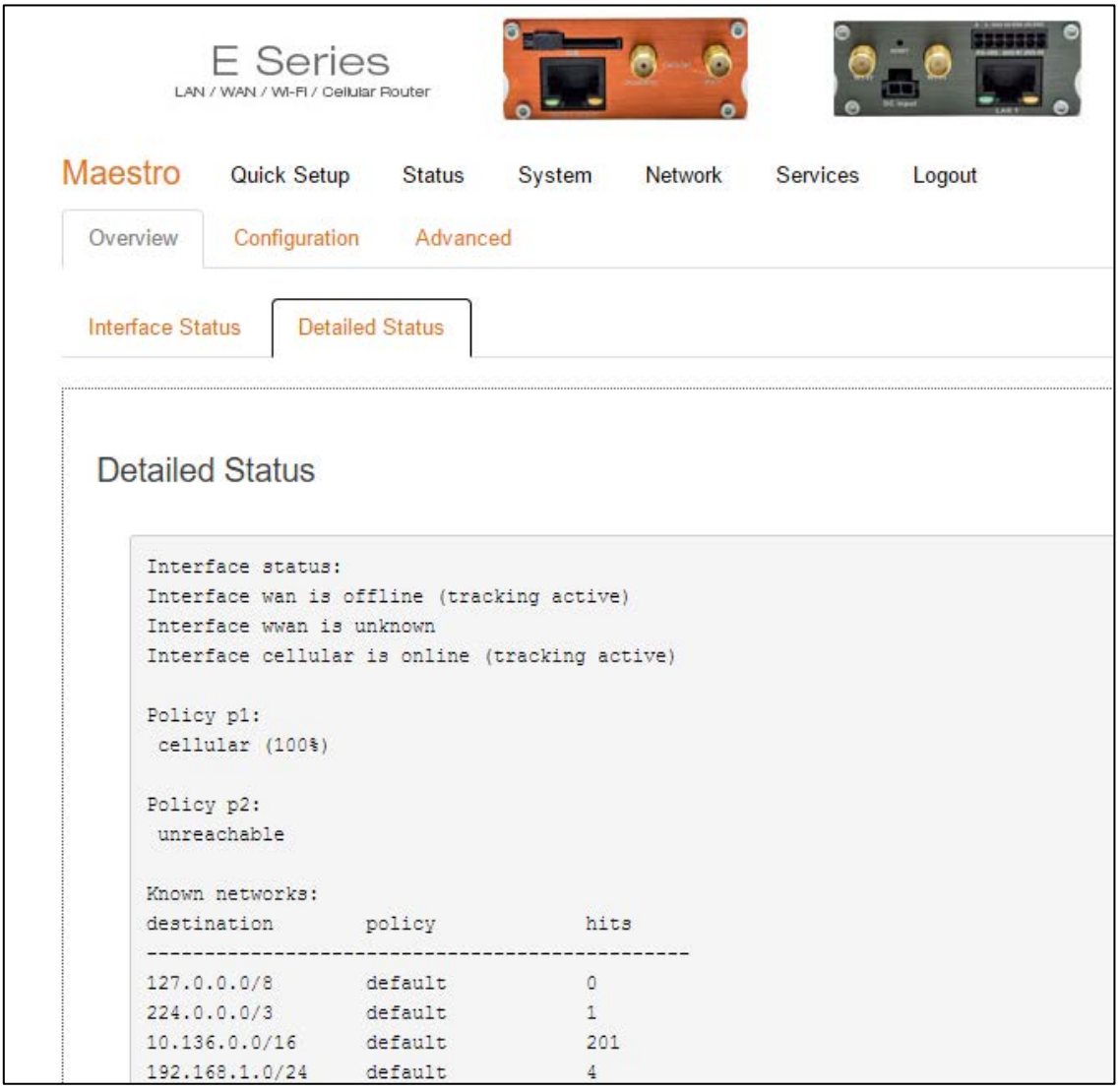


Screen 10-27: Live Status Overview of MWAN Interface

Parameters	Description
MWAN Interface Live Status	Displays the interface status: Online, Offline If more than two Interfaces are online and have same metric value, traffic will be balance amongst the Interfaces.
MWAN Interface Systemlog	Displays the event logs for interface status: Active, Inactive.

Table 10.2-1: Live Status Overview of MWAN Interface

B. Detailed Status



Screen 10-28: Detailed Status Overview of MWAN Interface

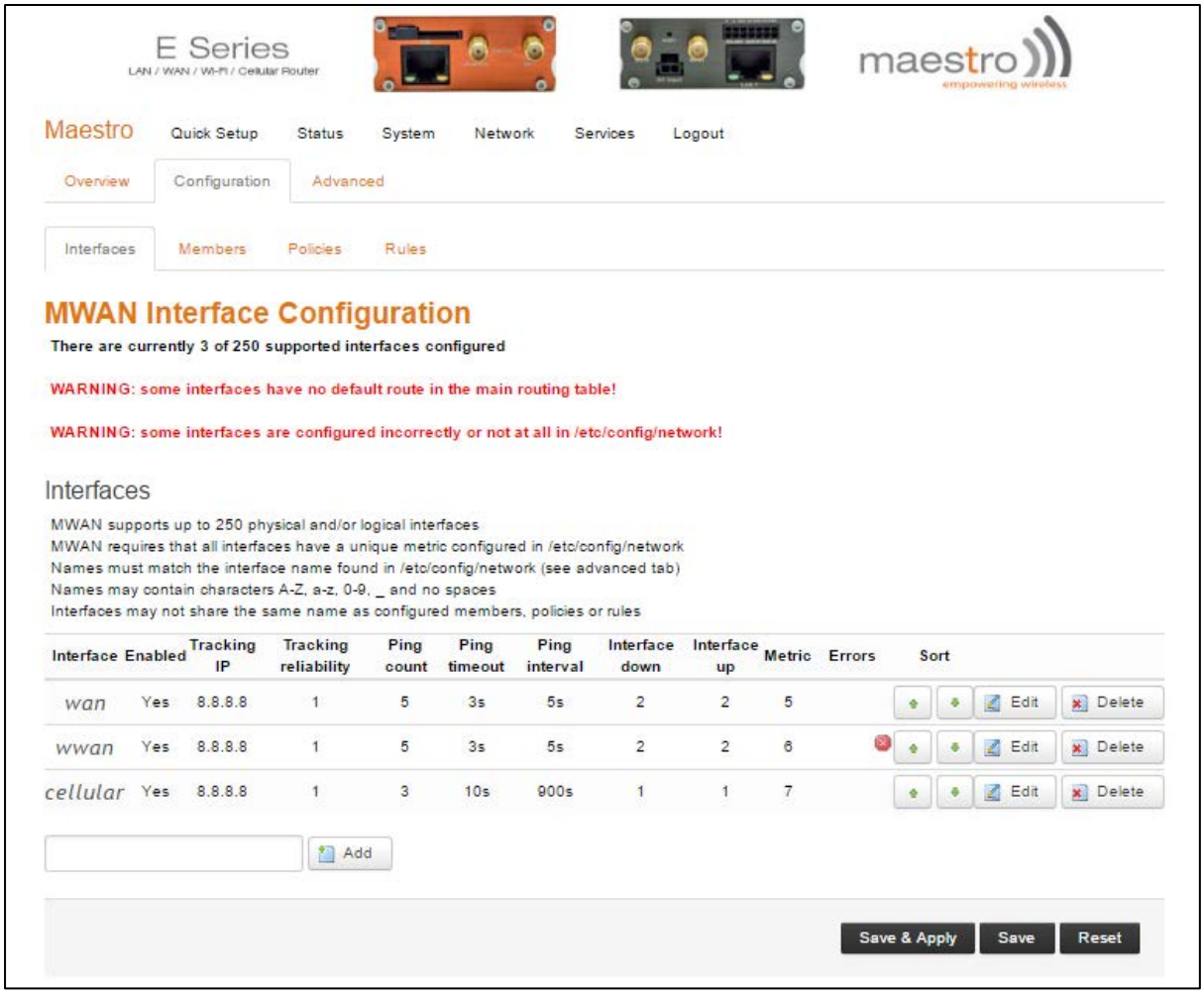
Parameters	Description
MWAN Status	Displays the detailed status for interface. These logs include the following information for all the available interfaces: • **Interface Live Status** – Online, Offline • **Each Policy Information –** Policy Name and interfaces configured for the policy • **Known Networks –** Destination IP Address, Policy applied, hits on the network • **Active Rules –** Rule configuration details that is Source IP Address, Destination IP Address, Protocols allowed, Source Port number, Destination Port number applied to the respective Policy, hits.

Table 10.2-2: Detailed Status Overview of MWAN Interface

10.2.2 Configuration

Network > Load Balancing > Configuration

A. Interface



Screen 10-29: Configuration details of MWAN Interface

Parameters	Description
Interface	Name of the available Interface.
Enabled	Displays the Interface status is enabled or disabled.
Tracking IP	Displays IP Address to which the ping request is sent from the 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 count	Displays the number of ping packets that will be sent.
Ping timeout	Time to wait for a response to ping request sent before declaring the ping failure. The wait time is in seconds.
Ping interval	Specifies the time in seconds between sending two successive ping packets.
Interface down	The number of consecutive failed attempts after which the interface

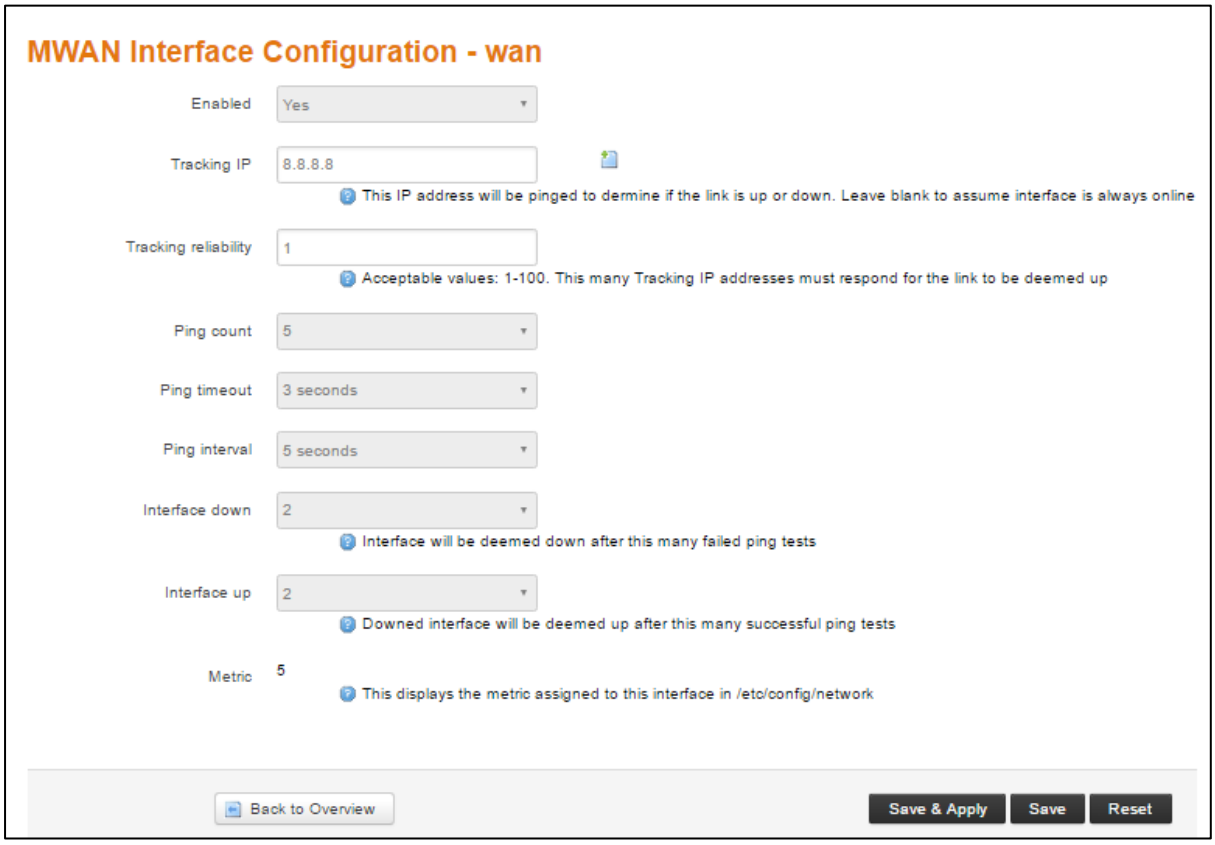
Parameters	Description
	is declared offline
Interface up	The number of consecutive successful ping after which the interface is declared online
Metric	Metric assigned to the Interface from the Advanced Interface Configuration Settings page.
Error	Displays if an error has occurred during the Interface configuration. Error messages are displayed a warnings.
Sort	Click to sort the interface. The same interface order will be reflected in the Overview page.

Table 10.2-3: Configuration details of MWAN Interface

Note

- ***Configuring a large number of Tracking IP Adresses, 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.***

a. Edit



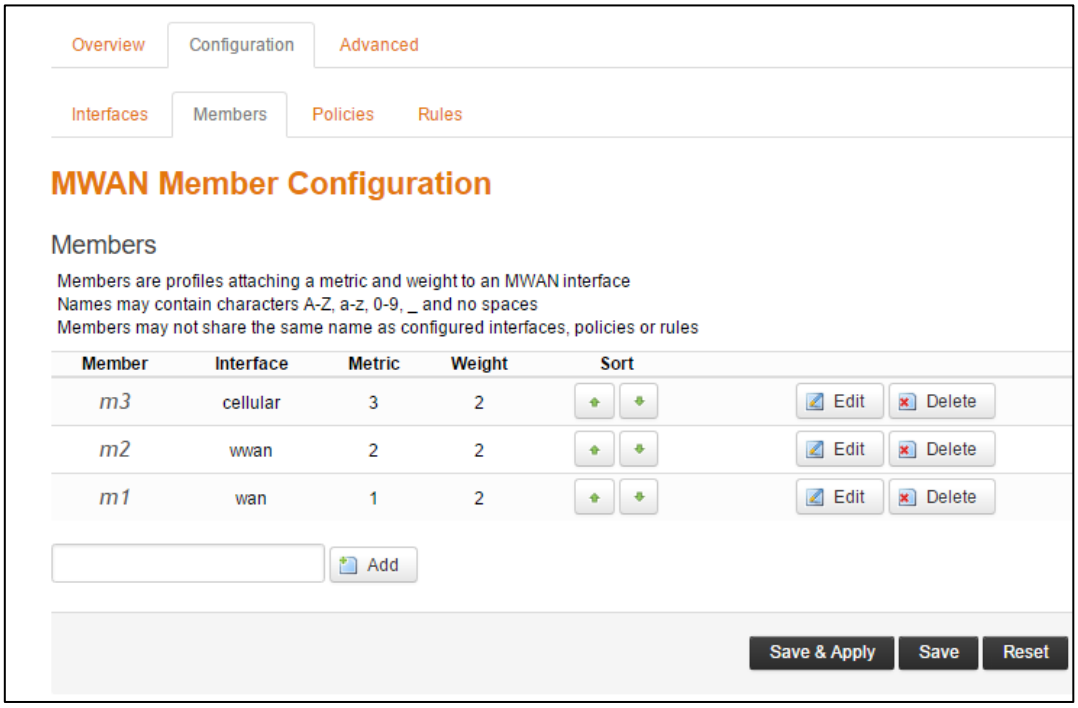
Screen 10-30: Modify MWAN Interface

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.
Tracking IP	IP Address to which the ping request are sent from the interface to determine if the interface is up or down. Leave the textbox blank to assume the interface is always online.
Tracking reliability	Enter the number of response 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 1.
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 timeout is 2 seconds.
Ping interval	Specifies the time in seconds between sending ping packets. The default ping interval is 5 seconds.
Interface down	The no. of consecutive failed attempts after which the interface is

Parameters	Description
	declared down. The default value for failed attempts is 3.
Interface up	The no. of consecutive successful attempts after which the interface to determine the reliability of the network connection through the interface. The default value for successful attempts is 3.
Metric	Enter 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 interface must have the same metric value on the Member Configuration page.

Table 10.2-4: Modify MWAN Interface

B. Members

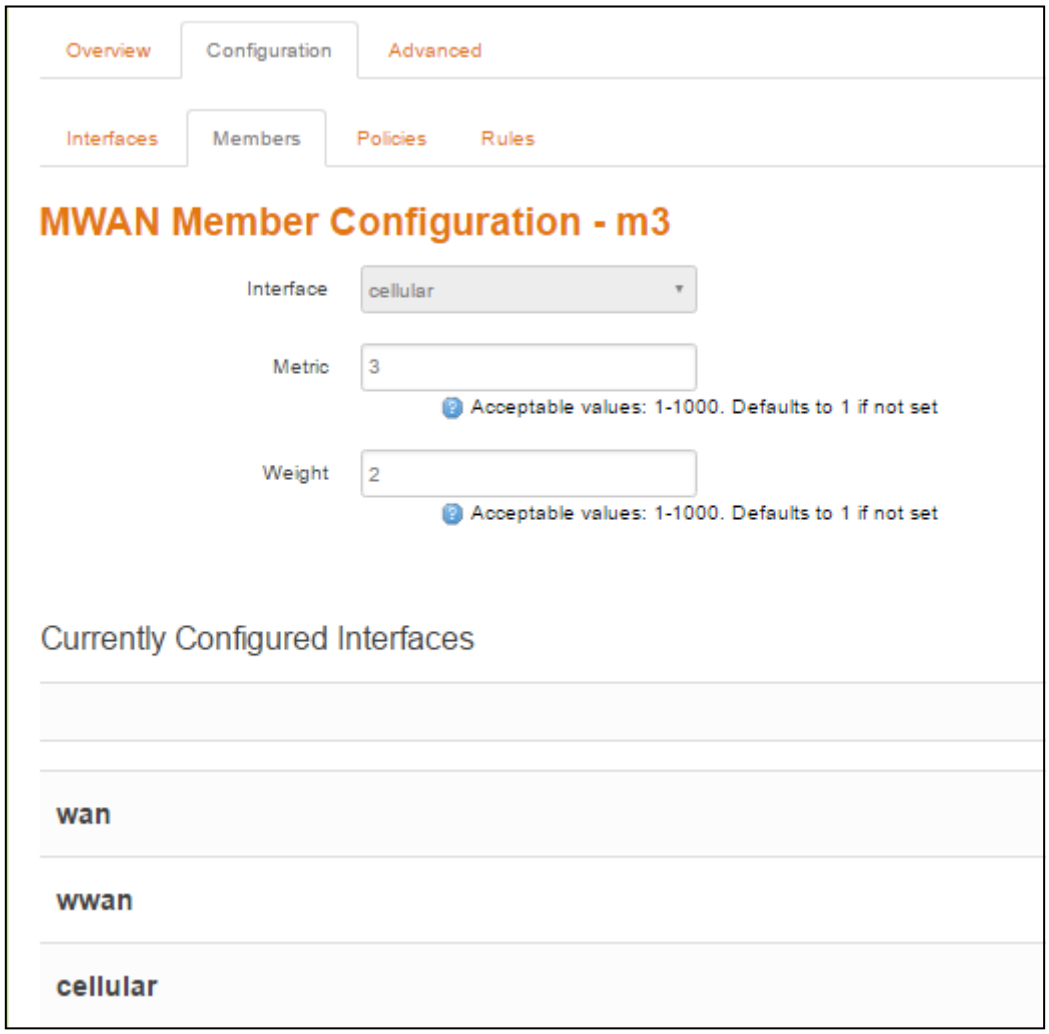


Screen 10-31: Member Configuration details of MWAN Interface

Parameters	Description
Member	Displays the Interface member notation number.
Interface	Displays the name of the interface.
Metric	Displays the metric assigned to the interface. The interface with the lowest metric has the highest priority and all data is always routed through it. ***Note*** • ***If two or more interfaces have same metric configured and that metric is lowest compared to other interfaces, then the data/load is balanced and data/load is distributed among the two interfaces in the ratio of the respective weight.***
Weight	Displays the weight assigned to the interface.
Sort	Click to sort the interface.
Add	Enter the name of the new interface to be added.

Table 10.2-5: Member Configuration details of MWAN Interface

a. Edit



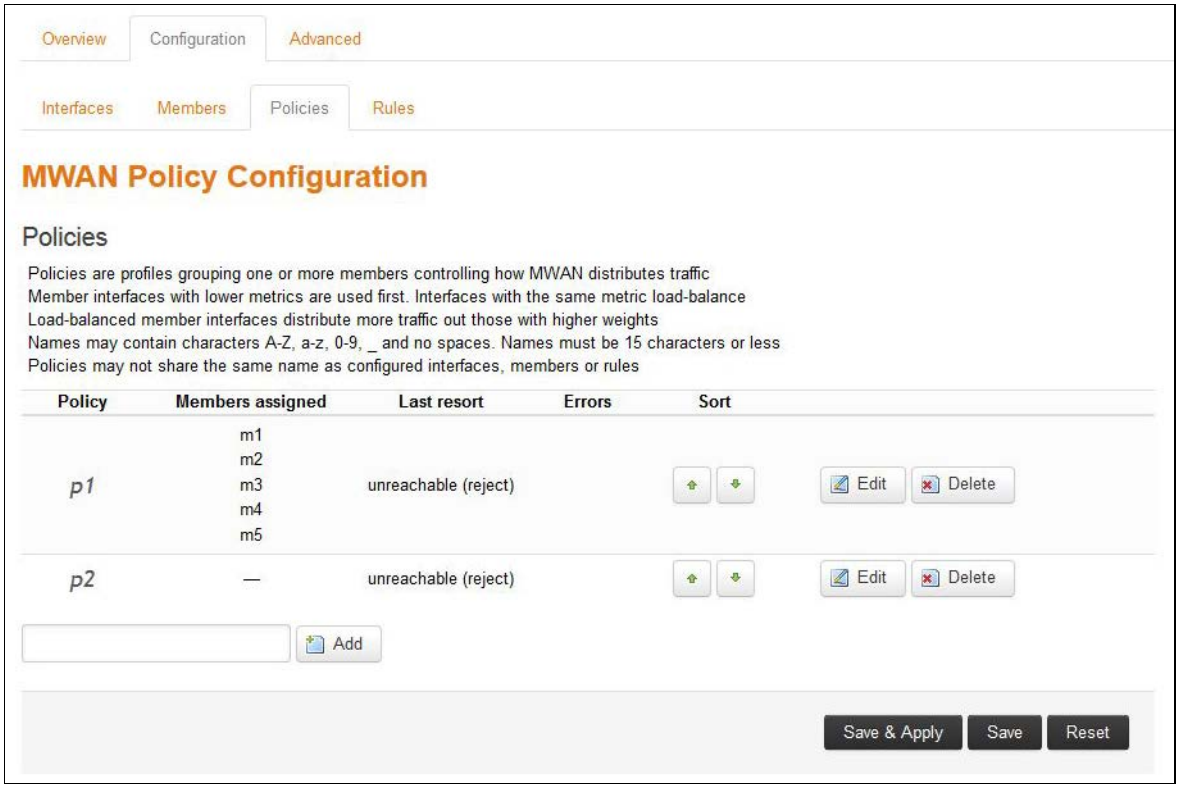
Screen 10-32: Modify the Member details of MWAN Interface

Parameters	Description
Interface	Displays the name of the interface.
Metric	Enter the Interface Metric. The route with least metric is considered as best route. For load balancing between two interfaces, both the interface must have the same metric value.
Weight	Enter the Interface Weight. The default metric assigned to the interface is 2.

Parameters	Description
	For load balancing between two interfaces, both the interface 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
Currently Configured Interfaces	List of currently configured Interfaces.

Table 10.2-6: Modify the Member details of MWAN Interface

C. Policies

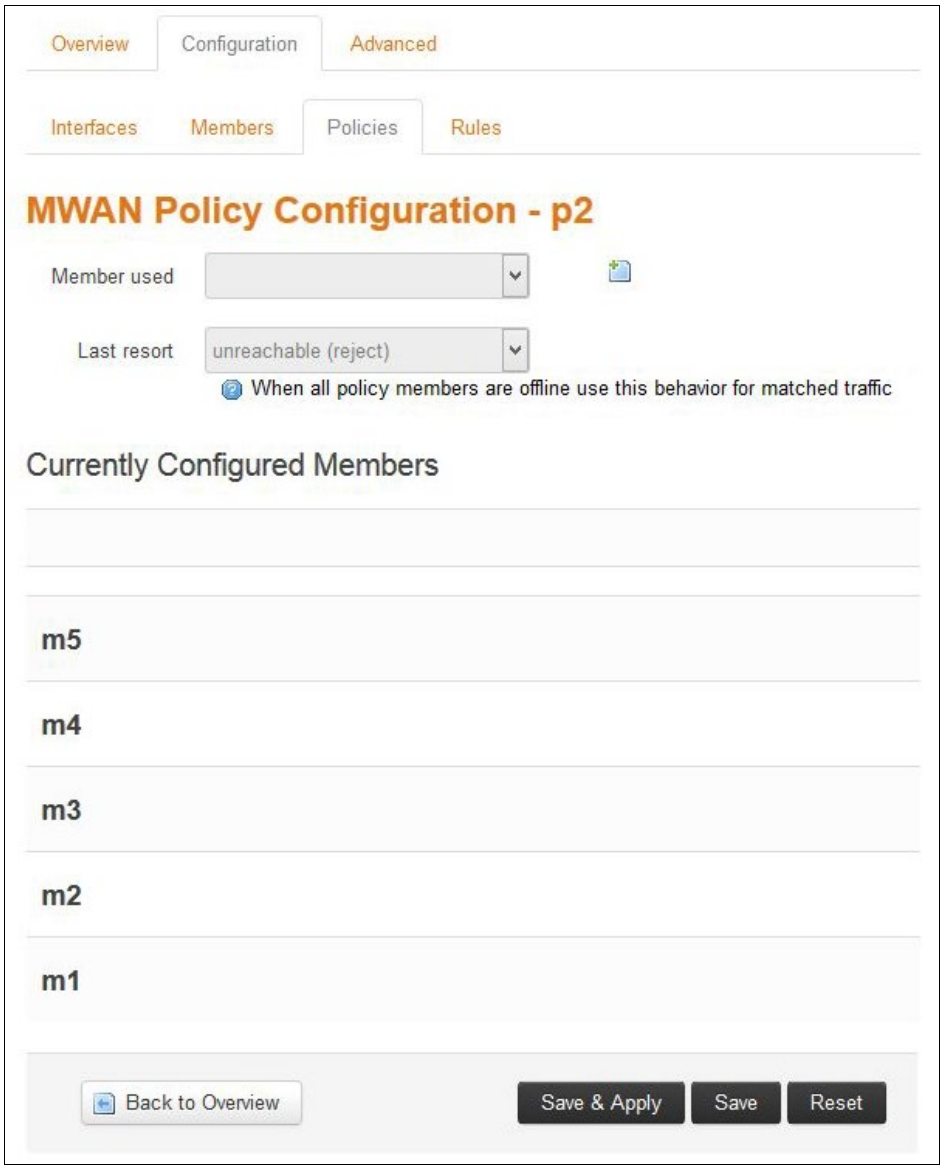


Screen 10-33: Policy Configuration details of MWAN Interface

Parameters	Description
Policy	Name of the policy
Members assigned	Interface members to which the policy is applied.
Last resort	When all the policy members are offline, use one of the available options for matching the traffic to policy.
Errors	Displays if an error has occurred during the Policy configuration. Error messages are displayed a warnings.
Sort	Click to sort the policies.
Add	Add a new policy

Table 10.2-7: Policy Configuration details of MWAN Interface

a. Edit

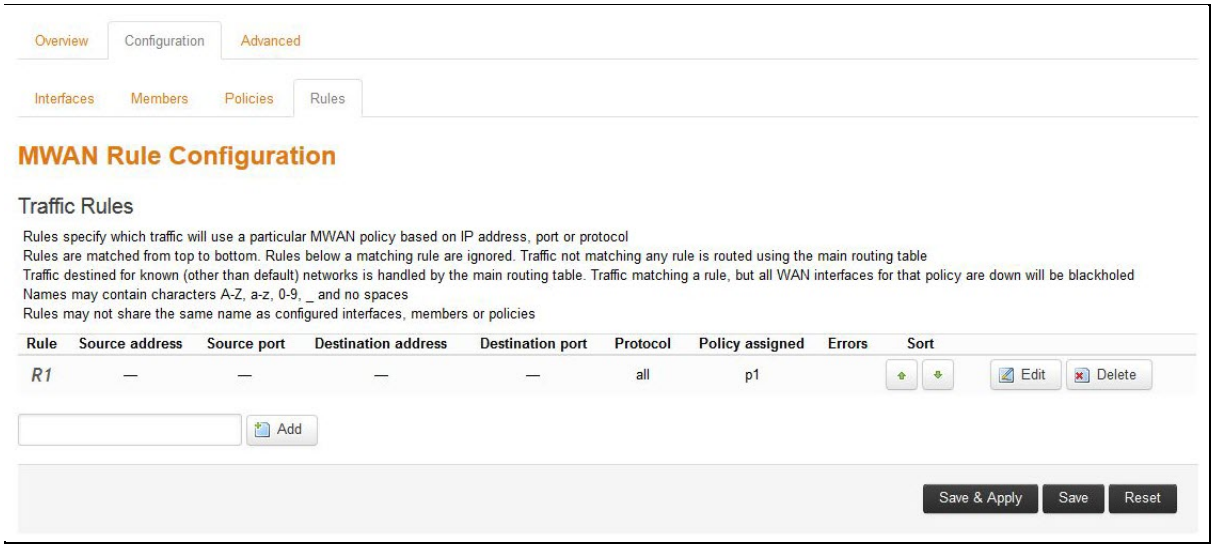


Screen 10-34: Modify Policy of MWAN Interface

Parameters	Description
Members used	Select the interface to apply the policy on traffic passing through the interface
Last Resort	When all the policy members are offline, use one of the following options for matching the traffic to policy.
Currently Configured Members	Interfaces configured in the policy.

Table 10.2-8: Modify Policy of MWAN Interface

D. Rules

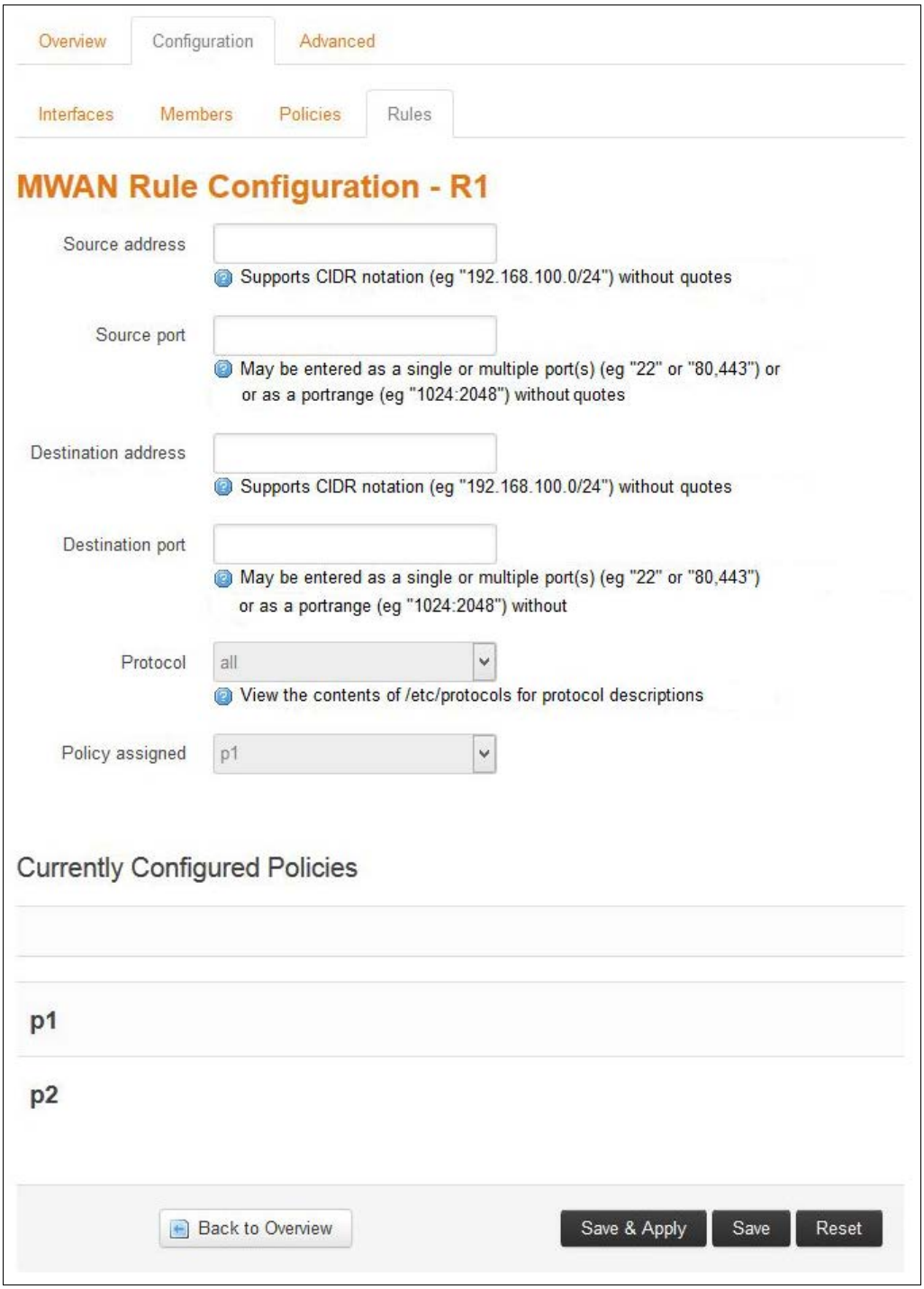


Screen 10-35: Rule Configuration details of MWAN Interface

Parameters	Description
Rule	Name of the Rule.
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 a warnings.
Sort	Click to sort the interface.
Add	Enter the name of the new rule.

Table 10.2-9: Rule Configuration details of MWAN Interface

a. Edit



Screen 10-36: Edit Rule details of MWAN Interface

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.

Parameters	Description
Protocol	Select the protocols on which the rule is applicable.
Policy assigned	Policy to be applied to the rule.
Currently Configured Policies	Policy already applied to the rule.

Table 10.2-10: Edit Rule details of MWAN Interface

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. Lower the metric, 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 short 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 boasts of 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.

So in a nutshell

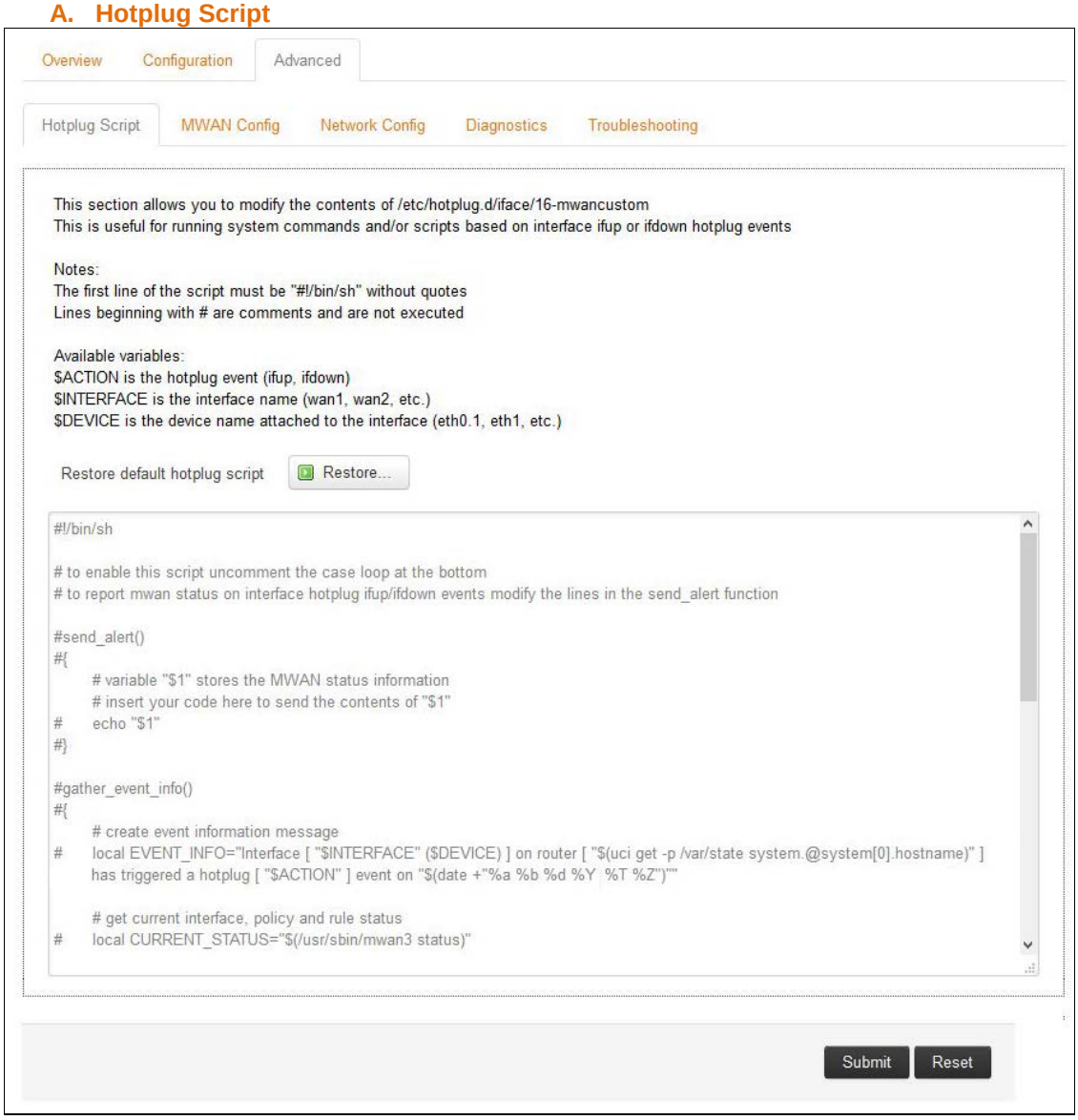
- Members correspond to individual interfaces where you can set metric and weight
- Policy consists of a member or group of members
- Rules are to be applied to a policy

10.2.3 Advanced Settings

Network > Load Balancing > Advanced Settings

This section details the same configuration as described in the earlier section but using a script and without the need to configure individual webpages

A. Hotplug Script

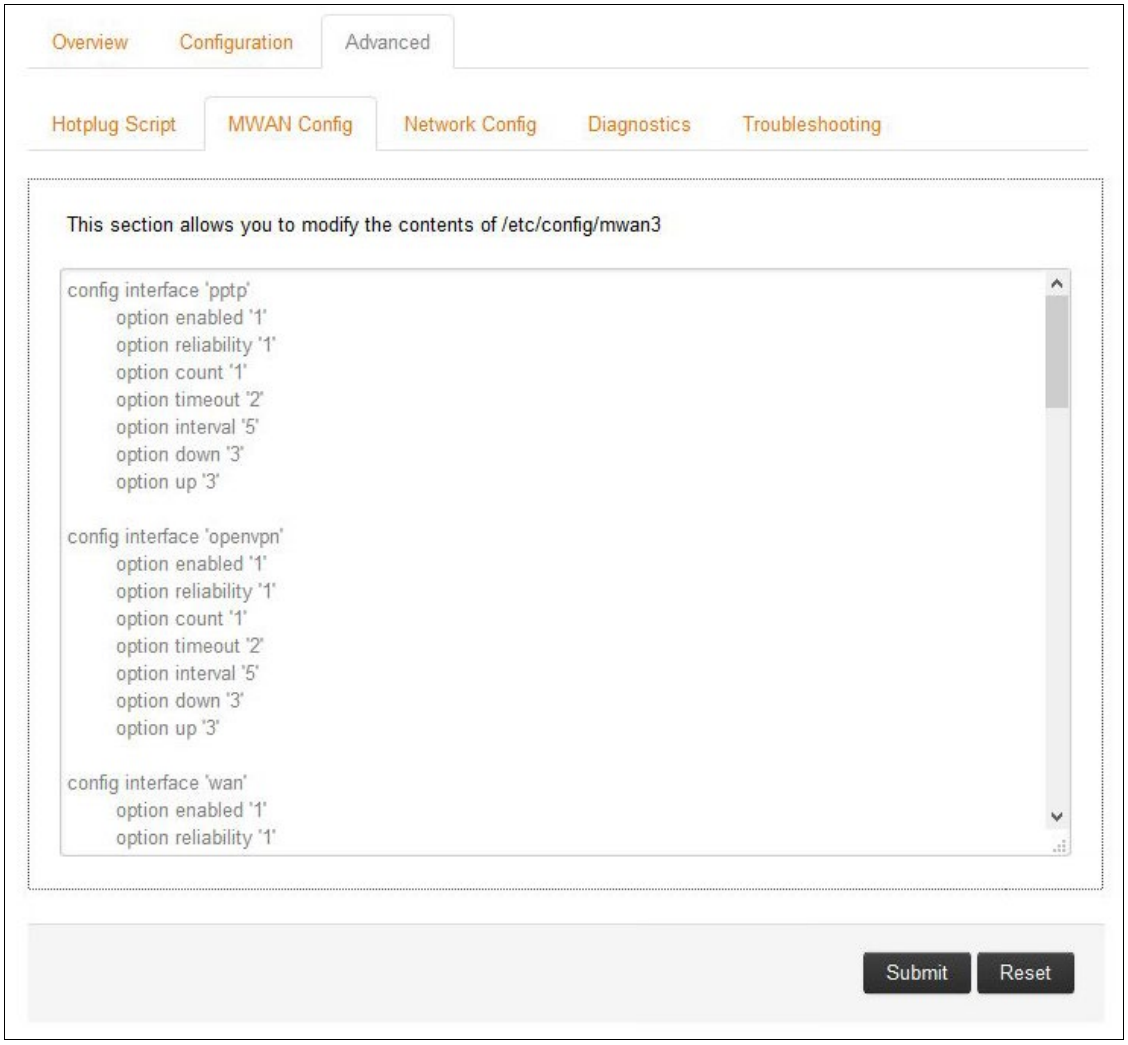


Screen 10-37: Advance Configuration for Hotplug Script

Parameters	Description
Hotplug Script	Hotplug scripts is a Linux kernel program that is used when the following two events occurs: • Interface comes up • Interface goes down Hotplug is automatically loads the drivers and runs arbitrary scripts based on events.

Table 10.2-11: Advance Configuration for Hotplug Script

B. MWAN Configuration

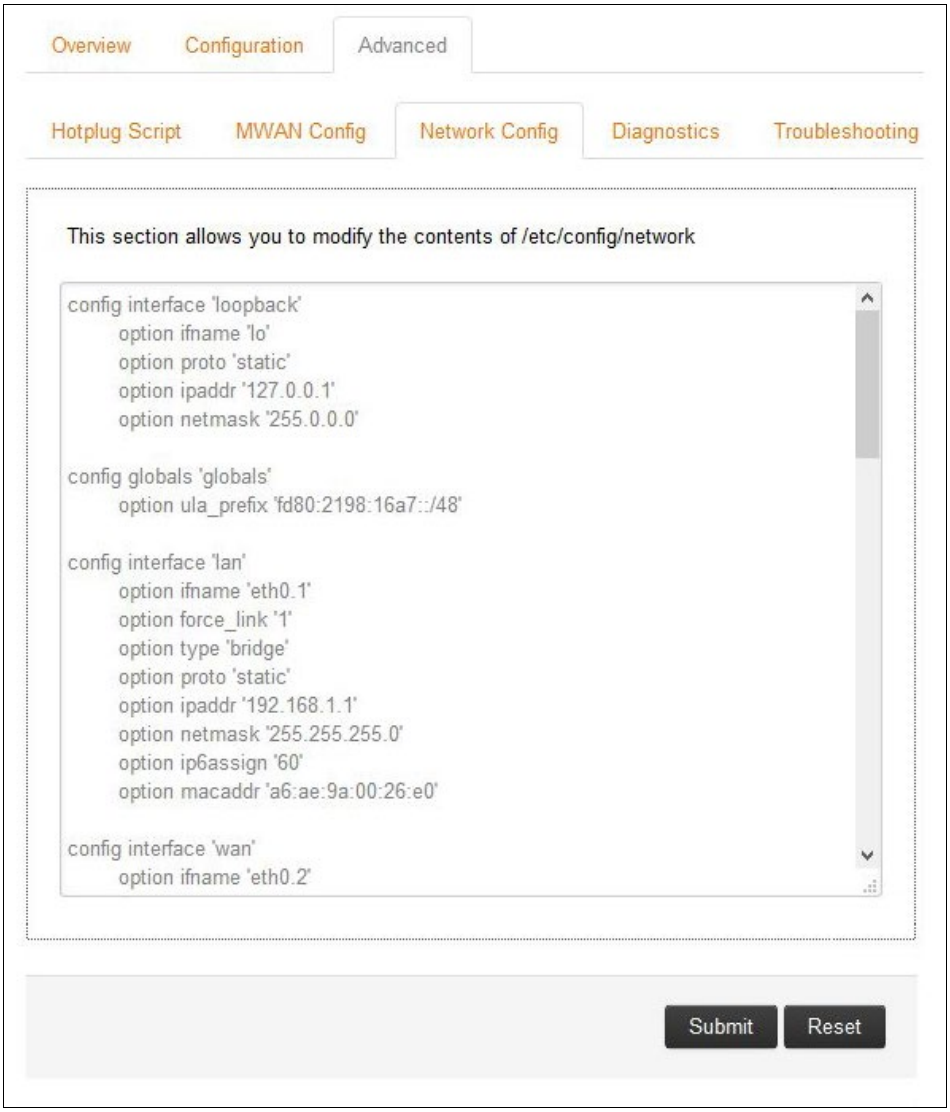


Screen 10-38: Advance Configuration for MWAN Interfaces

Parameters	Description
MWAN Config Details	Consolidated data of all the configured MWAN interfaces is available on this page. You may modify and update the each interface configuration from this page manually, instead of configuring it from respective MWAN Interface Advanced configuration page.

Table 10.2-12: Advance Configuration for MWAN Interfaces

C. Network Configuration

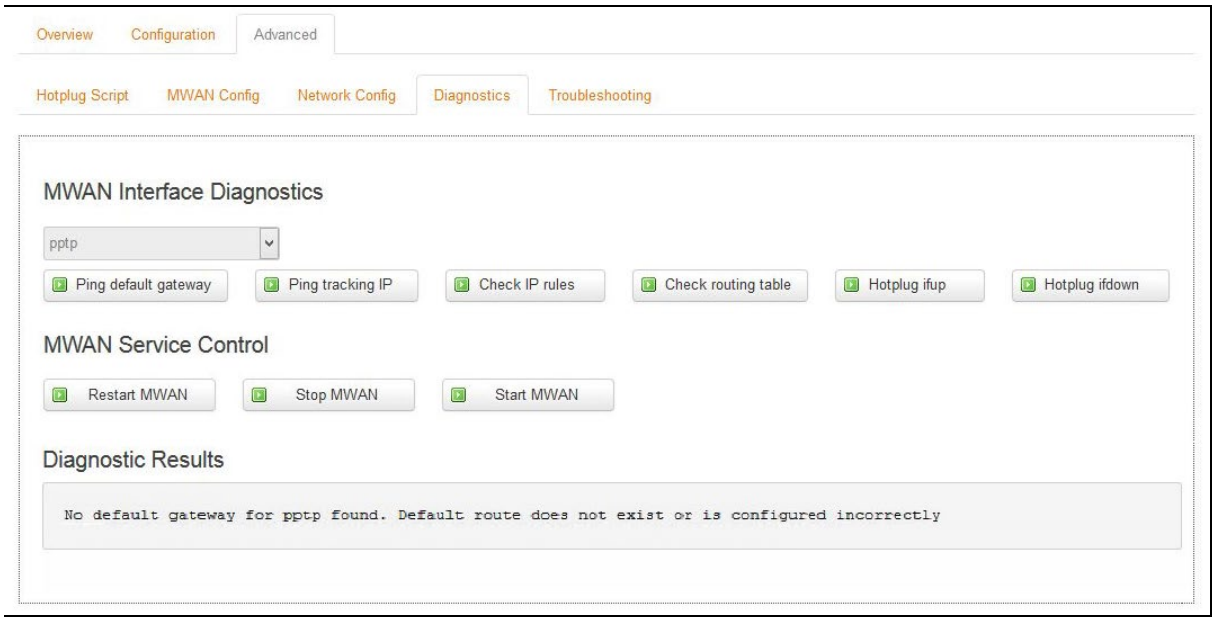


Screen 10-39: Advance Configuration for MWAN Network

Parameters	Description
Network Config Details	Consolidated data of all the configured Network interfaces is available on this page. You may modify and update the each interface configuration from this page manually, instead of configuring it from respective Network Interface Advanced configuration page.

Table 10.2-13: Advance Configuration for MWAN Network

D. Diagnostics

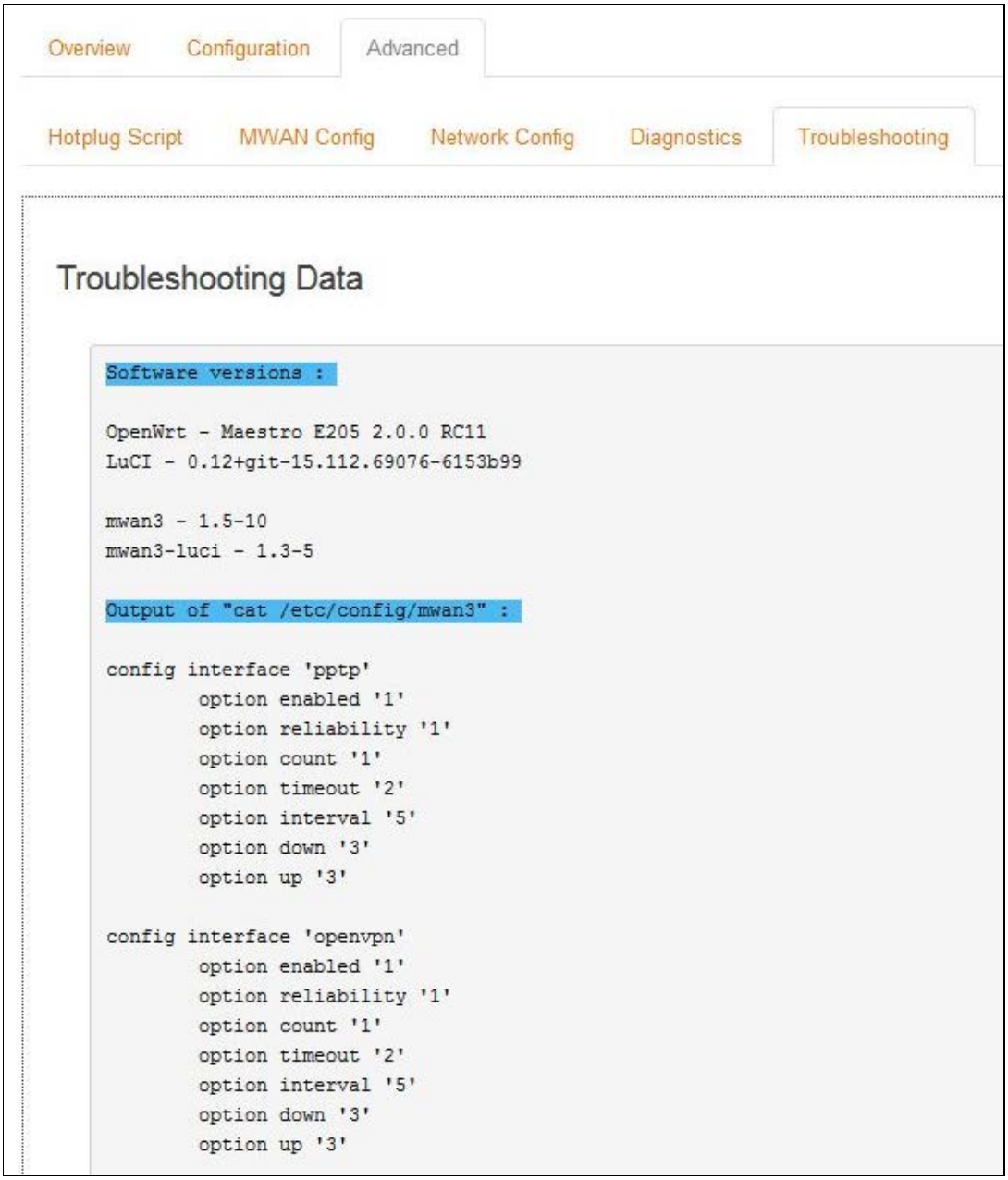


Screen 10-40: MWAN Interface and Service Diagnostics

Parameters	Description
MWAN Interface Diagnostics	Select the interface to run the diagnostic test on. Click one of the following diagnostic test that must be performed on the selected Interface: • **Ping Default Gateway –** Ping the default gateway configured for the Network Interface. The gateway is reachable if a ping response is received else there is a problem in the local network. • **Pink Tracking IP -** Ping the tracking IP Address configured in MWAN for the Network Interface. The tracking IP Address is reachable if a ping response is received else there is a conflict in the network configuration on the default gateway. • **Check IP Rules** – Click to verify the Interface. • **Check Routing Table** – Click to verify the routes present in the routing table of E200 Router. • **Hotplug ifup –** Click to turn-up the Interface using the hotplug script. ***Note*** • ***If the interface is already up, the hotplug script will restart the Interface.*** • **Hotplug ifdown –** Click to turn down the Interface using the hotplug script.
MWAN Service Control	Click the following buttons to perform following MWAN functionality: • **Start MWAN –** Starts load balancing/failover service. • **Stop MWAN –** Stops the running load balancing/failover service. • **Restart MWAN –** Stops the running load balancing/failover service and restart it.

Table 10.2-14: MWAN Interface and Service Diagnostics

E. Troubleshooting



Screen 10-41: Data for Troubleshooting

Parameters	Description
Troubleshooting Data	Displays the all the configuration details of the Router.

Table 10.2-15: Data for Troubleshooting

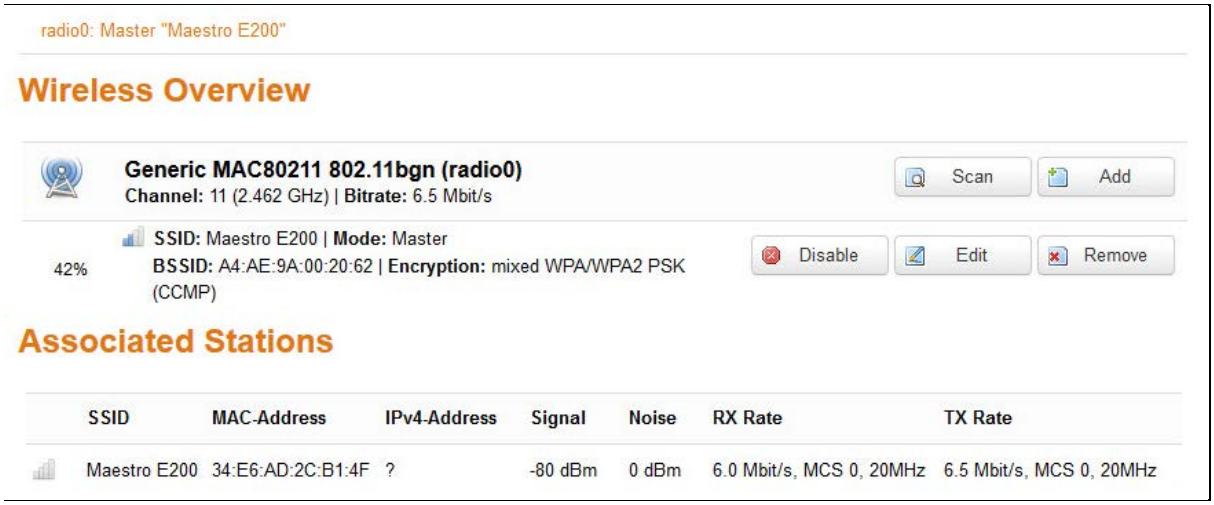
10.3 Wi-Fi

Network > Wi-Fi

The router can work in 2 modes:

- **Wi-Fi as access point:** It provides Internet to other host machines in its network over Wi-Fi. It can get Internet connection from WAN or cellular.
- **Wi-Fi as client mode:** 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.

At any point of time, the router can work either in client mode or in Master mode (Access Point).



Screen 10-42: Wireless Connection and Associated Stations Overview

Parameters	Description
Wireless Overview	Displays the following details: • **SSID –** A Service Set Identifier (SSID) is a public identifier of 32 characters that uniquely names a Wi-Fi connection. • **Mode –** Displays the mode of WLAN interface like Access Point Mode or Client Mode. • **Bitrate –** Data transfer rate • **BSSID –** Displays Basic Service Set Identification (BSSID); 24 bit MAC Address of Wireless Access Point. • **Encryption –** Displays the data encryption method. • **Signal Strength –** Displays the signal strength in percentage
Scan	Click to scan and detect the available wireless connections. Scanning must be done when Router must be changed from Master mode to client mode.
Associated Station	
SSID	SSID – A Service Set Identifier (SSID) is a public identifier of 32 characters that uniquely names a Wi-Fi connection.
MAC-Address	MAC Address of the computers and/or devices that are connected to the router.
IPv4-Address	IPv4 Address of the computers and/or devices that are connected to the router.

Parameters	Description
Signals	Signal strength in dBm.
Noise	Noise in dBm.
RX Rate	Data transfer rate at which the data is received.
TX Rate	Data transfer rate at which the data is transmitted.

Table 10.3-1: Wireless Connection and Associated Stations Overview

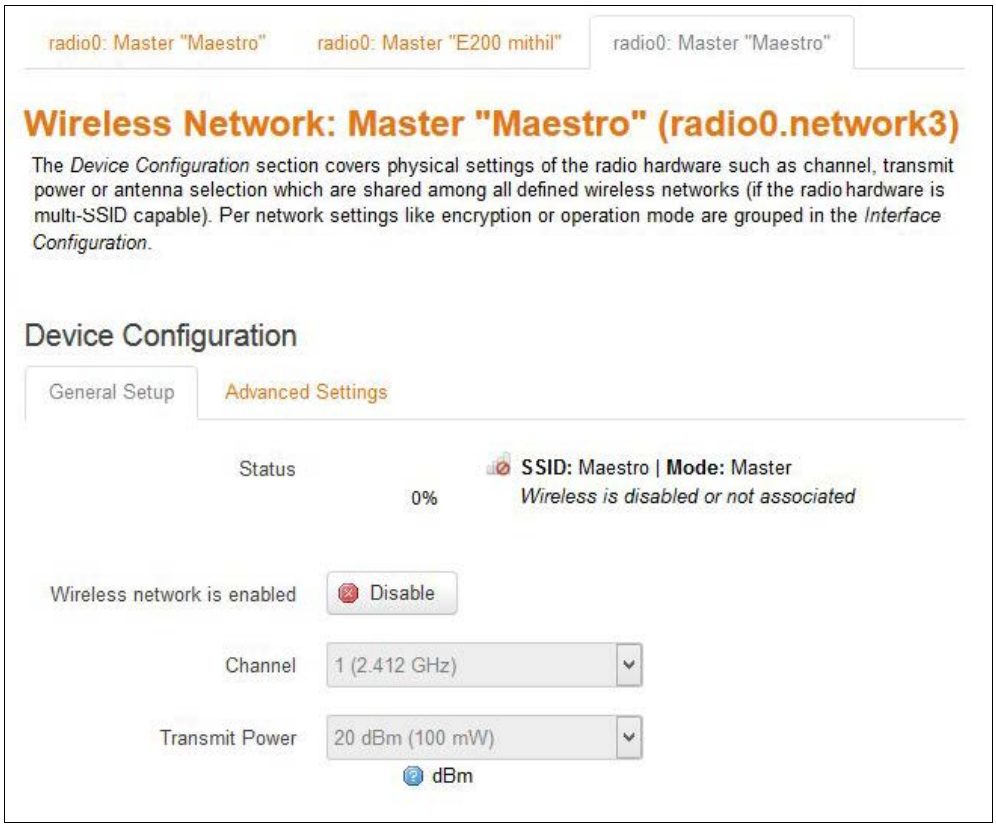
10.3.1 Add

Network > Wi-Fi > Add

> ***Note***
>
> - ***You can add a different SSID for same Wi-Fi Access Point.***

A. Device Configuration

a. General Settings



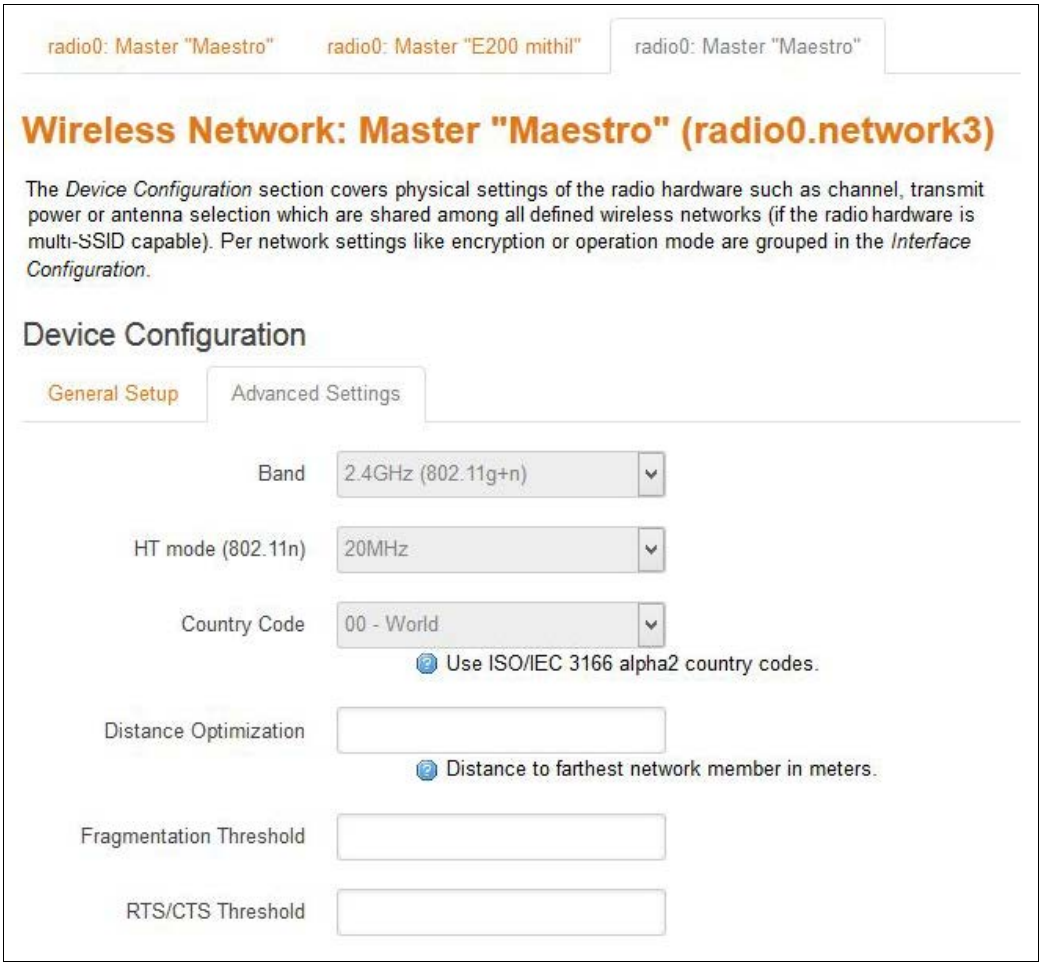
Screen 10-43: General Wireless Connection Configurations for a New Device

Parameters	Description
Status	Displays the following details: • **SSID –** A Service Set Identifier (SSID) is a public identifier of 32 characters that uniquely names a Wi-Fi connection. • **Mode –** Displays the mode of WLAN interface like Access Point Mode or Client Mode. • **BSSID –** Displays Basic Service Set Identification (BSSID); 24 bit MAC Address of Wireless Access Point. • **Encryption –** Displays the data encryption method. • **Signal Strength –** Displays the signal strength in percentage
Wireless network is enabled	Click the Enable button to start the wireless network.
Channel	Choose the channel frequency from the drop down menu, or choose 'auto', to select it automatically. There are 11 channels. A custom channel can be added.
Transmit Power	Select the transmit power.

Parameters	Description
	The default selection is 20dBm or 100mW.

Table 10.3-2: General Wireless Connection Configurations for a New Device

b. Advanced Settings



Screen 10-44: Advance Wireless Connection Configurations for a New Device

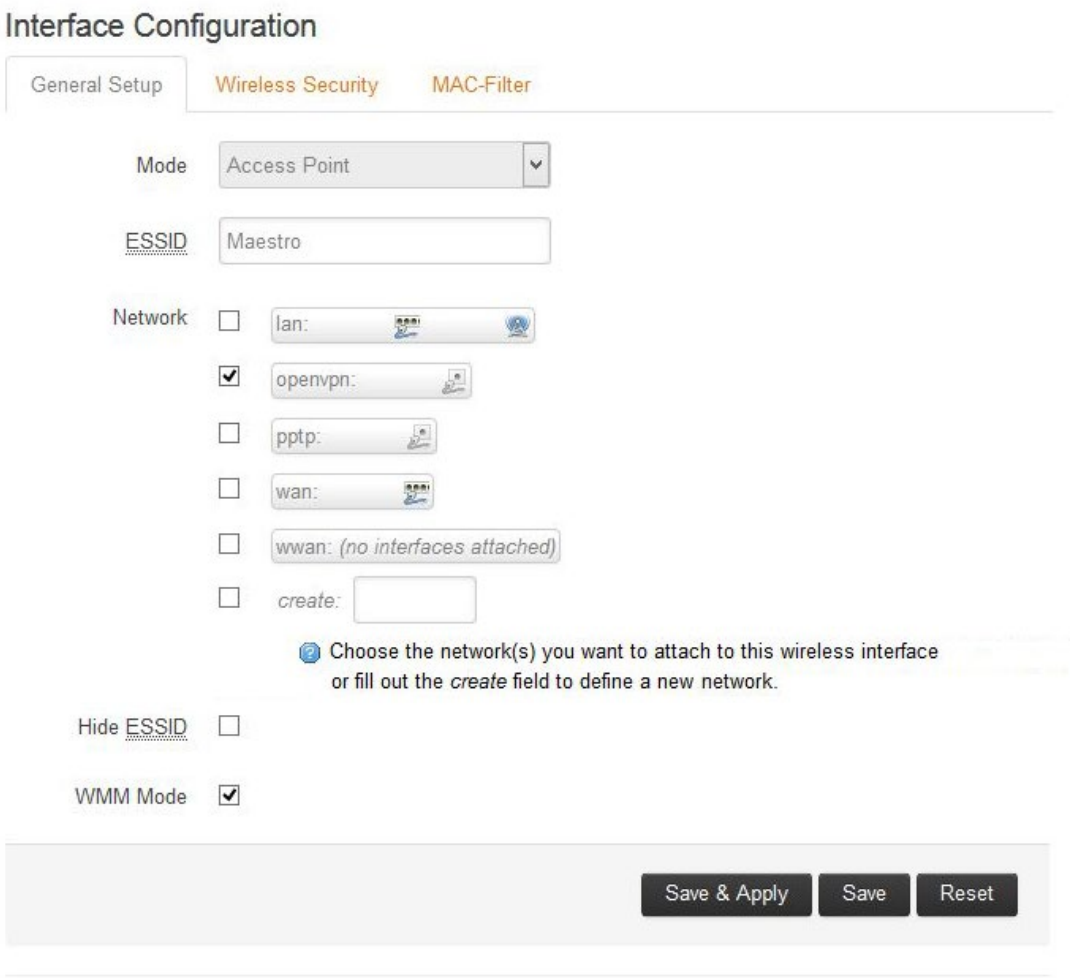
Parameters	Description
Band	Select the Wi-Fi band. The default band is 2.4GHz (802.11g+n).
HT mode (802.11n)	Select the HT mode for Wi-Fi connection. **Available Options** • 20 Mhz • 40Mhz • Disable The default HT mode value is 20Mhz
Country Code	Choose the country code corresponding to the country where the router is operational. This ensures that the channels available in that country are enabled. By choosing '00' (World), the router will select the appropriate channel in your country.
Distance Optimization	The operation of a Wi-Fi network can be optimized, if you know the distance of the farthest machine in your network from the router. Value is meter.
Fragmentation Threshold	Choose Fragmentation threshold value (in number of bytes). Fine-

Parameters	Description
	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.
RTS/CTS Threshold	You can choose 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. ***Note*** • ***In case of access point setting, it is recommended not to use RTS/CTS threshold.***

Table 10.3-3: Advance Wireless Connection Configurations for a New Device

B. Interface Configuration

a. General Setup



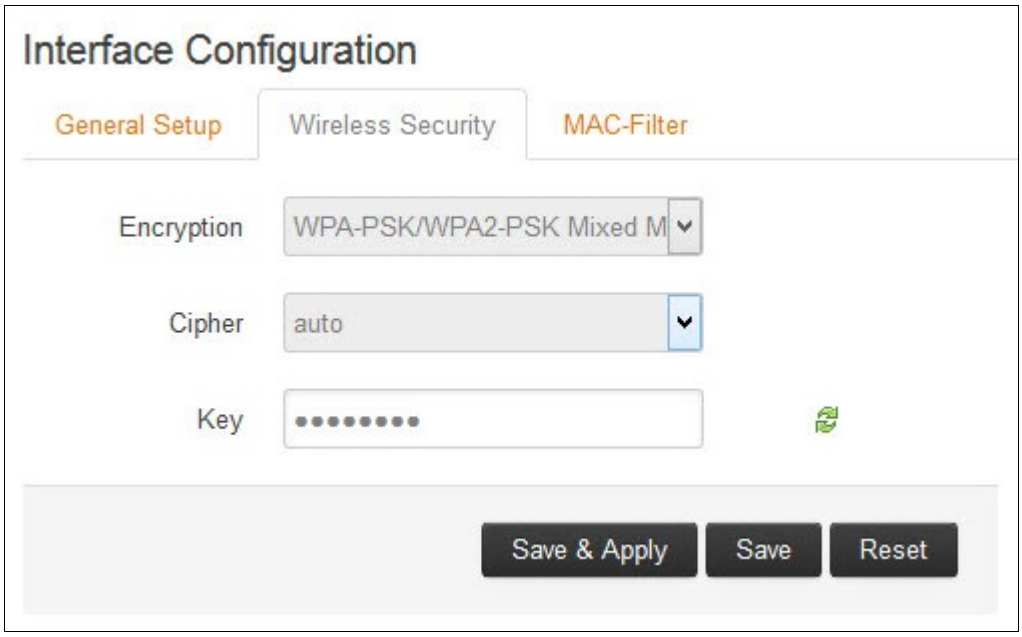
Screen 10-45: General Wireless Connection Configurations for a New Interface

Parameters	Description
Mode	Select the Wi-Fi Interface mode. **Available Options** • Access Point • Client • Ad-Hoc • 802.11s • Pseudo Ad-Hoc (ahdemo) • Monitor • Access Point (WDS) • Client (WDS) The default mode is Access Point.
ESSID	Displays the device name assigned to the router.

Parameters	Description
	The default name is Maestro E200.
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 SSID, to hide SSID when client machines scan for available Wi-Fi networks.
WMM Mode	Wi-Fi Multimedia (WMM), is a subset of the 802.11e wireless LAN (WLAN) specification that enhances quality of service (QoS) on a network by prioritizing data packets. ***Note*** • ***802.11n spec requires devices to support 802.11e (Quality of Service [QoS] enhancements for wireless LAN) in order to use HT (High Throughput) link rates, i.e. higher than 54 Mbps. WMM's Traffic Identifier (TID) field is key to aggregation mechanisms, including block acknowledgement (block ACK), that enable 802.11n's high throughput rates.*** Since WMM support is required for products to be certified for 802.11n, WMM comes enabled by default in all Wi-Fi Certified n APs and wireless routers. So even if you don't have any WMM-aware devices on your network, leave WMM enabled or you may find your clients connecting only at 54 Mbps rates.

Table 10.3-4: General Wireless Connection Configurations for a New Interface

b. Wireless Security

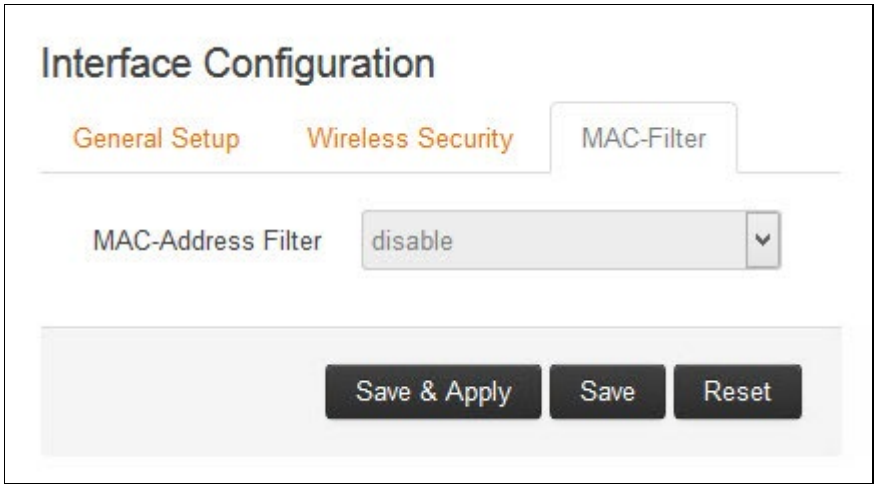


Screen 10-46: Wireless Security Configurations for a New Interface

Parameters	Description
Encryption	Select the Encryption mode for Wi-Fi network. **Available Options** • No Encryption • WPA-PSK/WPA2-PSK Mixed mode • WPA2-PSK • WPA-PSK • WEP Shared Key • WEP Open System The default encryption mode is WPA-PSK/WPA2-PSK Mixed mode.
Cipher	Select the cipher suitable to the Router. **Available Options** • Auto • Force CCMP (AES) • Force TKIP • Force TKIP and CCMP (AES) The default cipher is auto mode.
Key	Enter the key respective to cipher type

Table 10.3-5: Wireless Security Configurations for a New Interface

c. MAC-Filter (Only for Interface configuration mode selected as Access Point)



Screen 10-47: MAC Filter Configurations for a New Interface

Parameters	Description
MAC-Address Filter	MAC Address Filter is use to configure the white-listed or the black-listed MAC Address. **Available Options** • Disable • **Allow listed only** – Click to add the allowed MAC Address. • **Allow all except listed** – Click to add the allowed MAC Address. By default the MAC-Address Filter is disabled.

Table 10.3-6: MAC Filter Configurations for a New Interface

Concept of Wi-Fi in E Series

E Series treats Wi-Fi as an interface. By default there is on pre-created interface for Wi-Fi in access point mode. You can create multiple interfaces at the same time and assign multiple SSIDs to them.
However while creating multiple interfaces for Wi-Fi please make sure that you do not create a few in Hotspot mode and few in client mode.

10.4 DHCP and DNS

Network > DHCP and DNS

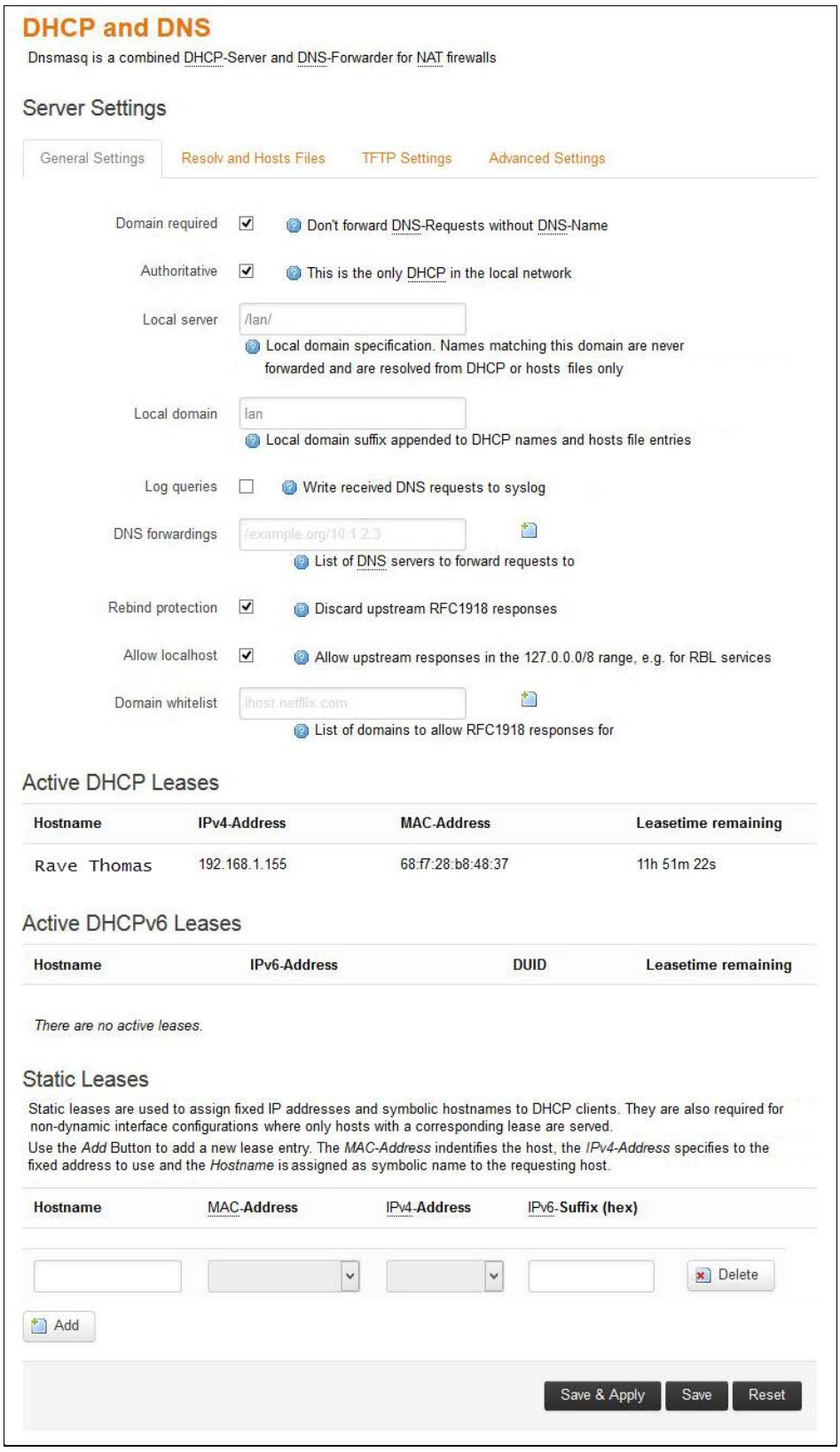
Dynamic Host Configuration Protocol (DHCP) is a network protocol that is used to configure network devices to communicate on an IP network. A DHCP client uses the DHCP protocol to acquire configuration information, such as an IP address, a default route, and one or more DNS server addresses from a DHCP 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 **Network > LAN > DHCP Server**.

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

10.4.1 General Settings

Network > DHCP and DNS > General Settings



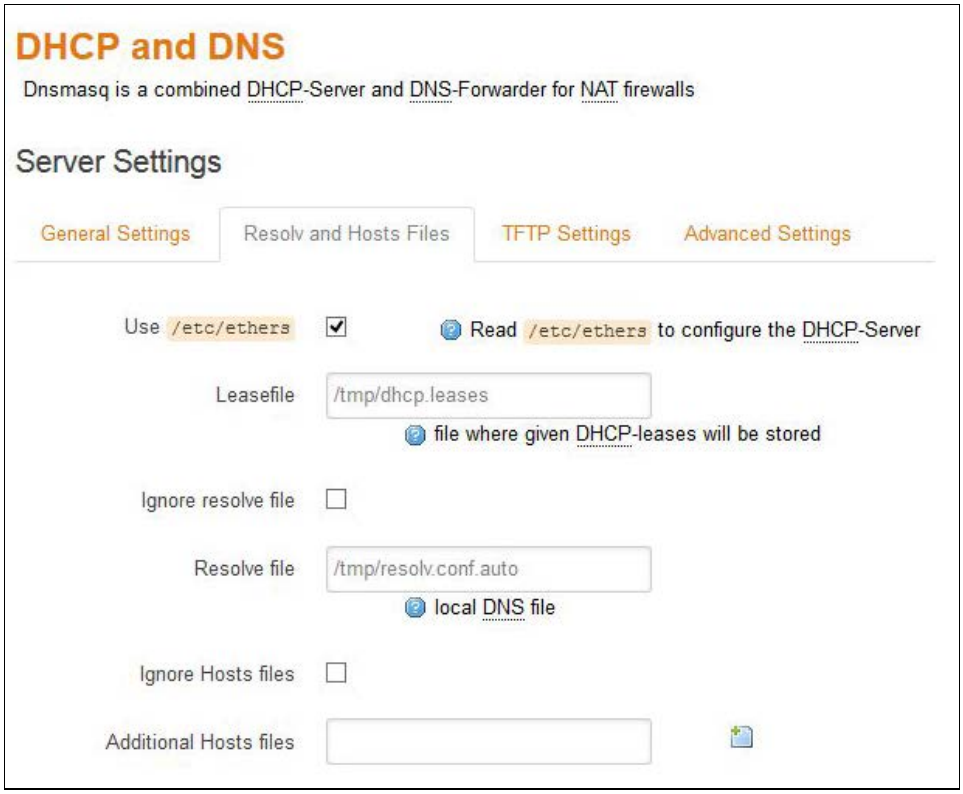
Screen 10-48: General Configuration of DHCP Server and DNS-Forwarder

Parameters	Description
Server Settings	
Domain required	Check to allow forwarding of DNS request only if they have domain name.
Authoritative	Check to authorize the DHCP in the local network.
Local server	Enter the local server domain specification. These domain names are only resoled 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.
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 file

Network > DHCP and DNS > Resolv and Host File



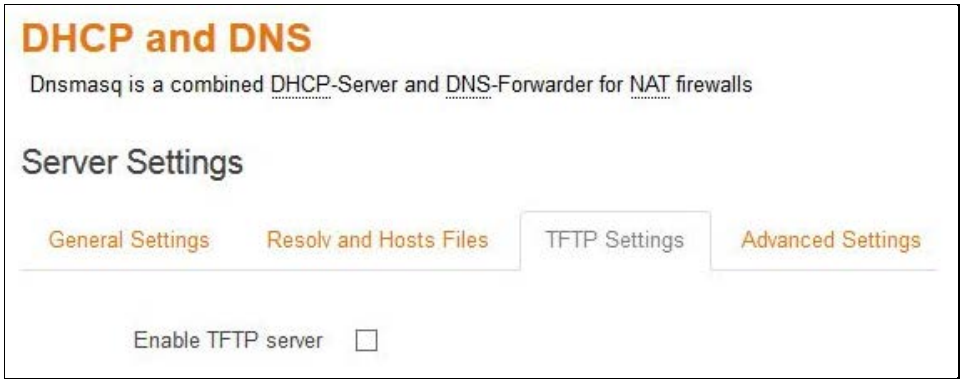
Screen 10-49: Resolv and Host File Configuration for DHCP and DNS

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

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

10.4.3 TFTP Settings

Network > DHCP and DNS > TFTP Settings



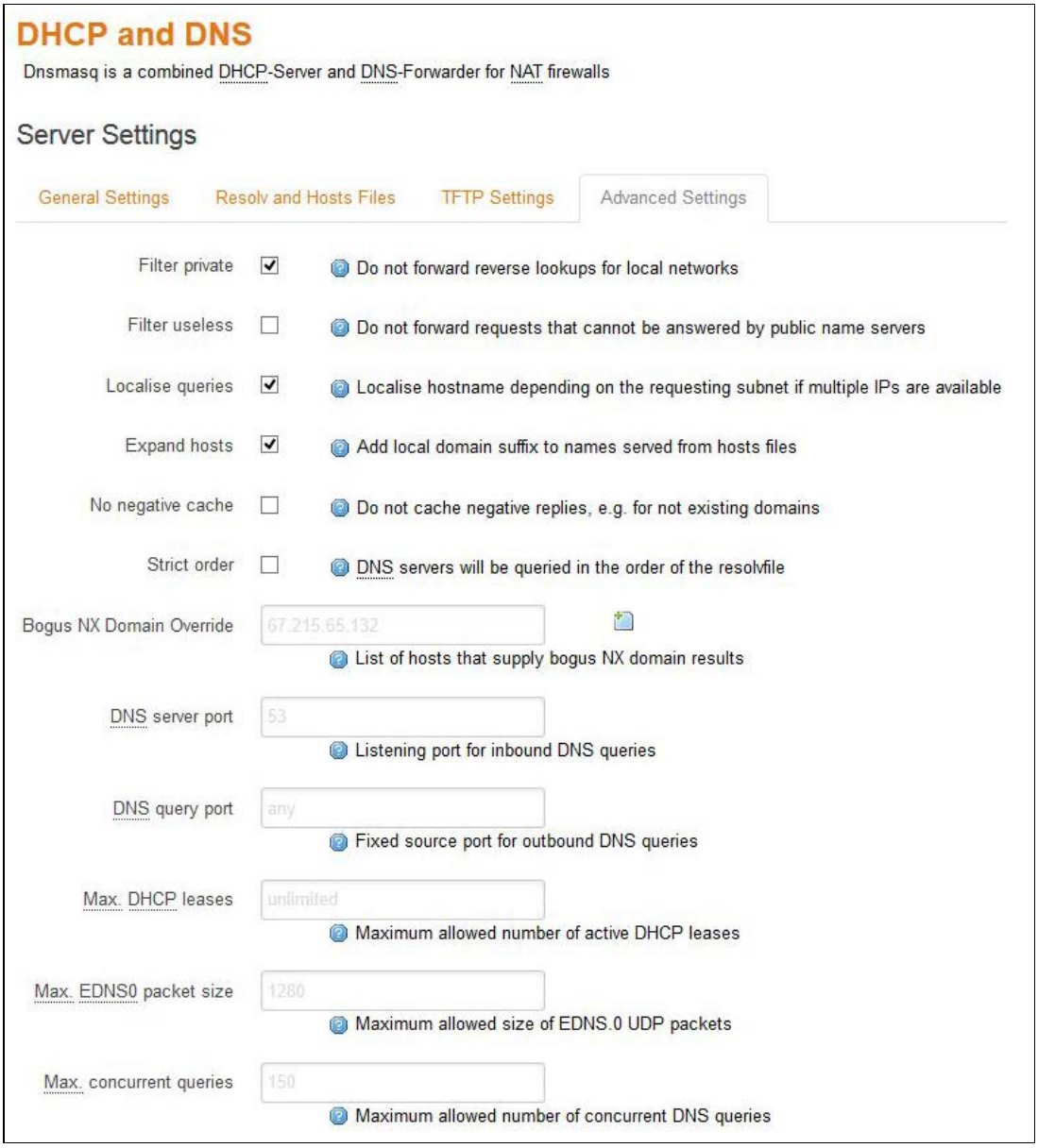
Screen 10-50: TFTP Configuration for DHCP and DNS

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



Screen 10-51: Advanced Configuration for DHCP and DNS

Parameters	Description
Server Settings	
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.

Parameters	Description
No negative cache	Check to deny caching the negative replies, e.g. for non-existing domains.
Strict order	DNS servers will be queried in the order of the resolve file.
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.

Table 10.4-4: Advanced Configuration for DHCP and DNS

10.5 Hostnames

Network > Hostnames

Screen 10-52: Hostnames Configuration

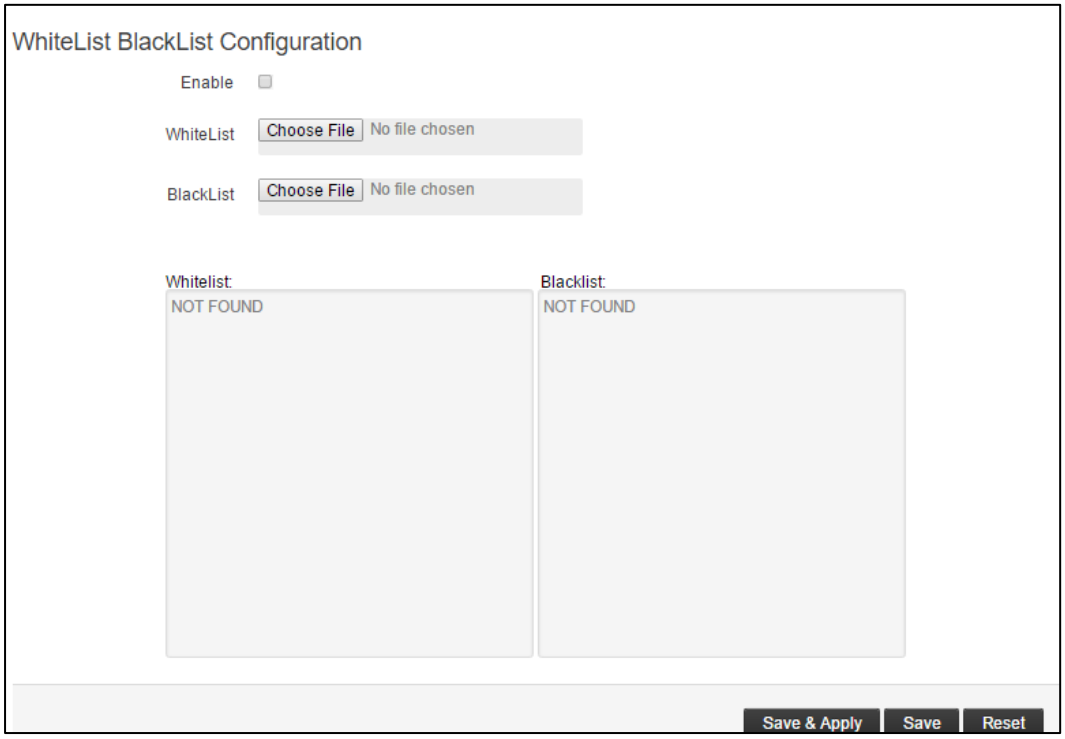
Parameters	Description
Host entries	
Hostname	Enter the Hostname.
IP address	Enter the IP Address of the host.

Table 10.5-1: Hostnames Configuration

10.6 Whitelist / Blacklist

You can configure Whitelisted operator networks and Blacklisted Operator networks. The Router will always give priority to a Whitelisted network and will never connect to a Blacklisted Network.

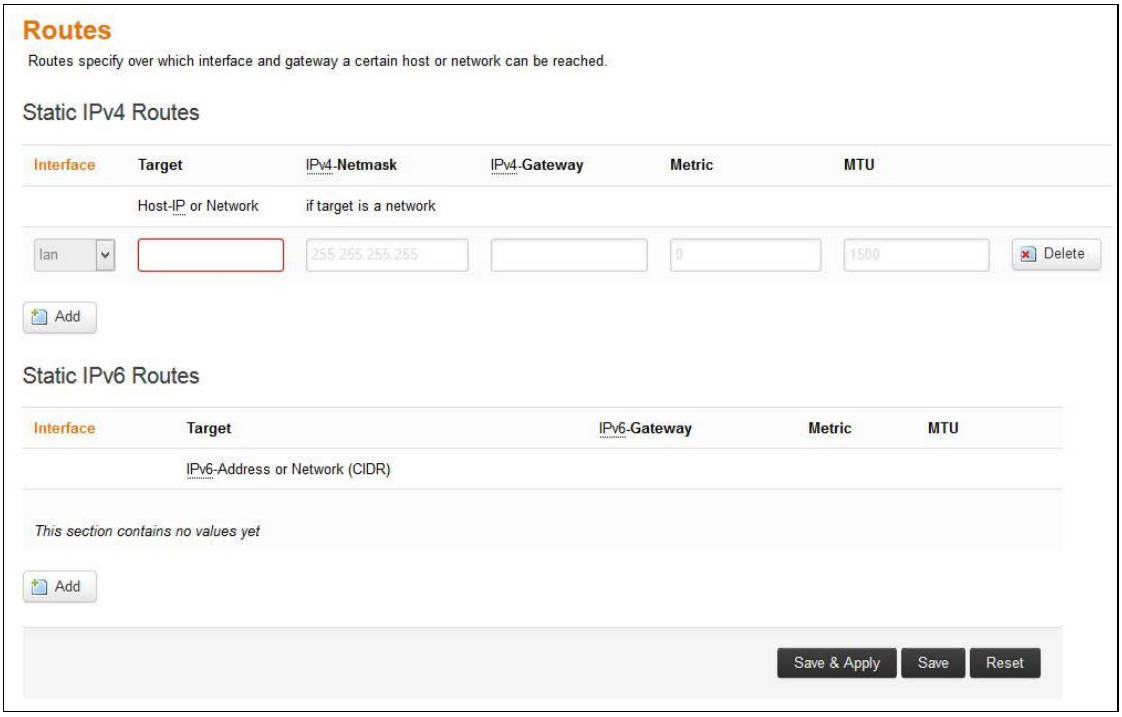
You need to upload .txt files using the upload tabs as given below. Each line of the .txt file should contain a network name or Network ID



10.7 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.



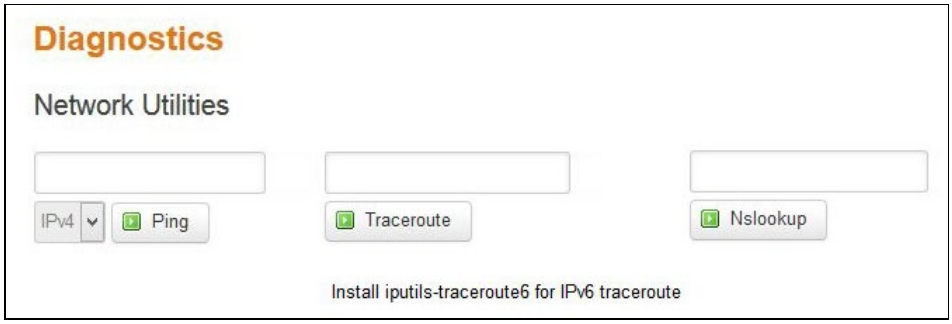
Screen 10-53: Static Routes Configuration

Parameters	Description
Static IPv4 Routes	
Interface	Displays the name of the interface assigned the static IPv4 Address.
Target	Displays the target host IPv4 Address or Network if the target is a network.
IPv4-Netmask	Displays the IPv4 Netmask of the static route.
IPv4-Gateway	Displays the IPv4 Gateway of the static route.
Metric	Displays the metric of the static route.
MTU	Displays the configured Maximum Transmission Unit (MTU).
Static IPv6 Routes	
Interface	Displays the name of the interface assigned the static IPv6 Address.
Target	Displays the target host IPv6 Address or Network CIDR if the target is a network.
IPv6-Gateway	Displays the IPv6 Netmask of the static route.
Metric	Displays the IPv6 Gateway of the static route.
MTU	Displays the metric of the static route.

Table 10.7-1: Static Routes Configuration

10.8 Diagnostics

Network > Diagnostics



Screen 10-54: Diagnostics Configuration

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 10.8-1: Diagnostics Configuration

10.9 Firewall

Network > Firewall

E200 follows a Zone Based firewall concept.

Every interface of E200 Router physical or virtual needs to be assigned to a Firewall Zone, however one firewall zone can have multiple interfaces.

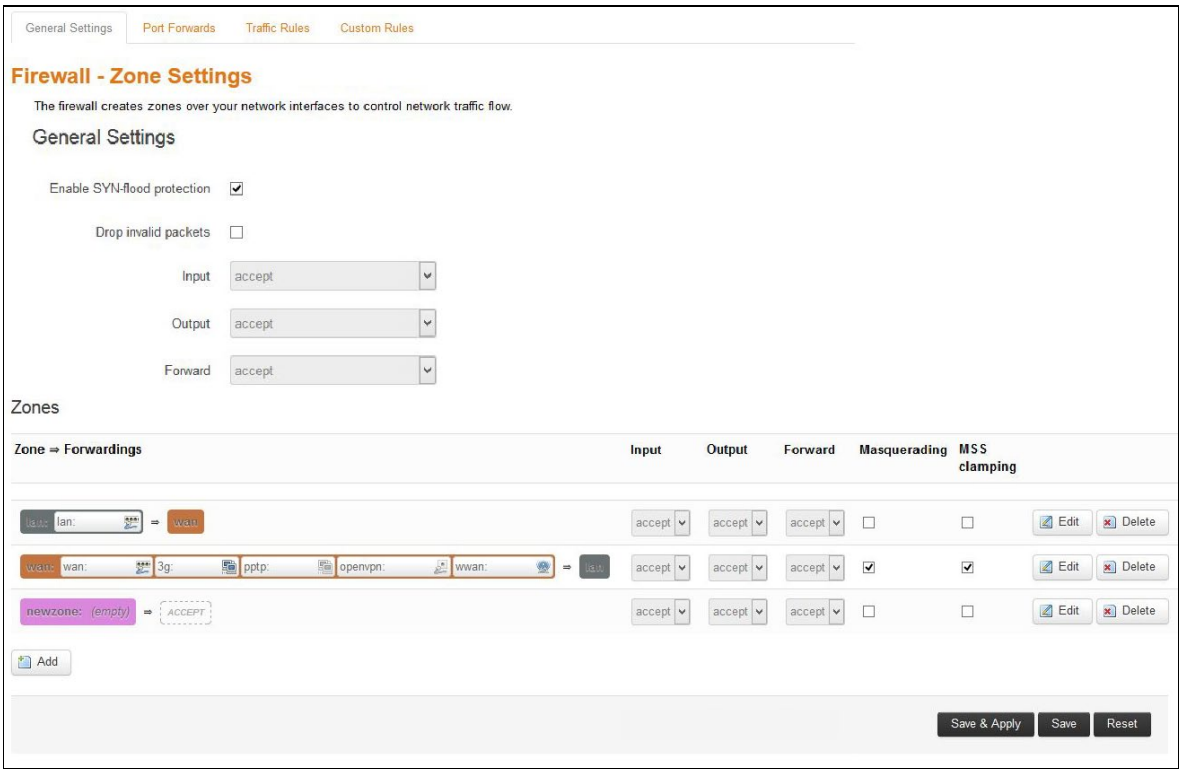
By default, there exist two zones. They are LAN zone and WAN zone as shown in the screenshot below.

You can create a new zone either from the Firewall section or when you create an additional network interface.

LAN or WAN side Firewall Zones can be created and you can associate multiple interfaces to the Firewall Zones and define the rules of communication between them.

10.9.1 General Setting

Network > Firewall > General Settings



Screen 10-55: General Configuration for Firewall Zone

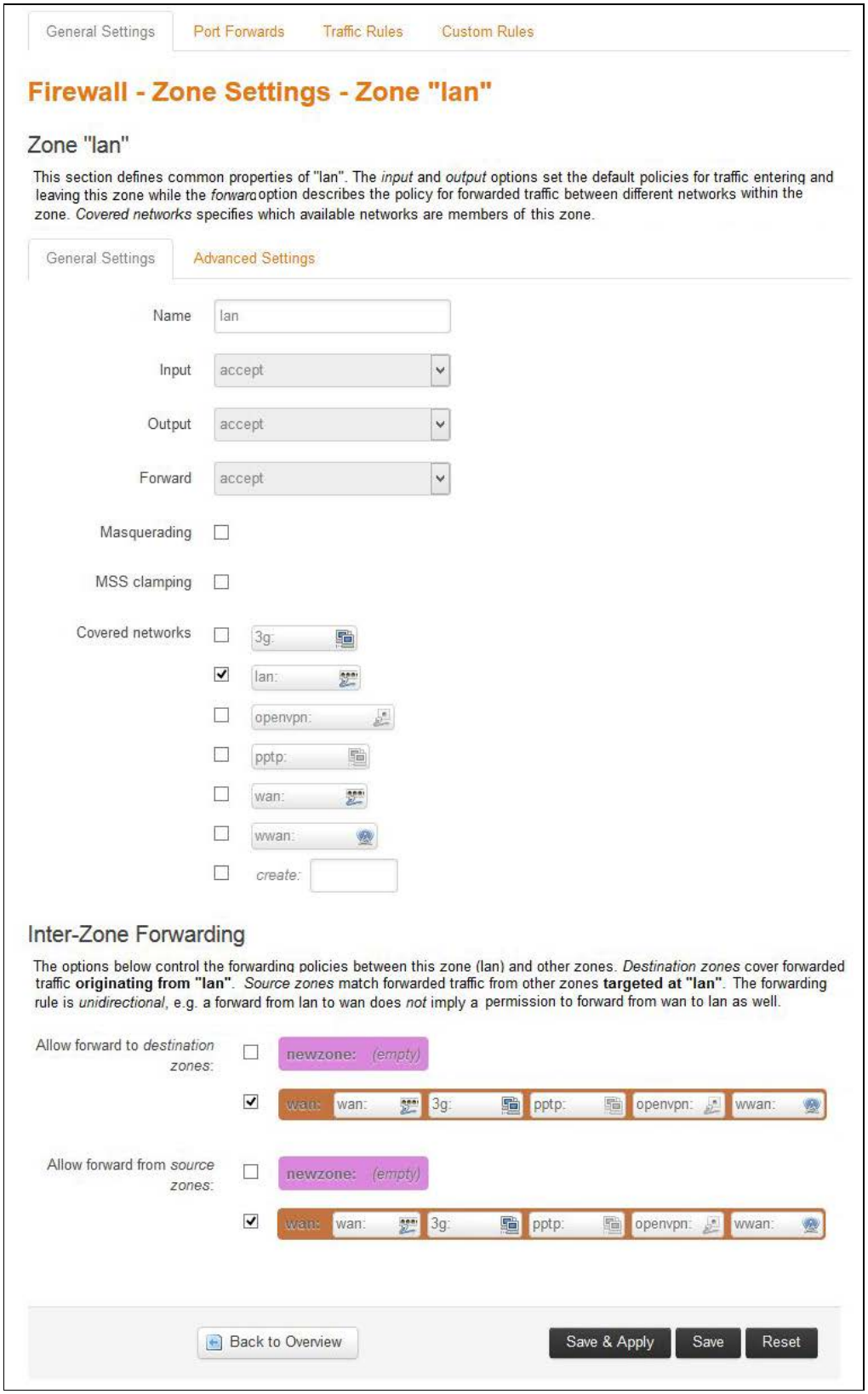
Parameters	Description
General Settings	
Enable SYN-flood protection	Check to enable SYN-flood protection. SYN-flood protection will enable spamming detection and block whenever there is a spam attack.
Drop invalid packet	Check to drop the invalid packets that are not matching any active connection.
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 (Applicable to configured zone)	

Parameters	Description
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.
Forward	Select to accept or reject the forwarded traffic from all the configured zones.
Masquerading	Check to allow IP Masquerading.
MSS clamping	Check to allow MSS clamping.

Table 10.9-1: General Configuration for Firewall Zone

A. Add

a. General Settings



Screen 10-56: General Configuration for Firewall Zone (LAN)

Parameters	Description
Static IPv4 Routes	
Name	Enter the name of the zone.
Input	Select to accept or reject the inbound traffic to all the configured zones.
Output	Select to accept or reject the outbound traffic from all the configured zones.
Forward	Select to accept or reject the forwarded traffic from all the configured zones.
Masquerading	Check to allow IP Masquerading.
MSS clamping	Check to allow MSS clamping.
Covered network	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 10.9-2: General Configuration for Firewall Zone (LAN)

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, Viz 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

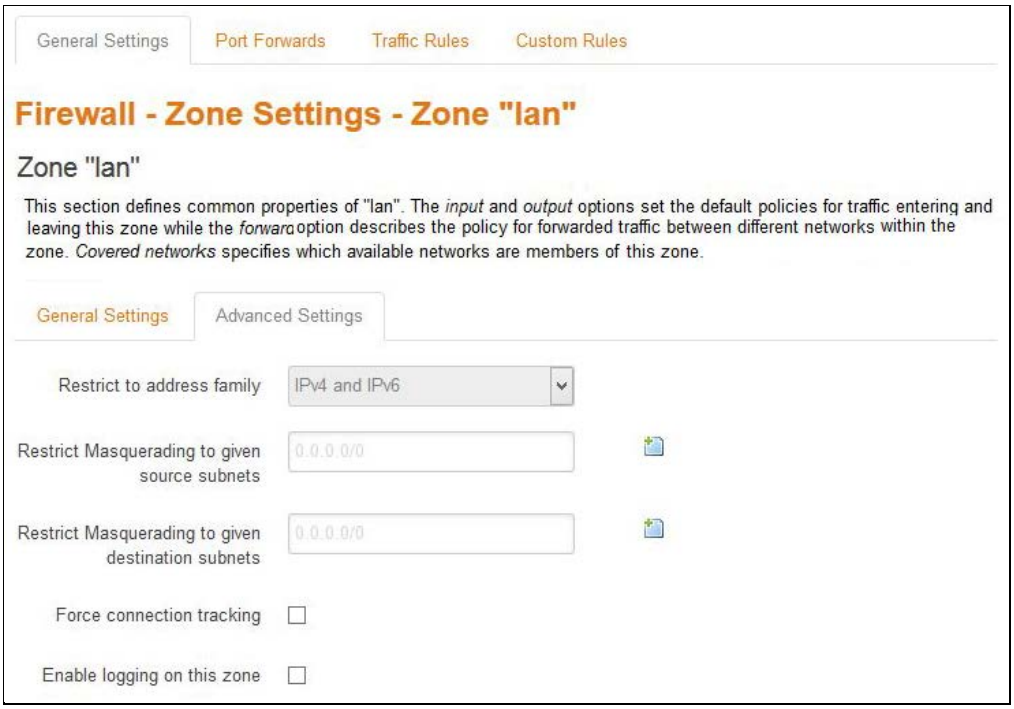
DROP

- 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)

b. Advanced Settings



Screen 10-57: Advance Configuration for Firewall Zone (LAN)

Parameters	Description
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.
Force connection tracking	Check to enable tracking of inbound connection to the router.
Enable logging on this zone	Check to enable logging of all the activities on the Zone.

Table 10.9-3: Advance Configuration for Firewall Zone (LAN)

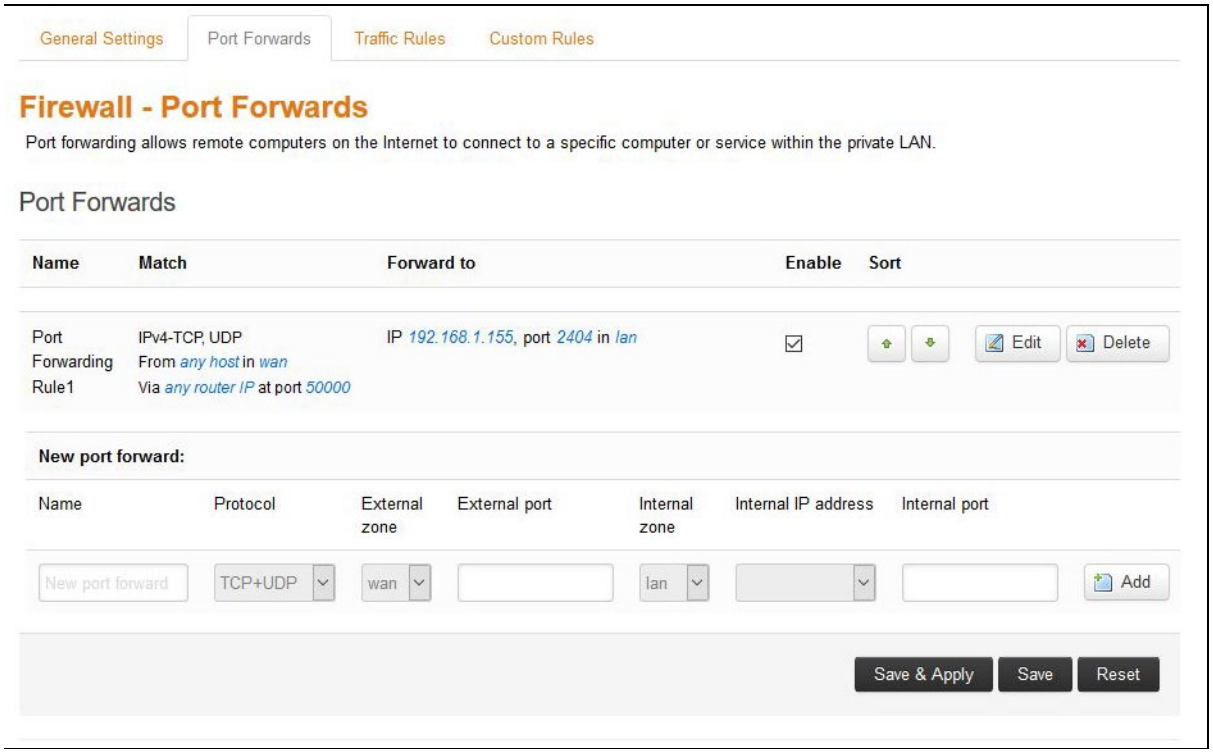
10.9.2 Port Forwarding

Network > Firewall > Port Forwarding

Since default configuration is all WAN side ports closed, port forwarding allows opening of a particular port and redirecting the connection (and data) on that port from an external IP to an internal IP

a. Configuring Port Forwarding

All the WAN side ports on E200 Router 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, E200 Router provides advance port-forwarding configurations, where in addition to WAN port; WAN IP Address can be mapped with LAN IP Address and LAN port.



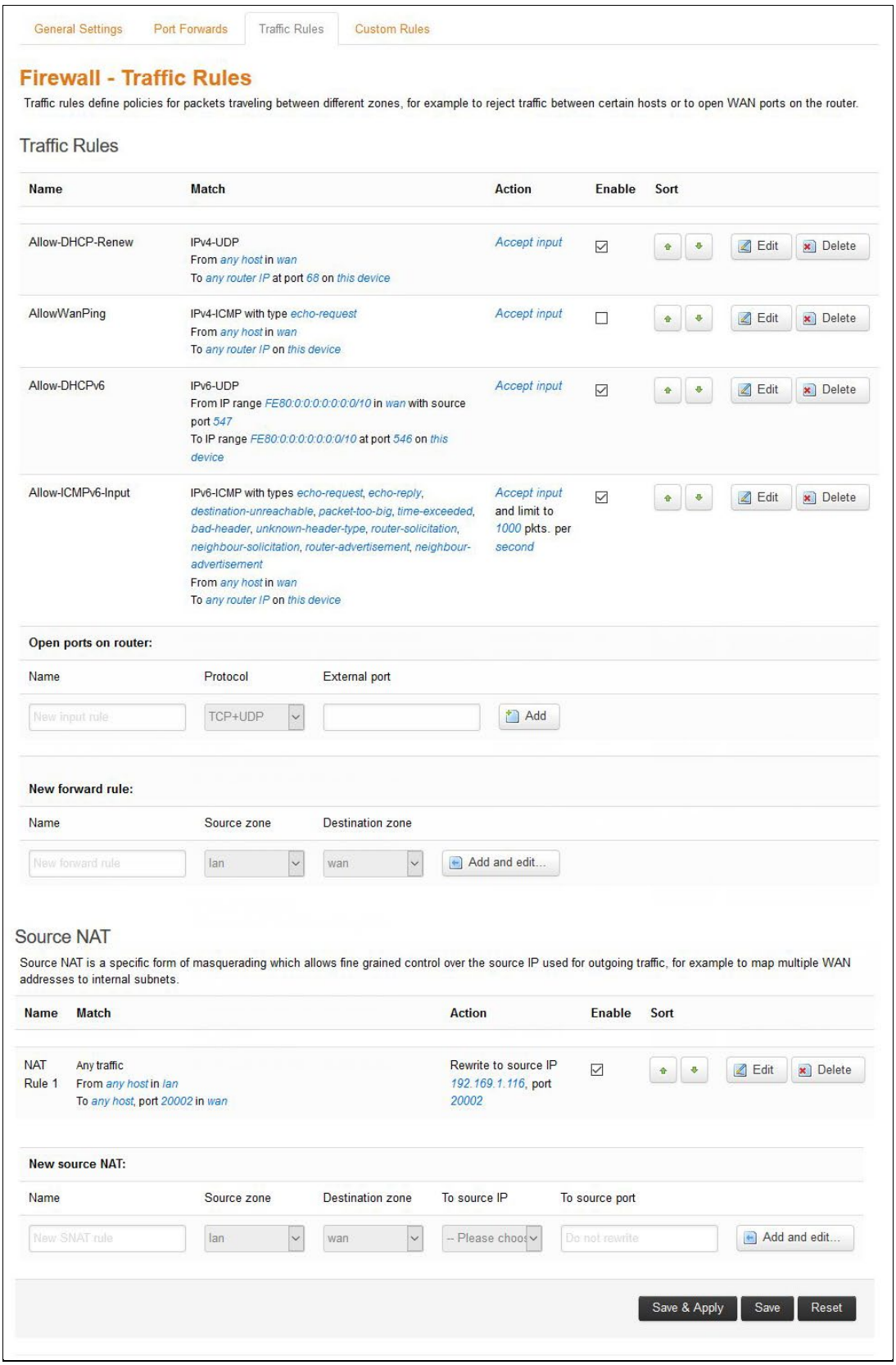
Screen 10-58: Port Forwarding Configuration for Firewall Zone

Parameters	Description
Port Forwards	
Name	Displays the name of the Port Forwarding Rule.
Match	Displays the WAN TCP/UDP ports for matching the conditions before forwarding it to LAN device.
Forward to	The destination IP Address to which the traffic must be forwarded.
Enable	Check to enable the Port Forwarding rule.
Sort	Click to sort the configured Port Forwarding Rule.

Table 10.9-4: Port Forwarding Configuration for Firewall Zone

10.9.3 Traffic Rules

Network > Firewall > Traffic Rules



Screen 10-59: Traffic Rule Overview for Firewall Zone

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.
Enable	Check to enable the Traffic Rule.
Sort	Click to sort the configured Traffic Rule.
Open ports on router **Opens the external port to access the Router for various tasks.** **By default, all the ports are closed except the available in list of Open ports.**	
Name	Enter the name of the Open port.
Protocol	Select the Protocol from the available options. **Available Options** • **TCP –** Allows only TCP traffic to the open port • **UDP –** Allows only UDP traffic to the open port • **TCP+UDP –** Allows both TCP and UDP traffic to the open port
External port	Enter the Port Number that must be opened.
New forward rule	
Name	Enter the name of the Forwarding Rule that will be used for forwarding traffic between two Firewall Zones.
Source zone	Select the source firewall zone.
Destination zone	Select the destination firewall zone.
Source NAT **Source NAT is a specific form of masquerading which allows fine grained control over the Source IP Address used for outgoing traffic.**	
Name	Displays the name of the Source NAT rule.
Match	Displays the details of the Source NAT Rule configuration and the conditions in which the rule is applicable.
Action	Action to be taken on the Source NAT when the rule conditions are satisfied.
Enable	Check to enable the Source NAT Rule.
Sort	Click to sort the configured Source NAT Rule.
New source NAT	
Name	Enter the name of the New source NAT.
Source zone	Select the source zone.
Destination zone	Select the destination zone.

Parameters	Description
	Note • ***Destination Zone must not be same as the Source Zone.***
To source IP	Select the source IP Address.
To source port	Select the source port.

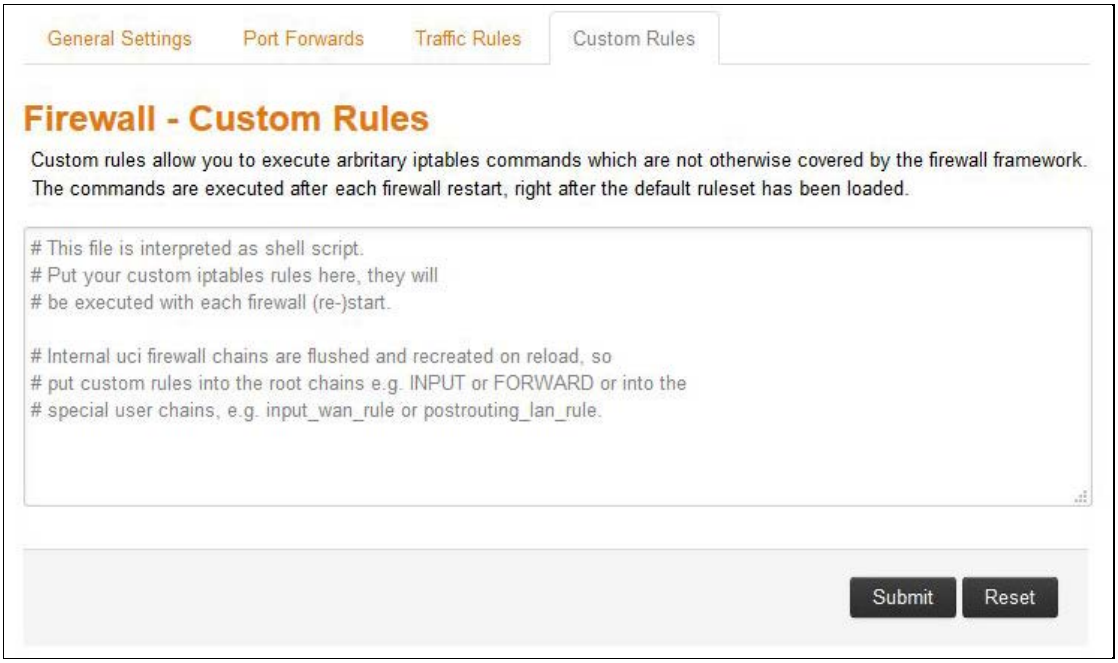
Table 10.9-5: Traffic Rule Overview for Firewall Zone

What can be achieved out of Traffic Rules

- 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

10.9.4 Custom Rules

Network > Firewall > Custom Rules



Screen 10-60: Custom Rules Configuration for Firewall Zone

You can configure customized rules for Firewall using shell script.

11. Services

E220 is equipped with features like SMS configuration, GPS and digital I/O. Services are the set of features complimenting the routing features. These features are:

- VPN
- Agents
- SMS
- DOTA
- Serial
- GPS
- Last Gasp
- Content Filtering
- Reporting Agent
- Events
- Dynamic DNS

11.1 VPN

Services > 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 is 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.

The table compares the type of VPN supported by various Routers.

VPN	E205	E206	E228	E225	E224	E225LITE
PPTP	Y	Y	Y	Y	Y	Y
L2TP	Y*	Y*	Y*	Y*	Y*	Y*
OpenVPN	Y	Y	Y	Y	Y	Y
IPsec	N	N	Y	Y	Y	Y
GRE	N	N	Y*	Y*	Y*	Y*

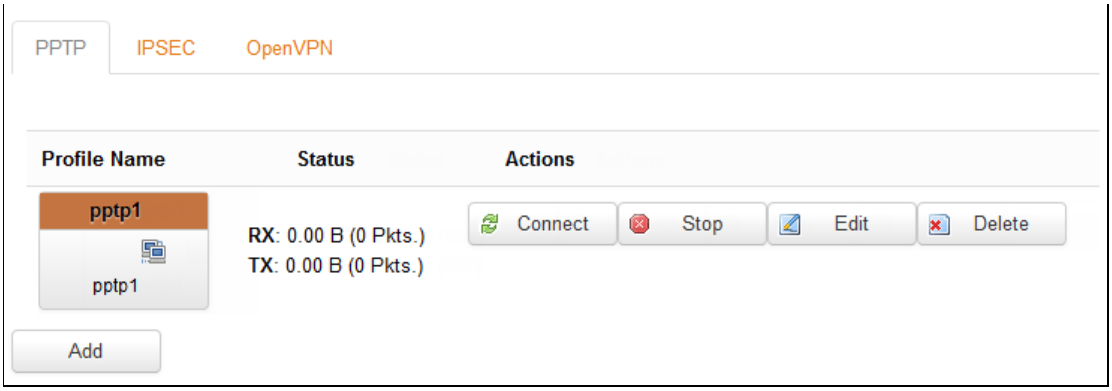
'*' – Not a part of the standard package but can be downloaded as an application package from D2Sphere.

11.1.1 PPTP

Network > Interface > PPTP

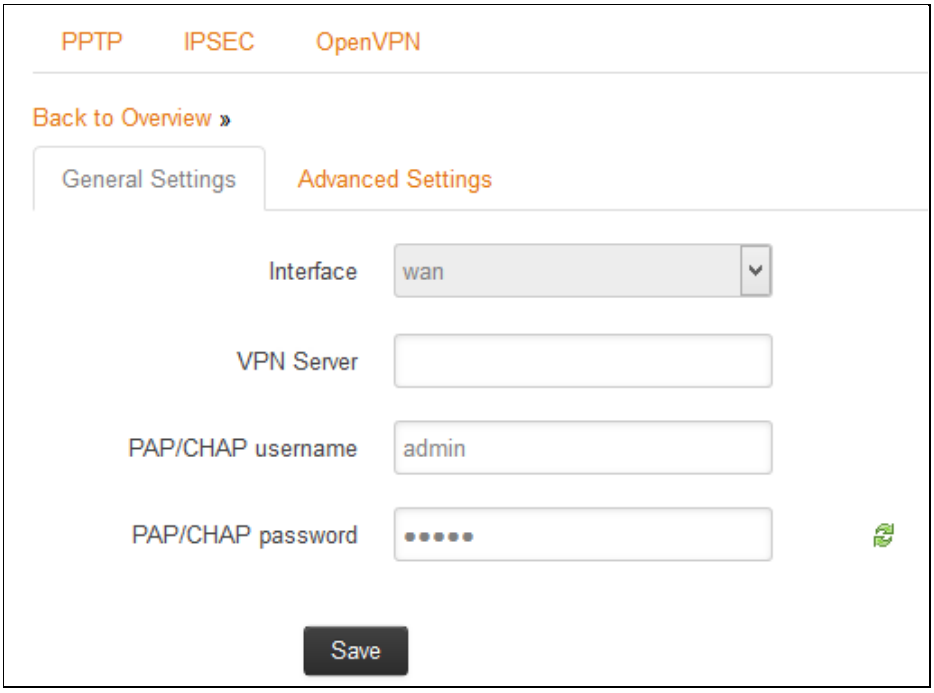
Point-to-Point Tunneling Protocol (PPTP) is the extension of Point-to-Point Protocol (PPP) for traditional dial-up network connection. It is the most common protocol that enables the corporates to implement Virtual Private Network (VPN) for extending their internal corporate network.

PPTP client/user connects to their VPN server using computer, router or any networking device that supports PPTP. A TCP control connection is then established from client to the server in order to create a virtual tunnel. PPTP provides security by authenticating the users and packet filtering. PPTP controls the mapping and managing of VPN tunnel and the data inside the tunnel by encrypting and maintaining the connection. It stores the data within a PPP packet, which are then further stored inside IP Packets to be used for their destination. PPTP encrypts and compresses these packets using PPP-based protocols such as PAP and CHAP. PPTP uses GRE (General Routing Encapsulation) to send/receive data.



Parameters	Description
Interface Overview	
Profile Name	Displays the all the configured PPTP Interfaces. The pre-configured interfaces for the router are • PPTP1 ***Note*** • ***Default Interfaces PPTP cannot be deleted.***
Status	Displays the following Interface details: • RX • TX
Actions	Select the action to be taken for the Interface. • **Connect –** Connects the interface or reconnects the already connected interface • **Stop –** Stops the Interface • **Edit –** Click to edit the Interface. • **Delete –** Click to delete the Interface.

A. General Settings

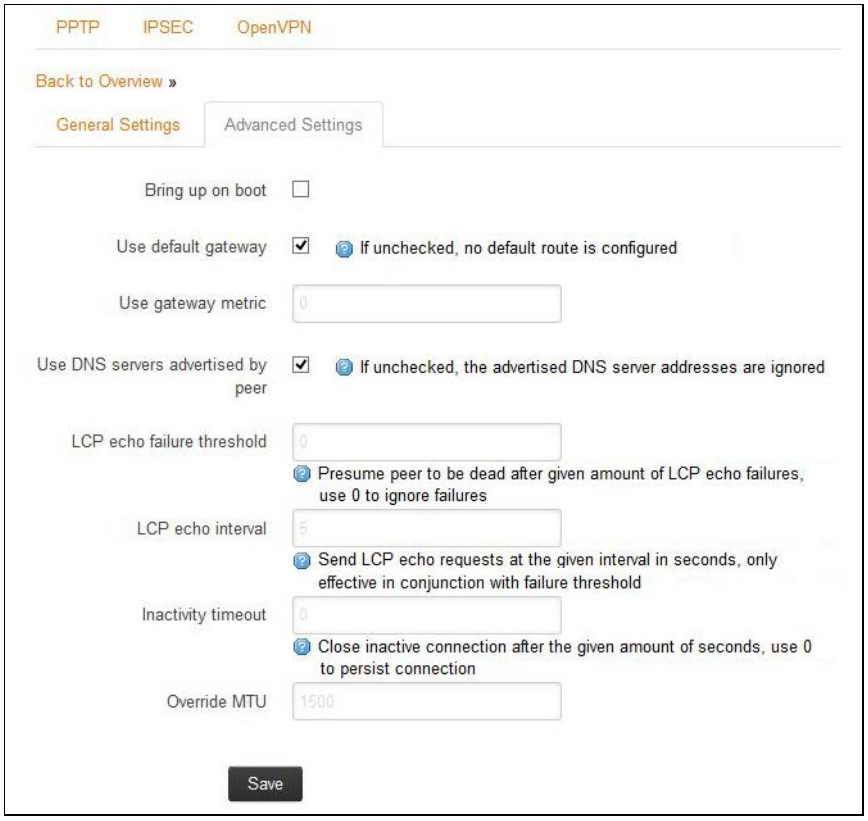


Screen 11-1: General Configurations for PPTP Interface

Parameters	Description
Interface	Select the interface to configure PPTP: • WAN • WWAN • 3G
VPN Server	Enter the DNS Name or Public IP Address of the VPN Server for PPTP connection.
PAP/CHAP username	Enter the Username for PAP/CHAP encryption.
PAP/CHAP password	Enter the Password for PAP/CHAP encryption.

Table 11.1-1: General Configurations for PPTP Interface

B. Advanced Settings



Screen 11-2: Advanced Configurations for PPTP

Parameters	Description
Bring up on boot	Allows the WAN interface to be live after every reboot. Bring up on boot for WAN interface is checked by default.
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 0.
Use DNS server advertised by peer	Allows advertising the DNS server address. Use DNS server advertised by peer for PPTP interface is checked by default.
LCP echo failure threshold	Presume peer to be dead after configured LCP echo failures. Use 0 to ignore failures
LCP echo interval	This is time the router should wait before sending an echo request to check whether the link is alive or not. The LCP echo interval by default is 5 seconds.
Inactivity timeout	The Router will wait for the LCP echo request response for the LCP Echo interval defined after every attempt. It declares LCP link as closed if it does not receive response after this defined period of

Parameters	Description
	attempts Use 0 seconds to persist the connection.
Overrride MTU	The Router will wait for the LCP echo request response for the LCP Echo interval defined after every attempt. It declares LCP link as closed if it does not receive response after this defined period of attempts Use 0 seconds to persist the connection.

Table 11.1-2: Advanced Configurations for PPTP

Note:

- ***Enabling PPTP will also enable a 20mins PPTP watchdog which will reboot the router in absence of an active PPTP connection for a period of 20 mins.***

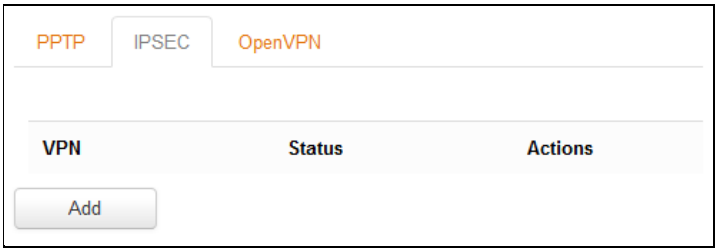
11.1.2 IPSec (Internet Protocol Security)

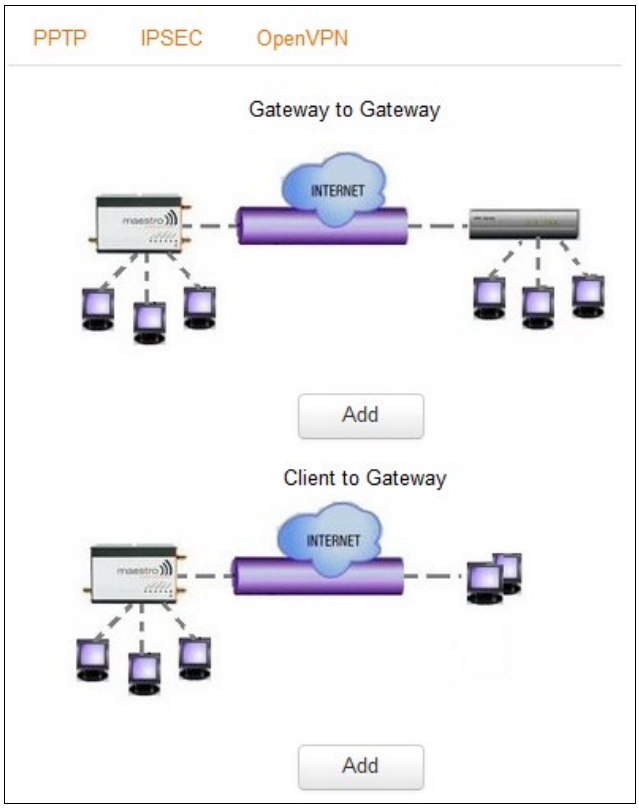
Network > Interface > IPSec

IP Security (IPSec) is a suite of protocols designed for cryptographically secure communication at the IP layer (layer 3). Lantronix Router E220 uses IPSec standard i.e. IPSec protocol to protect traffic. In IPSec, the identity of communicating users is checked with the user authentication based on Digital Certificates, public keys or Pre-shared Keys.

IPSec is used for both Gateway-to-Gateway VPN connection and Client-to-Gateway VPN connection.

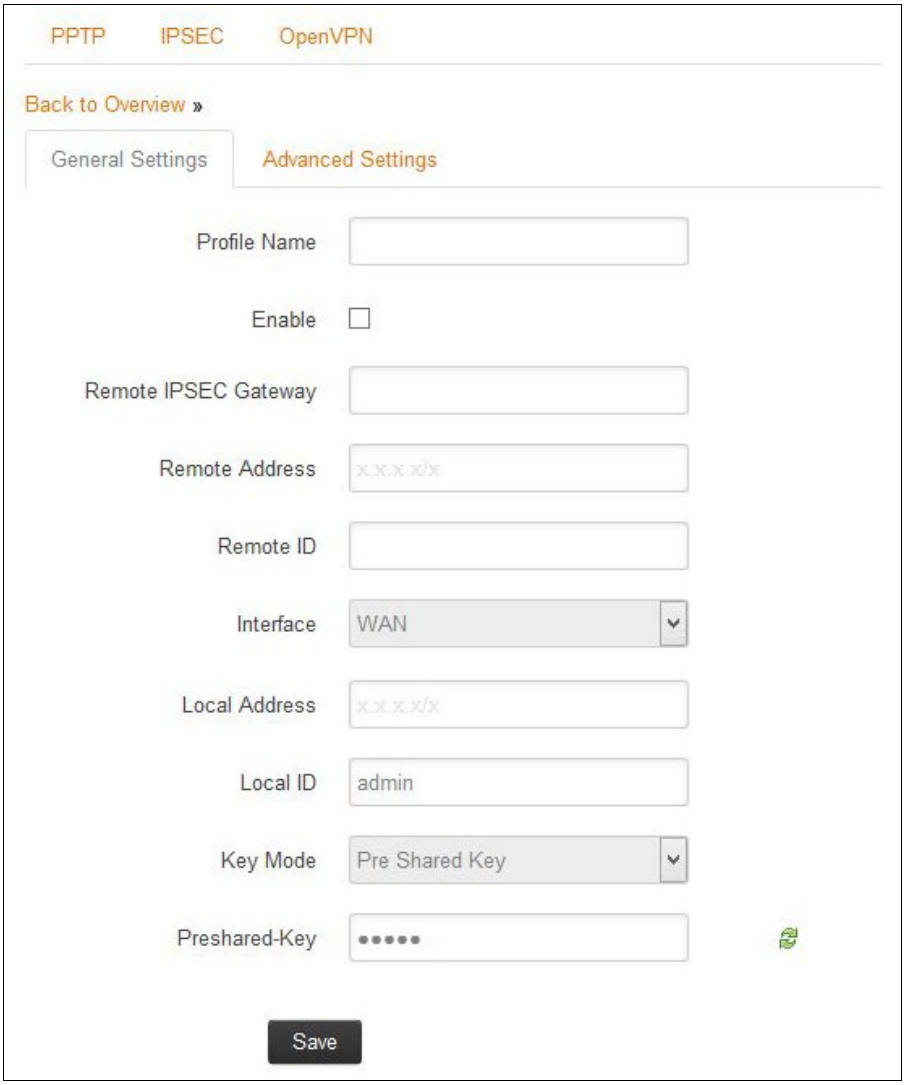
- Click Add button on IPSec page.
- Select the type of IPSec-VPN connection and click Add button for respective connection.





B. Gateway to Gateway

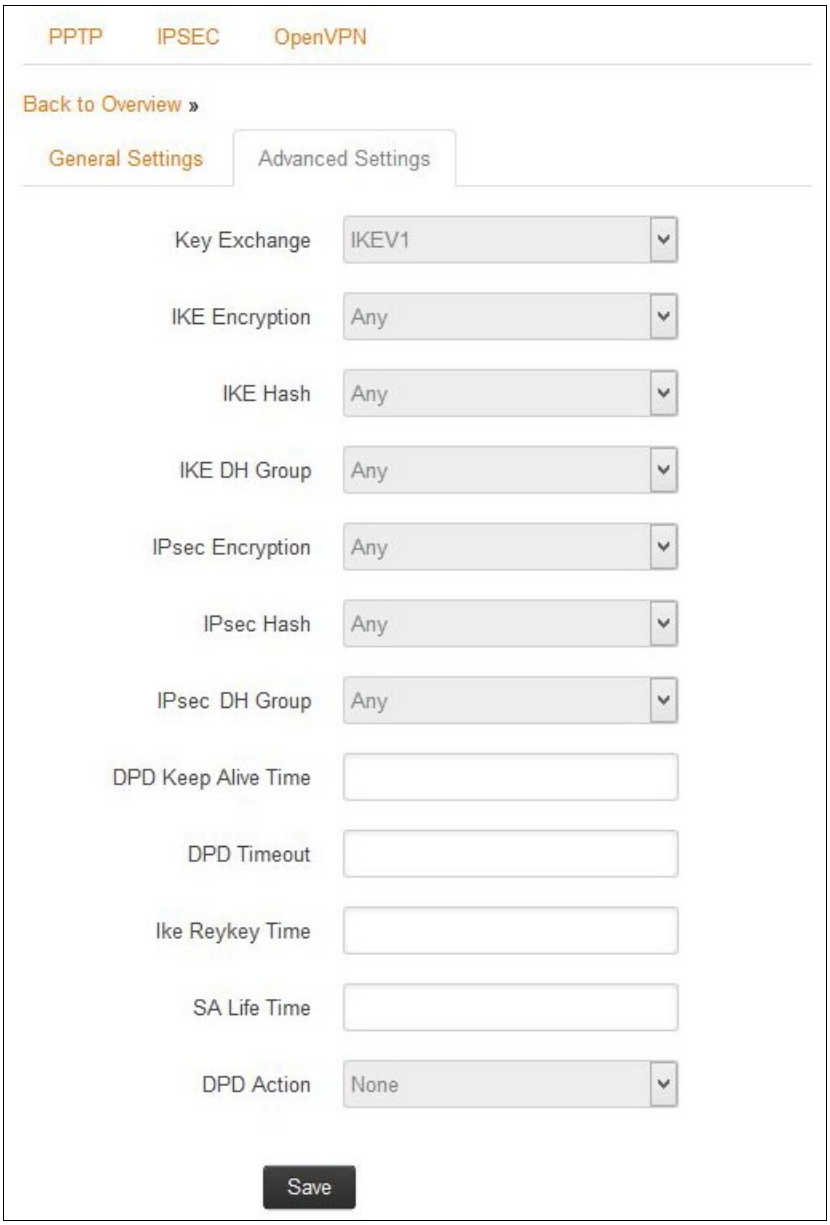
a. General Settings



Parameters	Description
Profile Name	Enter the Profile Name to identify the Gateway–to-Gateway IPSec VPN connection.
Enable	Check to enable the connection.
Remote IPSec Gateway	Enter the IP Address or domain name of the Remote IPSec Gateway server.
Remote Address	Enter the IP Address of the remote network for use on the VPN connection.
Remote ID	Enter the Domain Name of the remote network for use on the VPN connection.
Interface	Select the interface to configure IPSec: • WAN • WWAN • 3G

Parameters	Description
	• Auto Selecting a particular interface will bind the IPSec tunnel to that particular interaface. Selecting Auto means that the IPSec tunnel will be created over an active interface as defined in Load Balancer policies.
Local Address	Enter the IP Address and subnet mask of local network for use on the VPN connection.
Local ID	Enter the Domain Name of the local network for use on the VPN connection.
Key Mode	Select the type of Key mode in use for VPN connection: • Preshared Key • RSA Keys
Preshared-Key	Enter the Preshared key. The peer uses the key to authenticate each other from Internet Key Exchange.

b. Advanced Settings



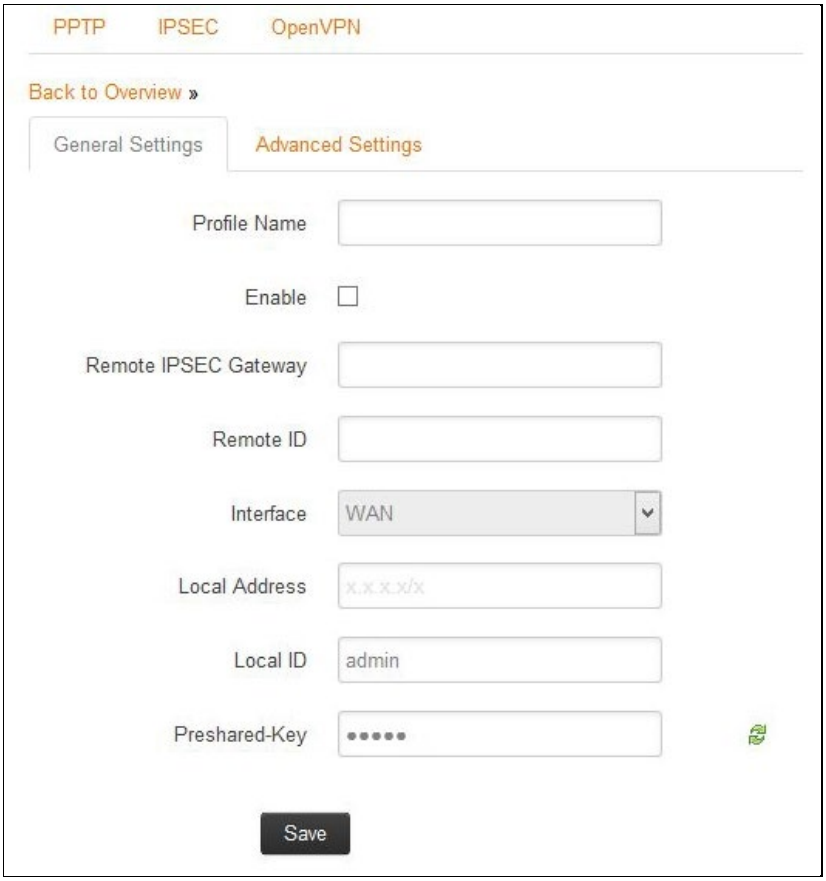
Parameters	Description
Key Exchange	Select the mode of encryption key exchange between two communicating peers: • IKEV1 • IKEV2 The default mode of Key Exchange is IKEV1.
IKE Encryption	Select the cipher type to use for the Internet Key Exchange (IKE): • Any • MD5 • SHA1

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

Parameters	Description
	The hash type “Any” is the default IPSec hash.
IPSec DH Group	Select the desired Diffie-Hellman group to use: • Any • Group 1 (768) • Group 2 (1024) • Group 5 (1536) • Group 14 (2048) • Group 15 (3072) • Group 16 (4096) • Group 15 (6144) • Group 16 (8192) Higher groups are more secure but also require longer to generate key. The group “Any” is selected by default.
DPD Keep Alive Time	Enter the time in seconds for interval between Dead Peer Detection keep alive messages.
DPD Timeout	Enter the time in seconds of no response from peer before Dead Peer Detection times out.
IKE Re-key Time	Enter the time in seconds between changes of the encryption key. To disable changing the key, set it to 0.
SA Life Time	Enter the time in seconds for the security association lifetime.
DPD Action	Select the desired Dead Peer Detection action. This action must be taken when a dead Internet Key Exchange Peer is detected.

C. Client to Gateway

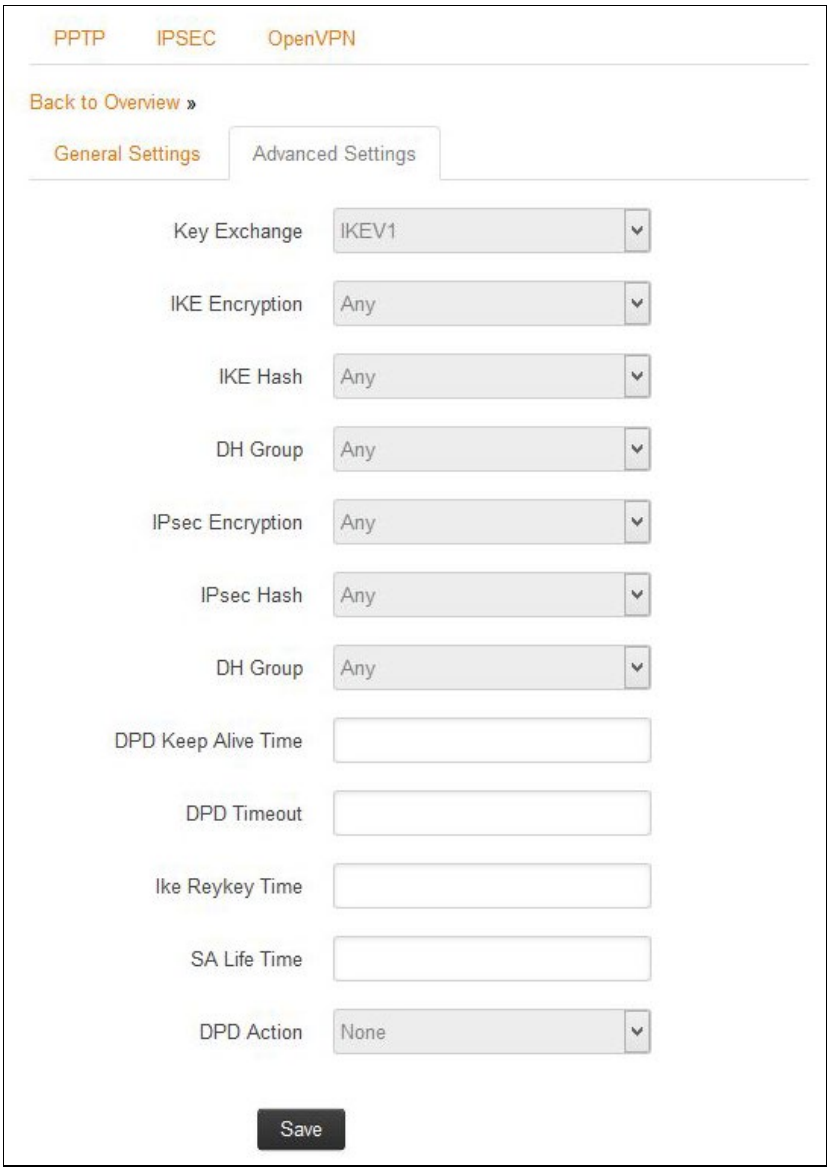
a. General Settings



Parameters	Description
Profile Name	Enter the Profile Name to identify the Client–to-Gateway IPSec VPN connection.
Enable	Check to enable the connection.
Remote IPSec Gateway	Enter the IP Address or domain name of the Remote IPSec Gateway server.
Remote ID	Enter the Domain Name of the remote network for use on the VPN connection.
Interface	Select the interface to configure IPSec: • WAN • WWAN • 3G • Auto Selecting a particular interface will bind the IPSec tunnel to that particular interaface. Selecting Auto means that the IPSec tunnel will be created over an active interface as defined in Load Balancer policies.
Local Address	Enter the IP Address and subnet mask of local network for use on the VPN connection.

Parameters	Description
Local ID	Enter the Domain Name of the local network for use on the VPN connection.
Preshared-Key	Enter the Preshared key. The peer uses the key to authenticate each other from Internet Key Exchange.

b. Advanced Settings



Parameters	Description
Key Exchange	Select the mode of encryption key exchange between two communicating peers: • IKEV1 • IKEV2 The default mode of Key Exchange is IKEV1.
IKE Encryption	Select the cipher type to use for the Internet Key Exchange (IKE): • Any • MD5 • SHA1 • SHA2

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

Parameters	Description
	The hash type “Any” is the default IPSec hash.
IPSec DH Group	Select the desired Diffie-Hellman group to use: • Any • Group 1 (768) • Group 2 (1024) • Group 5 (1536) • Group 14 (2048) • Group 15 (3072) • Group 16 (4096) • Group 15 (6144) • Group 16 (8192) Higher groups are more secure but also require longer to generate key. The group “Any” is selected by default.
DPD Keep Alive Time	Enter the time in seconds for interval between Dead Peer Detection keep alive messages.
DPD Timeout	Enter the time in seconds of no response from peer before Dead Peer Detection times out.
IKE Re-key Time	Enter the time in seconds between changes of the encryption key. To disable changing the key, set it to 0.
SA Life Time	Enter the time in seconds for the security association lifetime.
DPD Action	Select the desired Dead Peer Detection action. This action must be taken when a dead Internet Key Exchange Peer is detected.

11.1.3 L2TP

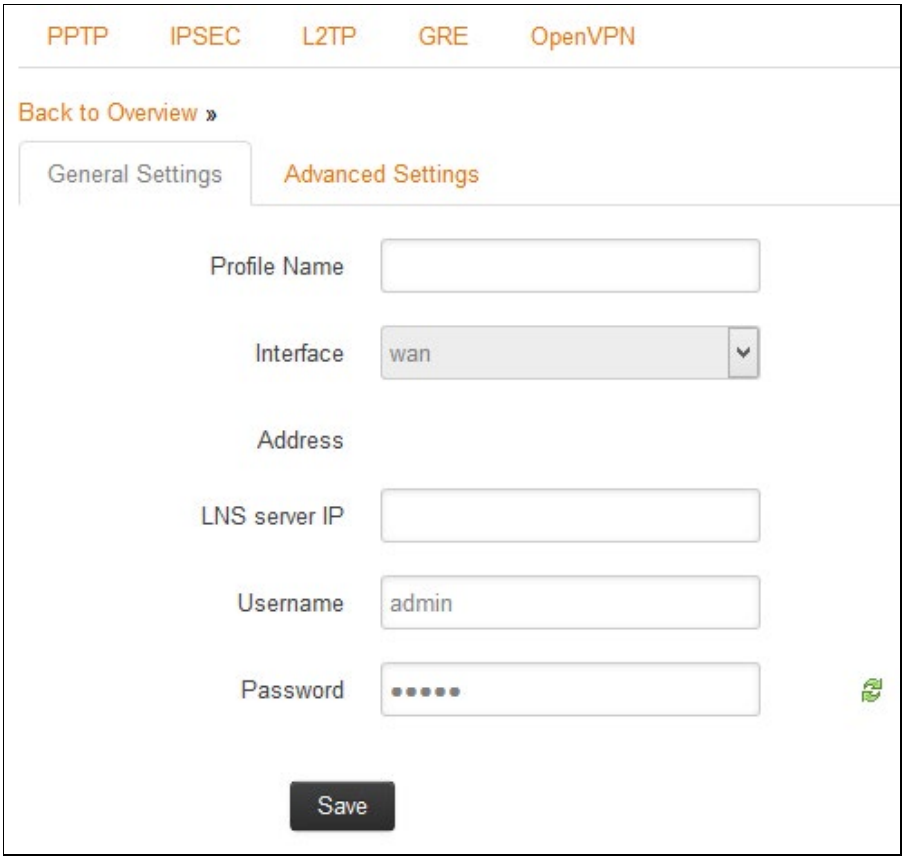
Lantronix router supports L2TP VPN. L2TP is not a part of the base firmware package and needs to be downloaded from D2Sphere.

For more information on how to download refer to Software on page 56.

Network > Interface > L2TP

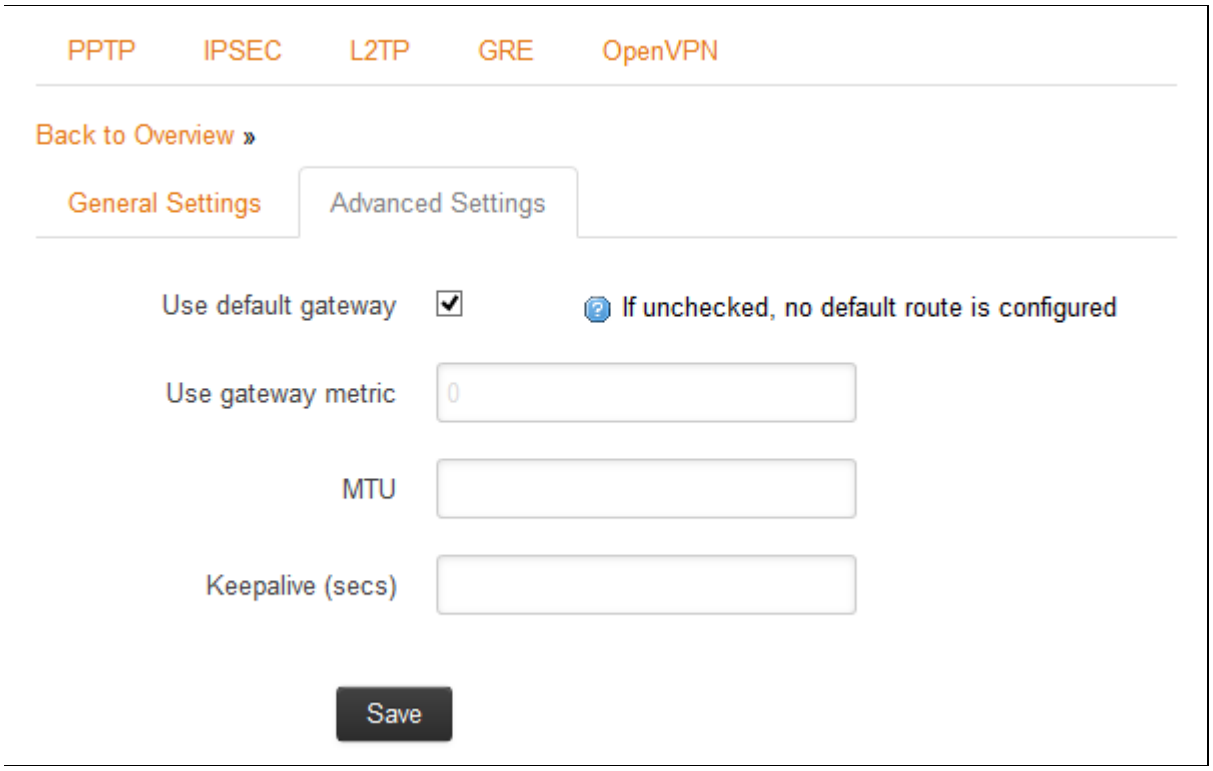
Parameters	Description
Interface Overview	
Profile Name	Displays the all the configured L2TP Interfaces. The pre-configured interfaces for the router are • L2TP1
Status	Displays the following Interface details: • RX • TX
Actions	Select the action to be taken for the Interface. • **Connect –** Connects the interface or reconnects the already connected interface • **Stop –** Stops the Interface • **Edit –** Click to edit the Interface. • **Delete –** Click to delete the Interface.

D. General Settings



Parameters	Description
Interface	Select the interface to configure PPTP: • WAN • WWAN • 3G • Auto Selecting a particular interface will bind the L2TP tunnel to that particular interaface. Selecting Auto means that the L2TP tunnel will be created over an active interface as defined in Load Balancer policies.
Address	Will display the IP address of the interface using which L2TP tunnel has been created
LNS Server	Enter the DNS Name or Public IP Address of the VPN Server for L2TP connection.
username	Enter the Username
password	Enter the Password

E. Advanced Settings

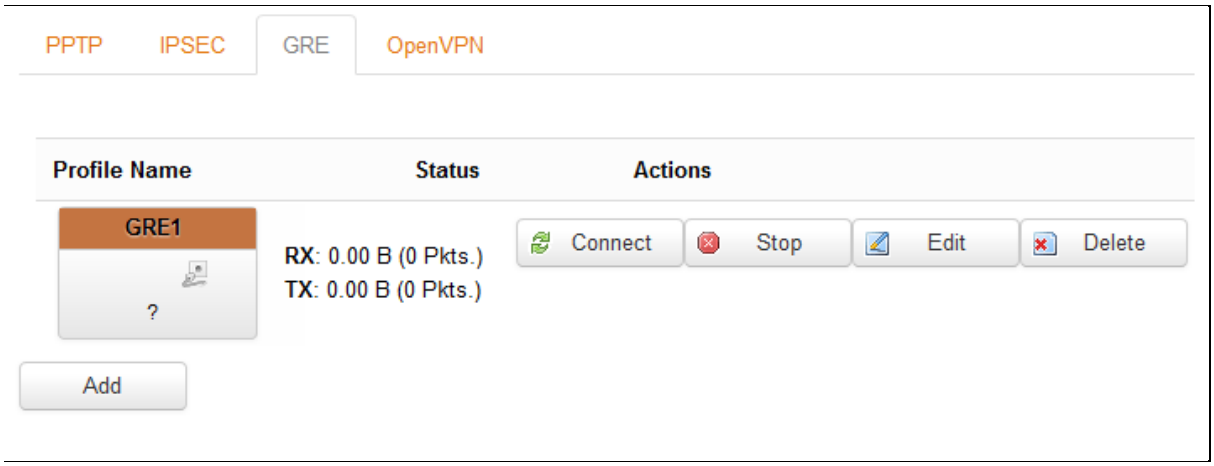


Parameters	Description
Use default gateway	Click to configure a default gateway route. None of the gateway routes are configured by default. If this is not checked, the traffic will not be routed via L2TP tunnel unless specific static routes are configured.
Use gateway metric	Enter the gateway metric. The default metric is 0.
MTU	If you wish to define your MTU size, you can. Blank will mean auto MTU size
Keepalive	The router will send keep alive packets to the L2TP server at the configured interval

11.1.4 GRE

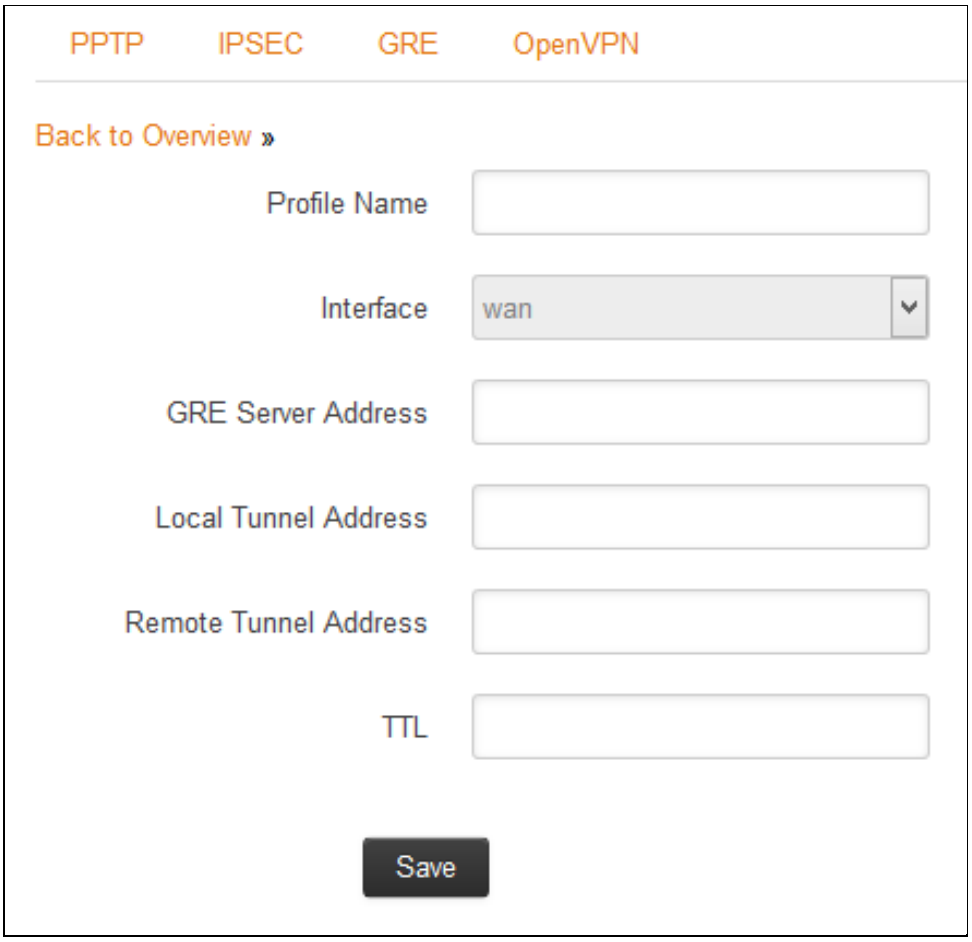
The E2xx series router supports GRE. GRE is not a part of the base firmware package and needs to be downloaded from D2Sphere.

For more information on how to download, please refer to section 10.3 - Softwares



Parameters	Description
Interface Overview	
Profile Name	Displays the all the configured GRE Interfaces. The pre-configured interfaces for the router are • GRE1
Status	Displays the following Interface details: • RX • TX
Actions	Select the action to be taken for the Interface. • **Connect –** Connects the interface or reconnects the already connected interface • **Stop –** Stops the Interface • **Edit –** Click to edit the Interface. • **Delete –** Click to delete the Interface.

a. Edit



Parameters	Description
Profile Name	Enter the Profile Name to identify the GRE connection.
Interface	Select the interface to configure PPTP: • WAN • WWAN • 3G Unlike other VPNs, GRE cannot move from one interface to another. It needs to be binded to a particular interface.
GRE Server Address	Enter the IP Address or domain name of the Remote GRE server.
Local Tunnel Address	Address to assign to the local GRE tunnel
Remote Tunnel Address	Address at the remote host (Router A) GRE tunnel
TTL	

11.1.5 OpenVPN

Services > VPN > OpenVPN

Open VPN 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 Open SSL library to provide encryption of both the data and control channels. Open VPN can run over User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) transports, multiplexing created SSL tunnels on a single TCP/UDP port. Open VPN fully supports IPv6 as protocol of the virtual network inside a tunnel and the Open VPN 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.

E220 series supports Open VPN client, Server and Pass Through.

A. Open VPN Client

You can access the Open VPN client in Services / Open VPN.
Open VPN Client will attach itself to the configured Open VPN server over any available WAN interface. If the auto-connect function is enables, Open VPN will not only connect over available WAN but also switch between WANs as and when one WAN fails-over to another and also auto starts in every reboot. This can be achieved by clicking on the enabled tick box.
You can either edit the sample client or create your own configuration from ground up.

Note

- ***Only OpenVPN client is supported.***
- ***You must manually enter the DNS from Network > DHCP and DNS.***

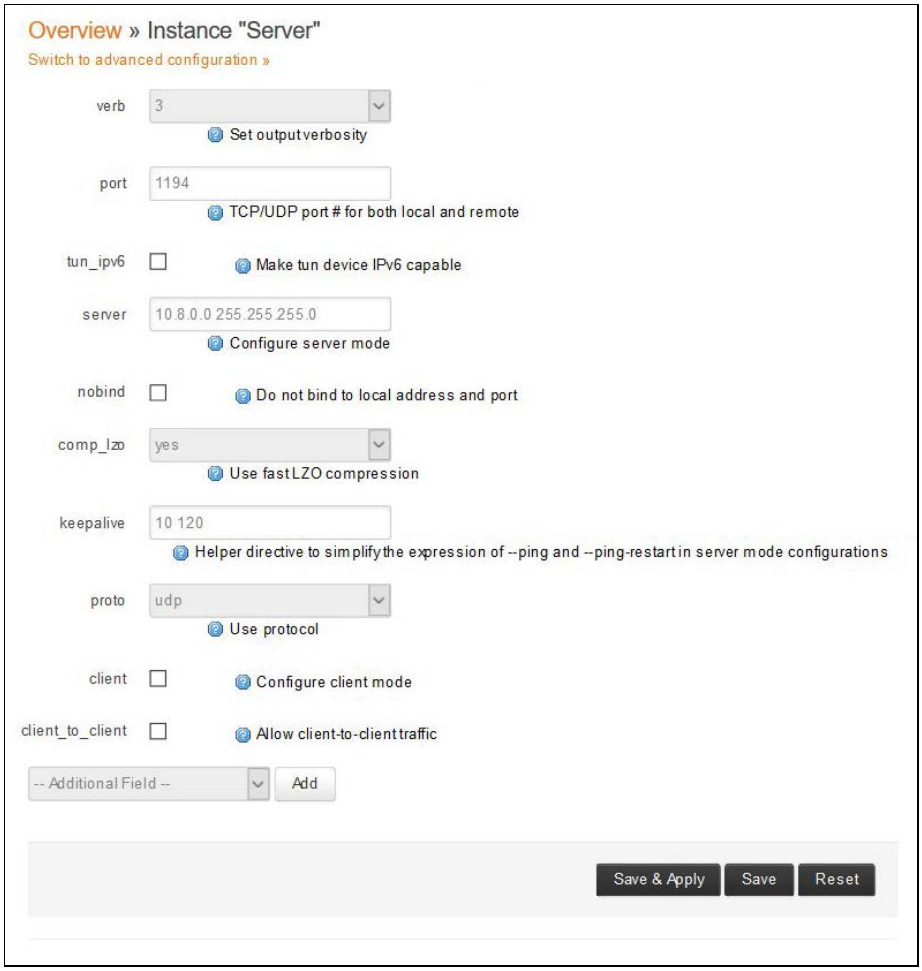
Screen 11-3: OpenVPN Service Configuration

Parameters	Description
OpenVPN instances	
Enabled	Click Enabled to allow restarting of OpenVPN in case the router is

Parameters	Description
	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.
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.
Add	Configure a customize configuration for server or client.

Table 11.1-3: OpenVPN Service Configuration

B. Edit



Screen 11-4: Edit OpenVPN Service Configuration

Parameters	Description
Verb	Select the output verbosity level. Higher the verbosity, higher will be the internal log details.
Port	Enter the TCP/UDP port number for local and remote
Tun_ipv6	Enable the tunnel to handle IPv6 Traffic
Server	Enter the IP Address and Subnet Mask for server mode
Nobind	Check to enable Nobind. Enabling Nobind, does not allow the binding of local address and port.
Comp_lzo	Select Yes to use fast lzo compression.
Keepalive	Server sends the keep alive packets to clients
Proto	Select the protocol TCP and UDP.
Client	Check to enable the OpenVPN client mode and disable the OpenVPN server mode. ***Note*** • ***Only OpenVPN Client mode is supported in Router Firmware Version Lantronix E205 2.0.0 and Lantronix E206 2.0.0***
client_to_client	Check to facilitate communication between the Clients connected over the same VPN.

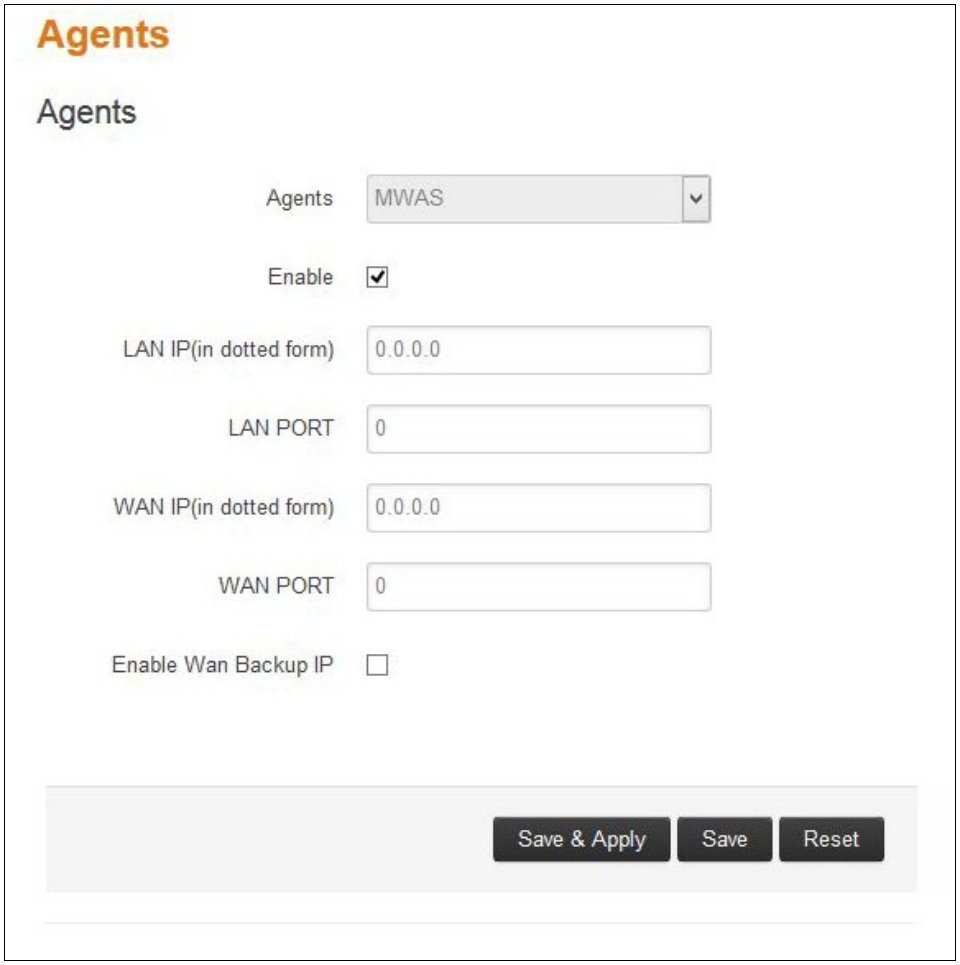
Table 11.1-4: OpenVPN Service Configuration

11.2 Agents

Services > Agents

Agents are customized applications loaded on the router that are basically used for communication 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 Routers on the field (mainly using dynamic IP Address SIM cards) and a MWAS Server located centrally, communicating with the head-end system.



Screen 11-5: Agent Configurations

Parameters	Description
Agents	
Agents	Select the Agent from the dropdown list: • MWAS – Lantronix Wireless Acquisition System
Enable	Click to enable the selected agent.
LAN IP(in dotted form)	Enter the IP Address of remote/field device.
LAN PORT	Enter the Port number of remote/field device.
WAN IP(in dotted form)	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. Enter the IP Address of backup M2M Gateway. Enter the Port number of backup M2M Gateway.

Table 11.2-1: Agent Configurations

11.3 SMS

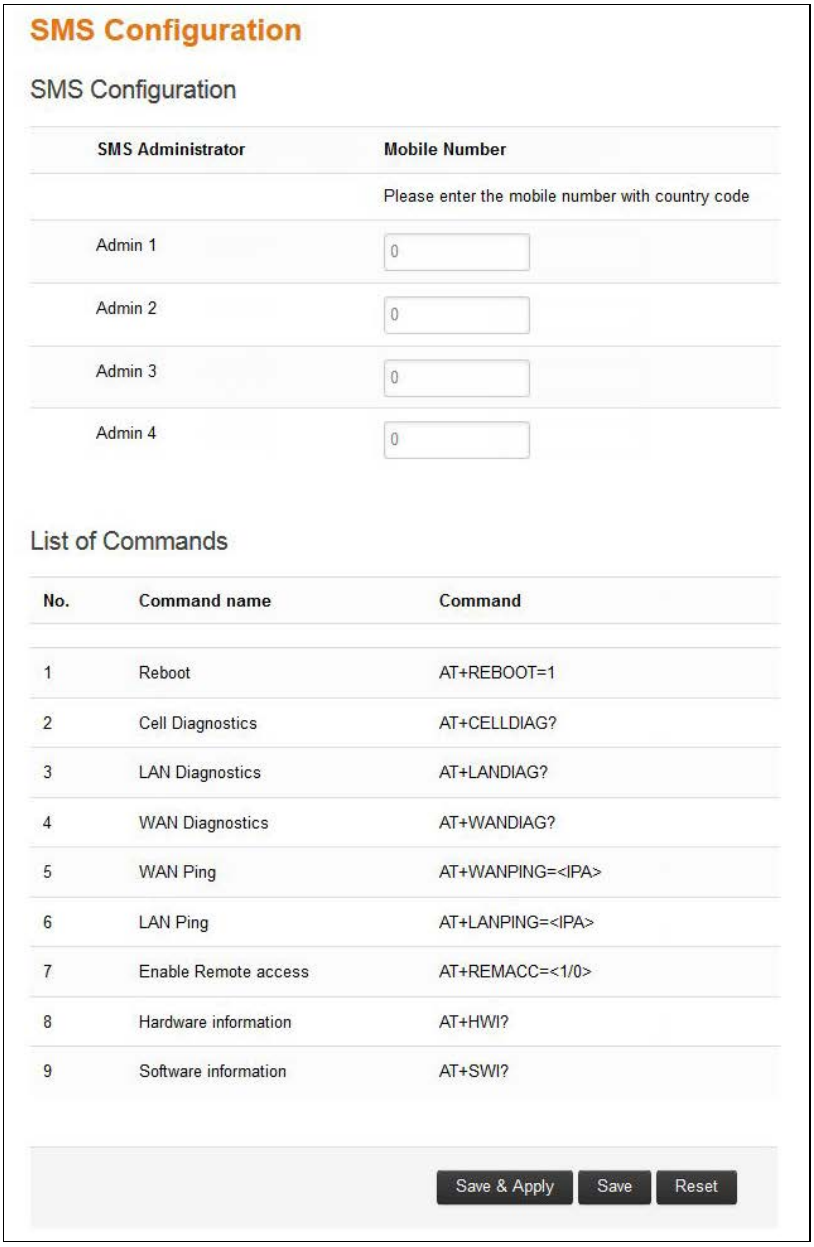
Services > SMS

11.3.1 SMS Configuration

Services > SMS > SMS Configuration

SMS diagnostic let you configure up to 4 admins to receive diagnostic information of the router after a command is send by SMS.

International number format is as follow: <countrycode><phonenumber> without a preceding special character “plus (+)”.
E.g. 919876543210



Screen 11-6: SMS Service Configurations

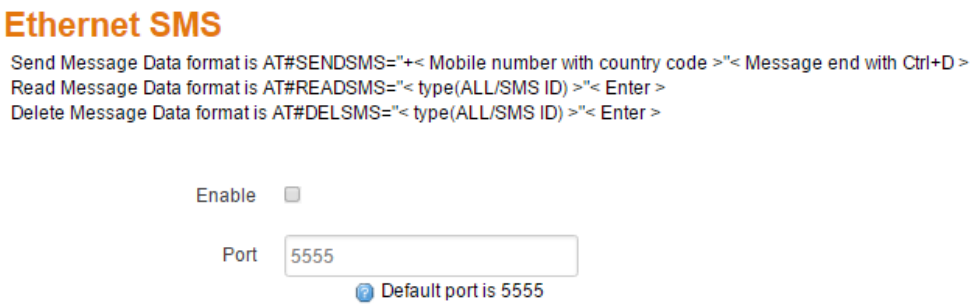
Parameters	Description
SMS Configuration	
SMS Administrator	Displays the number of Administrators configured to receive the diagnostics information of the router after they send the command using SMS. Maximum 4 SMS Administrator can be configured. ***Note*** • ***If no number is configured than the router will accept SMS from any number.***
Mobile Number	Enter the mobile number. The format of mobile number must be: • <countrycode><phonenumber> E.g. 919876543210 ***Note*** • ***The phone number must not include a special character "plus (+)" preceding it.*** If no number is configured than the router will accept SMS from any number.
List of Commands	
Command name	Command
AT+REBOOT=1	Reboot: reboot the modem
AT+CELLDIAG?	Cell diagnostics: will give you IMEI, CREG, COP, CSIG
AT+LANDIAG?	LAN diagnostics: Will give LAN IP address,
AT+WANDIAG?	Wired WAN diagnostics:
AT+WANPING=<IPA>	Wired WAN ping: will ping the wired WAN interface
AT+LANPING=<IPA>	LAN ping: will ping the wired LAN interface
AT+REMACC=<1/0>	Remote access: will enable; AT+REMACC=<1> or disable AT+REMACC=<0> remote access
AT+HWI?	Hardware information: will give you hardware information such as model number
AT+SWI?	Software information: will give you software information such as firmware version

Table 11.3-1: SMS Service Configurations

11.3.2 Ethernet SMS

Services > SMS > Ethernet SMS

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



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

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

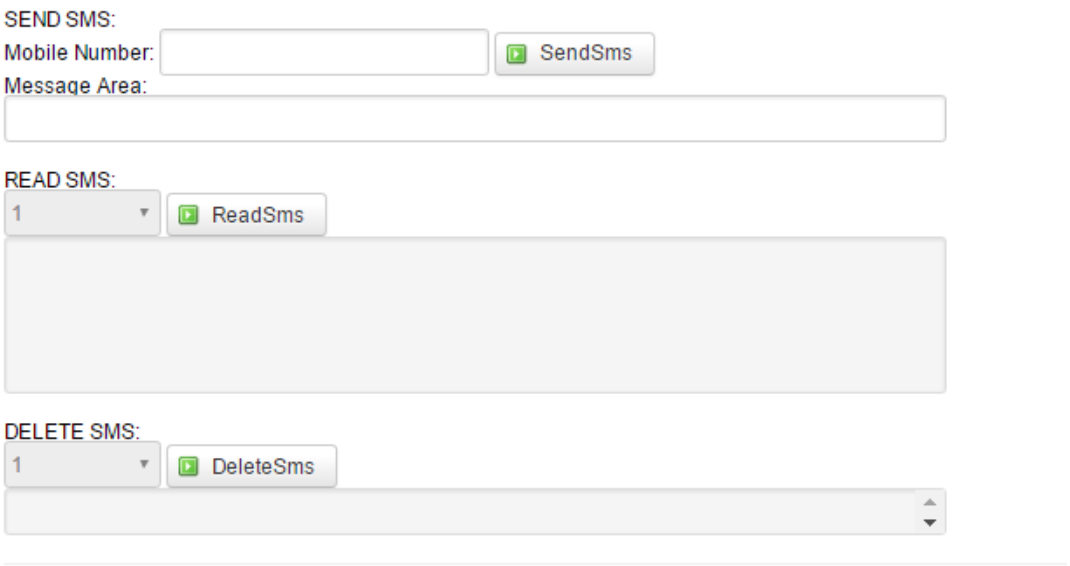
To send an SMS
AT#SENDSMS=+<Mobile Number with Country Code><Message with CTRL+D>

To read an incoming SMS
AT#READSMS=<ALL or SMS ID><Enter>

To delete and SMS
AT#DELSMS=<ALL or SMS ID><Enter>

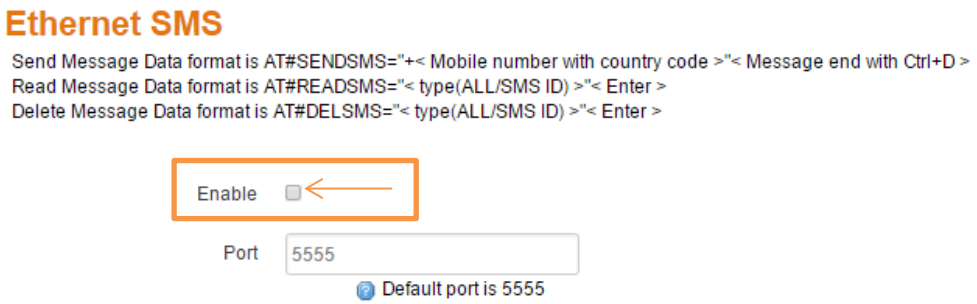
The internal SMS buffer is 10 messages – meaning, 11th incoming SMS will be over written on the 1st SMS

Sending SMS from Web Interface: You can also send SMS, read SMS and delete SMS from the Web GUI as shown in the screenshot below



Note:

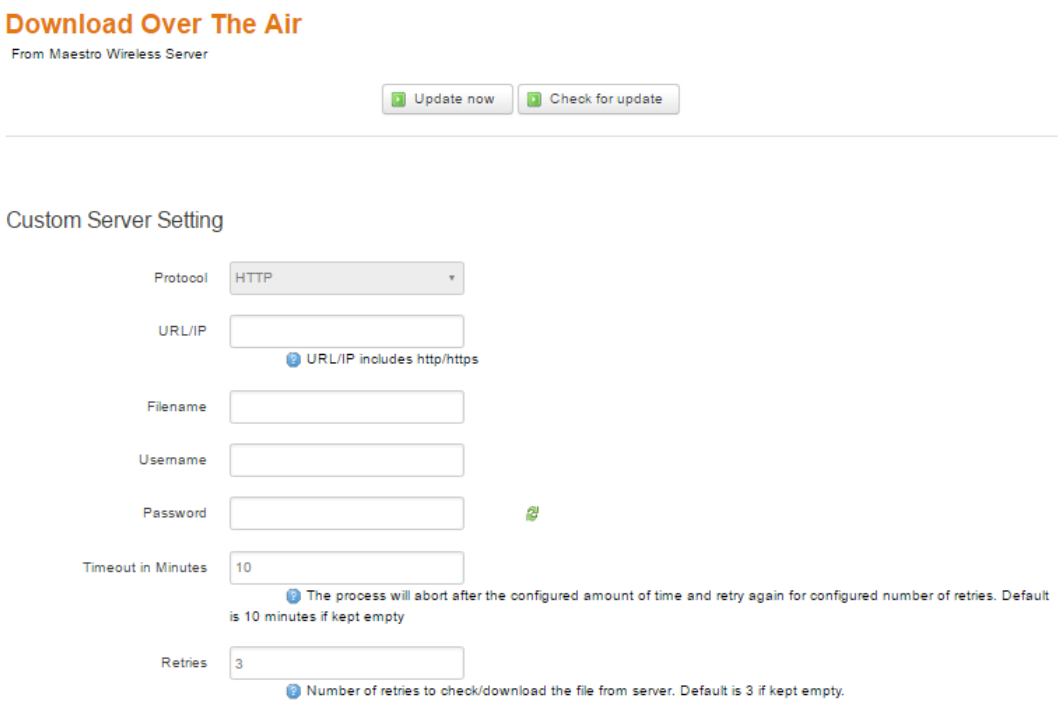
- ***To activate this feature, you need to first select enable and save and apply the settings as shown below***



11.4 DOTA

Services > DOTA

DOTA (download over the air) will allow you to remotely update your firmware, enter your server IP address the filename, username and password.



Screen 11-4: DOTA Service Configuration

Parameters	Description
Update now	Click Update now button to download a latest firmware version from HTTP/HTTPS Server. In absence of DOTA server, the either from D2Sphere
Check for update	Click to check for available updates on D2Sphere.
Custom Server Settings	
If customer server is not configured, DOTA service will configure D2Sphere server.	
HTTP/HTTPS Server	Select the type of your custom server
URL	Enter the IP / URL of custom DOTA server
Filename / Username / Password	Enter the name of the File to be accessed for updates and credentials of the server.
Timeout in Minutes	Enter the time in minutes expected to download the latest firmware file. The download process will automatically get aborted after the configured time. The default Expected time is 10 minutes.
Retries	Enter the number of retries to check and download the latest

Parameters	Description
	firmware file from the server. The default number of retries is 3.

Table 11.4-1: DOTA Service Configuration

Note:

- ***DOTA can also be triggered using SMS by sending an SMS AT+DOTA=1 from a registered Mobile Number***

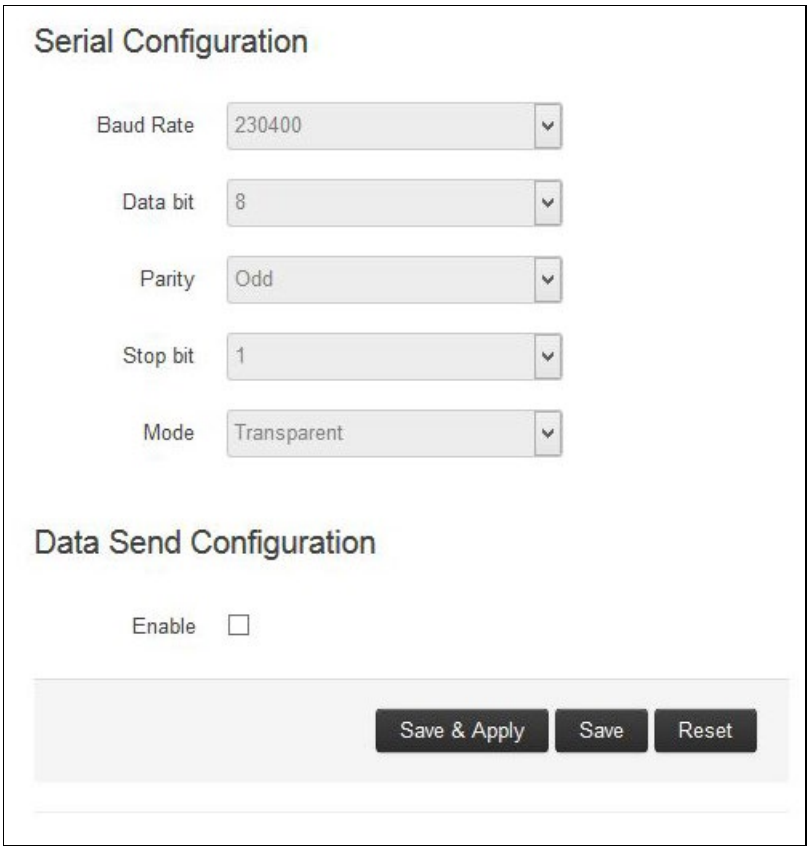
11.5 Serial

Services > Serial

RS485 is a protocol supported by the serial port of Lantronix Router E220. Using a switch located on the hardware, you can configure RS485 in half-duplex or full-duplex mode.

If RS485 is selected in half-duplex mode, you need to connect (short)
B pin to Z pin
A pin to Y pin

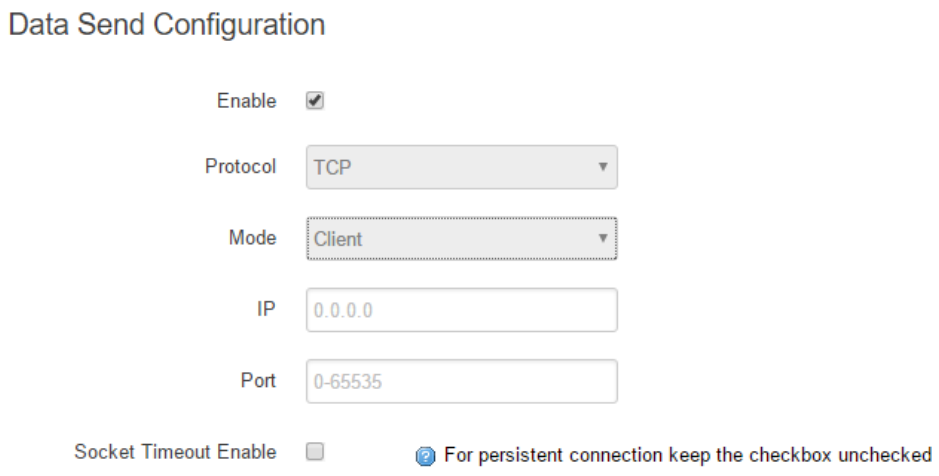
For more details, please refer section 13.1

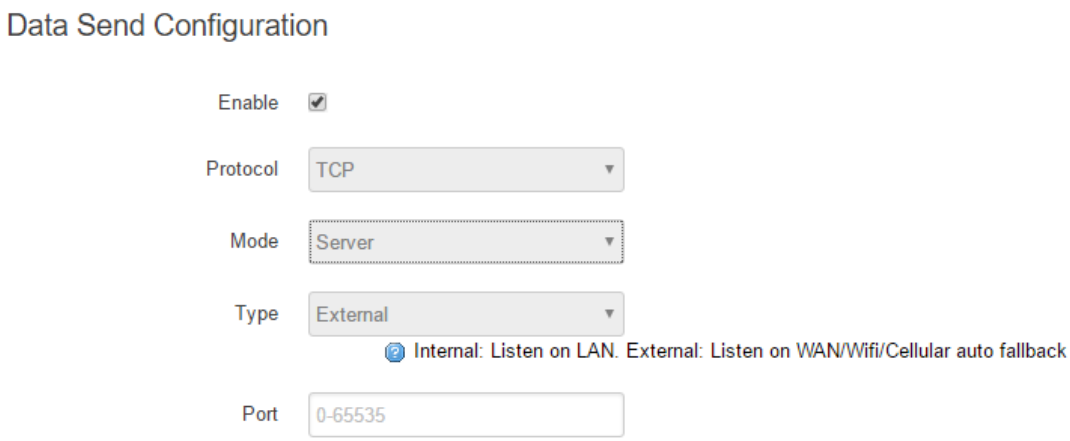


Screen 12-5a: Serial Configuration

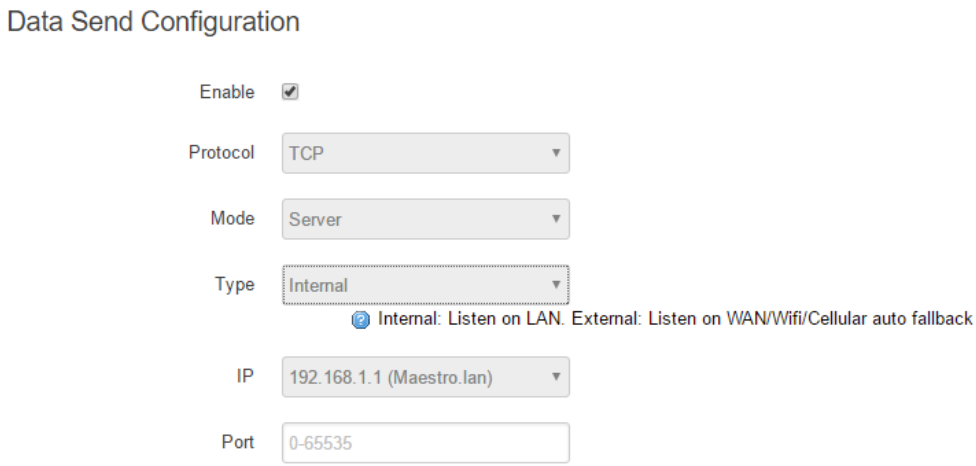
Parameters	Description
Serial Configuration	
Baud Rate	Select a baud rate from the dropdown lis. • 230400 • 115200 • 57600 • 38400 • 19200 • 9600

Parameters	Description
	• 4800 • 2400 The default baud rate is 230400.
Data bit	Select the number of data bits: • 8 • 7 • 6 • 5 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. They are used for detecting error. Select the parity bit: • Odd • Even • None The default data rate is None.
Stop bit	Select the number of stop bits: • 1 • 2 The default stop bit is 1.
Mode	Select the mode of serial communication: • **Transparent** Transparent mode of communication do not alter any data structure before or during the data communication. • **Modbus RTU or Modbus TCP**: It converts the Modbus RTU data to/from RS485 to modbus TCP before transmitting over TCP network.





Screen 12-5c: Data Send configuration – Static IP SIM



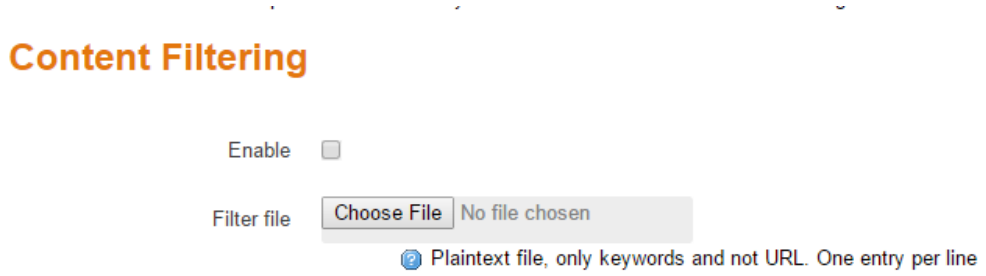
Screen 12-5d: Data Send configuration – Static IP SIM

Send Data Configuration
The data from RS485 port can be sent either via TCP or UDP using any of the available TCP interfaces. **If a dynamic IP SIM is inserted in the Router, the router needs to be configured in client mode sending data to an external (WAN) or internal (LAN) server** **If a static IP SIM is inserted in the router, the router needs to be configured in server mode listening either on an external WAN IP or an internal LAN IP**

11.6 Content Filtering

Services > Content Filtering

Content filtering is an approach to address the application security. It uses blacklisting to identify, block the URL or Domain that are denied access to the network/service.



Screen 12-6a: Content Filtering

Parameters	Description
Enable	Enable content filtering service
Filter File	Click "Browse" button to browse and select the plain text file with domain names or URL's to be filtered. For Example – to block www.xyzabc.com and www.cbazyx.com the content of the test file should be xyzabc (on the first line) cbazyx (on the second line)

11.7 Reporting Agent

Services > Reporting Agent

Reporting agent has been designed with a view to capture required information from the router on a periodic basis and send the same to a generic device management server using TCP/UDP/HTTP/HTTPS protocol.

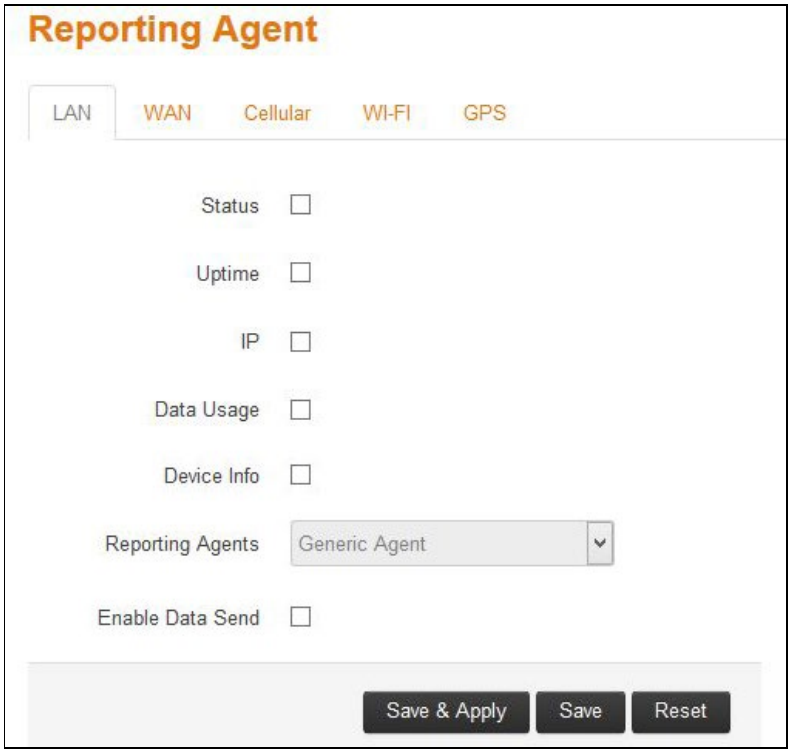
Information to be obtained from the Router are grouped as below.

- LAN
- WAN
- Cellular
- Wi-Fi
- GPS
- Device Info

11.7.1 LAN

Services > Reporting Agent > LAN

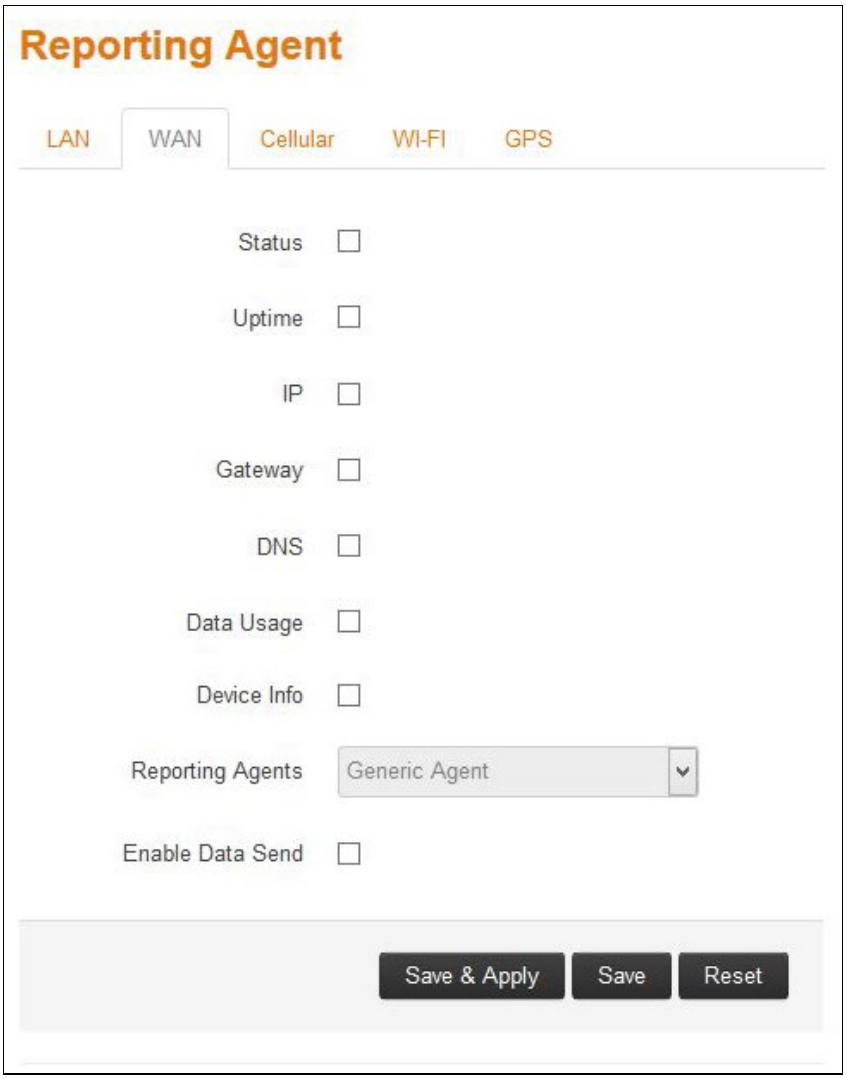
LAN reporting agent provides real–time analysis by providing information of status, uptime, IP, data usage, device information. Further it allows to select the reporting agent and to enable sending the data to server.



11.7.2 WAN

Services > Reporting Agent > WAN

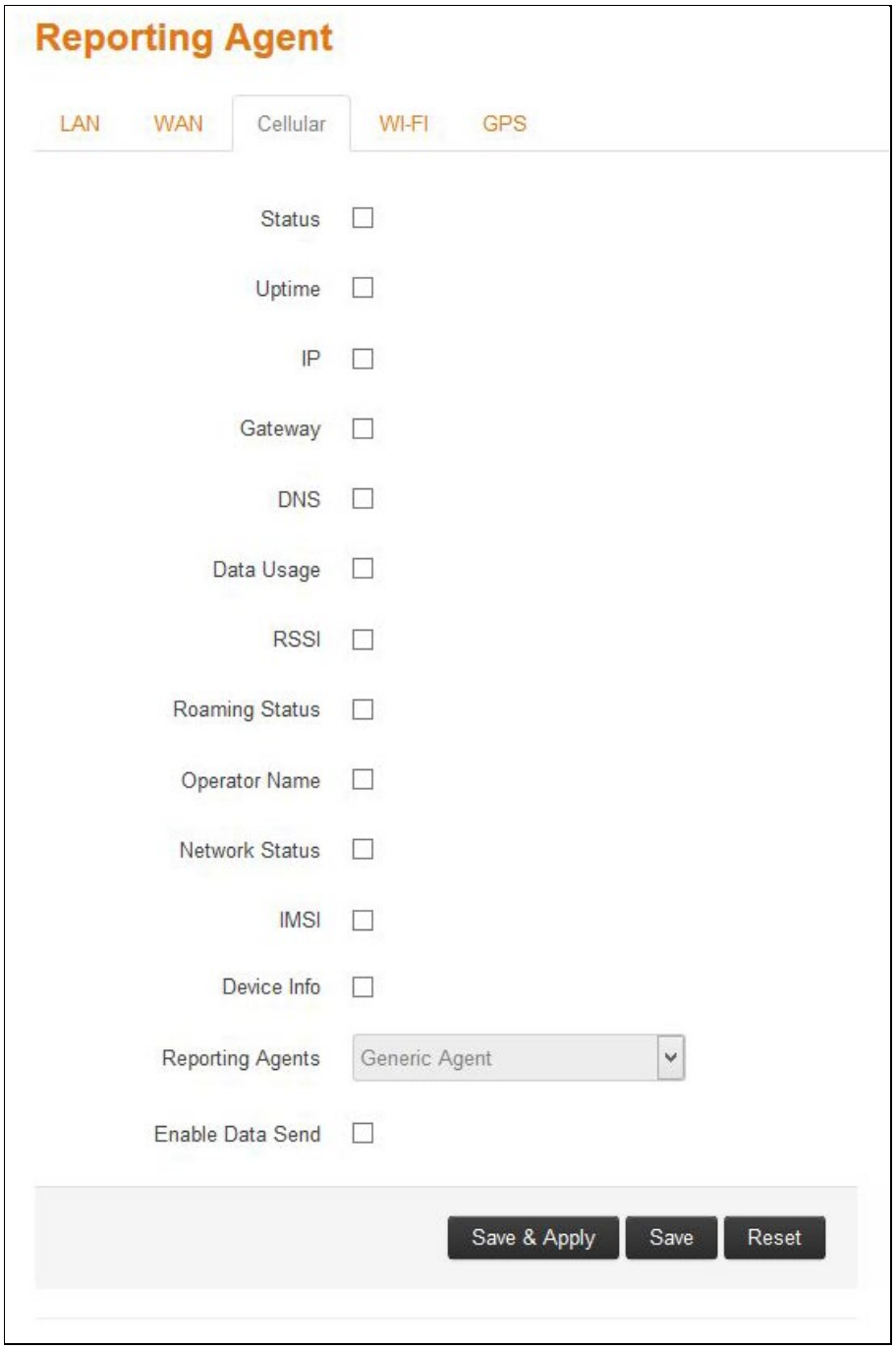
WAN reporting agent provides real–time analysis by providing information of status, uptime, IP, gateway, DNS, data usage, device information. Further it allows to select the reporting agent and to enable sending the data to server.



11.7.3 Cellular

Services > Reporting Agent > Cellular

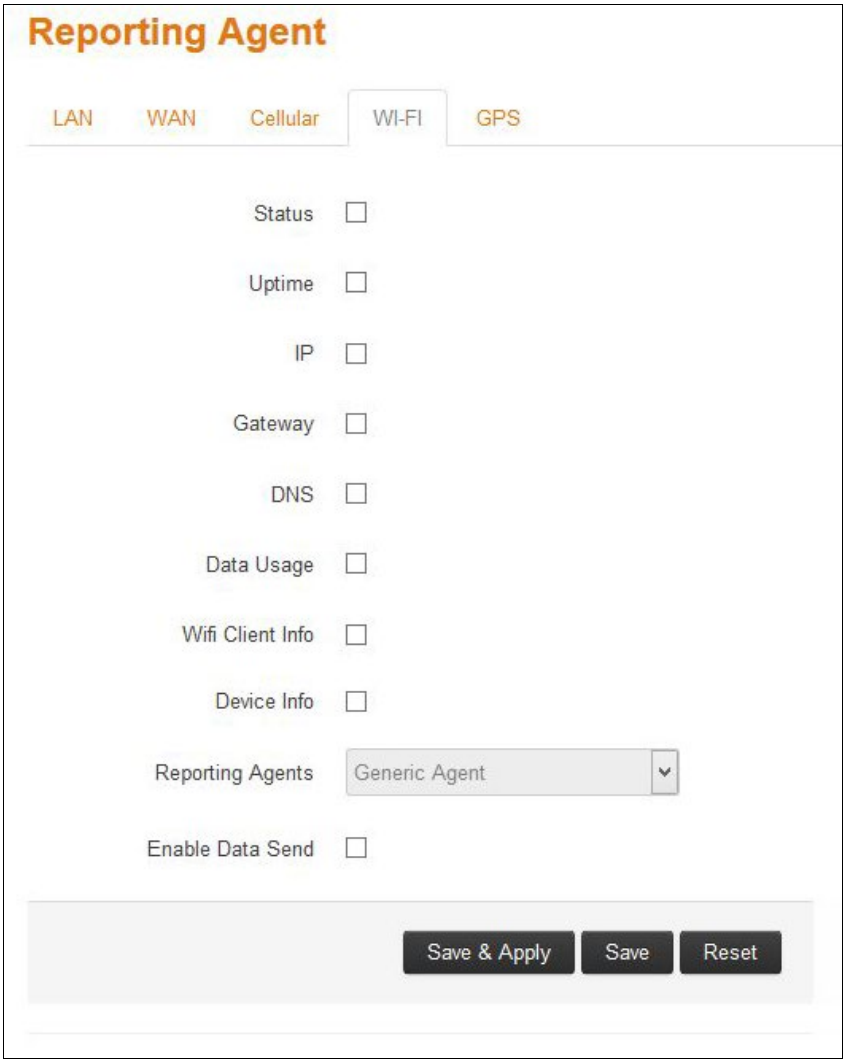
Cellular reporting agent provides real–time analysis by providing information of status, uptime, IP, data usage, RSSI, roaming status, operator name, network status, IMSI, device information. Further it allows to select the reporting agent and to enable sending the data to server.



11.7.4 Wi-Fi

Services > Reporting Agent > Wi-Fi

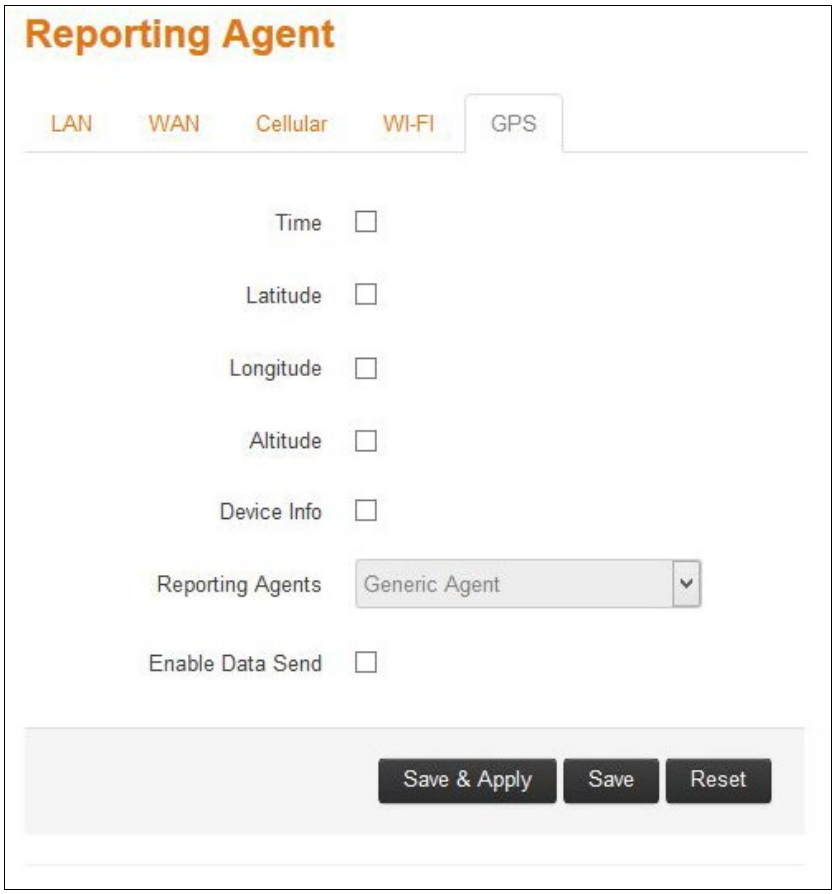
Wi-Fi reporting agent provides real–time analysis by providing information of status, uptime, IP, gateway, DNS, data usage, Wi-Fi client information, device information. Further it allows to select the reporting agent and to enable sending the data to server.



11.7.5 GPS

Services > Reporting Agent > GPS

LAN reporting agent provides real–time analysis by providing information of time, latitude, longitude, altitude, device information. Further it allows to select the reporting agent and to enable sending the data to server.

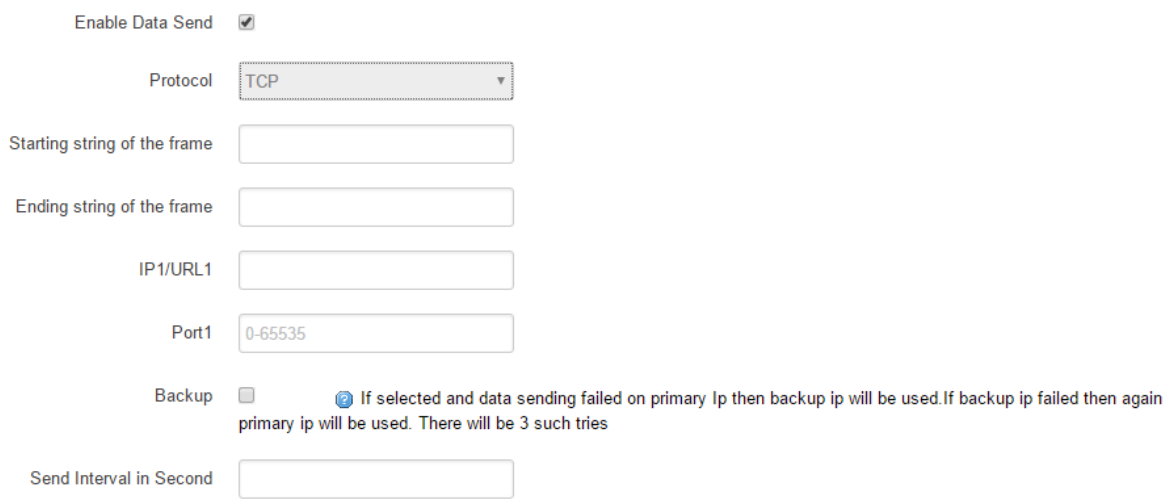


11.7.6 Sending Data

Services > Reporting Agent > Enable data Send

Captured data can be sent to any server using TCP/UDP/HTTP/HTTPS. When sending data over TCP, a custom start of frame and end of frame sequence can be defined.

Back-up server can be configured – The router will start to send data to the back-up server if it fails to send data to the main device management server 3 times. It will then continue to send data to the back-up server until the back-up server fails or the device reboots.



11.7.7 Data Sending Format

Examples: Considering all parameters selected in LAN, WAN, Cellular, Wi-Fi and GPS and when TCP sending is selected

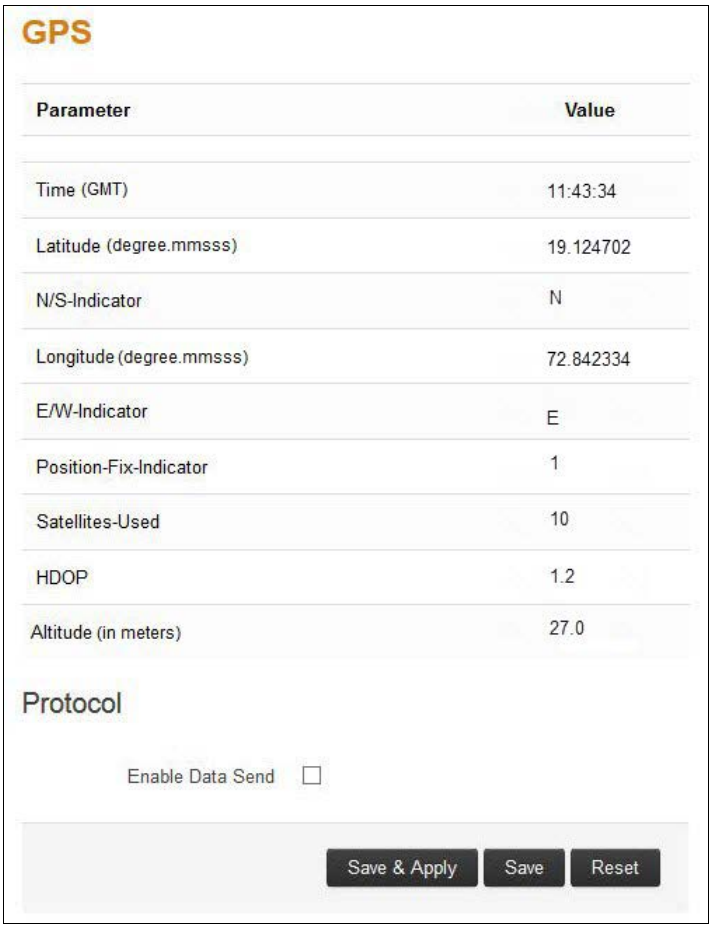
```
@IMEI=352948070039411,Lan Status=Connected,Lan IP(IPv4)=192.168.1.1,Lan
Uptime(Seconds)=329501,Lan TX bytes=572260469,Lan RX bytes=117212098,Wan
Status=Connected,Wan IP(IPv4)=192.169.1.110,Wan Uptime(Seconds)=329389,Wan
Gateway=192.169.1.1,Wan DNS=27.109.1.2 27.109.1.3,Wan TX bytes=75455301,Wan RX
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=#
```

11.8 GPS

Services > GPS

E200Router has an in-built GPS receiver that communicates with GPS satellites for synchronizing the GPS time and position data. This data can be sent to an external TCP server on real-time basis.



Screen 11-7: GPS Service Configurations

Parameters	Description
GPS Parameters	
Time	Time in hhmms.sss
Latitude	Latitude in ddmm.mmmm
N/S-Indicator	N = North or S = South
Longitude	Longitude in ddmm.mmmm
E/W-Indicator	E = East
Position-Fix-Indicator	Indicates • **0 –** Fix not available or invalid • **1 –** GPS SPS Mode, fix valid • **2 –** Differential GPS, SPS Mode, fix valid • **3 to 5 –** Not supported • **6 –** Dead Reckoning Mode, fix valid
Satellite-Used	Number of satellite used to receive GPS signals.

Parameters	Description
	The range for the number of satellite used is 0 to 12.
HDOP	Horizontal Dilution of Precision
MSL-Altitude	Altitude in meters
Protocol	

Enable Data Send	Click Enable Data Send to data to the selected server. It sends the GPS information in NMEA format.
	• **Protocol –** Select the TCP protocol only.
	• **IP1 –** Enter the primary IP Address.
	• **Port1 –** Enter the Port Number.
	• **Backup –** Click to allow using of backup IP, in case sending of the data fails using primary IP Address. In case the backup IP Address fails, primary IP Address will be used. Three such trials will be executed.
	  • **IP2 –** Enter the backup IP Address.
	  • **Port2 –** Enter the backup Port Number.
	• **Send Interval in Minute –** Time interval in minutes to try sending the data using primary IP Address and backup IP each time.

Table 11.8-1: GPS Service Configurations

a. Sample GPS Frames

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

IMEI number is now added in 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 11.8-2: 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.

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

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

Table 11.8-3: GGA Data Format

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

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

Table 11.8-4: 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.

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

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

Table 11.8-5: 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.

- $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 11.8-6: GSA Data Format

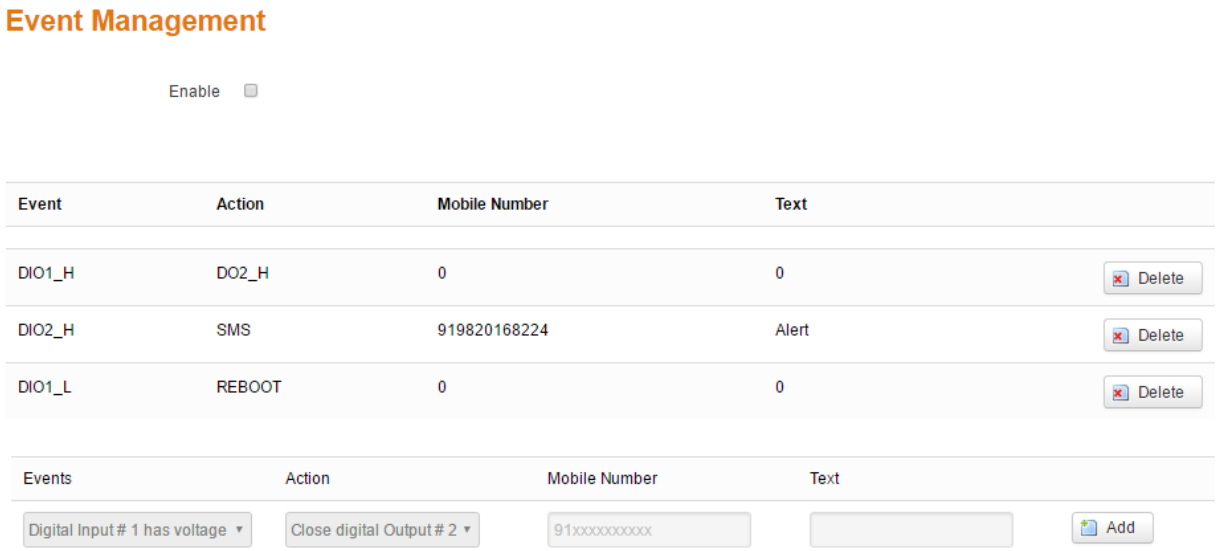
(1) Satellite used in solution.

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

11.9 Events

Services > Events

E200 and E220 Router is 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. Event page allows you to mapping actions to events respective to digital I/O's.



Screen 11-8: Event Service Configuration

Parameters	Description
EVENT	
Enable	Click to enable the events
Event	Select the event from the available options • DIO_H – High voltage state on DI • DIO_L – Low voltage state on DI DIO is by default are pulled up to high voltage level.
Action	Select the action from options. • SMS – to send the event details using the SMS. • Switch Digital Output – Change the state of Digital Output • Reboot – To reboot the router.
Mobile Number	Enter the mobile number. The mobile number format must be: <countrycode><phonenumber>
Text	Enter the text message that will be sent to the configured mobile number in case of event occurs.

Table 11.9-1: Event Service Configuration

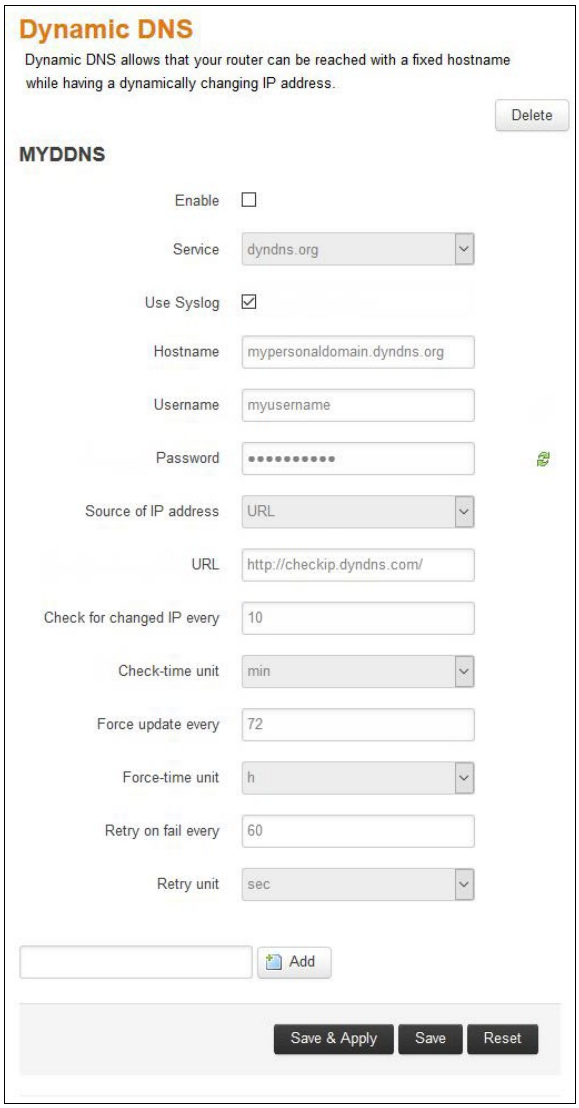
11.10 Dynamic DNS

Services > Dynamic DNS

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

Powered by Dynamic Domain Name System (DDNS), you can now access your router server by the domain name, not the dynamic IP address. DDNS will tie a domain name (e.g. mydomainname.com) to your dynamic IP Address.

You can add a new dynamic DNS by choosing a name and clicking on ADD button



Screen 11-9: Dynamic DNS Configurations

Parameters	Description
MYDDNS	
Enable	Dynamic DNS allows the router to be reached with a fixed hostname

Parameters	Description
	while having a dynamically changing IP Address.
Service	Select the DynDNS service provider from the available opitons. **Available Options** • dyndns.org • easydns.com • namecheap.com • no-ip.com • zoneedit.com
Use Syslog	Saves the logs in Syslog server. Uncheck to disable using the Syslog. By default the logs are saved.
Hostname	Name to identify the host that you want to use on DDNS server i.e. domain name that you registered with your DDNS service provider. Hostname is received from DynDNS service provider.
Username	Specify your DDNS account's Login name. Username is received from DynDNS service provider.
Password	Specify your DDNS account's Password. Password is received from DynDNS service provider.
Source of IP address	Select the IP Address source: Network, Interface, and URL. If Network is chosen, select the type of Network from LAN, WAN, 3G, WWAN, OpenVPN, and PPTP. If Interface is chosen, select one interface from the available interfaces If URL is chosen, enter the URL to be used. The source IP Address by default is URL.
URL	URL to find the WAN-side IP Address of the Router.
Check for changed IP every	Specify the time interval after which DDNS server should check and update the IP address of your server if changed. Default - 10.
Check-time unit	Specify the time unit in hours or minutes. Default - minutes. For example, if time interval is set to 10 minutes, after every 10 minutes, DDNS server will check for any changes in your server IP address.
Force update every	Specify the time interval after which DDNS server should check for updates and force updates the IP address of your server if changed.

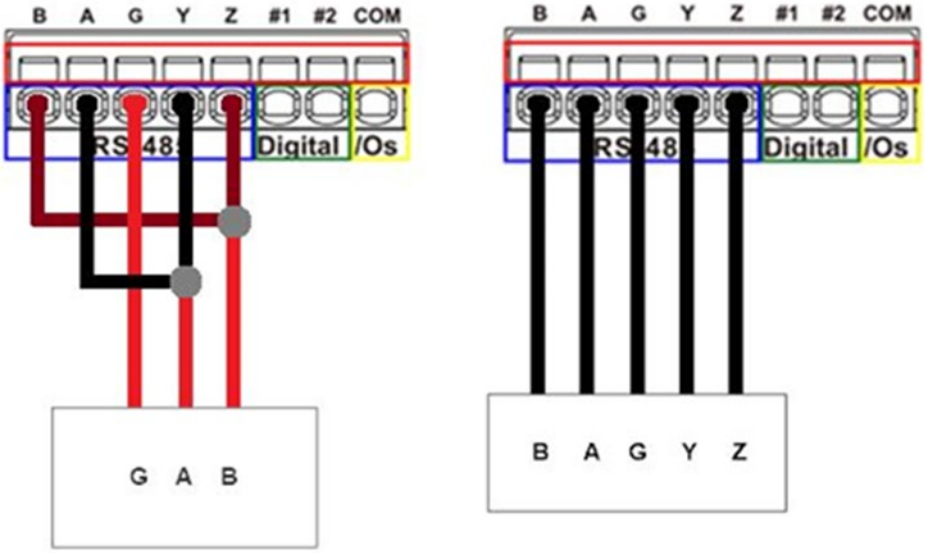
Parameters	Description
	Default – 10
Force-time unit	Specify the time unit in hours or minutes. Default - minutes. For example, if time interval is set to 10 minutes, after every 10 minutes, DDNS force updates the IP address of your server.
Retry on fail every	Enter the time in minutes/seconds after which the Router must retry to update the obtained WN IP Address with the DNS name or the host name.
Retry unit	Select the unit for the configure retrial time.

Table 11.10-1: Dynamic DNS Configurations

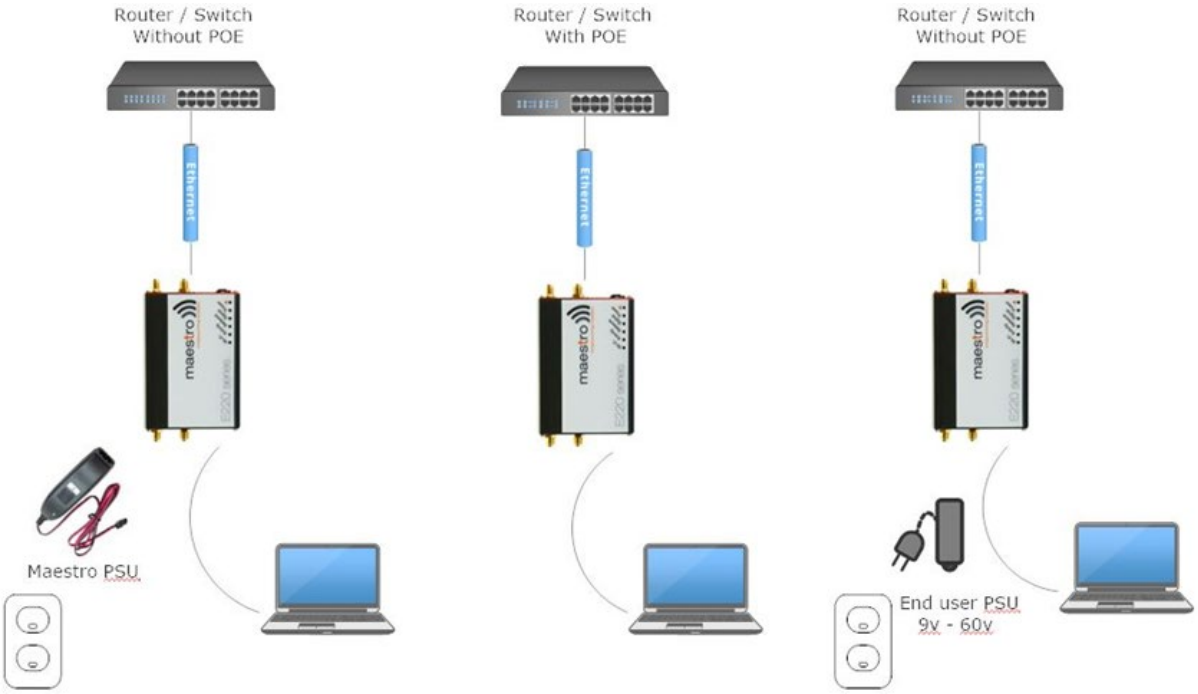
12. Wiring Diagrams

12.1 RS485 Wiring diagram:

Half Duplex (Left) RS485 Full Duplex (Right)



12.2 Power over Ethernet



13. List of Acronym

Acronym	Description
2G	2nd Generation
3G	3rd Generation
ADSL	Asymmetric digital subscriber line, ADSL is a type of DSL broadband communications technology used for connecting to the Internet
AES	Advanced Encryption Standard
AP Client	Access Point Client
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.
DIN	DIN connector is an electrical connector that was originally standardized by the Deutsches Institut für Normung (DIN)
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
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
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
LAN	Local Area Network
Acronym	Expansion / Meaning
LLTD	Link Layer Topology Discovery is a proprietary Link Layer protocol

Acronym	Description
	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
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
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
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
SIM	Subscriber identity module
SMA	SMA (Sub Miniature version A) connectors are semi-precision coaxial RF connectors
SMS	Short Message Service
SPI	Serial Peripheral Interface
SSID	Service set identification
TCP	Transmission Control Protocol
TKIP	Transmission Control Protocol
Tx	Transmission
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
VPN	Virtual private network
WAN	Wide Area network

Table 12.2-1: List of Acronyms