Maestro E-Series

USER MANUAL

VERSION 2.0.1

Maestro Wireless Solutions

Address: 9th Floor, Wing Cheong Factory Building,
121 King Lam Street, Cheung Sha Wan, Kowloon, Hong Kong
Phone: +852 3955 0222
Fax: +852 35684833
Email: contact@maestro-wireless.com http://support.maestro-wireless.com

Copyright

Note

- ***This document is subject to change without notice.***

This manual covers the following products:

- Maestro E200 Series
- Maestro E220 Series

Document Version No.	Date
2.0.1	06 November, 2015

This manual is written without any warranty.
Maestro Wireless Solutions Ltd. reserves the right to modify or improve the product and its accessories which can also be withdrawn without prior notice.

Our company stresses the fact that the performance of the product and its accessories depends on the proper use conditions as well as the surrounding environment.

Maestro Wireless Solutions Ltd. assumes no liability for damage incurred directly or indirectly from errors, omissions or discrepancies between the router and this manual.
This software, solution or application is provided on an "as is" basis. No warranty whether expressed or implied is given by **Maestro Wireless Solutions Ltd.** in relation to this software, solution or application. User shall assume the entire risk of using or relying on this software, solution, and application.

In no event will **Maestro Wireless Solutions Ltd.** be liable for any loss or damage including without limitation, indirect or consequential loss, damage, or any loss, damage whatsoever arising from loss of data or profit arising out of, or in connection with, the use of this router product. Every effort is made to keep the product and its software up and running smoothly. However, **Maestro Wireless Solutions Ltd.** takes no responsibility for, and will not be liable for, the product or its software being temporarily unavailable due to technical issues beyond our control.

The above terms and conditions are subject to change without prior notice. The present use of this product solution implies that the user approves and understands all the above terms and conditions.

Table of Contents

1.Overview

With high-speed cellular (3G and beyond), WAN, LAN and Wi-Fi connectivity, the Maestro's E200 series of router 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.

The Maestro E200 series include:

- **E205XT02 –** A dual-band (900MHz/2100MHz) High-Speed Downlink Packet Access (HSDPA) router with quad-band GSM/GPRS (850/900/ 1800/1900MHz) for 2G fallback operation.
- **E205XT04 –** A tri-band (800MHz/850MHz/2100MHz) High-Speed Downlink Packet Access (HSDPA) router with quad-band GSM/GPRS (850/900/ 1800/1900MHz) for 2G fallback operation.
- **E206XT –** It is a dual mode router, with quad-band High Speed Packet Access (HSPA+: 800/850/1900/2100MHz) and dual-band Evolution-Data Optimized (EVDO: 800/1900MHz) as primary modes of operation, as well as quad-band GSM/GPRS (850/900/ 1800/1900MHz) and dual-band CDMA 1X (800/1900MHz) for 2G fallback operation.

Note

- ***All the screenshot in this User Manual are taken from E205 Router.***
- ***The sections that explicit for ONLY to E206 include the screenshot from E206 Router.***

2.Prerequisite

Before continuing with the installation of your E200 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 Maestro 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. Checking the Package Content

Note

- ***All the components are exclusive of the Maestro Router and must be purchased.***

Check the Package contents. Check that the package contents are complete.

- One Maestro Router - E200XT
- One AC Power connector cable – 4 pin connector for power supply and digital input/output – ACC-PS01
- One Straight through Ethernet Cable – ACC-CA29
- Wi-Fi Antenna – ACC-A21
- Cellular / GPS Antenna – ACC-A22 (98-960 / 1575.42 / 1710~2700 MHz)
- Quick Start Guide

If any component(s) from the package are missing, please contact Maestro Support at support@maestro-wireless.com.

4. Default Configuration

Note

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

4.1 Web Admin Page

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

Table 4.1-1: Default Web Admin Page Credentials

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

Parameter	Details
SSID	Maestro E200
WPA Key	W1rele$$

Table 4.2-1: Default Wi-Fi Credentials (WPA/WPA TKIP)

4.3 Connection

- WAN (Ethernet) Connection – Automatic (DHCP client- Automatic IP Address allocation)
- Active DHCP with starting IP Address: 192.168.1.100 with pool of 100 clients.
- WAN as automatic IP, with Cellular backup
- Cellular default Access Point Name (APN) is “**internet**”

5.Understanding the Maestro Router

5.1 LAN Panel Details

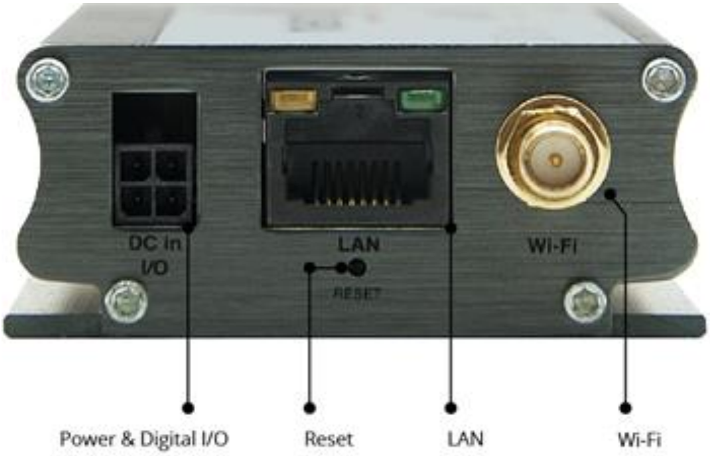


Figure 5.1-1: Maestro Router LAN Panel

- Power Supply – 4 pin Micro-fit Molex connector (Power and input/output)
- Ethernet port (LAN) – Straight-through Ethernet cable connects to LAN.
- Reset Button – Push the reset button for 5 seconds and device will be factory reset to default settings.

Note

- ***Use a paper clip to push the reset button gently.***

- Wi-Fi Connector – RP-SMA antenna connector

5.1.1 Power Requirement

A. For E205XT

- Input voltage: 9V to 60VDC
- Rated current: 650mA

DC Input	9V	12V	24V	48V
Idle state (Ethernet, Wi-Fi & Cellular n/c)	180mA	140mA	70mA	40mA
Ethernet connected (Wi-Fi & Cellular n/c)	230mA	160mA	80mA	50mA

Ethernet & Wi-Fi connected (Cellular n/c)	230mA	160mA	80mA	50mA
Ethernet & Wi-Fi connected Cellular transmitting at max power	400mA	270mA	130mA	70mA

B. For E206XT

- Input voltage: 9V to 60VDC
- Rated current: 850mA

DC Input	9V	12V	24V	48V
Idle state (Ethernet, Wi-Fi & Cellular off)	110mA	82mA	43mA	23mA
Ethernet connected (Wi-Fi & Cellular off)	150mA	112mA	57mA	31mA
Ethernet connected & Wi-Fi on ,(Cellular off)	202mA	151mA	76mA	41mA
Ethernet & Wi-Fi on (Cellular standby)	222mA	167mA	84mA	46mA

5.2 WAN Panel Details

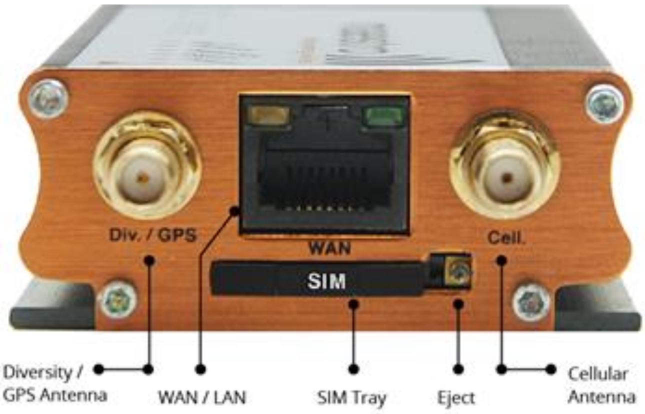


Figure 5.2-1: Maestro Router WAN Panel

- GPS SMA Antenna Connector
- Ethernet port (WAN)
  - 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.
- SIM Card holder
- SIM Eject Button
- Cellular SMA Antenna Connector

5.3 Front Panel Details

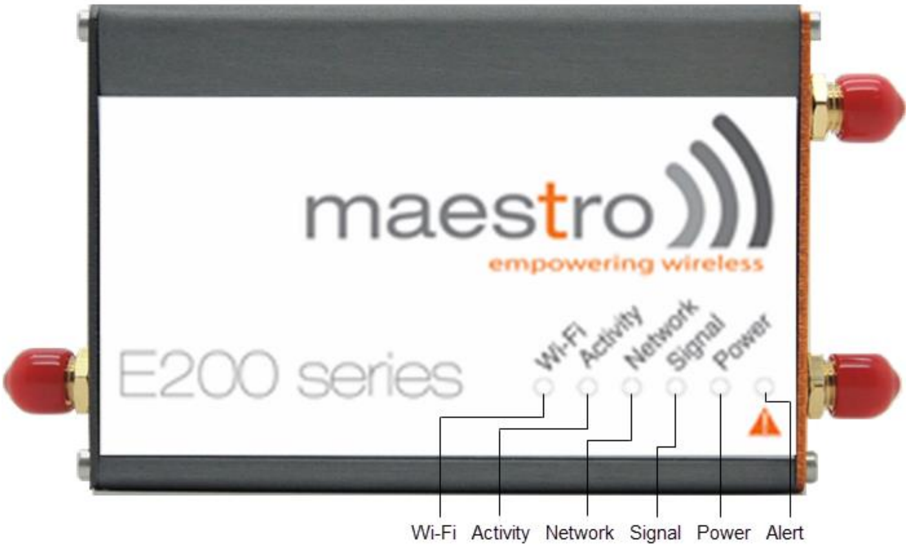


Figure 5.3-1: Front Panel

The top panel of Maestro E200 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 or SIM card)
Power	⊘	OFF	Power off
	🟢	Green ON	Power on
Signal	⊘	OFF	No signal (CSQ=0 to 5, 97, 98, 99)
	✷	Amber Flashing	Weak signal (CSQ > 6 to 12)
	🟠	Amber ON	Strong signal (CSQ >12)
Network	⊘	OFF	Not registered on a cellular network.

Name	Colour and State		Description
	☀	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 5.3-1: LED States and Description

Connecting Maestro Router

Step1. Press the end of a paper clip straight into the eject button next to SIM Tray. Press firmly until the SIM tray pops out.

Note

- ***DO NOT pull out the SIM tray without pushing the eject button.***

Step2. Pull out the SIM holder and place the SIM card in it, following the shape of the tray.

Note

- ***Make sure it fits perfectly and the golden circuit side of the SIM is faced upwards.***

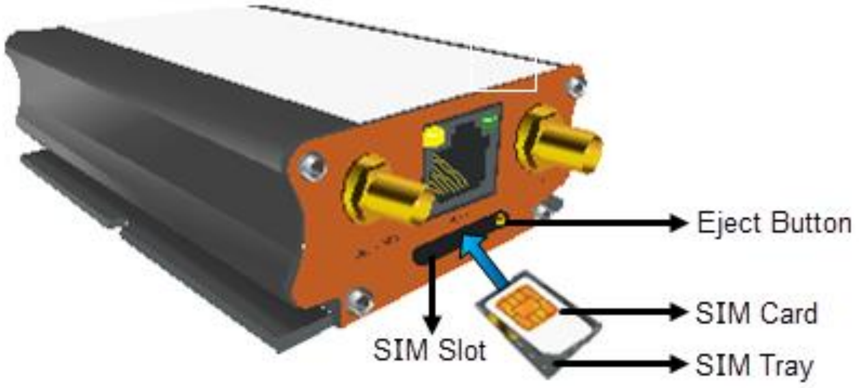


Figure 0-1: Insert SIM Card

Step3. Carefully push the SIM tray containing the SIM card back into the Maestro Router.

Step4. Connect GSM antenna with "Cell" connector on the Maestro Router. Make sure the antenna is tightly secured.

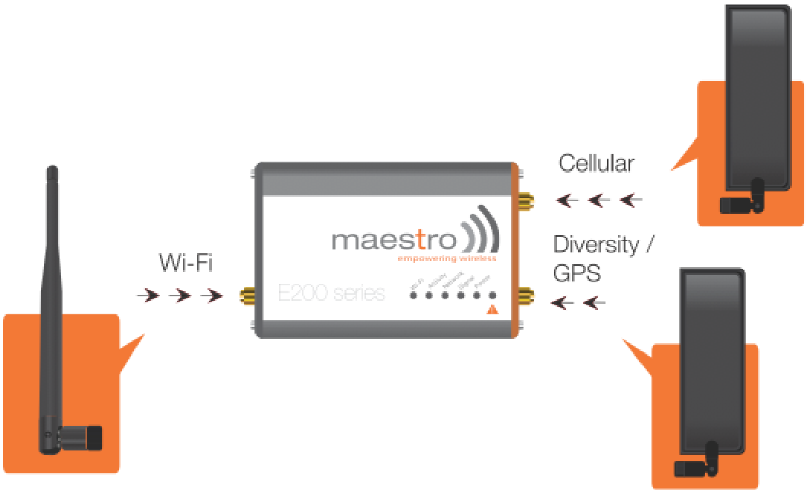


Figure 0-2: Connecting the Antennas

Step5. Connect GPS antenna with "Div/GPS" connector.

Note

- ***We strongly recommend connecting the GPS antenna with "Div/GPS" connector, if the Maestro Router package content includes it. A dual antenna provides diversification that is improved signal strength and thus better performance.***
- ***For certain circumstances/environments may require a higher quality of antenna or one mounted in a different location. In this case, Maestro has many antenna options to choose from, please contact Maestro Support at support@maestro-wireless.com.***

Step6. Use standard Ethernet cable to connect the existing WAN access to WAN port of Maestro Router.

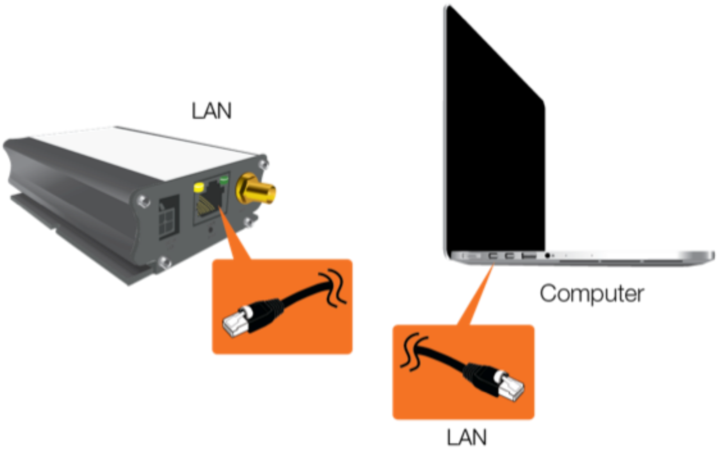


Figure 0-3: Ethernet cable connection for LAN/WAN access

Step7. Use standard Ethernet cable to connect "LAN" port with the LAN port of the computer.

Step8. Connect the AC power connector into the “DC in” jack on LAN-side panel of the Maestro Router. Plug the other side of the cord to a standard AC receptacle and turn the power switch ON. The power LED will light when power is applied.

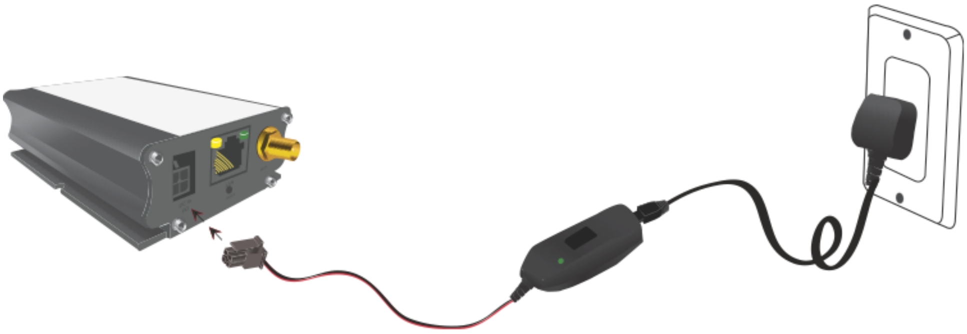


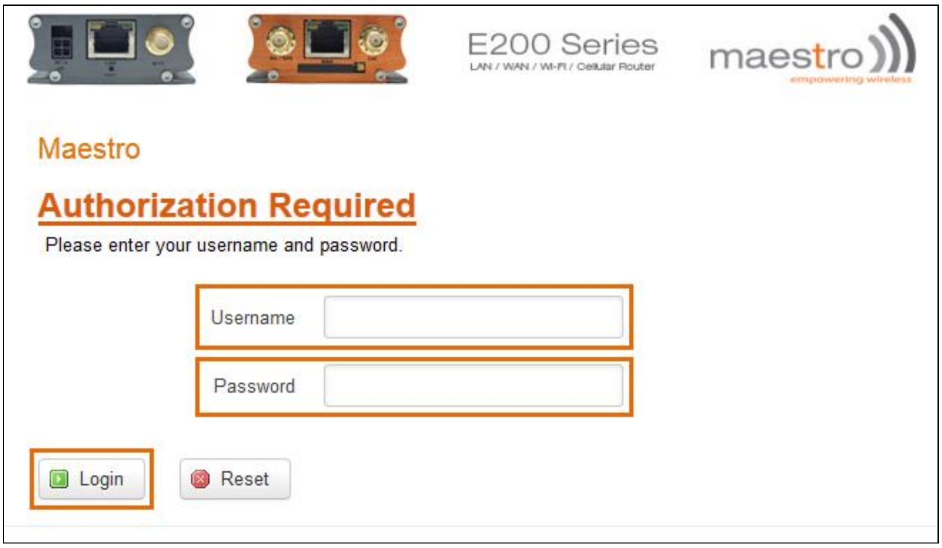
Figure 0-4: Connecting to AC receptacle

6. Logon Procedure

Open a Web browser on the computer, and enter the LAN IP Address http://192.168.1.1 of Maestro 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 Maestro Router is 192.168.1.1.***
- ***DHCP must be enabled on the computer to access Maestro Router with LAN IP Address 192.168.1.1. For more information refer How to Enable DHCP?***



Screen 0-1: 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 0-1: Login Page

7.Common Icons and Buttons

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

> ***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.

8.Quick Setup

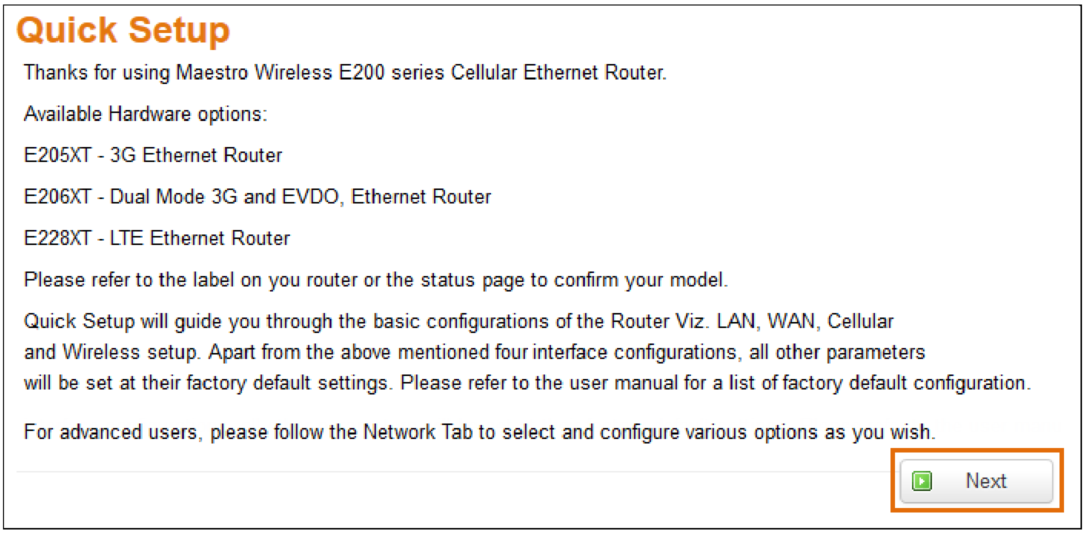
8.1 Quick Setup

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.***



Quick Setup

Thanks for using Maestro Wireless E200 series Cellular Ethernet Router.

Available Hardware options:

E205XT - 3G Ethernet Router

E206XT - Dual Mode 3G and EVDO, Ethernet Router

E228XT - LTE Ethernet Router

Please refer to the label on you router or the status page to confirm your model.

Quick Setup will guide you through the basic configurations of the Router Viz. LAN, WAN, Cellular and Wireless setup. Apart from the above mentioned four interface configurations, all other parameters will be set at their factory default settings. Please refer to the user manual for a list of factory default configuration.

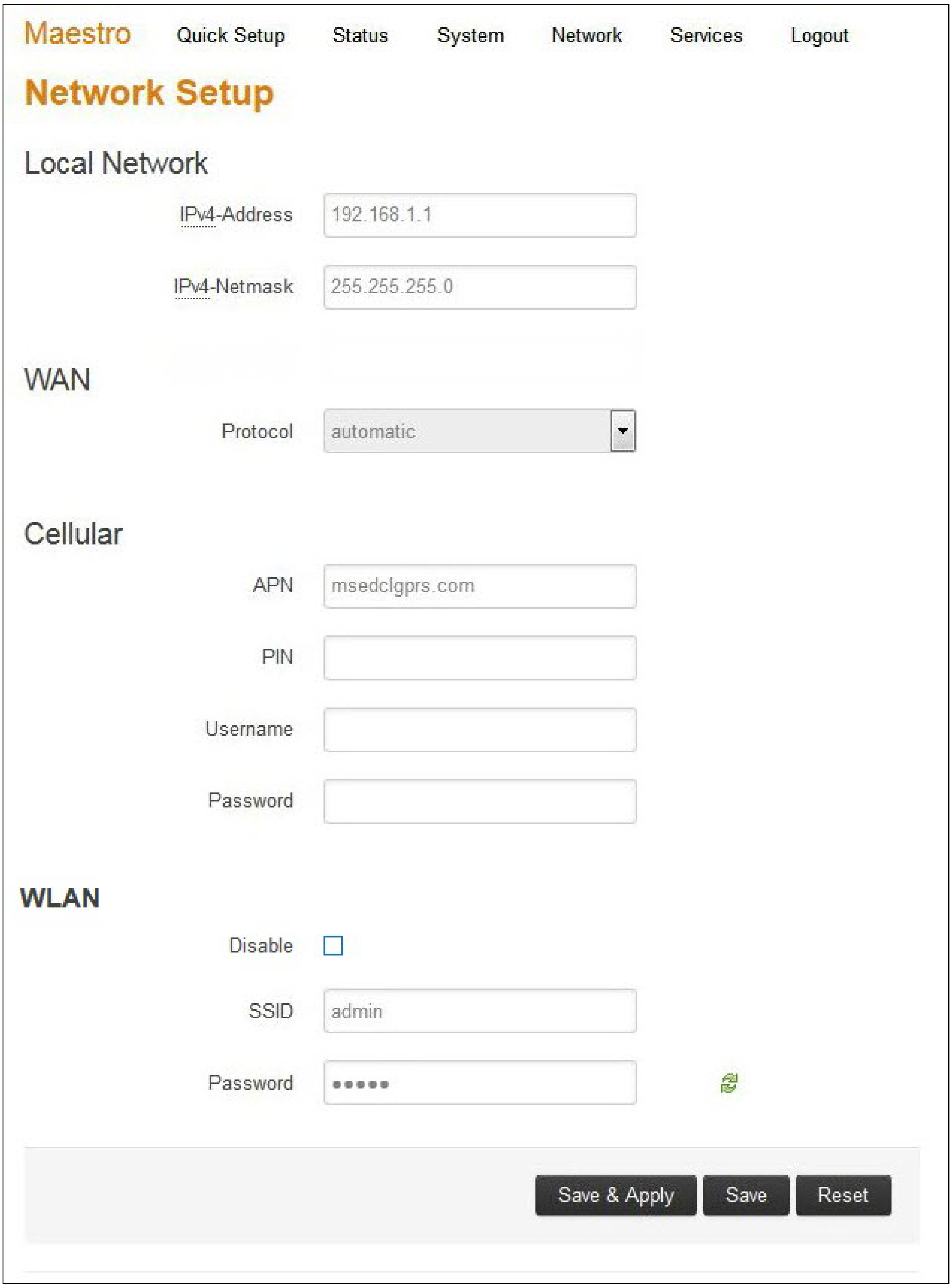
For advanced users, please follow the Network Tab to select and configure various options as you wish.

Screen 8.1-1: Router Information

8.2 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.



Network Setup

Local Network

IPv4-Address: 192.168.1.1

IPv4-Netmask: 255.255.255.0

WAN

Protocol: automatic

Cellular

APN: msedclgprs.com

PIN:

Username:

Password:

WLAN

Disable ☐

SSID: admin

Password: •••••

Screen 8.2-1: 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.
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 8.2-1: Quick Start Network Configuration

9.Status

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

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

9.1 Overview

Status > Overview

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

9.1.1 Status

Status > Overview > Status

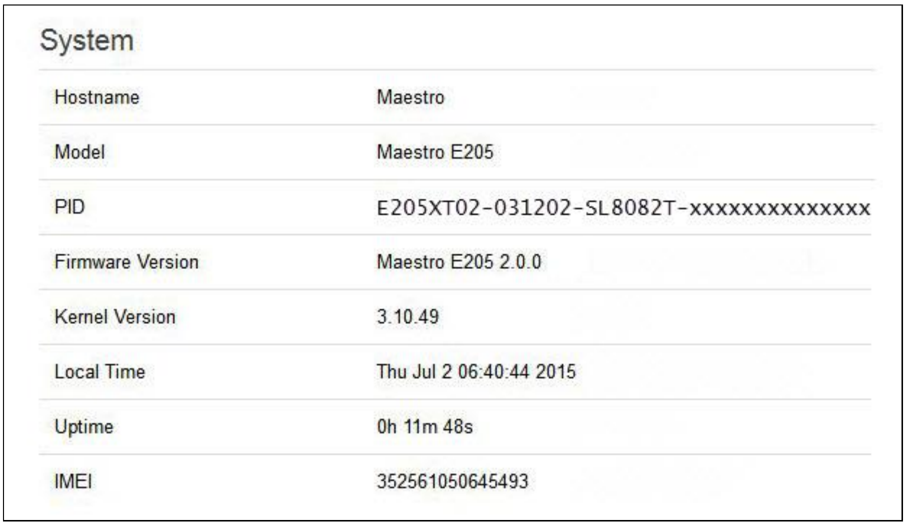
Status Overview page outlines the setting details of basic sub-modules that must be configured for the Router. Status Overview uses tables to display information. The Status page provides information about:

- 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 E205
PID	E205XT02-031202-SL8082T-xxxxxxxxxxxxxx
Firmware Version	Maestro E205 2.0.0
Kernel Version	3.10.49
Local Time	Thu Jul 2 06:40:44 2015
Uptime	0h 11m 48s
IMEI	352561050645493

Screen 9.1-1 System Status Overview

Parameters	Description
Hostname	Name assigned to the router for addressing purposes.
Model	Model number of the router that is deployed. Example – Maestro E205
PID	Display 35 characters long, unique Product Identification number (PID). Consider an example of PID E205XT02-031202-SL8082T-xxxxxxxxxxxxxx. It is composed of: 8 characters SKU: E205XT02 **6 characters UID:** 031202 (WAN, GNSS, Wi-Fi, 2x LAN, SIM) 7 character Module Name: SL8082T 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). PID read script is open to use. **Command:** readpid Response PID: E205XT02-031202-SL8082T-xxxxxxxxxxxxxx
Firmware Version	Base Firmware Version number.

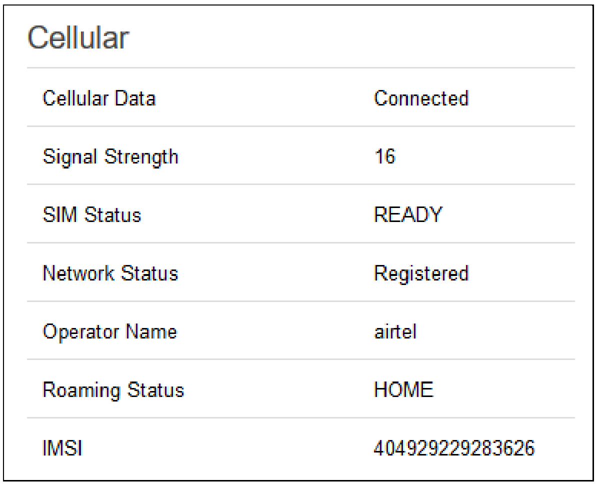
Kernel Version	The Linux Kernel version number on the router.
Local Time	Displays the day of the week, month, date, time and year configured on the router. The format is Day Month Date hh:mm:ss Year. The time is displayed in 24 hour clock format.
Up Time	Displays the time for which the router is up and running since last power ON. The format is hh:mm:ss. The time is displayed in 24 hour clock format.
IMEI/MEID **(MEID is available only in E206 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 to note 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 9.1-1: 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 9.1-2: 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.

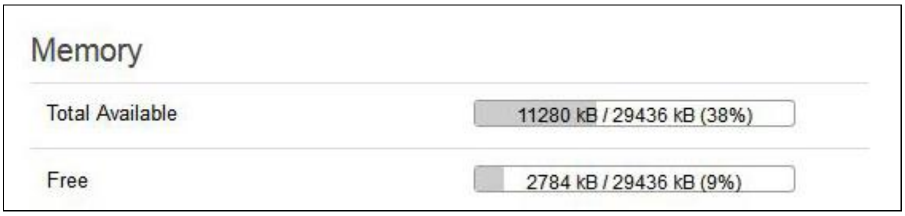
Network Status	The registration status of the router on the current cellular network.
Operator Name	Name of the current cellular operator in use.
Roaming Status	The roaming status of the router: - Home - Roaming
IMSI	Displays the IMSI Number. In case of UMTS, it is read from the SIM card. An International 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 (For E206)	Displays the ESN number of cellular module. It must be subscribed for a Verizon account (EVDO).
Revision (For E206)	Displays the Firmware revision number of the cellular module.
Cellular Module Info (For E206)	Displays the critical parameters from the cellular module.

Table 9.1-2: Cellular Status Overview

C. Memory

Status > Overview > Status

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



Memory

Total Available: 11280 kB / 29436 kB (38%)

Free: 2784 kB / 29436 kB (9%)

Screen 9.1-3: Memory Status Overview

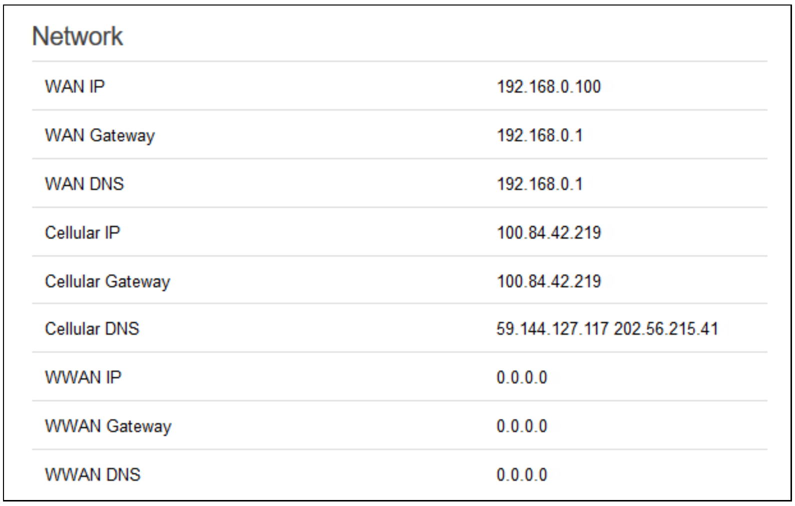
Parameters	Description
Total Available	Total available RAM memory. Total Memory is summation of used memory, free memory, buffered memory and cached memory. Grey highlight and the percentage value display the amount of used memory.
Free	Free RAM memory. Grey highlight and the percentage value display the amount of used memory.

Table 9.1-3: 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 9.1-4: 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.

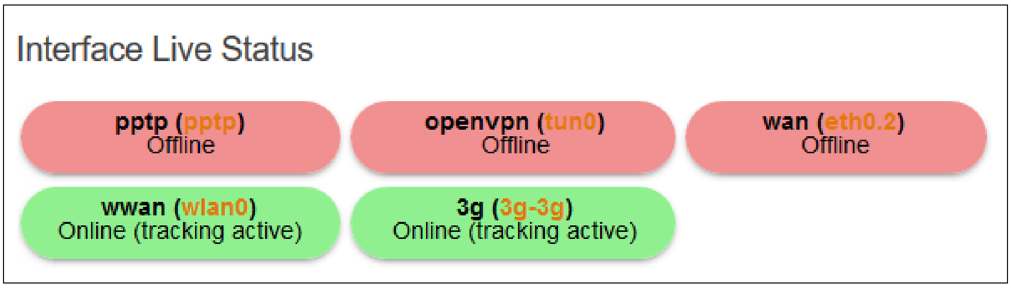
Table 9.1-4: Network Status Overview

E. MWAN Interface Live Status

Status > Overview > Status

The Multiple Wide Area Network (MWAN) capability enables an administrator to configure multiple external interfaces, each on different subnet. This allows the router to be connected to more than one Internet Service Provider (ISP), ensuring a redundant support for the users connected to the router and providing a constant Internet connection. It is popularly called as Load Balancing. The order of Interface priority depends on the metric assigned to the interface.

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**.



Interface Live Status

pptp (pptp)
Offline

openvpn (tun0)
Offline

wan (eth0.2)
Offline

wwan (wlan0)
Online (tracking active)

3g (3g-3g)
Online (tracking active)

Screen 9.1-5: MWAN Interface Live Status

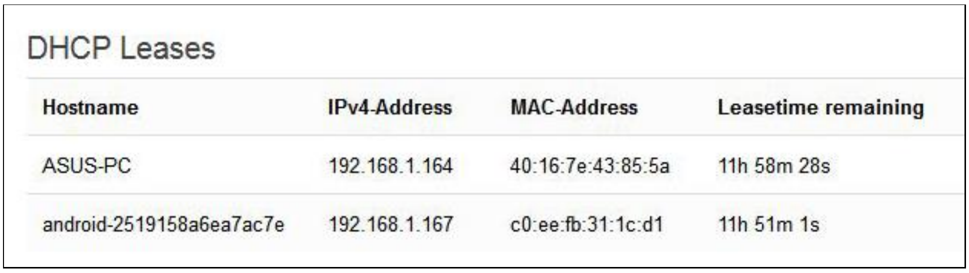
Parameters	Description
Multiple WAN Interface Live Status **Indicates the current status of the interferes – PPTP, OpenVPN, WAN, WWAN, 3G**	
Offline	The interfaces that are not connected to network are marked in RED.
Online	The interfaces that are connected to the network are marked in GREEN. **Status** **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 9.1-5: 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 9.1-6: DHCP Lease Status Overview

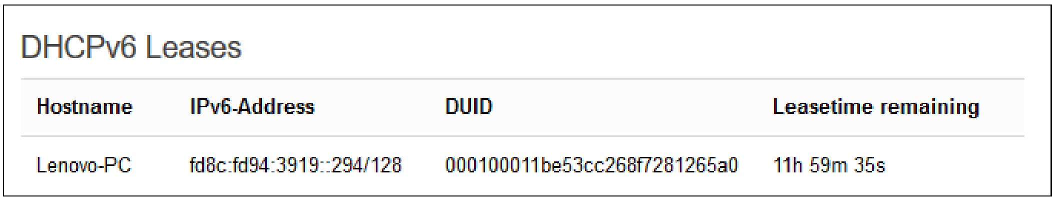
Parameters	Description
Host Name	Name of the device (laptop, mobile, etc.) that is connected to the router and has been leased an IPv4 Address by the router's DHCP server.
IPv4 Address	IPv4 Address assigned to the device connected to the router.
MAC Address	MAC address of the device connected to the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

Table 9.1-6: 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 9.1-7: DHCPv6 Lease Status Overview

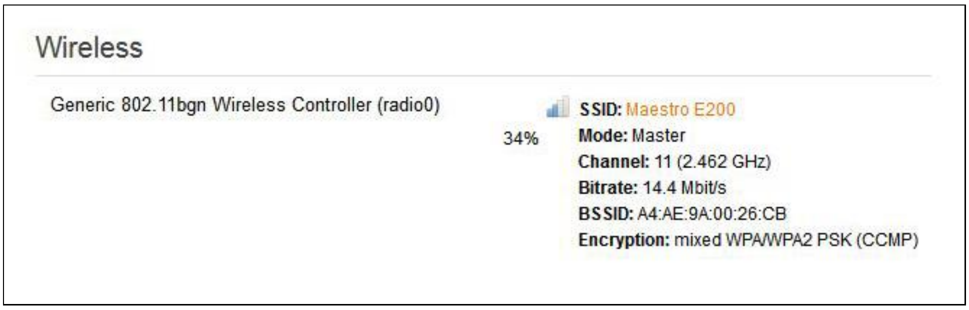
Parameters	Description
Host Name	Name of the device (laptop, mobile, etc.) that is connected to the router and has been leased an IPv6 Address by the router's DHCPv6 server.
IPv6 Address	IPv6 Address assigned to the device connected to the router.
DUID	DUID (Device Unique Identifier) of the device connected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

Table 9.1-7: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.



Wireless

Generic 802.11bgn Wireless Controller (radio0)

34%

SSID: Maestro E200
Mode: Master
Channel: 11 (2.462 GHz)
Bitrate: 14.4 Mbit/s
BSSID: A4:AE:9A:00:26:CB
Encryption: mixed WPA/WPA2 PSK (CCMP)

Screen 9.1-8: 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.

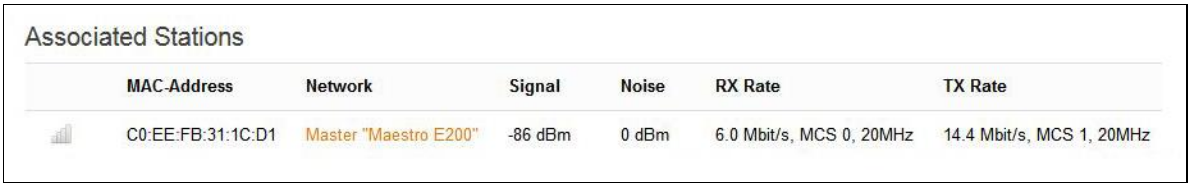
Table 9.1-8: Wireless Status Overview

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 9.1-9: 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

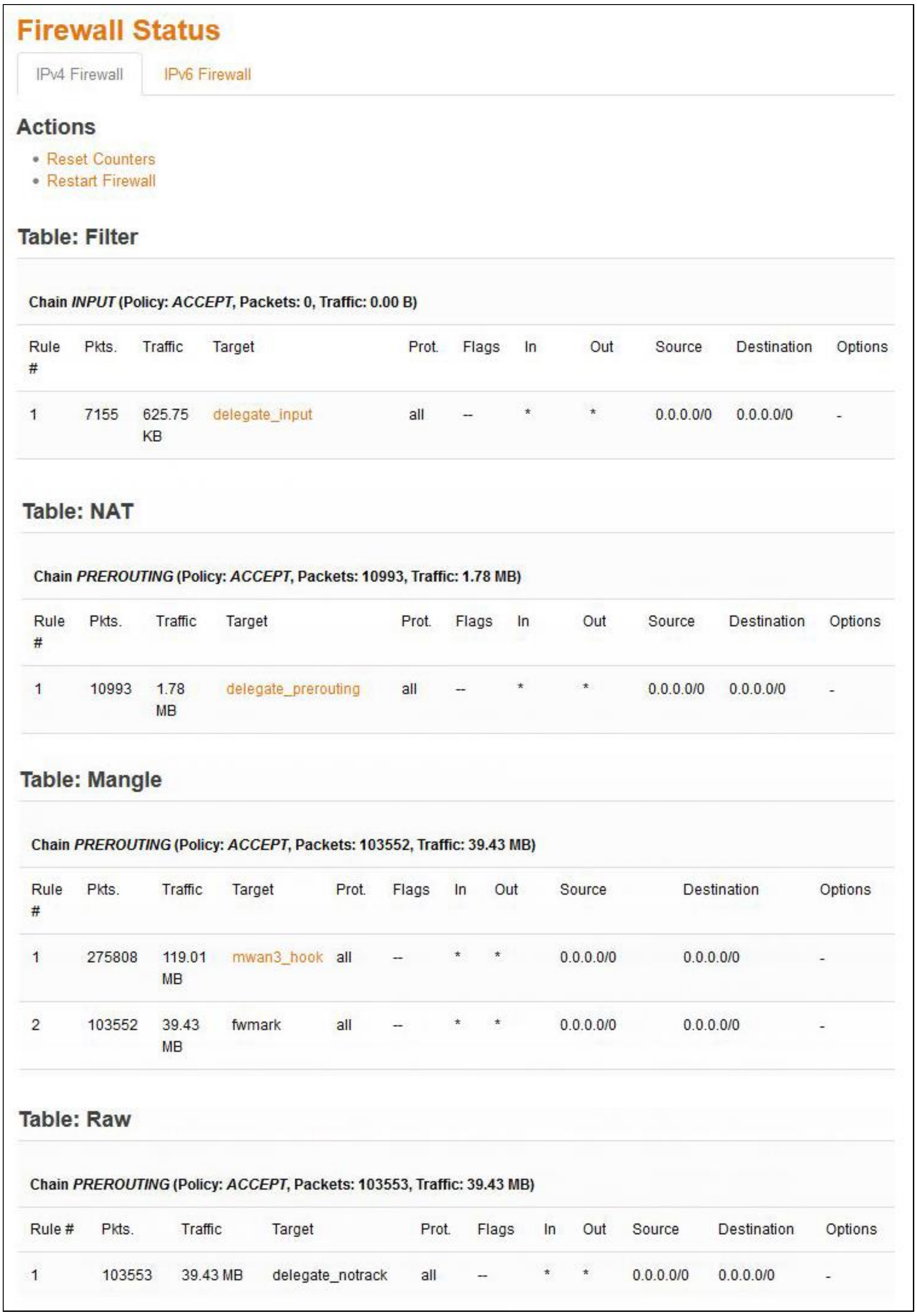
Table 9.1-9: Associated Stations Status Overview

9.2 Firewall

Status > Firewall

9.2.1 IPv4 Firewall

Status > Firewall > IPv4 Firewall



Firewall Status

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 9.2-1: IPv4 Firewall Status

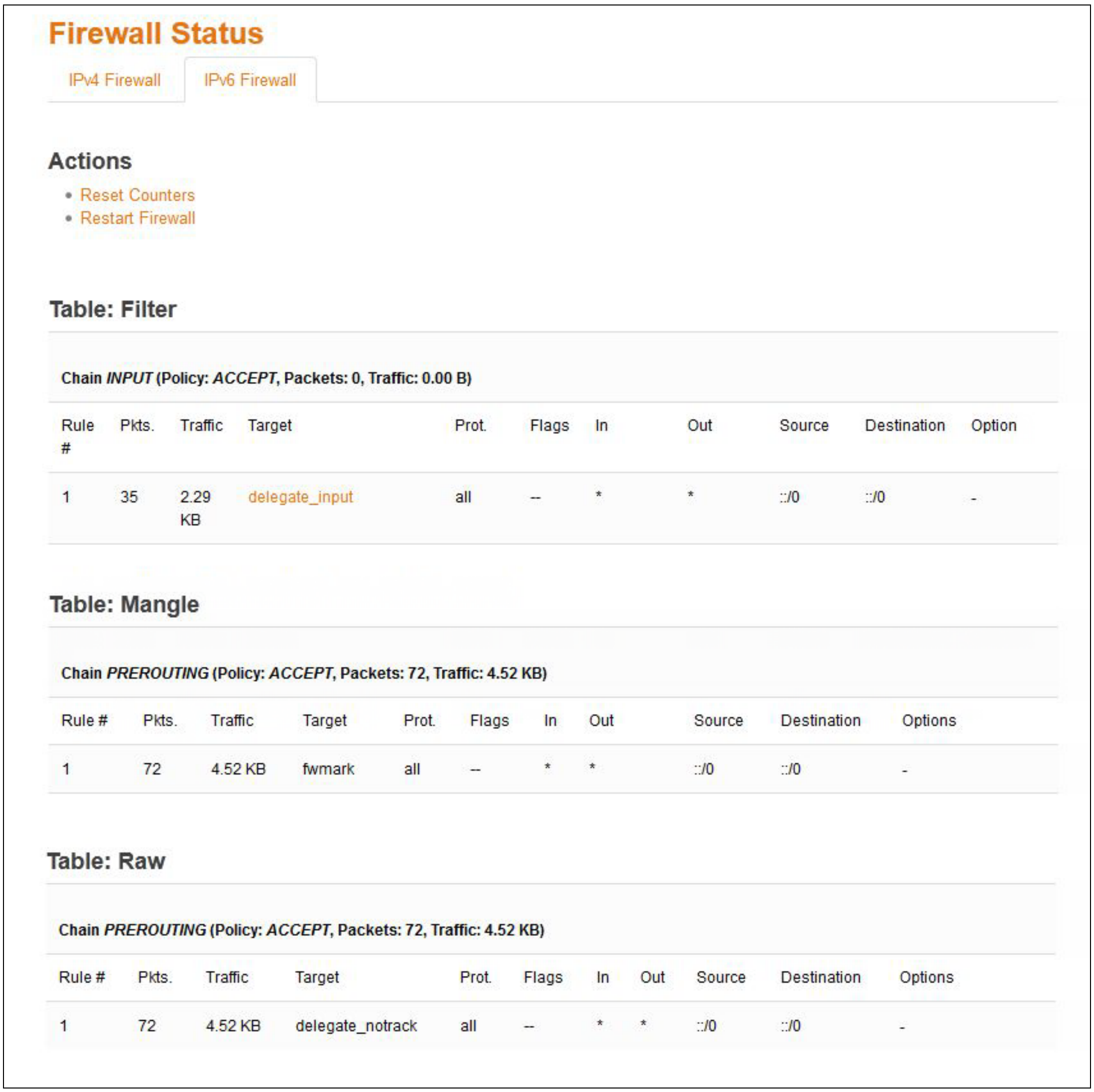
Parameters	Description

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 9.2-1: IPv4 Firewall Status

9.2.2 IPv6 Firewall

Status > Firewall > IPv6 Firewall



Firewall Status

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	Option
1	35	2.29 KB	delegate_input	all	--	*	*	::/0	::/0	-

Table: Mangle

Chain *PREROUTING* (Policy: *ACCEPT*, Packets: 72, Traffic: 4.52 KB)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	72	4.52 KB	fwmark	all	--	*	*	::/0	::/0	-

Table: Raw

Chain *PREROUTING* (Policy: *ACCEPT*, Packets: 72, Traffic: 4.52 KB)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	72	4.52 KB	delegate_notrack	all	--	*	*	::/0	::/0	-

Screen 9.2-2 IPv6 Firewall Status

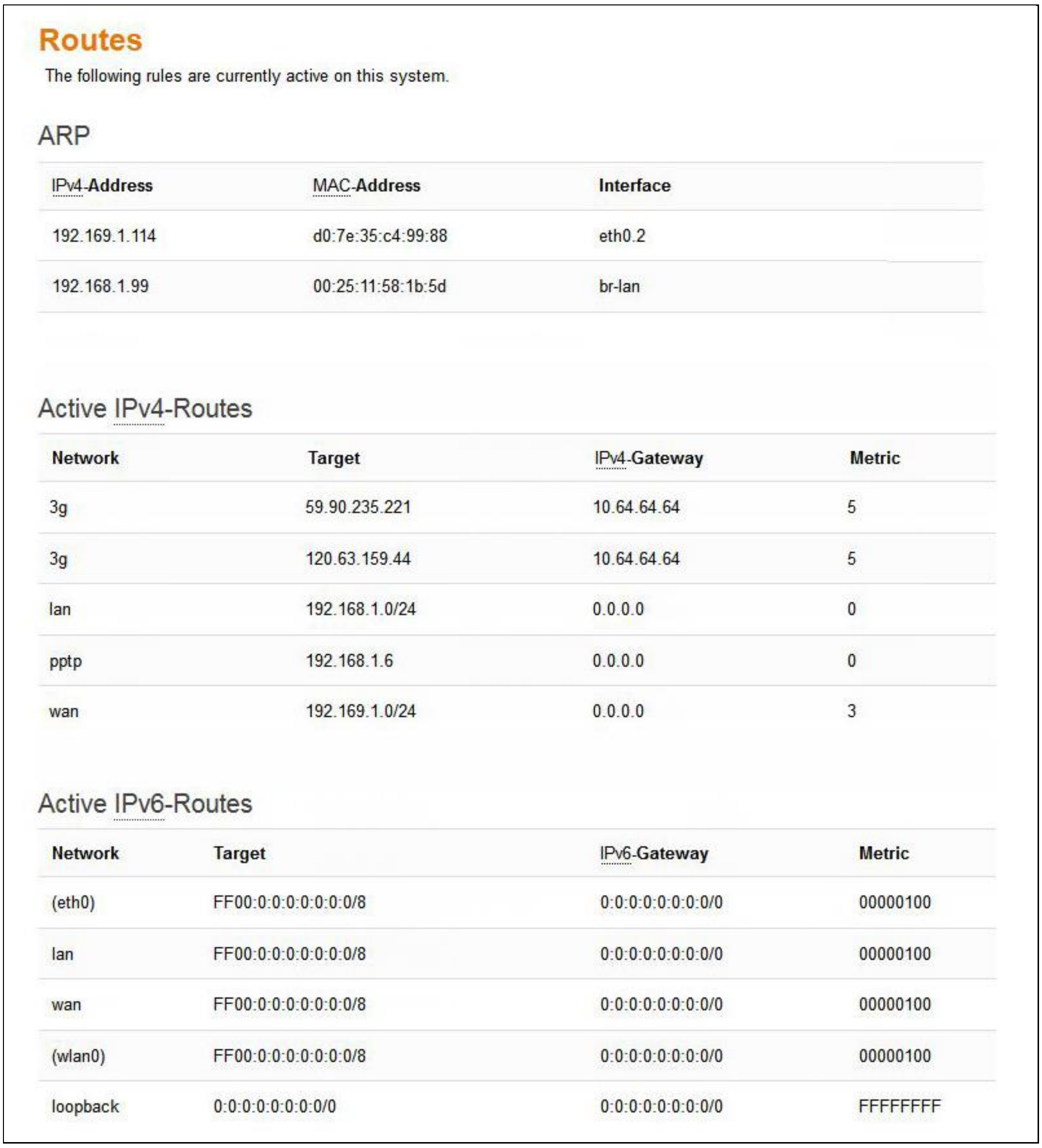
Parameters	Description
Reset Counters	Click to rest counters Packets and Traffic.
Reset Firewall	Click to reload the existing Firewall configuration of every interface.
Rule #	Displays the serial number of Firewall Rule.
Pkts	Displays the number of accepted packets.
Traffic	Displays the amount of traffic 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.
Destination	Displays the destination IPv6 Address.
Options	Displays the destination IPv4 Address.

Table 9.2-2: IPv6 Firewall Status

9.3 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 9.3-1: Routes Status

Parameters	Description
ARP – ARP table provides information about the peripherals connected on each interface	
IPv4 Address	Displays the IPv4 Address.
MAC Address	Displays MAC Address of the peripheral device.
Interface	Displays the interface name connected to the peripheral device.
Active IPv4 Routes – Displays the active IPv4 network route information.	
Network	Displays the network Type used by the active IPv4

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

Table 9.3-1: Routes Status

9.4 System Logs

Status > System Logs

Maestro 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.

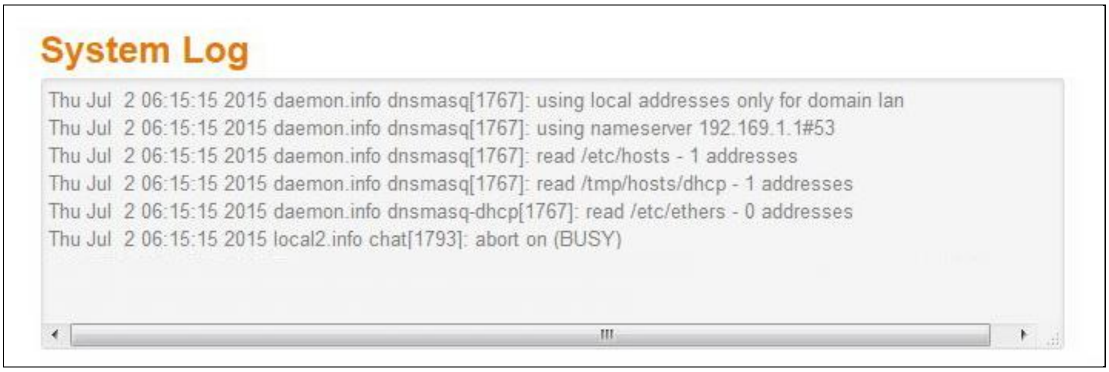
Maestro Router can either store logs locally or send logs to external syslog servers for storage and archival purposes.

Maestro Router can log many different network activities and traffic including:

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

Maestro Router supports a single syslog servers for remote logging and it can be configured from **System > System > Logging**.

Maestro Router can either store logs locally or send to the Syslog UDP servers.



System Log

```
Thu Jul  2 06:15:15 2015 daemon.info dnsmasq[1767]: using local addresses only for domain lan
Thu Jul  2 06:15:15 2015 daemon.info dnsmasq[1767]: using nameserver 192.169.1.1#53
Thu Jul  2 06:15:15 2015 daemon.info dnsmasq[1767]: read /etc/hosts - 1 addresses
Thu Jul  2 06:15:15 2015 daemon.info dnsmasq[1767]: read /tmp/hosts/dhcp - 1 addresses
Thu Jul  2 06:15:15 2015 daemon.info dnsmasq-dhcp[1767]: read /etc/ethers - 0 addresses
Thu Jul  2 06:15:15 2015 local2.info chat[1793]: abort on (BUSY)
```

Screen 9.4-1: System Logs

9.5 Realtime Graphs

Status > Realtime Graphs

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

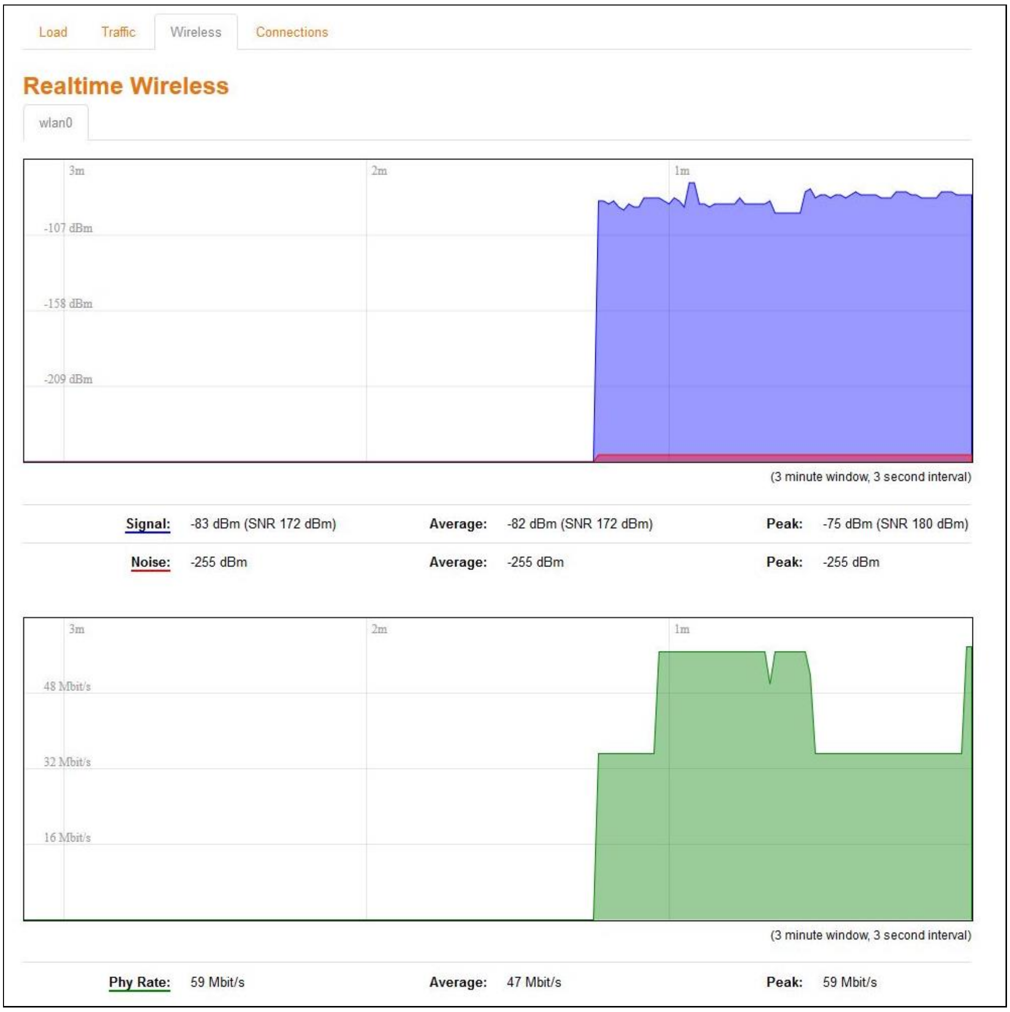
The period wise graph will display the following graphs for the selected period: Load Average, Interface Traffic information (LAN, WAN, Tunnel, Wi-Fi), Wireless usage Information and Connection detailed information.

9.5.1 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.



Realtime Wireless

(3 minute window, 3 second interval)

Signal:	-83 dBm (SNR 172 dBm)	Average:	-82 dBm (SNR 172 dBm)	Peak:	-75 dBm (SNR 180 dBm)
Noise:	-255 dBm	Average:	-255 dBm	Peak:	-255 dBm

(3 minute window, 3 second interval)

Phy Rate:	59 Mbit/s	Average:	47 Mbit/s	Peak:	59 Mbit/s

Screen 9.5-1: Real Time Wireless Traffic Graph

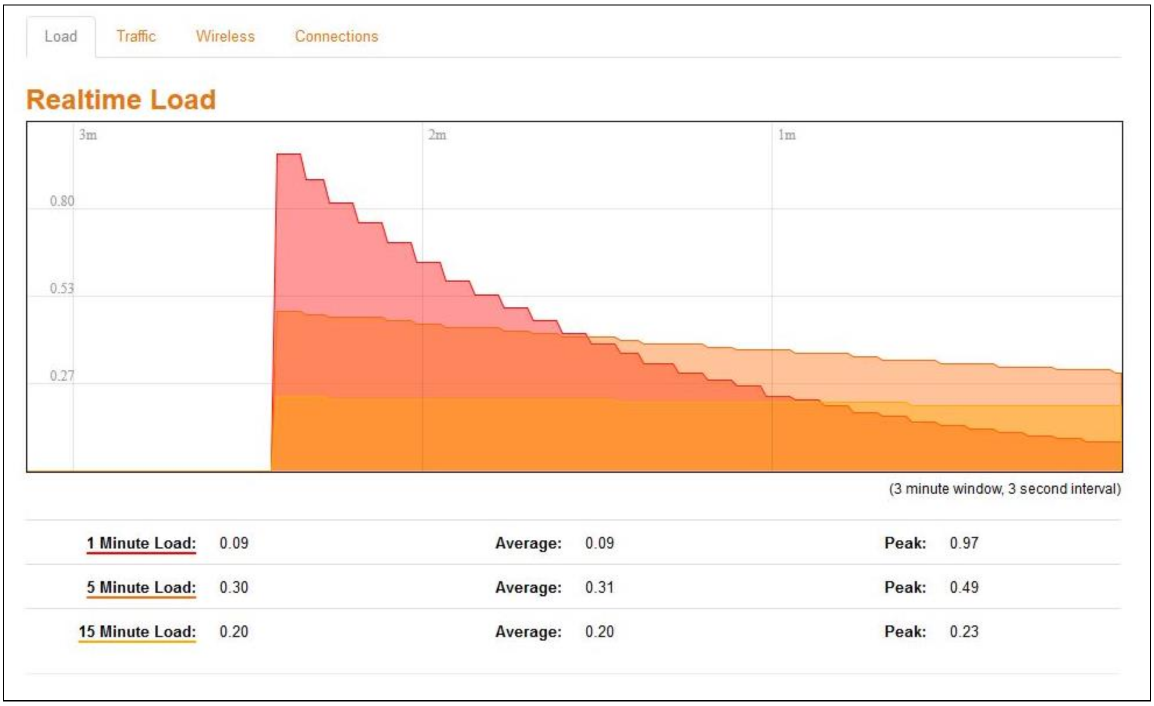
Parameters	Description
WLAN Interface	
Signal	Graph shows the periodic average of Signal and Noise on the Router. **Details** X axis – Time Interval (1 minute) Y axis – Data Rate (Mbit/s) **Legends** Blue – Signal Red – Noise Green – Physical Rate

Table 9.5-1: Real Time Wireless Traffic Graph

9.5.2 Load

Status Realtime Graphs > Load

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



Realtime Load

(3 minute window, 3 second interval)

1 Minute Load:	0.09	Average:	0.09	Peak:	0.97
5 Minute Load:	0.30	Average:	0.31	Peak:	0.49
15 Minute Load:	0.20	Average:	0.20	Peak:	0.23

Screen 9.5-2: 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 9.5-2: Real Time Load Graph

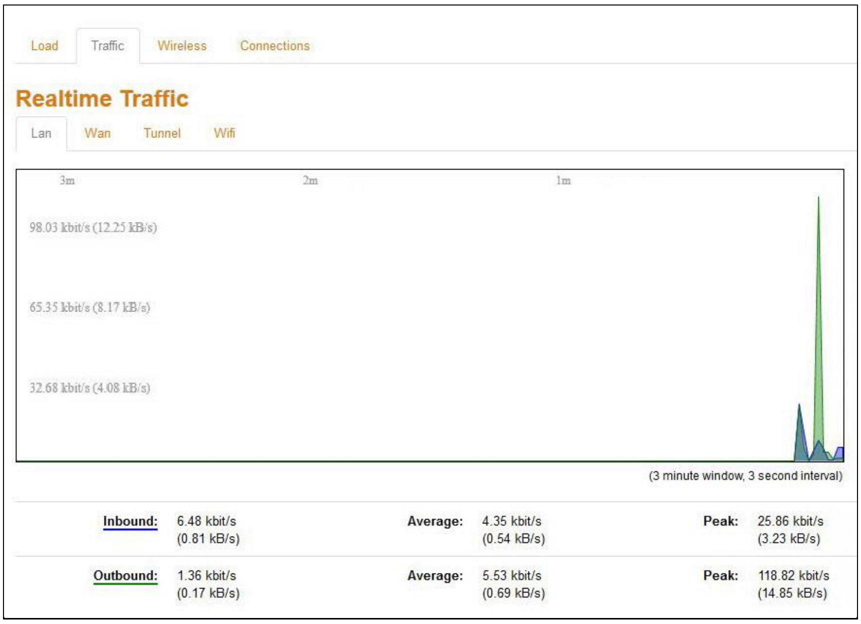
9.5.3 Traffic

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.



Inbound:	6.48 kbit/s (0.81 kB/s)	Average:	4.35 kbit/s (0.54 kB/s)	Peak:	25.86 kbit/s (3.23 kB/s)
Outbound:	1.36 kbit/s (0.17 kB/s)	Average:	5.53 kbit/s (0.69 kB/s)	Peak:	118.82 kbit/s (14.85 kB/s)

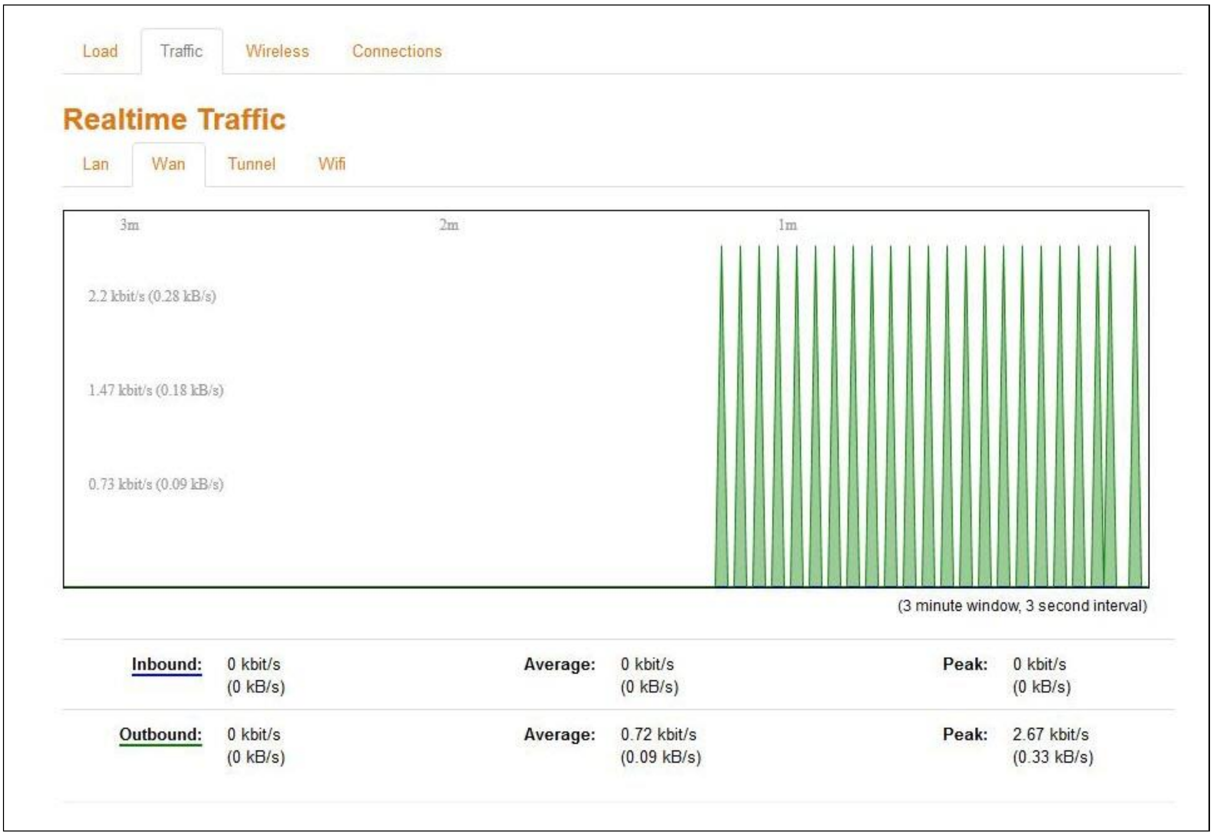
Screen 9.5-3: Real Time LAN Traffic Graph

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 9.5-3: 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.



Inbound:	0 kbit/s (0 kB/s)	Average:	0 kbit/s (0 kB/s)	Peak:	0 kbit/s (0 kB/s)
Outbound:	0 kbit/s (0 kB/s)	Average:	0.72 kbit/s (0.09 kB/s)	Peak:	2.67 kbit/s (0.33 kB/s)

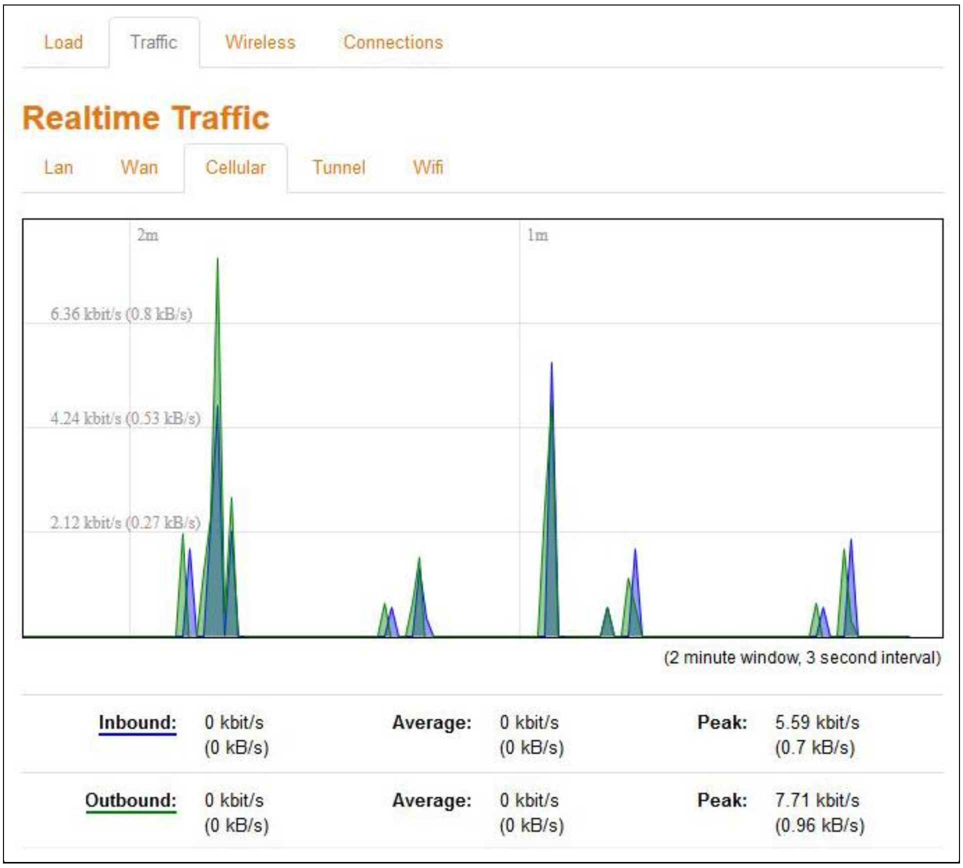
Screen 9.5-4: Real Time WAN Traffic Graph

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 9.5-4: Real Time WAN Traffic Graph

C. Cellular (Only for E206)

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



Inbound:	0 kbit/s (0 kB/s)	Average:	0 kbit/s (0 kB/s)	Peak:	5.59 kbit/s (0.7 kB/s)
Outbound:	0 kbit/s (0 kB/s)	Average:	0 kbit/s (0 kB/s)	Peak:	7.71 kbit/s (0.96 kB/s)

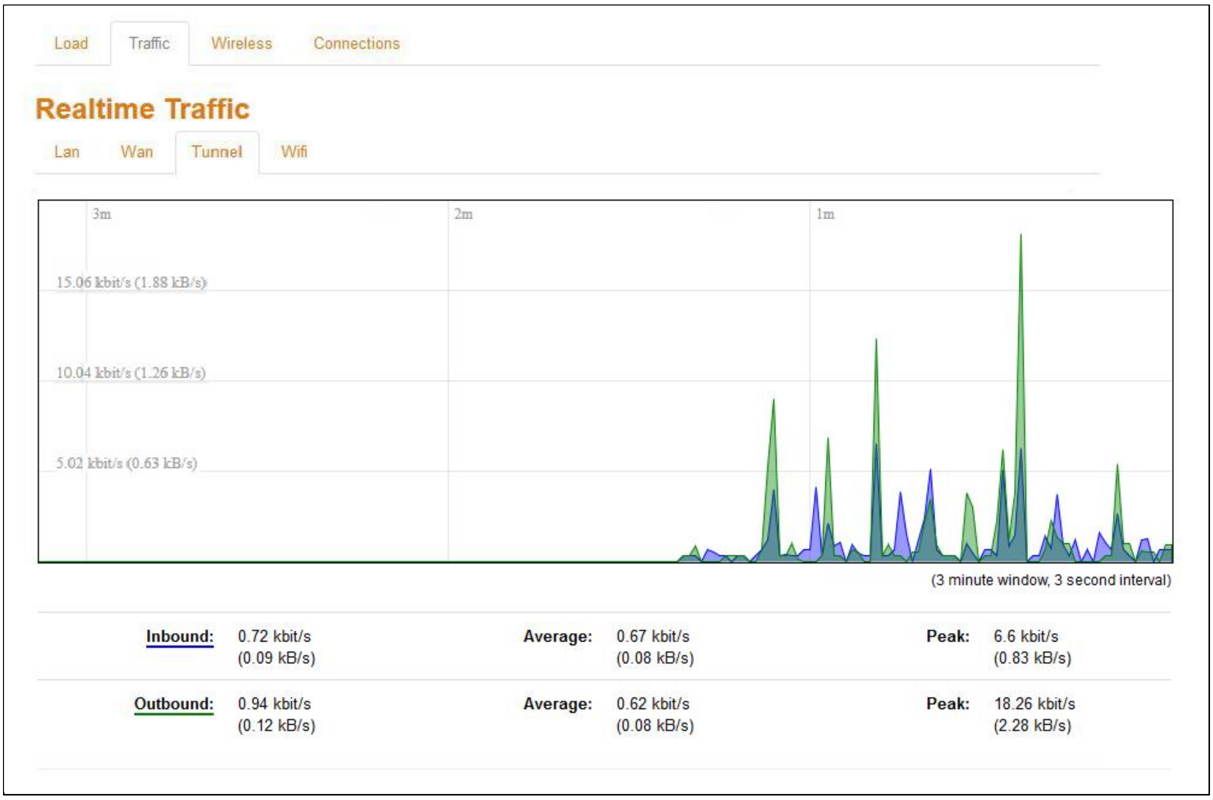
Screen 9.5-5: Real Time Cellular Traffic Graph

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 9.5-5: Real Time Cellular Traffic Graph

D. Tunnel

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



Inbound:	0.72 kbit/s (0.09 kB/s)	**Average:**	0.67 kbit/s (0.08 kB/s)	**Peak:**	6.6 kbit/s (0.83 kB/s)
Outbound:	0.94 kbit/s (0.12 kB/s)	**Average:**	0.62 kbit/s (0.08 kB/s)	**Peak:**	18.26 kbit/s (2.28 kB/s)

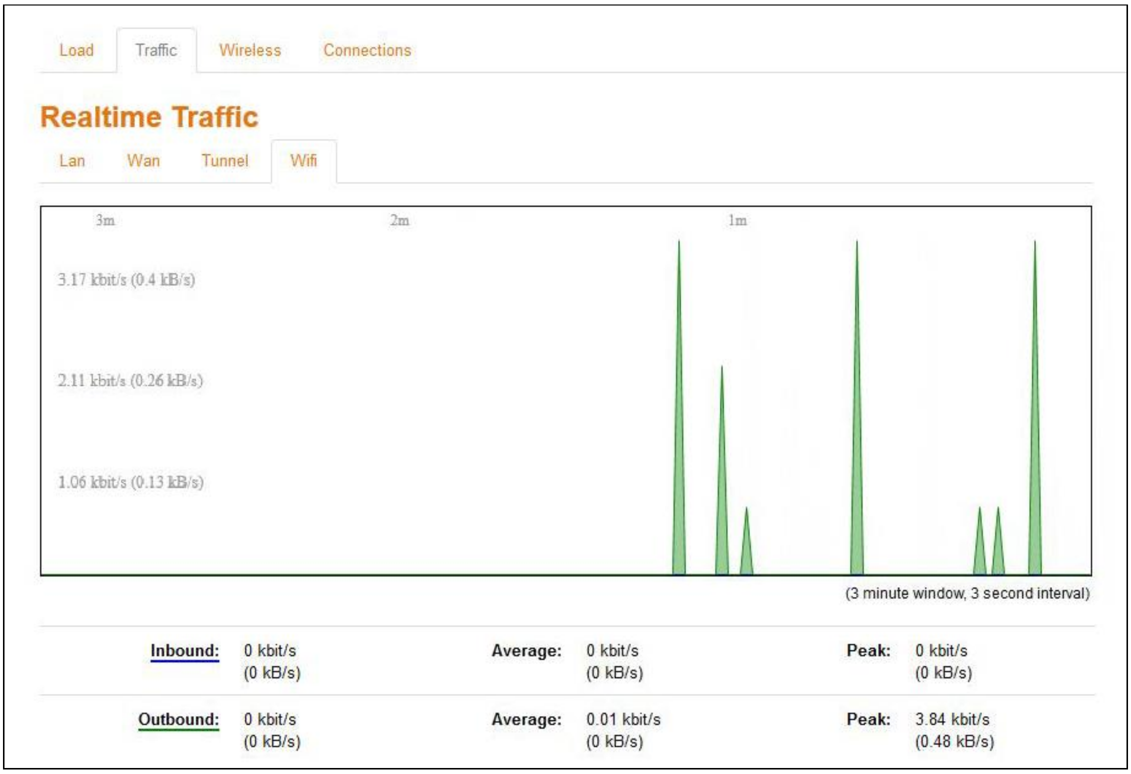
Screen 9.5-6: Real Time Tunnel Traffic Graph

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 9.5-6: 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.



(3 minute window, 3 second interval)

Inbound:	0 kbit/s (0 kB/s)	Average:	0 kbit/s (0 kB/s)	Peak:	0 kbit/s (0 kB/s)
Outbound:	0 kbit/s (0 kB/s)	Average:	0.01 kbit/s (0 kB/s)	Peak:	3.84 kbit/s (0.48 kB/s)

Screen 9.5-7: Real Time Wi-Fi Traffic Graph

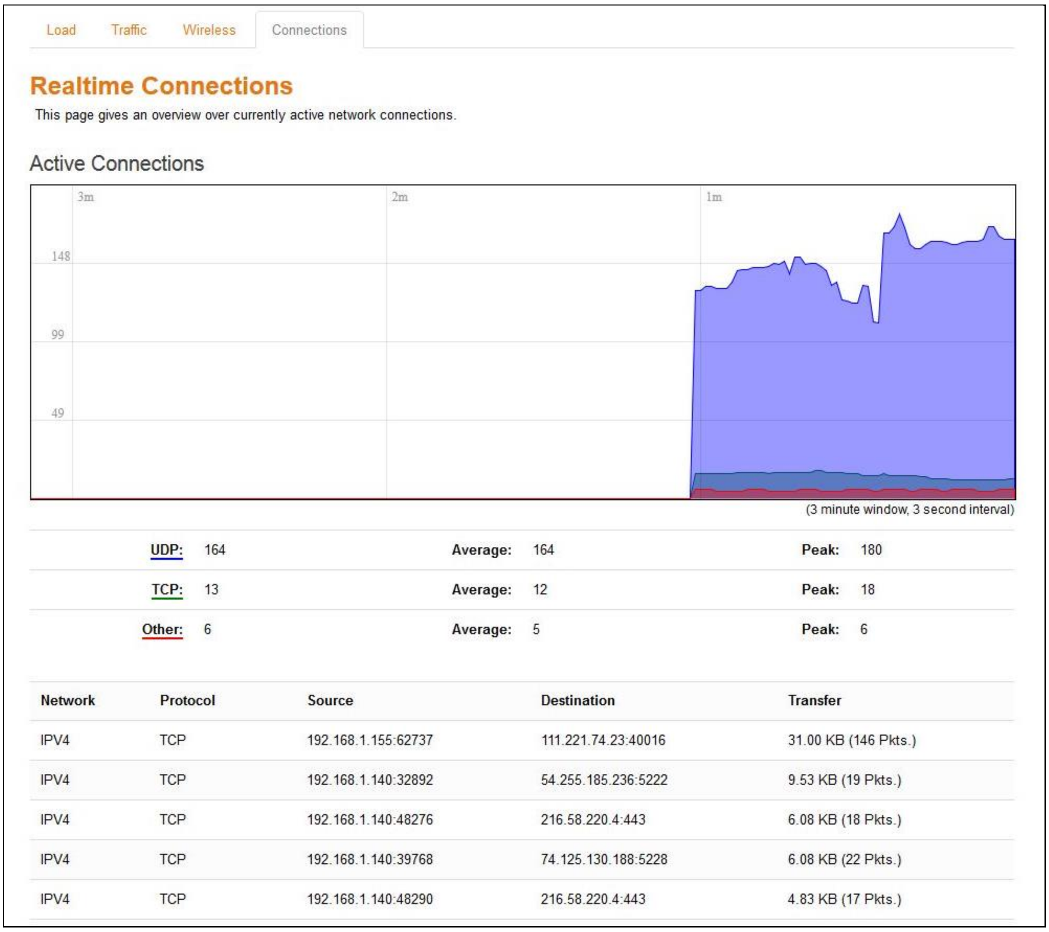
Parameters	Description
Traffic (Inbound / Outbound)	Graph shows the periodic average Wi-Fi Traffic on the Router. **Details** X axis – Time Interval (1 minute) Y axis – Wi-Fi Traffic (kB/s) **Legends** Blue – Inbound Traffic Green – Outbound Traffic

Table 9.5-7: Real Time Wi-Fi Traffic Graph

9.5.4 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.



Realtime Connections

This page gives an overview over currently active network connections.

Active Connections

(3 minute window, 3 second interval)

UDP:	164	Average:	164	Peak:	180
TCP:	13	Average:	12	Peak:	18
Other:	6	Average:	5	Peak:	6

Network	Protocol	Source	Destination	Transfer
IPV4	TCP	192.168.1.155:62737	111.221.74.23:40016	31.00 KB (146 Pkts.)
IPV4	TCP	192.168.1.140:32892	54.255.185.236:5222	9.53 KB (19 Pkts.)
IPV4	TCP	192.168.1.140:48276	216.58.220.4:443	6.08 KB (18 Pkts.)
IPV4	TCP	192.168.1.140:39768	74.125.130.188:5228	6.08 KB (22 Pkts.)
IPV4	TCP	192.168.1.140:48290	216.58.220.4:443	4.83 KB (17 Pkts.)

Screen 9.5-8: 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.
Transfer	Displays the total data transferred using the specific network connection.

Table 9.5-8: Real Time Connection Traffic Graph

10.System

System allows configuration and administration of router for secure and remote management including the localization of GUI. It also provides the basic system settings and language settings of the GUI.

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

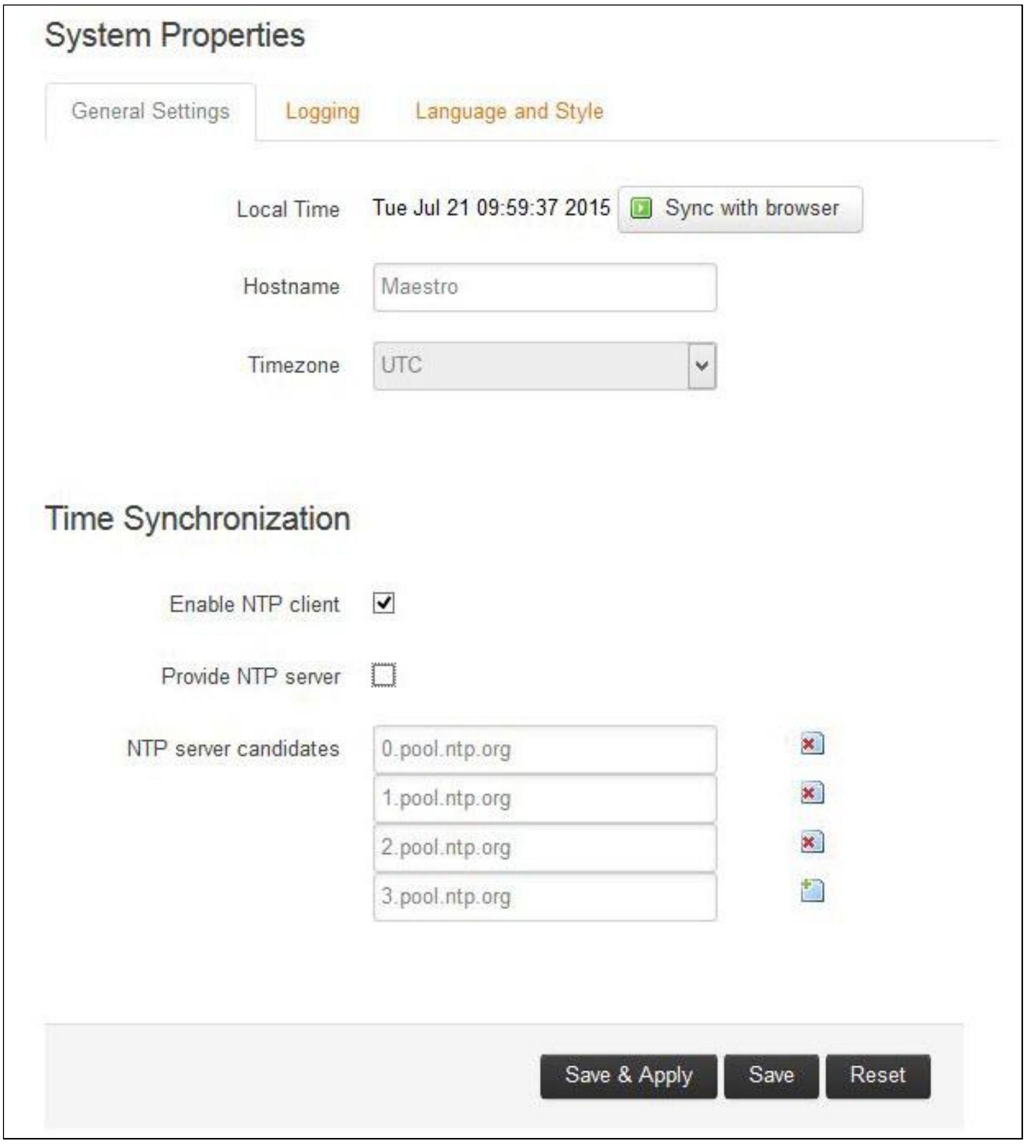
10.1 Systems

System > System

10.1.1 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.



System Properties

General Settings | Logging | Language and Style

Local Time: Tue Jul 21 09:59:37 2015

Hostname: Maestro

Timezone: UTC

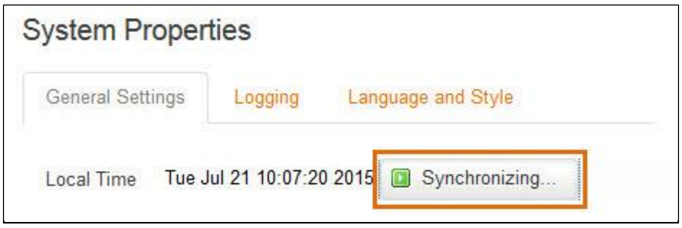
Time Synchronization

Enable NTP client ☑

Provide NTP server □

NTP server candidates: 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org, 3.pool.ntp.org

Screen 10.1-1: System General Settings

Parameters	Description
Local Time	Current router time. Click “Sync with browser” button to synchronize router clock with the local computer browser.  System Properties General Settings | Logging | Language and Style Local Time Tue Jul 21 10:07:20 2015 Synchronizing... ***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	
Enable NTP Client	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.
NTP Server Candidates	Displays the NTP server candidates. If NTP Server fails, the Router will try connecting to other configured NTP Server candidates in round robin manner. Click ☒ to delete the NTP server candidate. Click ➕ to add the NTP server candidate.

Table 10.1-1: System General Settings

10.1.2 Logging

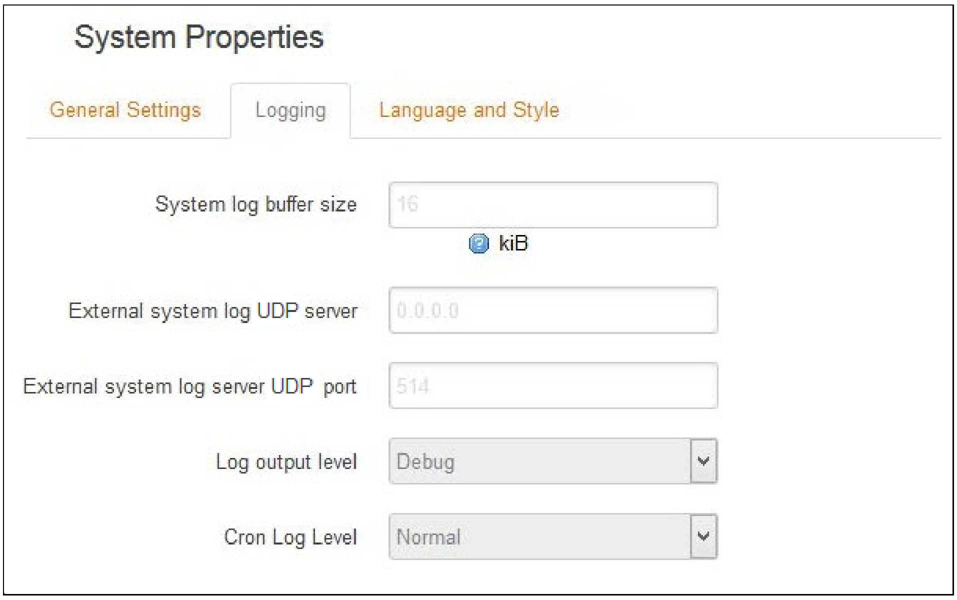
System > System > Logging

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.



System log buffer size: 16 kiB

External system log UDP server: 0.0.0.0

External system log server UDP port: 514

Log output level: Debug

Cron Log Level: Normal

Screen 10.1-2: 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

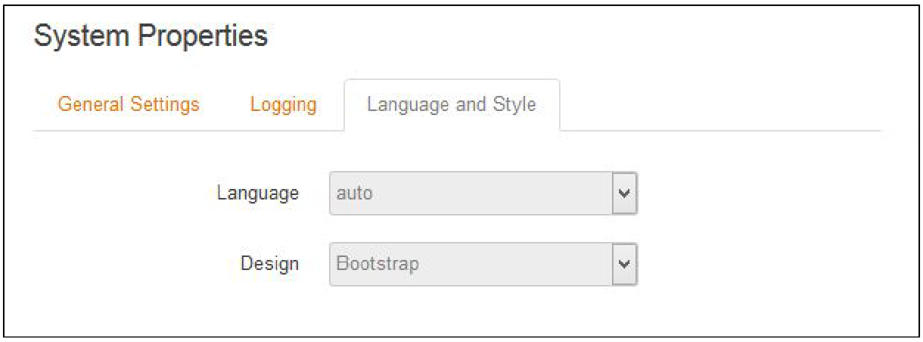
	time logs. The default IP Address of external log server is 0.0.0.0 ***Note*** • ***Enabling Remote Log features requires a Router to be manually rebooted.***
External system log UDP server port	Enter the Port number of an External UDP server system. UDP server is used to store the system logs The default 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 Maestro 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*** • ***We recommend you to contact Maestro Support team at support@maestro-wireless.com, if a warning message is received.*** - **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*** • ***We recommend you to contact Maestro Support team at support@maestro-wireless.com, if a warning message is received.***

Table 10.1-2: Syslog Configurations

10.1.3 Language and Style

System > System > Language and Style



System Properties

Language: auto

Design: Bootstrap

Screen 10.1-3: Language and Style Configurations

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

Table 10.1-3: Language and Style Configurations

10.2 Administration

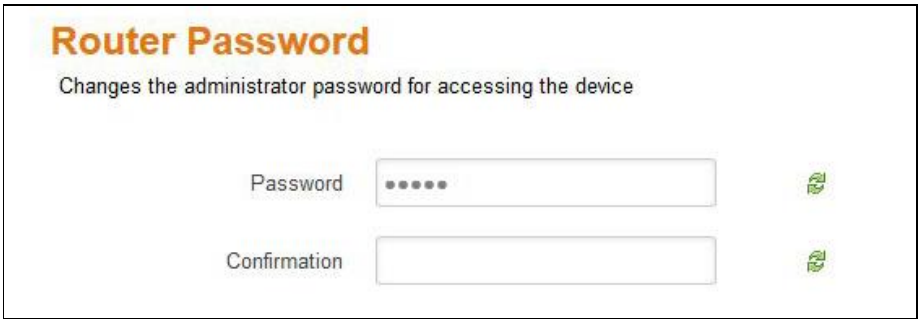
System > Administration

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

10.2.1 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.



Router Password

Changes the administrator password for accessing the device

Password: •••••

Confirmation:

Screen 10.2-1: 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 10.2-1: Router Credential Configurations

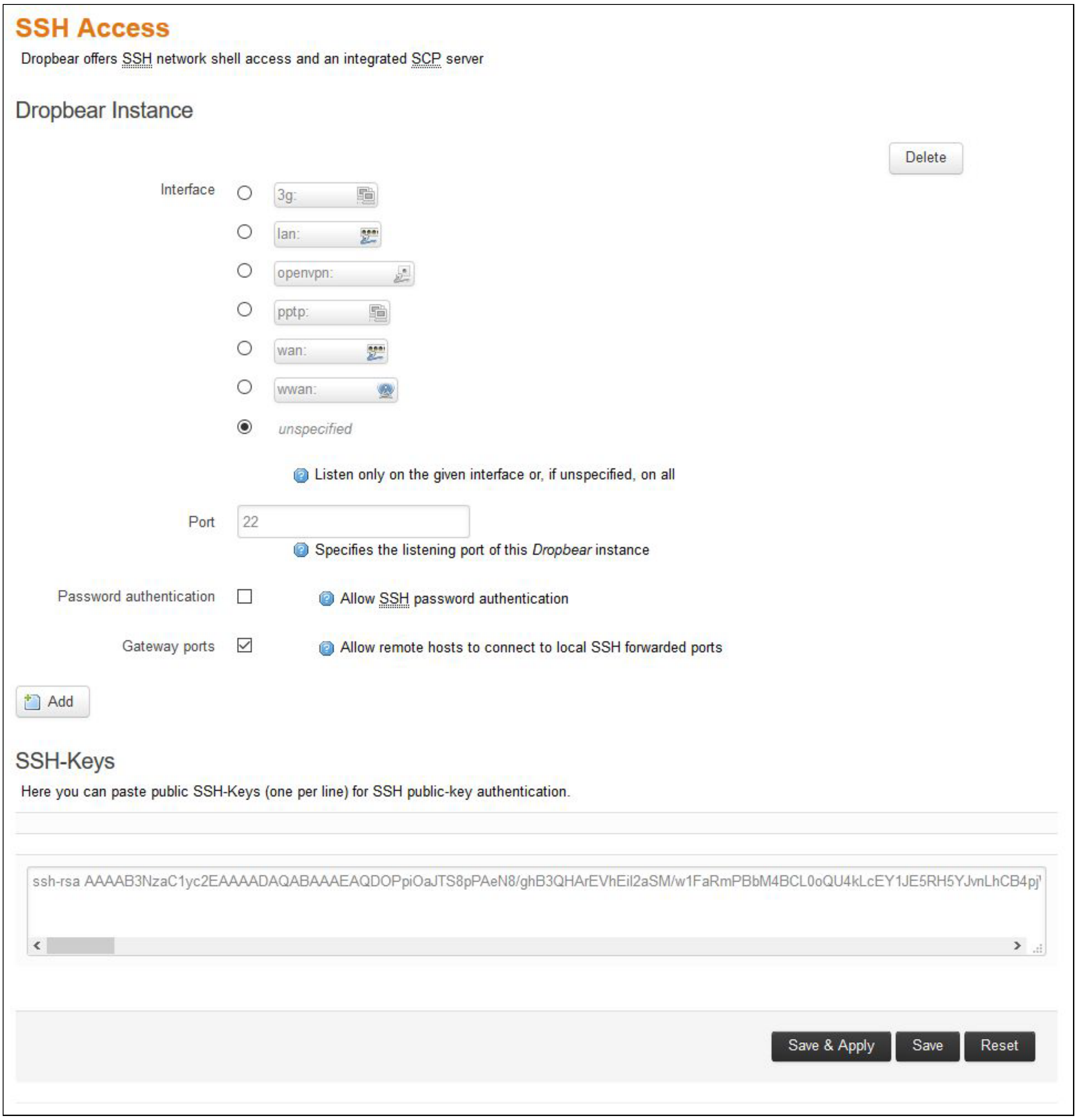
10.2.2 SSH Access

System > Administration > SSH Access

The E200 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.



SSH Access

Dropbear offers SSH network shell access and an integrated SCP server

Dropbear Instance

Interface ○ 3g: ○ lan: ○ openvpn: ○ pptp: ○ wan: ○ wwan: ● *unspecified*

Listen only on the given interface or, if unspecified, on all

Port: 22

Specifies the listening port of this *Dropbear* instance

Password authentication □ Allow SSH password authentication

Gateway ports ☑ Allow remote hosts to connect to local SSH forwarded ports

SSH-Keys

Here you can paste public SSH-Keys (one per line) for SSH public-key authentication.

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAEAQDOPpiOaJTS8pPAeN8/ghB3QHArEVhEil2aSM/w1FaRmPBbM4BCL0oQU4kLcEY1JE5RH5YJvnLhCB4pj
```

Screen 10.2-2: 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 10.2-2: SSH Access Configurations

10.3 Software

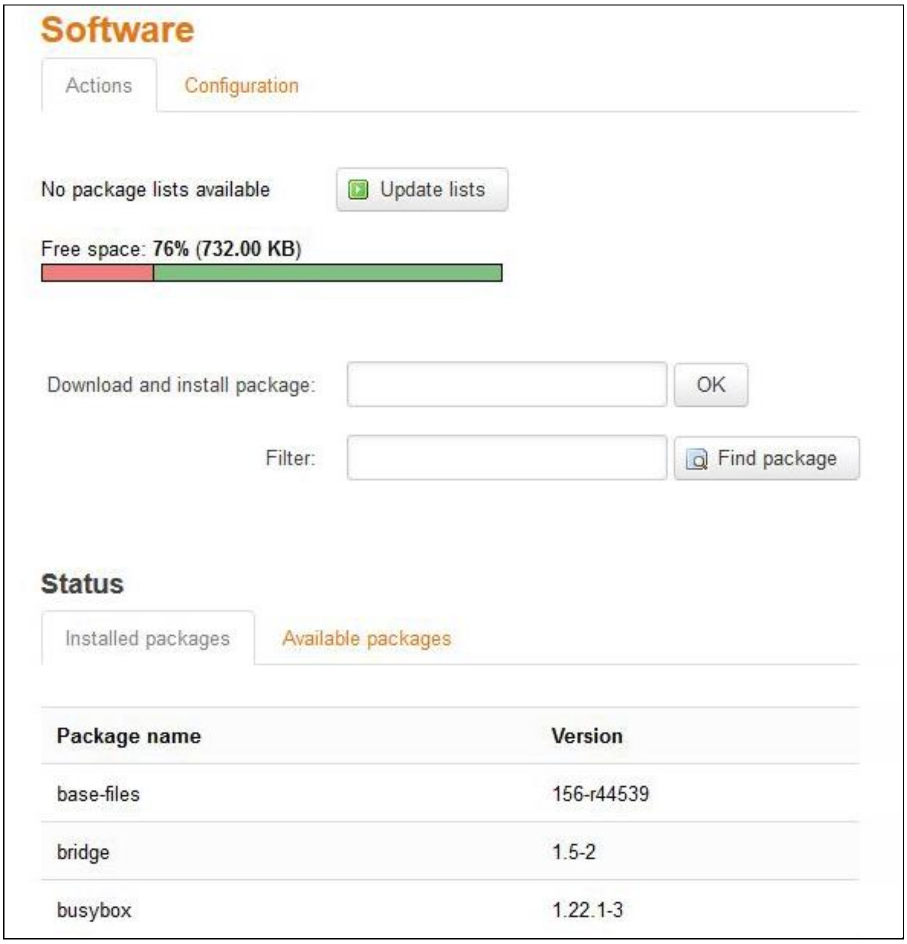
System > Software

Software page give you access to the list of installed as well as available software package or filter installed on your router.

10.3.1 Actions

System > Software > Actions

A. Installed



Software

No package lists available

Free space: 76% (732.00 KB)

Download and install package:

Filter:

Status

Package name	Version
base-files	156-r44539
bridge	1.5-2
busybox	1.22.1-3

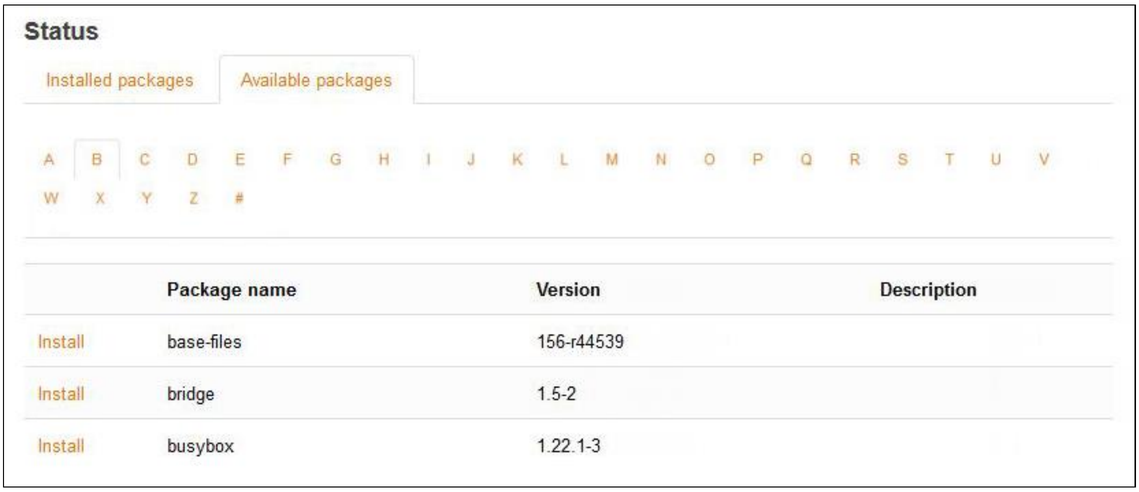
Screen 10.3-1: Software Installation and Installed Package Details

Parameters	Description
Update lists	Click to update the package list from the package repository servers.
Free space	Indicates the free space and used space. **Legends** 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 10.3-1: Software Installation and Installed Package Details

B. Available



Status

Installed packages | Available packages

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z #

	Package name	Version	Description
Install	base-files	156-r44539	
Install	bridge	1.5-2	
Install	busybox	1.22.1-3	

Screen 10.3-2: Software Packages Available for Installation

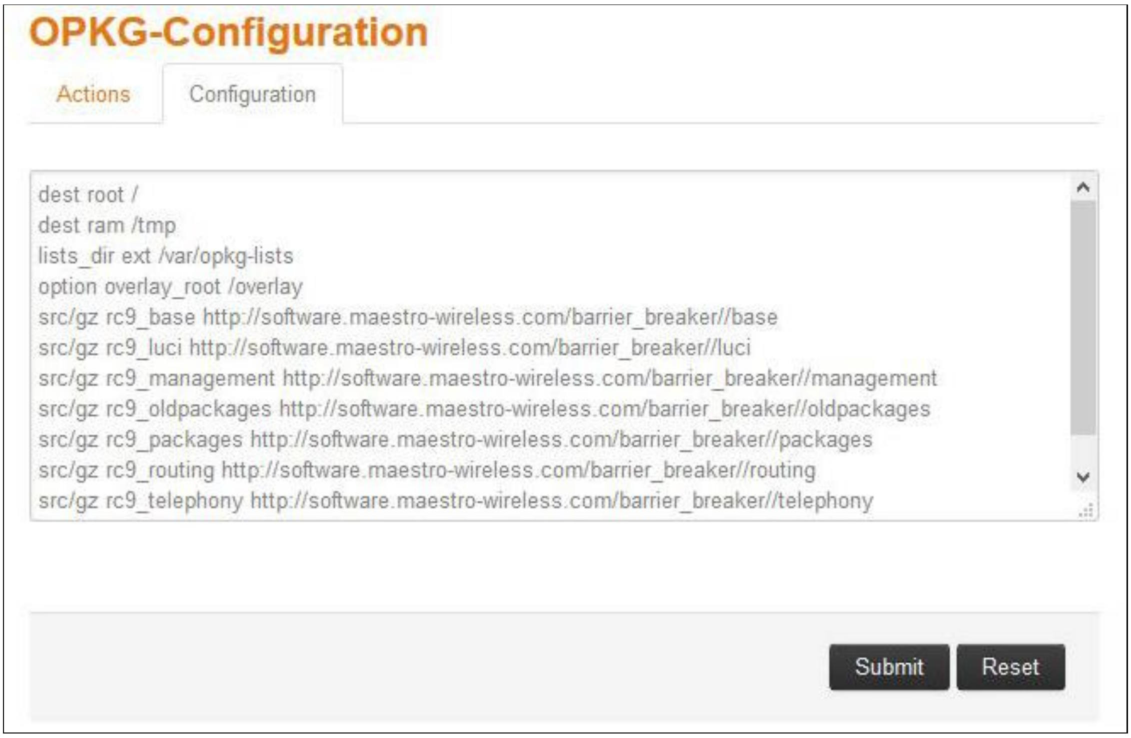
Parameters	Description
Install	Click Install against respective Package to install it.
Package name	Displays the name of package.
Version	Displays the version of package.
Description	Displays the description of package.

Table 10.3-2: Software Packages Available for Installation

10.3.2 Configuration

System > Software > Configuration

This configuration page enlists the available servers. You can look-up a server to search and update packages.



```
dest root /
dest ram /tmp
lists_dir ext /var/opkg-lists
option overlay_root /overlay
src/gz rc9_base http://software.maestro-wireless.com/barrier_breaker//base
src/gz rc9_luci http://software.maestro-wireless.com/barrier_breaker//luci
src/gz rc9_management http://software.maestro-wireless.com/barrier_breaker//management
src/gz rc9_oldpackages http://software.maestro-wireless.com/barrier_breaker//oldpackages
src/gz rc9_packages http://software.maestro-wireless.com/barrier_breaker//packages
src/gz rc9_routing http://software.maestro-wireless.com/barrier_breaker//routing
src/gz rc9_telephony http://software.maestro-wireless.com/barrier_breaker//telephony
```

Screen 10.3-3: Software Configuration - OPKG

10.4 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. There are many ways of taking backup and just as many types of media to use as well.

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.

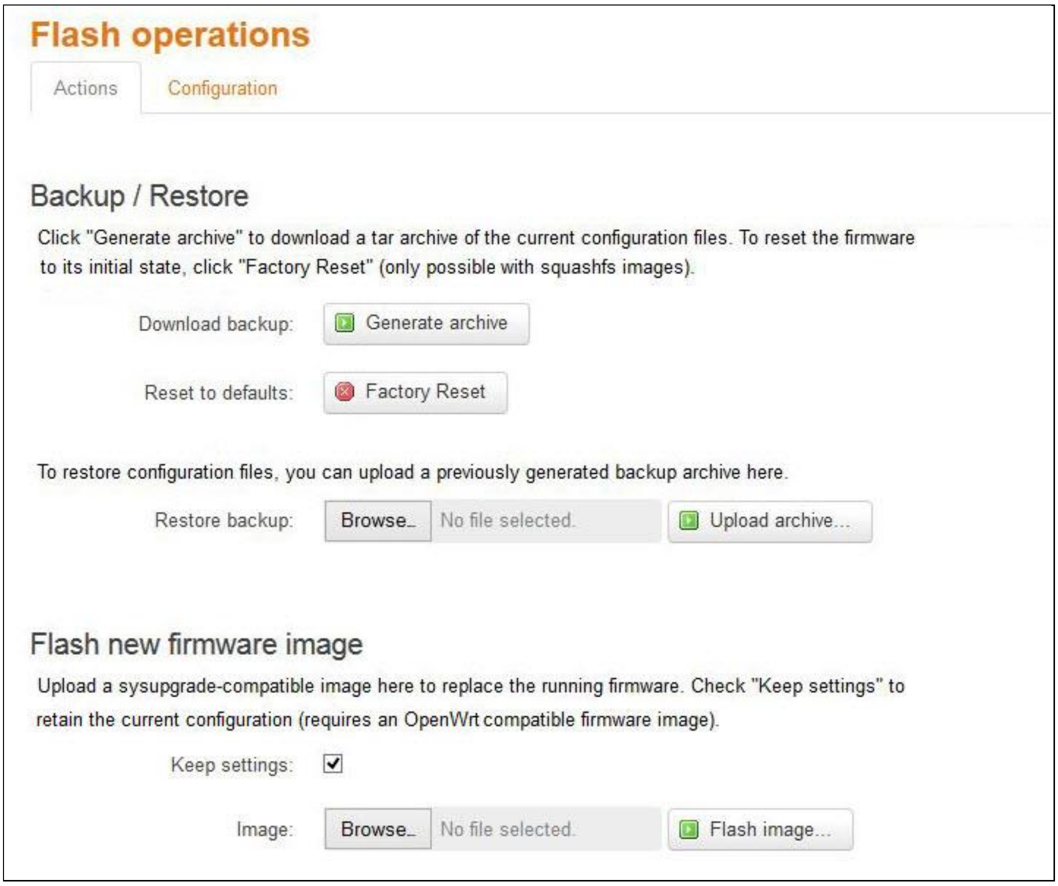
Note

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

10.4.1 Flash Operation

System > Backup / Flash Firmware > Flash Operation

A. Actions



Flash operations

Actions | Configuration

Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Factory Reset" (only possible with squashfs images).

Download backup: Generate archive

Reset to defaults: Factory Reset

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup: Browse... No file selected. Upload archive...

Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an OpenWrt compatible firmware image).

Keep settings: ☑

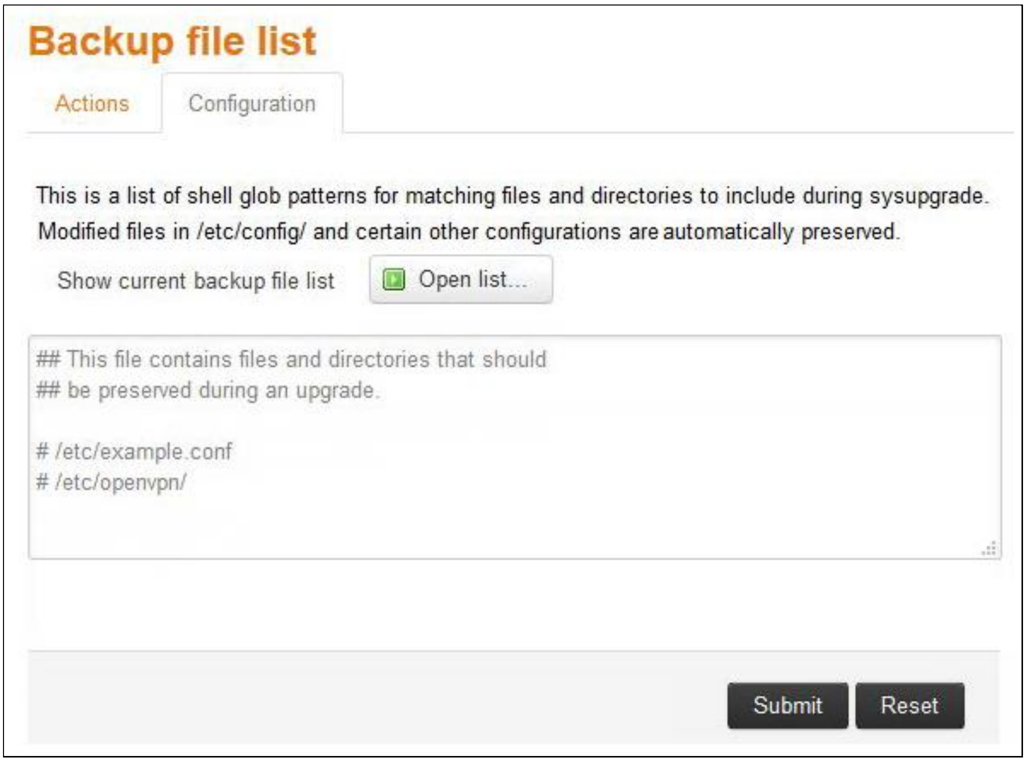
Image: Browse... No file selected. Flash image...

Screen 10.4-1: 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 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 by Maestro Wireless Solutions personnel.

Table 10.4-1: Backup - Restore and Flash Operations

B. Configurations



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

Show current backup file list Open list...

```
## This file contains files and directories that should
## be preserved during an upgrade.

# /etc/example.conf
# /etc/openvpn/
```

Screen 10.4-2: Backup File Configurations

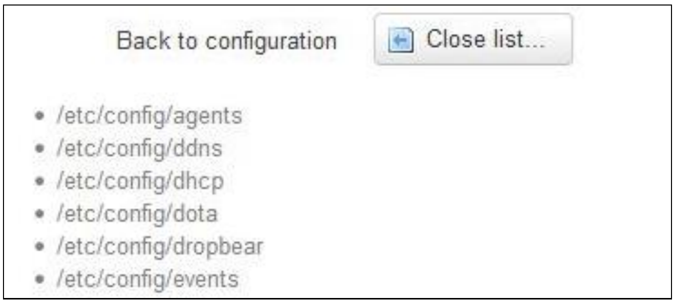
Parameters	Description
Open list	Click to open the list of files and directories that should be preserved during an upgrade.  Back to configuration Close list... • /etc/config/agents • /etc/config/ddns • /etc/config/dhcp • /etc/config/dota • /etc/config/dropbear • /etc/config/events

Table 10.4-2: Backup File Configurations

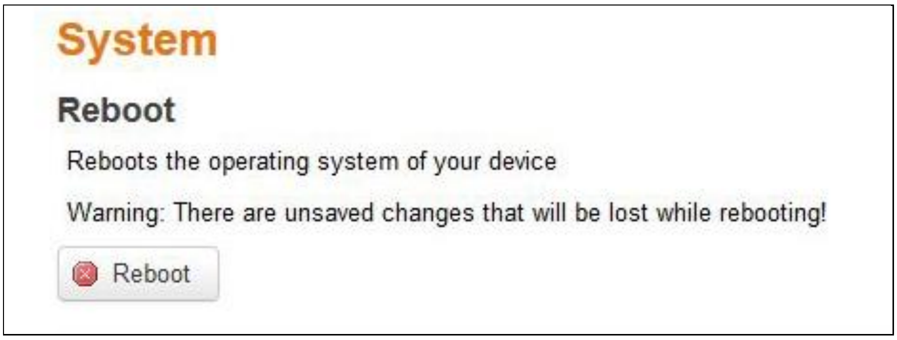
10.5 Reboot

System > Reboot

Router will be rebooted and will reload the configuration.

Note

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



System

Reboot

Reboots the operating system of your device

Warning: There are unsaved changes that will be lost while rebooting!

Screen 10.5-1: System Reboot

11.Network

E200 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
- Static Routes
- Diagnostics
- Firewall

11.1 Interfaces

Network > Interface

Interface sub-module provides the overview of the interface configuration that includes the network configuration, interface status, VPN configuration. 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
- 3G (Only for E205)
- CELLDHCP (Only for E206)
- CELLULAR
- WAN
- PPTP
- LAN
- WWAN
- OpenVPN

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, 3G, WAN 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:

Interface→ Protocols↓	LAN	WAN	OpenVPN	PPtP	WWAN	Cellular/3G	CELLDCHP (E206)
Static Address	✓	✓	✗	✗	✗	✗	✗
DHCP Client	✗	✓	✗	✗	✓	✗	✓
Unmanaged	✗	✗	✓	✗	✗	✗	✗
PPTP	✗	✗	✗	✓	✗	✗	✗
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

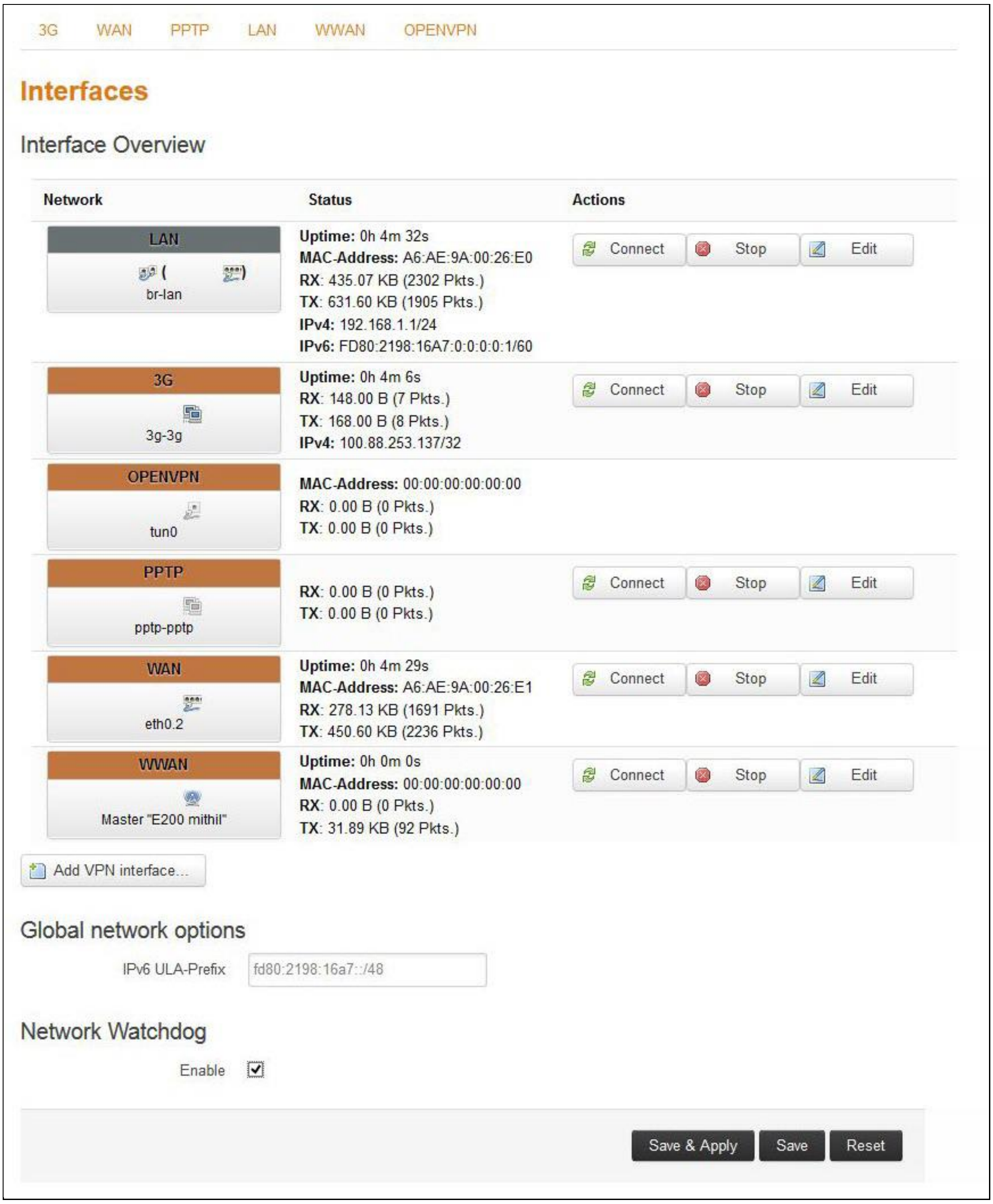
	custom DNS servers. - **IPv6 assignment length –** Select the IPv6 assignment length. Available Options • **64 –** Assign a part of the given length of public IPv6-prefix to this interface. • **disabled** • **--custom-- –** Assign a part of the given length of public IPv6-prefix to this interface. IPv6 assignment length is disabled by default. - **IPv6 address -** Enter the IPv6 Address. - **IPv6 gateway -** Enter the IPv6 Address for Gateway. - **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.
Unmanaged	Enter the metric for the unmanaged gateway.
PPtP	- **VPN Server –** Enter the name of the VPN

	Server. - **VPN Server –** Enter the name of the VPN Server. The default VPN Server name is admin. - **PAP/CHAP username –** Enter the PAP/CHAP username. Click 🔄 to reset the password. The default password is admin.
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. - **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:

	• **UTMS/GPRS –** The router selects the best available service. • **UTMS Only –** The router connects only to 3G/UMTS network. • **GPRS Only –** The router connects only to GPRS network. **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.
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.

11.1.1 Interface Overview

Network > Interface > Interface Overview



Interfaces

Interface Overview

Network	Status	Actions
LAN br-lan	**Uptime:** 0h 4m 32s **MAC-Address:** A6:AE:9A:00:26:E0 **RX**: 435.07 KB (2302 Pkts.) **TX**: 631.60 KB (1905 Pkts.) **IPv4:** 192.168.1.1/24 **IPv6:** FD80:2198:16A7:0:0:0:0:1/60	Connect Stop Edit
3G 3g-3g	**Uptime:** 0h 4m 6s **RX**: 148.00 B (7 Pkts.) **TX**: 168.00 B (8 Pkts.) **IPv4:** 100.88.253.137/32	Connect Stop Edit
OPENVPN tun0	**MAC-Address:** 00:00:00:00:00:00 **RX**: 0.00 B (0 Pkts.) **TX**: 0.00 B (0 Pkts.)	
PPTP pptp-pptp	**RX**: 0.00 B (0 Pkts.) **TX**: 0.00 B (0 Pkts.)	Connect Stop Edit
WAN eth0.2	**Uptime:** 0h 4m 29s **MAC-Address:** A6:AE:9A:00:26:E1 **RX**: 278.13 KB (1691 Pkts.) **TX**: 450.60 KB (2236 Pkts.)	Connect Stop Edit
WWAN Master "E200 mithil"	**Uptime:** 0h 0m 0s **MAC-Address:** 00:00:00:00:00:00 **RX**: 0.00 B (0 Pkts.) **TX**: 31.89 KB (92 Pkts.)	Connect Stop Edit

Global network options

IPv6 ULA-Prefix: fd80:2198:16a7::/48

Network Watchdog

Enable ☑

Screen 11.1-1: Interface Overview

Parameters	Description
Interface Overview	
Network	Displays the all the configured Network Interfaces. The pre-configured interfaces for the router are - LAN - 3G (Only for E205)

	CELLDHCP (Only for E206) CELLULAR (Only for E206) WAN WWAN PPTP OpenVPN ***Note*** • ***Default Interfaces LAN, 3G, WAN, WWAN, PPTP and OpenVPN cannot be deleted.*** • ***When Wi-Fi is configured as Client, Interface WWAN will become active.***
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 Interfaces may need some complex configuration modification in load balancer settings. We recommend you to contact Maestro Wireless Support before adding an interface.***
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.

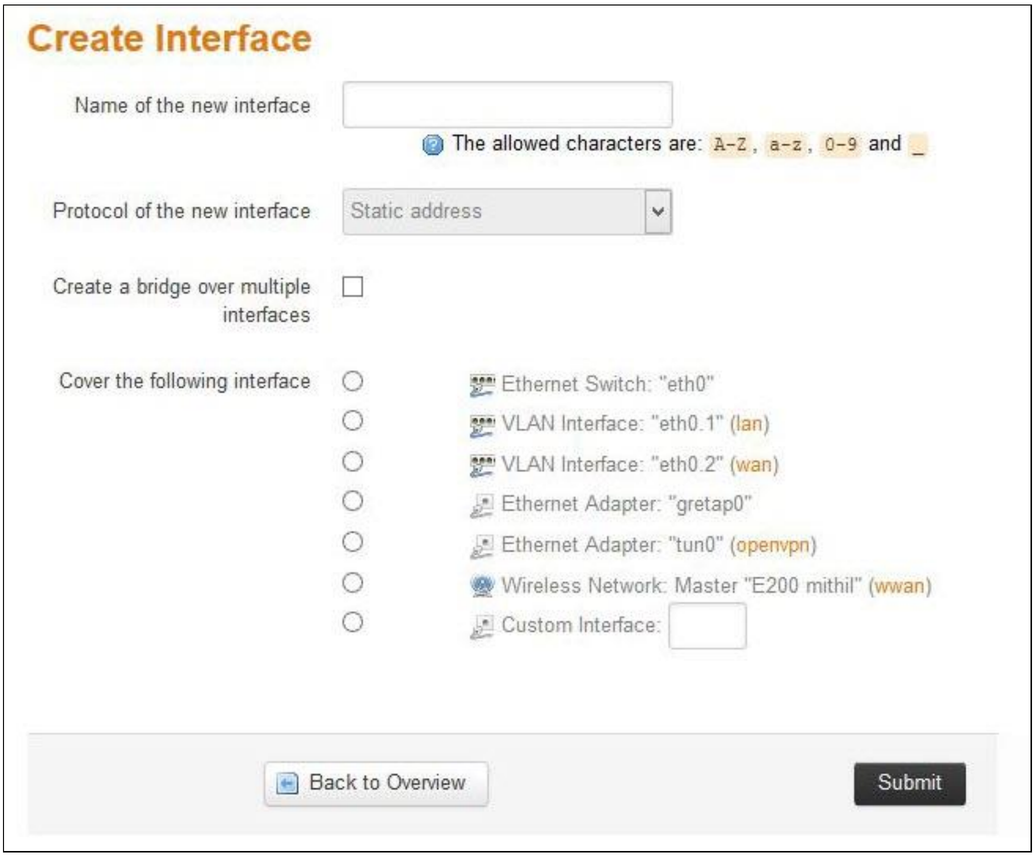
	By default, the network watchdog is in disable mode.

Table 11.1-1: Interface Overview

A. Add VPN Interface

Note

- ***Adding a Virtual Interfaces may need some complex configuration modification in load balancer settings. We recommend you to contact Maestro Wireless Support before adding an interface.***



Create Interface

Name of the new interface:

The allowed characters are: A-Z, a-z, 0-9 and _

Protocol of the new interface: Static address

Create a bridge over multiple interfaces: □

Cover the following interface:
- ○ Ethernet Switch: "eth0"
- ○ VLAN Interface: "eth0.1" (lan)
- ○ VLAN Interface: "eth0.2" (wan)
- ○ Ethernet Adapter: "gretap0"
- ○ Ethernet Adapter: "tun0" (openvpn)
- ○ Wireless Network: Master "E200 mithil" (wwan)
- ○ Custom Interface:

Screen 11.1-2: 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)

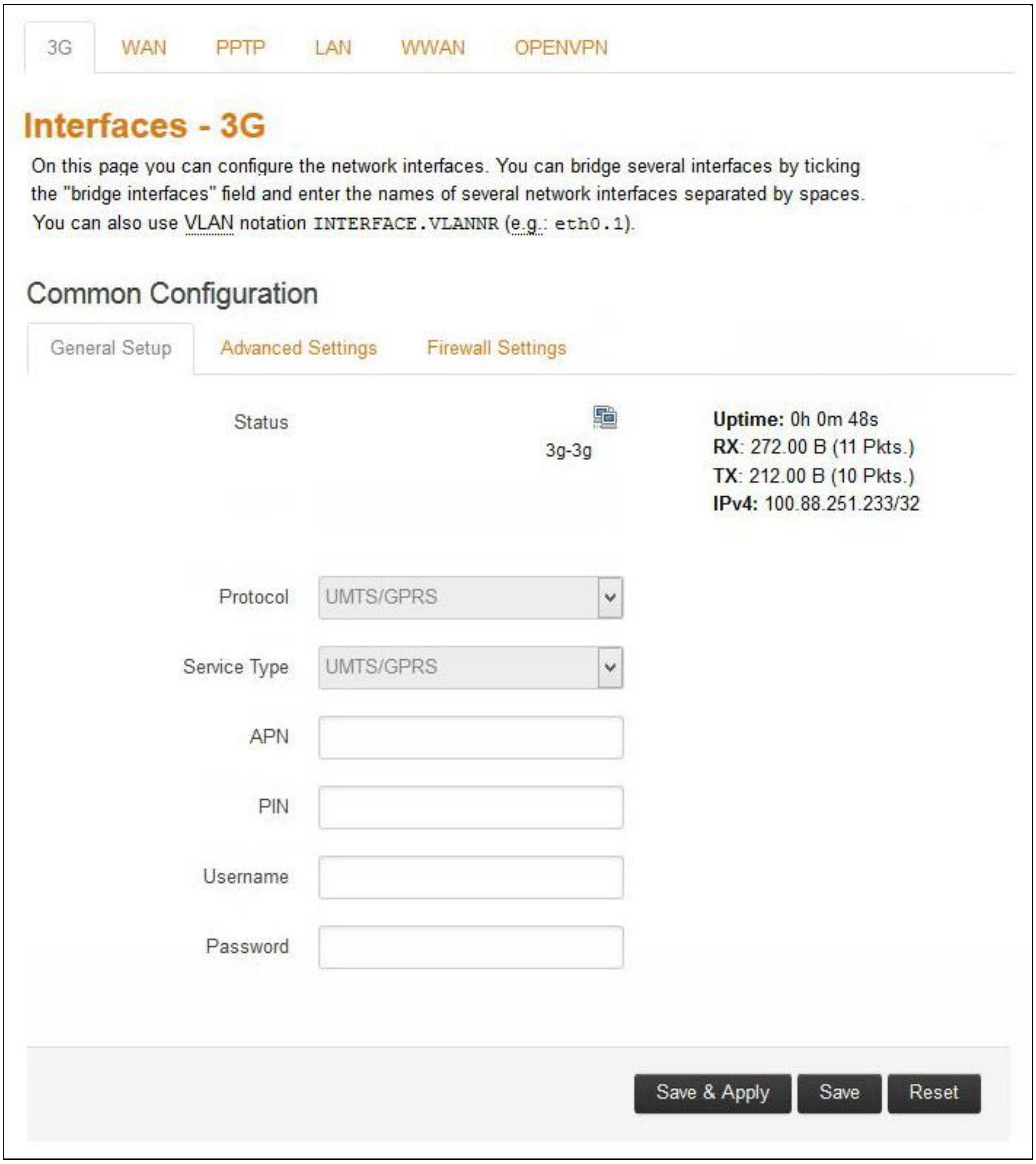
Create a bridge over multiple interface	Click to enable creating a bridge over multiple interfaces.
Cover the following interfaces	Select the interface to be configured. Select more than one interface, if a parameter creating a bridge over multiple interfaces is enabled.
Back to Overview	Click to return to Interface Overview page.

Table 11.1-2: Configure VPN Interface

11.1.2 3G (Only for E205)

Network > Interface > 3G

A. General Setup



Interfaces - 3G

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Status 3g-3g

Uptime: 0h 0m 48s
RX: 272.00 B (11 Pkts.)
TX: 212.00 B (10 Pkts.)
IPv4: 100.88.251.233/32

Protocol: UMTS/GPRS

Service Type: UMTS/GPRS

APN

PIN

Username

Password

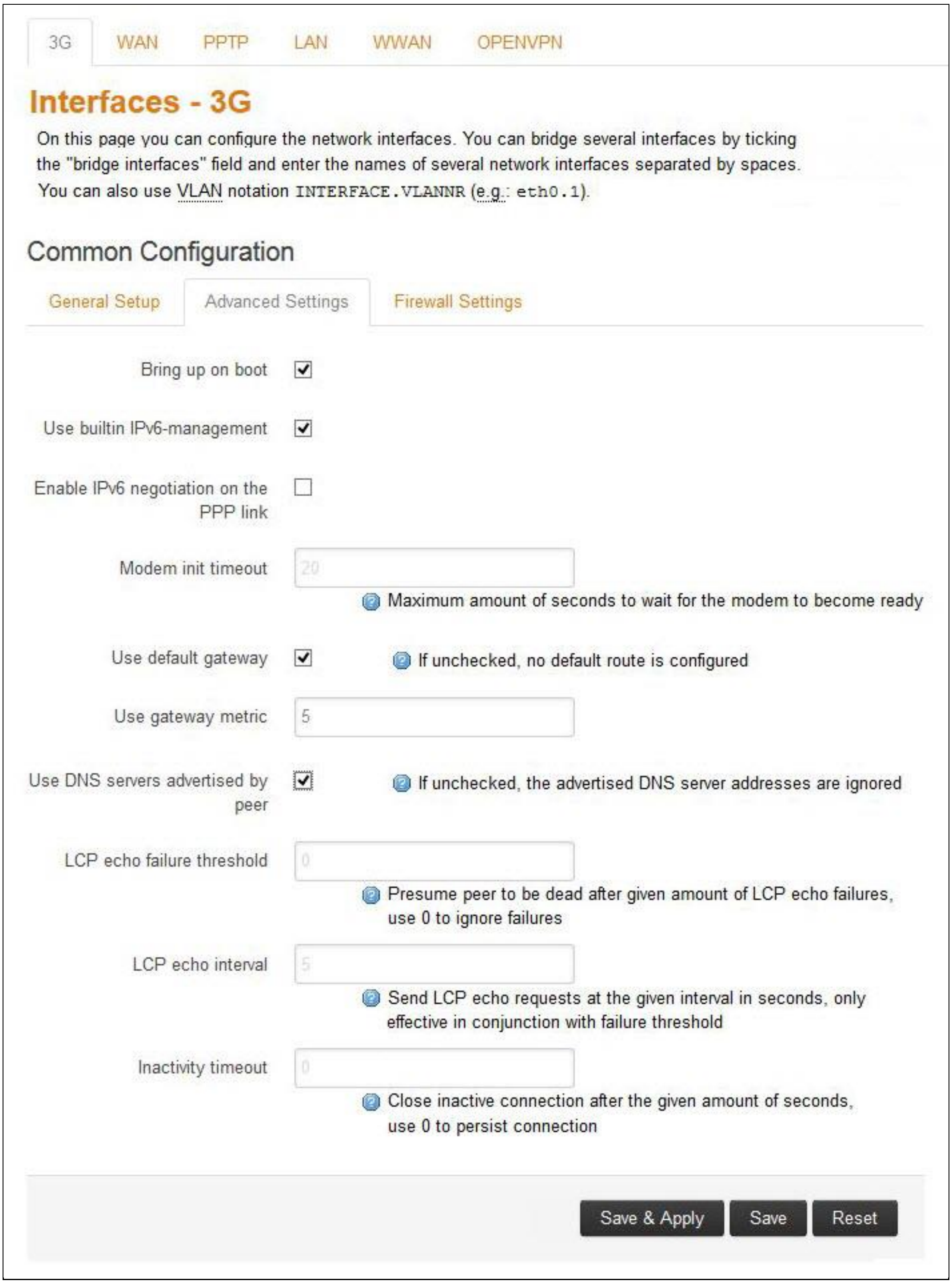
Screen 11.1-3: General Configurations for 3G Interface

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*** • ***DO NOT select any other protocol.***
Service Type	Select the type of service from the available: • **UTMS/GPRS –** The router selects the best available service. • **UTMS –** The router connects only to 3G/UMTS network. • **GPRS –** The router connects only to GPRS network.
APN	Enter the APN provided by your network operator.
PIN	Enter the SIM PIN if any.
Username	Enter the Username for the Data connection if any.
Password	Enter the Password for the Data connection if any.

Table 11.1-3: General Configurations for 3G Interface

B. Advanced Settings



Interfaces - 3G

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Bring up on boot ☑

Use builtin IPv6-management ☑

Enable IPv6 negotiation on the PPP link □

Modem init timeout: 20
Maximum amount of seconds to wait for the modem to become ready

Use default gateway ☑
If unchecked, no default route is configured

Use gateway metric: 5

Use DNS servers advertised by peer ☑
If unchecked, the advertised DNS server addresses are ignored

LCP echo failure threshold: 0
Presume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures

LCP echo interval: 5
Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold

Inactivity timeout: 0
Close inactive connection after the given amount of seconds, use 0 to persist connection

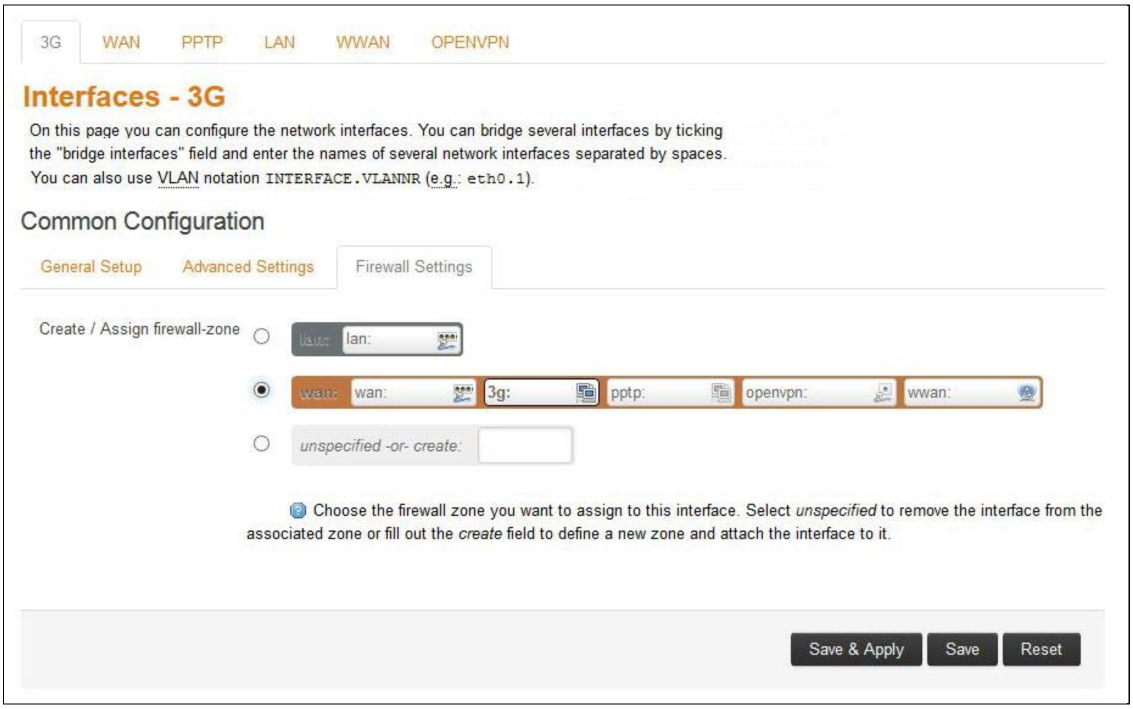
Screen 11.1-4: Advanced Configurations for 3G Interface

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 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 11.1-4: Advanced Configurations for 3G Interface

C. Firewall Settings



Interfaces - 3G

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Create / Assign firewall-zone ○ lan: lan:
● wan: wan: 3g: pptp: openvpn: wwan:
○ unspecified -or- create:

Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

Screen 11.1-5: Firewall Configuration for 3G

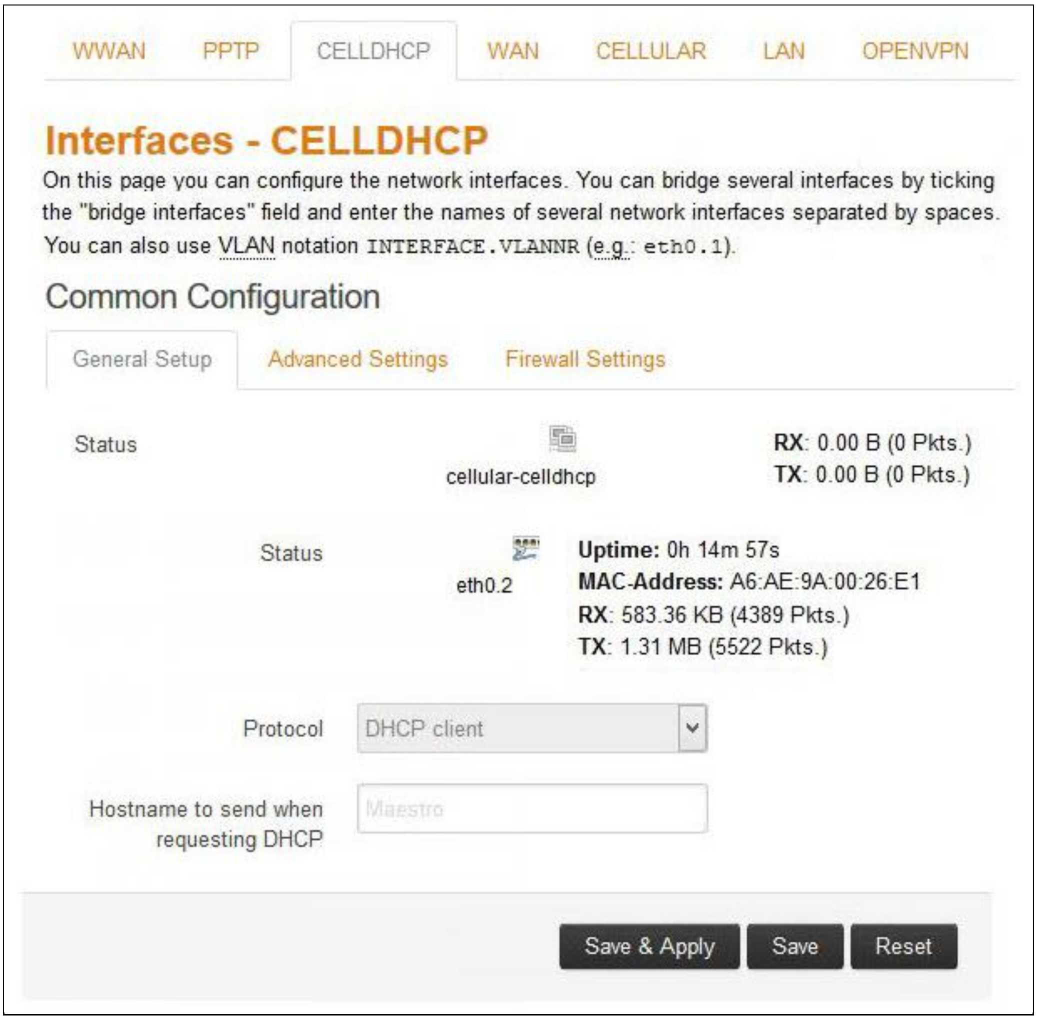
Parameters	Description
Create/Assign firewall -zone	Select the firewall zone to be assigned to the interface. Select **unspecified – or – create** to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box and click Save & Apply button. 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 11.1-5: Firewall Configuration for 3G

11.1.3 CELLDHCP (Only for E206)

Network > Interface > CELLDHCP

A. General Setup



Interfaces - CELLDHCP

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Status: cellular-celldhcp — **RX**: 0.00 B (0 Pkts.) **TX**: 0.00 B (0 Pkts.)

Status: eth0.2 — **Uptime:** 0h 14m 57s **MAC-Address:** A6:AE:9A:00:26:E1 **RX**: 583.36 KB (4389 Pkts.) **TX**: 1.31 MB (5522 Pkts.)

Protocol: DHCP client

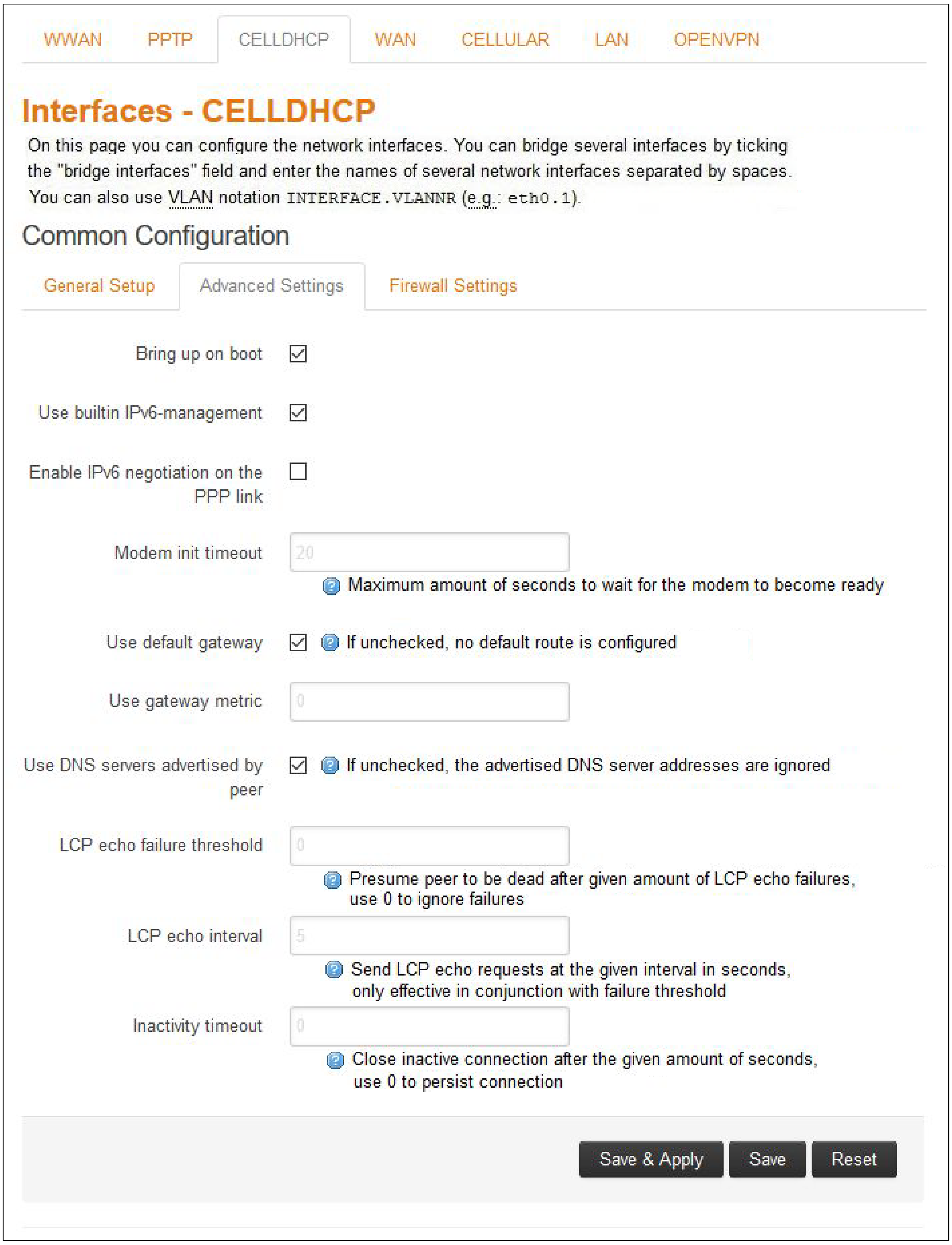
Hostname to send when requesting DHCP: Maestro

Screen 11.1-6: 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 11.1-6: General Configuration of CELLDHCP Interface

B. Advanced Settings



Interfaces - CELLDHCP

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Bring up on boot ☑

Use builtin IPv6-management ☑

Enable IPv6 negotiation on the PPP link □

Modem init timeout 20
Maximum amount of seconds to wait for the modem to become ready

Use default gateway ☑ If unchecked, no default route is configured

Use gateway metric 0

Use DNS servers advertised by peer ☑ If unchecked, the advertised DNS server addresses are ignored

LCP echo failure threshold 0
Presume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures

LCP echo interval 5
Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold

Inactivity timeout 0
Close inactive connection after the given amount of seconds, use 0 to persist connection

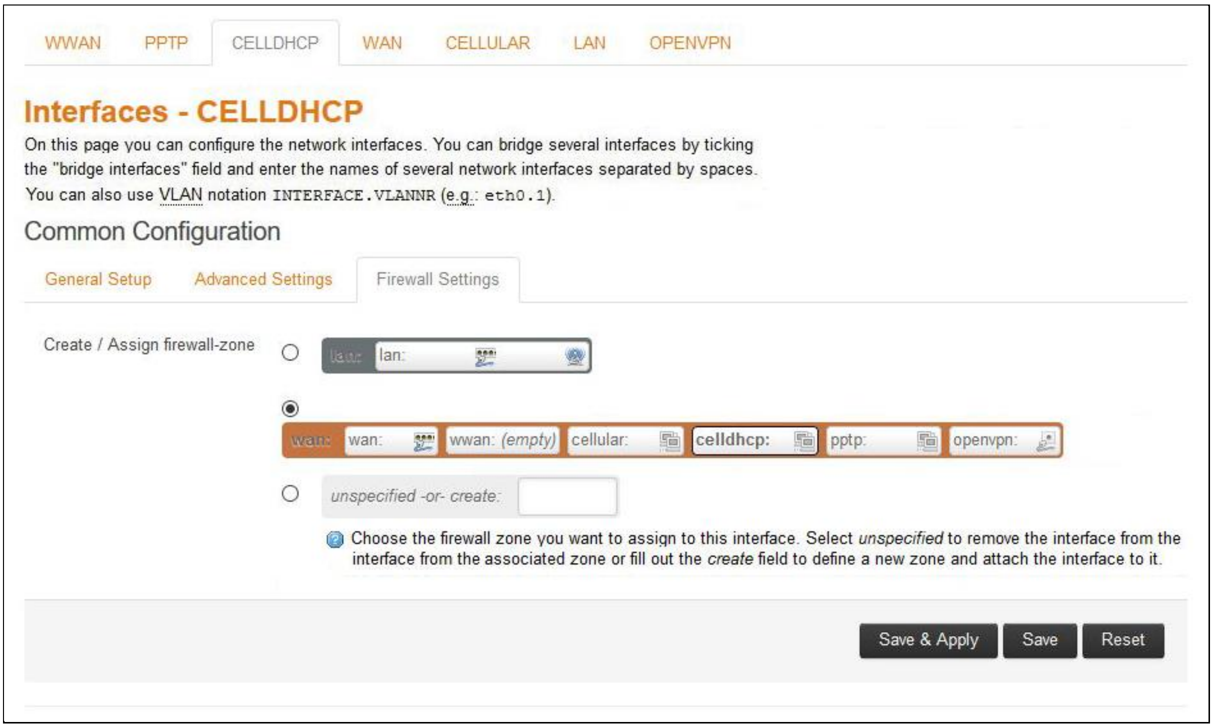
Screen 11.1-7: Advance Configuration of CELLDHCP Interface

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 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 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 11.1-7: Advance Configuration of CELLDHCP Interface

C. Firewall Settings



Interfaces - CELLDHCP

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Create / Assign firewall-zone

○ lan: lan:

● wan: wan: wwan: *(empty)* cellular: **celldhcp:** pptp: openvpn:

○ *unspecified -or- create:*

Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

Screen 11.1-8: Firewall Configuration of CELLDHCP Interface

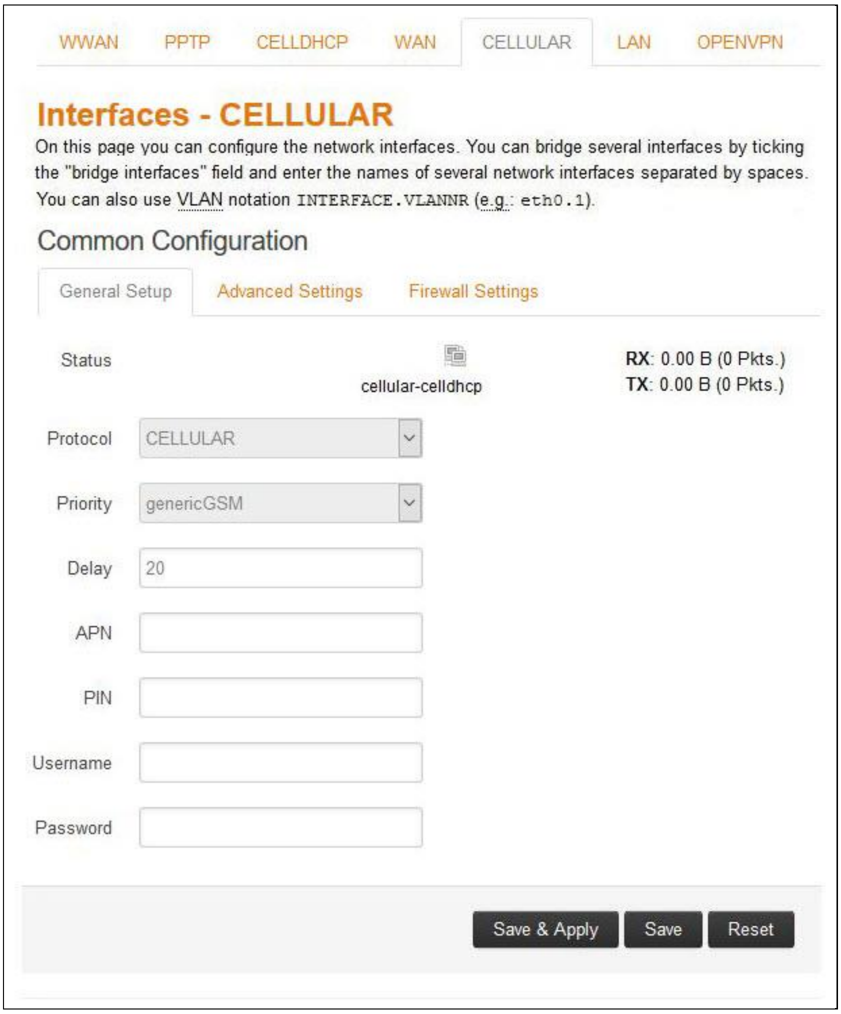
Parameters	Description
Create/Assign firewall -zone	Select the firewall zone to be assigned to the interface. Select unspecified – or – create to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box and click Save & Apply button.

Table 11.1-8: Firewall Configuration of CELLDHCP Interface

11.1.4 CELLULAR

Network > Interface > CELLULAR

A. General Setup



Interfaces - CELLULAR

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Status: cellular-celldhcp — RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)

Protocol: CELLULAR

Priority: genericGSM

Delay: 20

APN:

PIN:

Username:

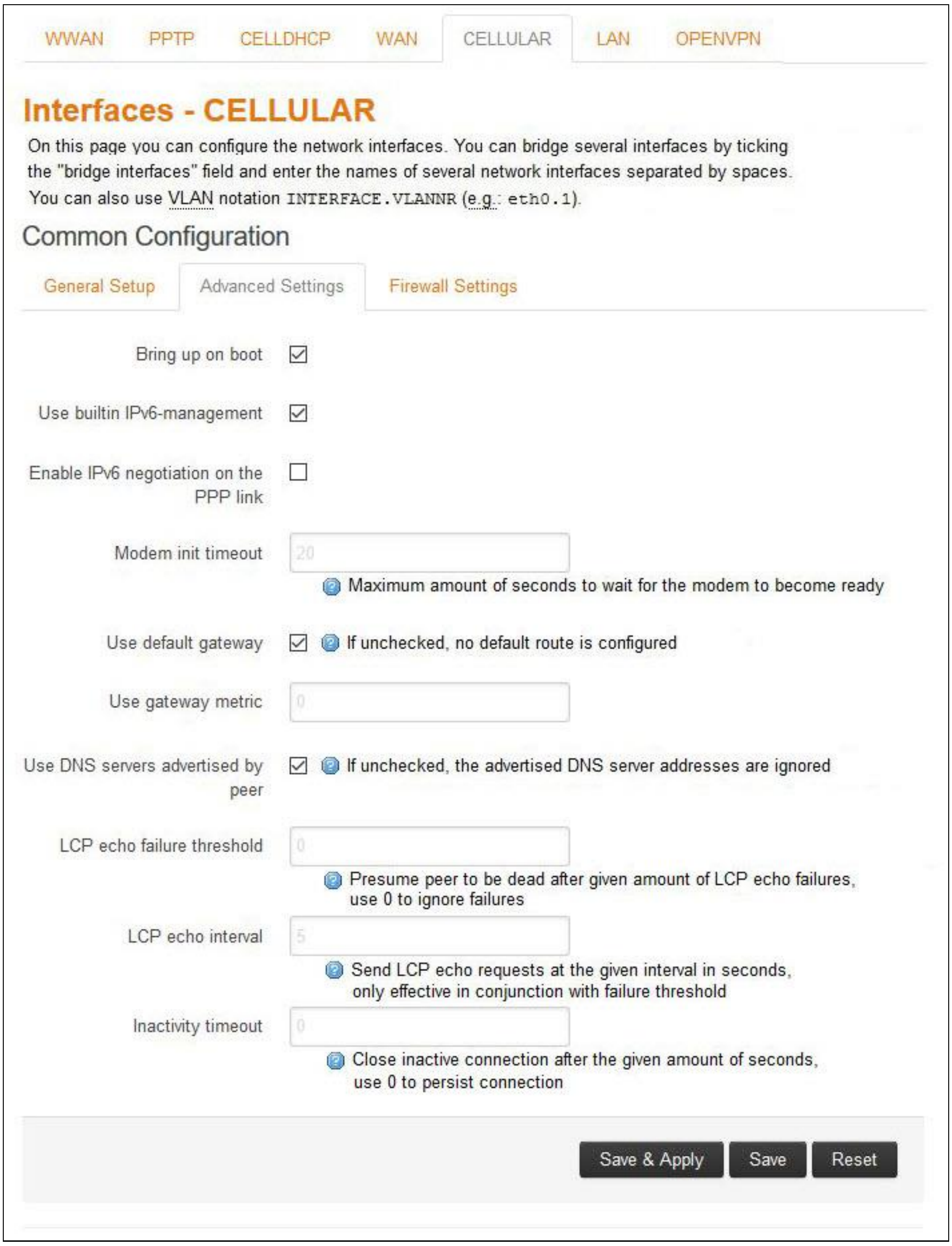
Password:

Screen 11.1-9: 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 11.1-9: General Configuration of CELLULAR Interface

B. Advanced Settings



Interfaces - CELLULAR

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Bring up on boot ☑

Use builtin IPv6-management ☑

Enable IPv6 negotiation on the PPP link ☐

Modem init timeout 20
Maximum amount of seconds to wait for the modem to become ready

Use default gateway ☑ If unchecked, no default route is configured

Use gateway metric 0

Use DNS servers advertised by peer ☑ If unchecked, the advertised DNS server addresses are ignored

LCP echo failure threshold 0
Presume peer to be dead after given amount of LCP echo failures, use 0 to ignore failures

LCP echo interval 5
Send LCP echo requests at the given interval in seconds, only effective in conjunction with failure threshold

Inactivity timeout 0
Close inactive connection after the given amount of seconds, use 0 to persist connection

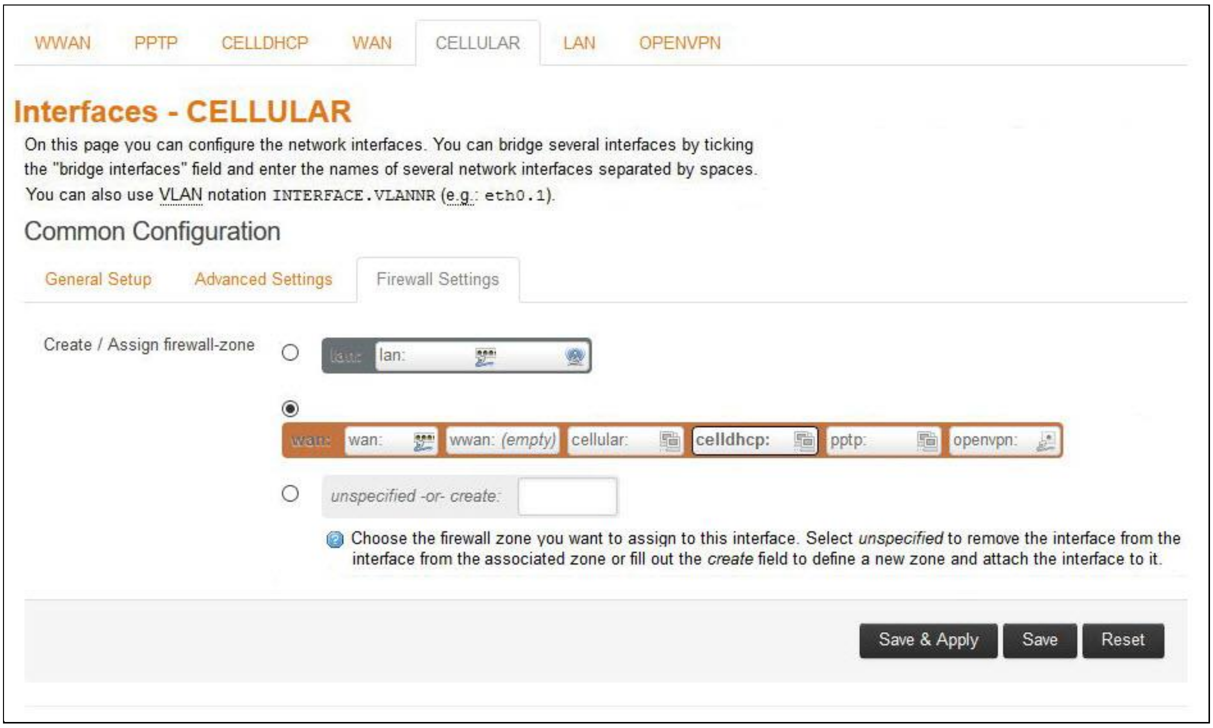
Screen 11.1-10: Advance Configuration of CELLULAR Interface

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 -	Allows to use the built in IPv6 management

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 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 11.1-10: Advance Configuration of CELLULAR Interface

C. Firewall Settings



Interfaces - CELLULAR

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Create / Assign firewall-zone

○ lan: lan:

● wan: wan: wwan: (empty) cellular: celldhcp: pptp: openvpn:

○ unspecified -or- create:

Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

Screen 11.1-11: Firewall Configuration of CELLULAR Interface

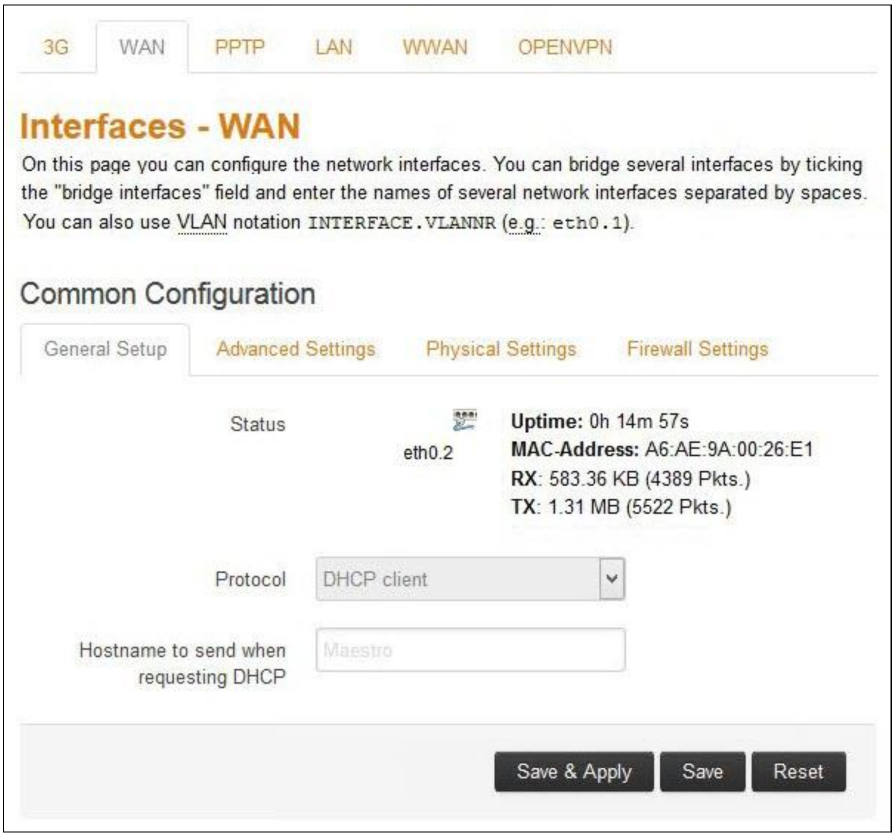
Parameters	Description
Create/Assign firewall -zone	Select the firewall zone to be assigned to the interface. Select unspecified – or – create to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box and click Save & Apply button.

Table 11.1-11: Firewall Configuration of CELLULAR Interface

11.1.5 WAN

Network > Interface > WAN

A. General Setup



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Status: eth0.2 — **Uptime:** 0h 14m 57s; **MAC-Address:** A6:AE:9A:00:26:E1; **RX**: 583.36 KB (4389 Pkts.); **TX**: 1.31 MB (5522 Pkts.)

Protocol: DHCP client

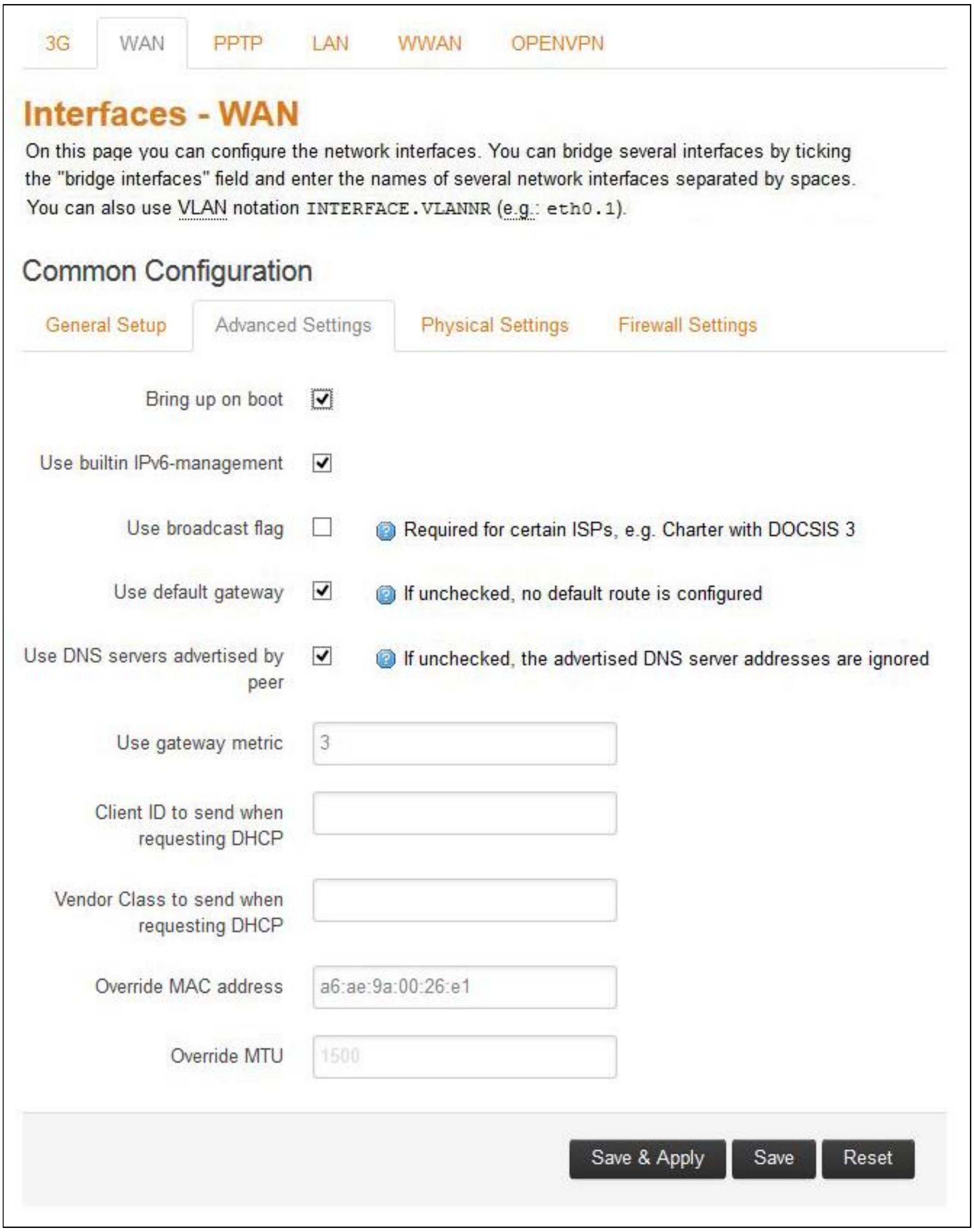
Hostname to send when requesting DHCP: Maestro

Screen 11.1-12: 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 11.1-12: General Configurations for WAN Interface

B. Advanced Settings



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Bring up on boot ☑

Use builtin IPv6-management ☑

Use broadcast flag ☐ Required for certain ISPs, e.g. Charter with DOCSIS 3

Use default gateway ☑ If unchecked, no default route is configured

Use DNS servers advertised by peer ☑ If unchecked, the advertised DNS server addresses are ignored

Use gateway metric: 3

Client ID to send when requesting DHCP:

Vendor Class to send when requesting DHCP:

Override MAC address: a6:ae:9a:00:26:e1

Override MTU: 1500

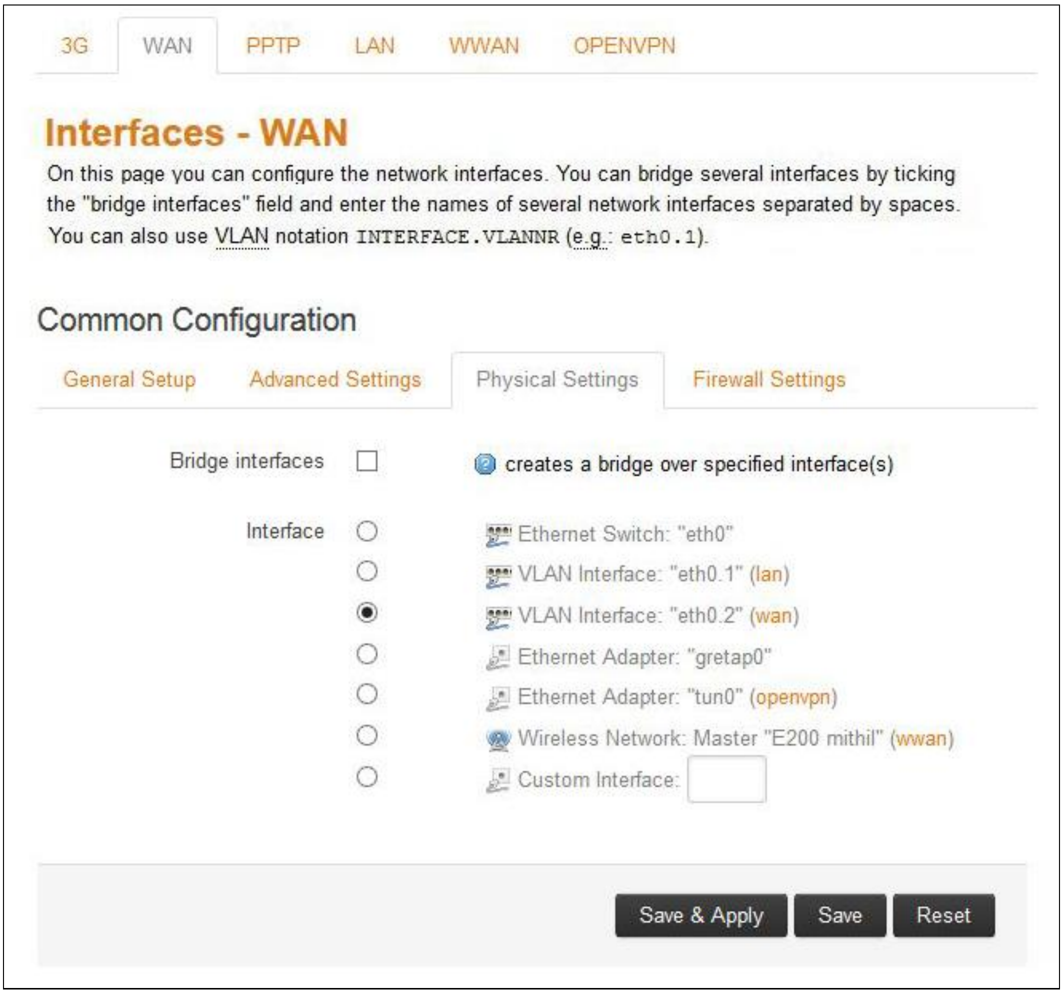
Screen 11.1-13: Advanced Configurations of WAN Interface

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 -	Allows to use the built in IPv6 management

management	configuration.
Use broadcast flag	Check to use the broadcast flag. This flag is generally used by the ISP's.
Use default gateway	Click to configure a default gateway route. None of the gateway routes are configured by default.
Use DNS server advertised by peer	Allows advertising the DNS server address. Use DNS server advertised by peer for WAN interface is checked by default. If unchecked, the advertised DNS server addresses are ignored.
Use gateway metric	Enter the gateway metric. 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 11.1-13: Advanced Configurations of WAN Interface

C. Physical Settings



Interfaces - WAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Bridge interfaces □ creates a bridge over specified interface(s)

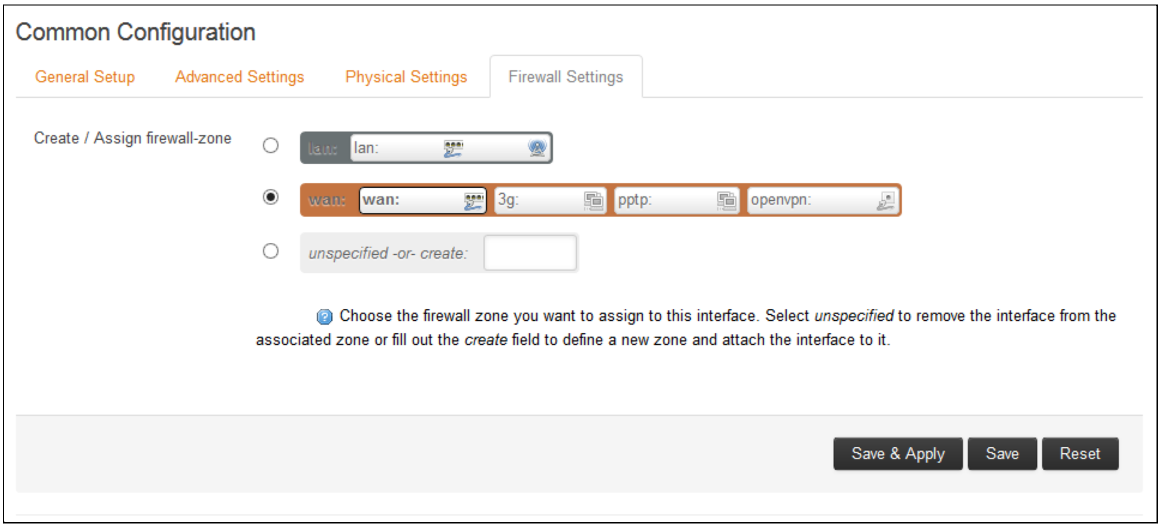
Interface
○ Ethernet Switch: "eth0"
○ VLAN Interface: "eth0.1" (lan)
● VLAN Interface: "eth0.2" (wan)
○ Ethernet Adapter: "gretap0"
○ Ethernet Adapter: "tun0" (openvpn)
○ Wireless Network: Master "E200 mithil" (wwan)
○ Custom Interface:

Screen 11.1-14: 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 11.1-14: Physical Configurations for WAN interface

D. Firewall Settings



Common Configuration

Create / Assign firewall-zone

○ lan: lan:

● wan: wan: 3g: pptp: openvpn:

○ unspecified -or- create:

Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

Screen 11.1-15: Firewall Configurations for WAN Interface

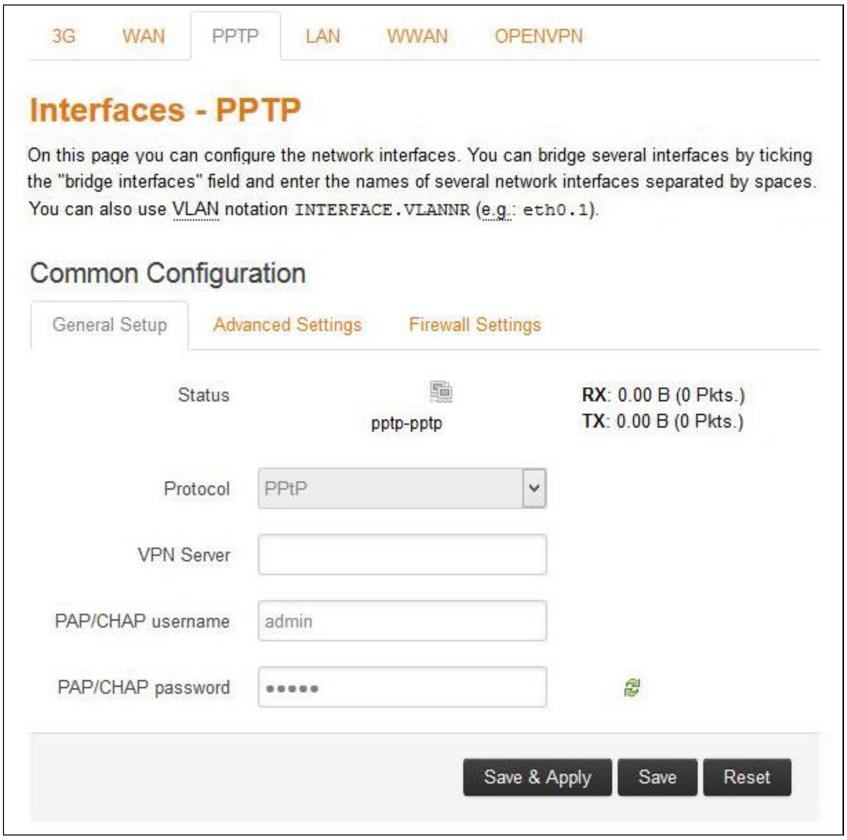
Parameters	Description
Create/Assign firewall -zone	Select the firewall zone to be assigned to the interface. Select **unspecified – or – create** to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box and click Save & Apply button.

Table 11.1-15: Firewall Configurations for WAN Interface

11.1.6 PPTP

Network > Interface > PPTP

A. General Setup



Interfaces - PPTP

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Status: pptp-pptp — RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.)

Protocol: PPtP

VPN Server:

PAP/CHAP username: admin

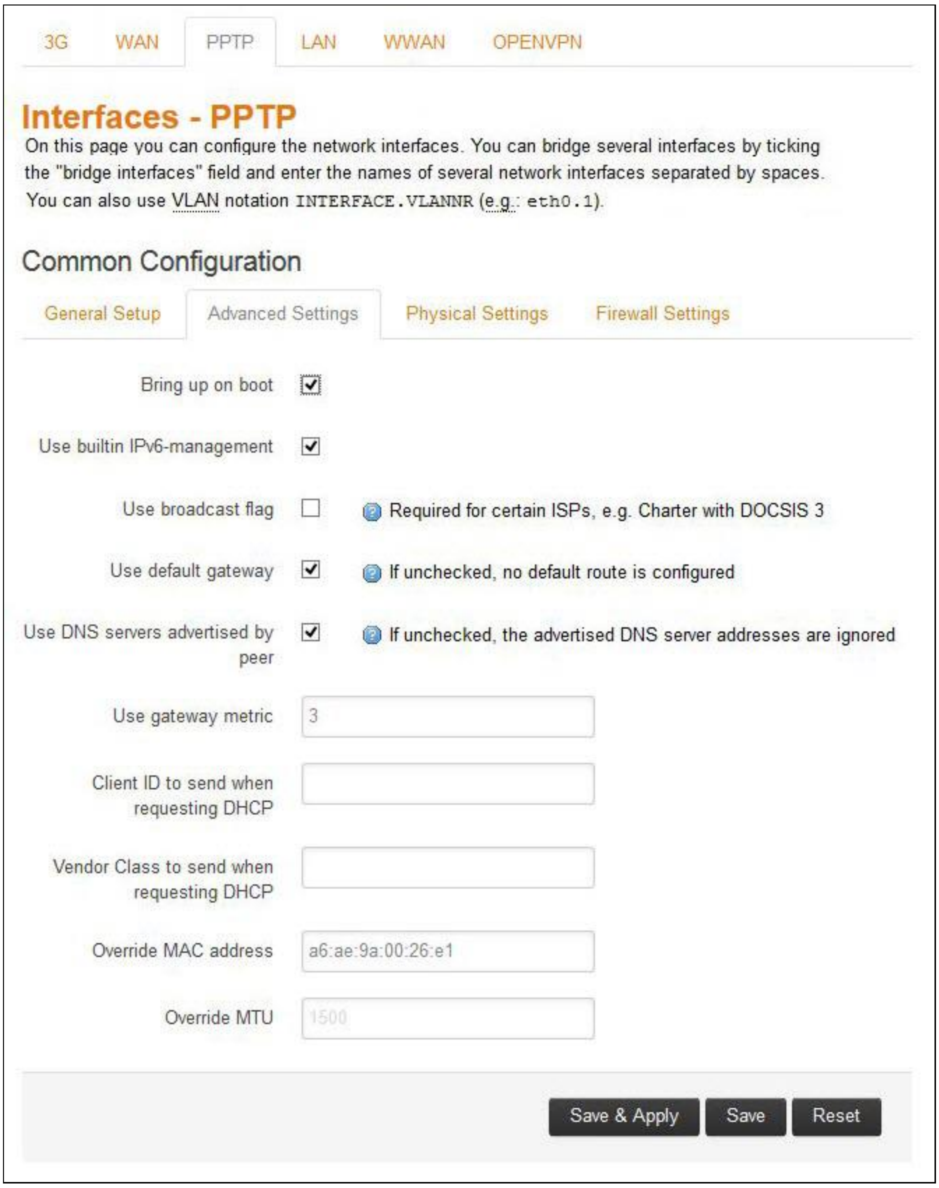
PAP/CHAP password: •••••

Screen 11.1-16: General Configurations for PPTP 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 WAN protocol, select the protocol and click Switch Protocol button. PPtP is the supported protocol. Default configuration is MPPE 128 bit encryption Auto Authentication (MSCHAP V2 / MSCHAP)

Table 11.1-16: General Configurations for PPTP Interface

B. Advanced Settings



Interfaces - PPTP

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Bring up on boot ☑

Use builtin IPv6-management ☑

Use broadcast flag □ Required for certain ISPs, e.g. Charter with DOCSIS 3

Use default gateway ☑ If unchecked, no default route is configured

Use DNS servers advertised by peer ☑ If unchecked, the advertised DNS server addresses are ignored

Use gateway metric: 3

Client ID to send when requesting DHCP:

Vendor Class to send when requesting DHCP:

Override MAC address: a6:ae:9a:00:26:e1

Override MTU: 1500

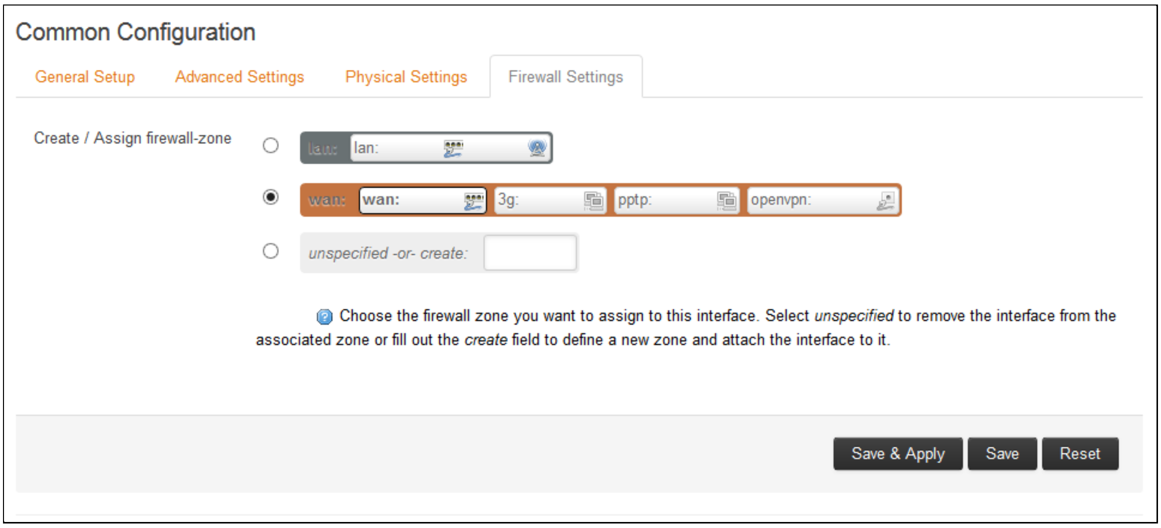
Screen 11.1-17: Advanced Configurations for PPTP

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 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.

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 3.
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.
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.
Inactivity timeout	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.
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 11.1-17: Advanced Configurations for PPTP

C. Firewall Settings



Common Configuration

Create / Assign firewall-zone

○ lan: lan:

● wan: wan: 3g: pptp: openvpn:

○ unspecified -or- create:

Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

Screen 11.1-18: Firewall Configurations for WAN Interface

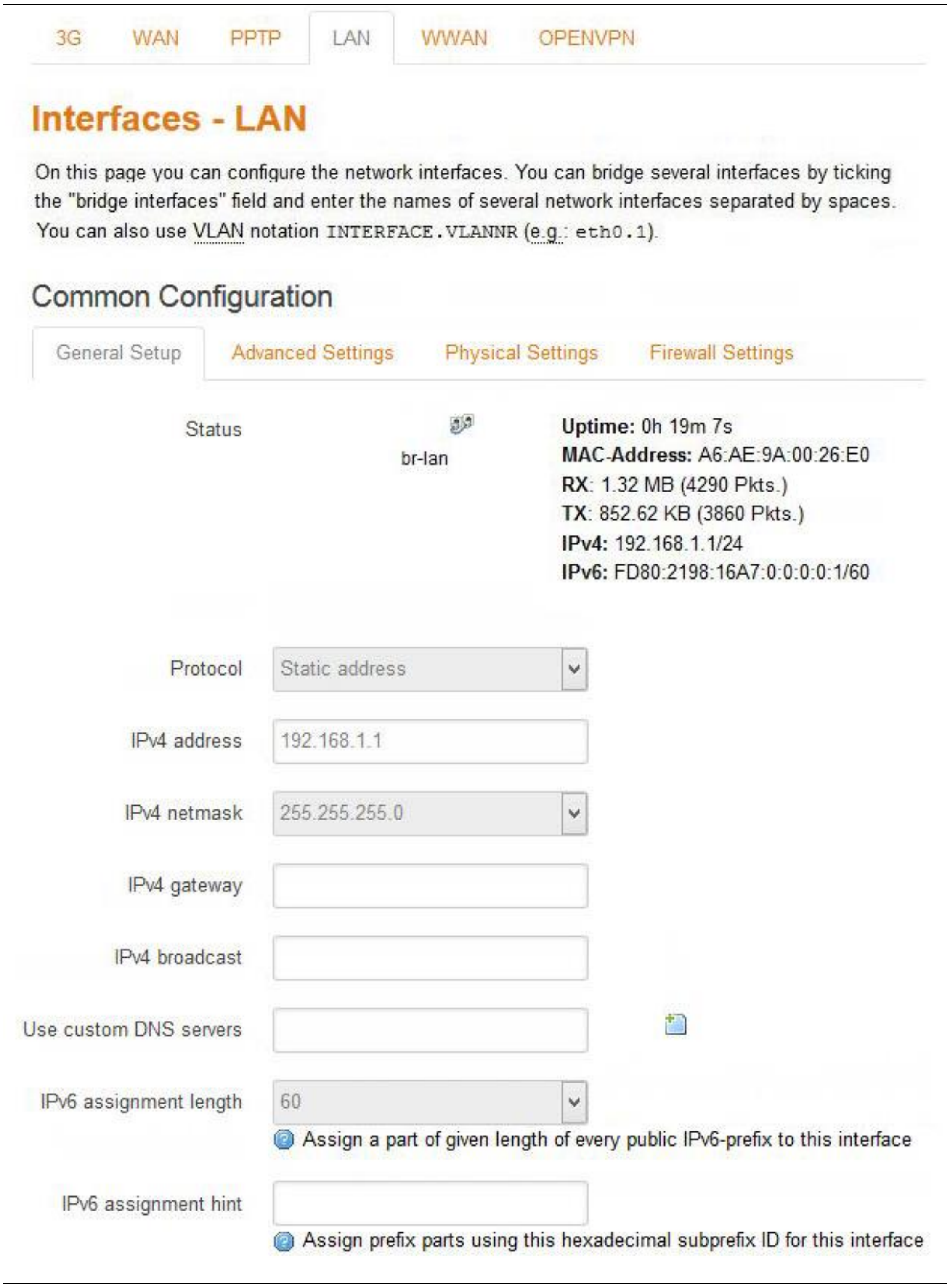
Parameters	Description
Create/Assign firewall -zone	Select the firewall zone to be assigned to the interface. Select **unspecified – or – create** to remove the interface or assign a new zone to the interface respectively. Enter the name of the new zone in the text box and click Save & Apply button.

Table 11.1-18: Firewall Configurations for WAN Interface

11.1.7 LAN

Network > Interface > LAN

A. General Setup



Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Status: br-lan

Uptime: 0h 19m 7s
MAC-Address: A6:AE:9A:00:26:E0
RX: 1.32 MB (4290 Pkts.)
TX: 852.62 KB (3860 Pkts.)
IPv4: 192.168.1.1/24
IPv6: FD80:2198:16A7:0:0:0:0:1/60

Protocol: Static address

IPv4 address: 192.168.1.1

IPv4 netmask: 255.255.255.0

IPv4 gateway:

IPv4 broadcast:

Use custom DNS servers:

IPv6 assignment length: 60

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

IPv6 assignment hint:

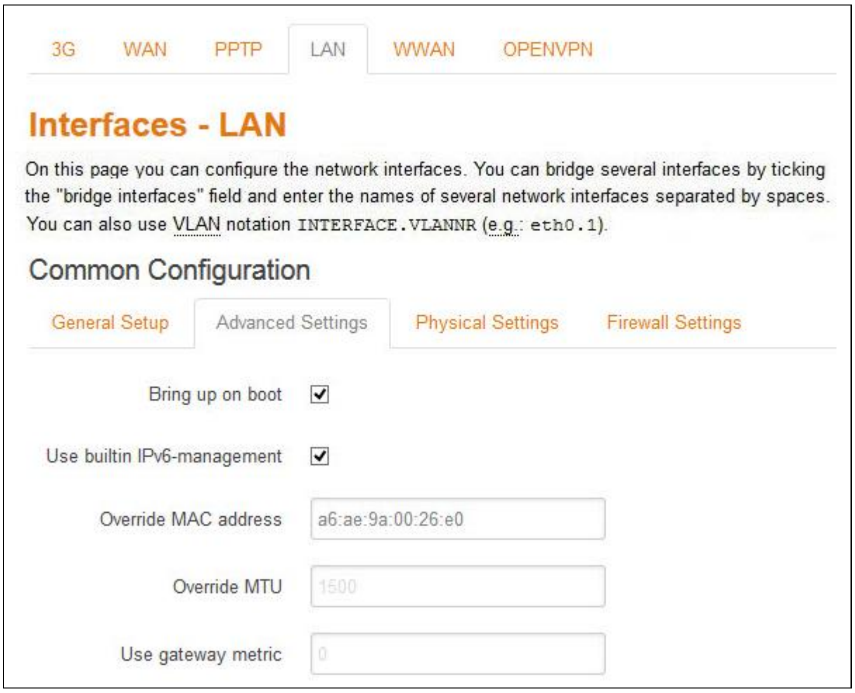
Assign prefix parts using this hexadecimal subprefix ID for this interface

Screen 11.1-19: 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 11.1-19: General Configurations of LAN Interface

B. Advanced Settings



Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Bring up on boot ☑

Use builtin IPv6-management ☑

Override MAC address: a6:ae:9a:00:26:e0

Override MTU: 1500

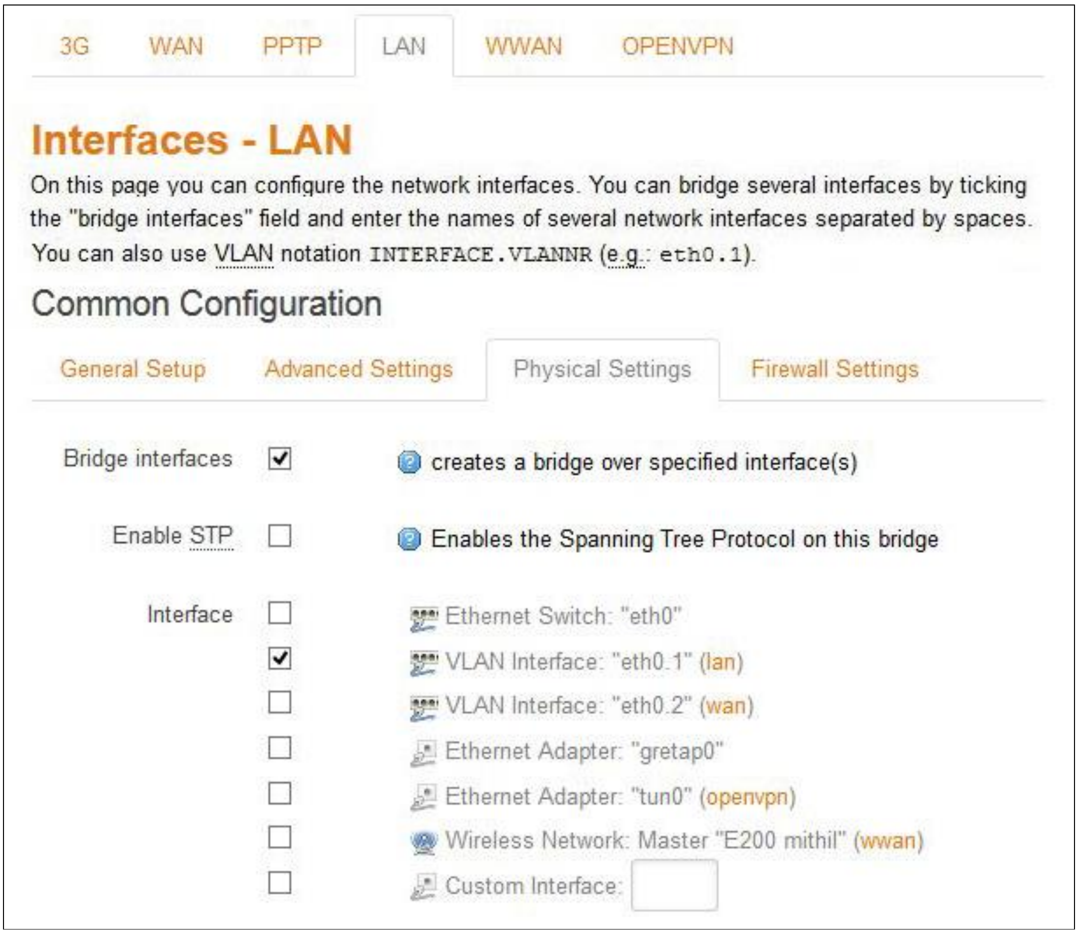
Use gateway metric: 0

Screen 11.1-20: 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 11.1-20: Advanced Settings for LAN Interface

C. Physical Settings



Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Bridge interfaces ☑ creates a bridge over specified interface(s)

Enable STP □ Enables the Spanning Tree Protocol on this bridge

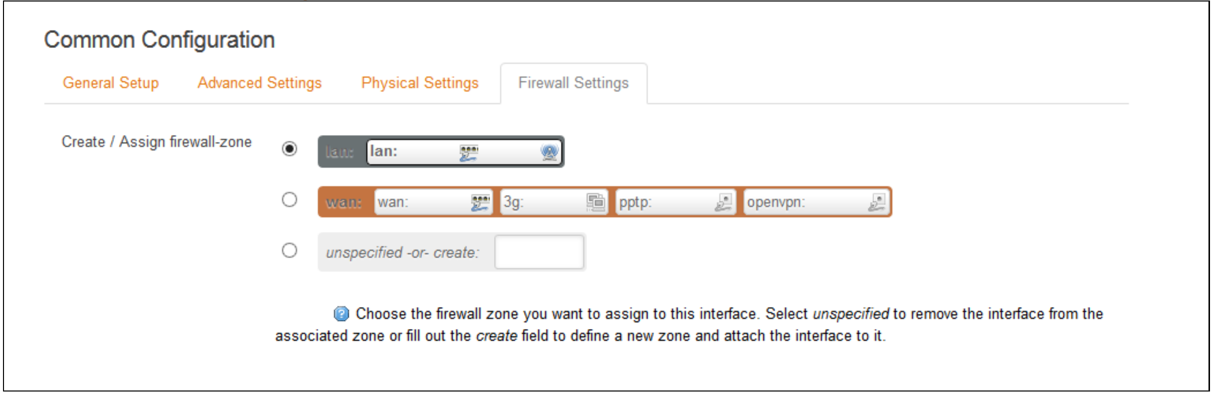
Interface
□ Ethernet Switch: "eth0"
☑ VLAN Interface: "eth0.1" (lan)
□ VLAN Interface: "eth0.2" (wan)
□ Ethernet Adapter: "gretap0"
□ Ethernet Adapter: "tun0" (openvpn)
□ Wireless Network: Master "E200 mithil" (wwan)
□ Custom Interface:

Screen 11.1-21: 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 11.1-21: Physical Configurations of LAN Interface

D. Firewall Settings



Common Configuration

Create / Assign firewall-zone
● lan: lan:
○ wan: wan: 3g: pptp: openvpn:
○ unspecified -or- create:

Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

Screen 11.1-22: 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 11.1-22: Firewall Configurations of LAN Interface

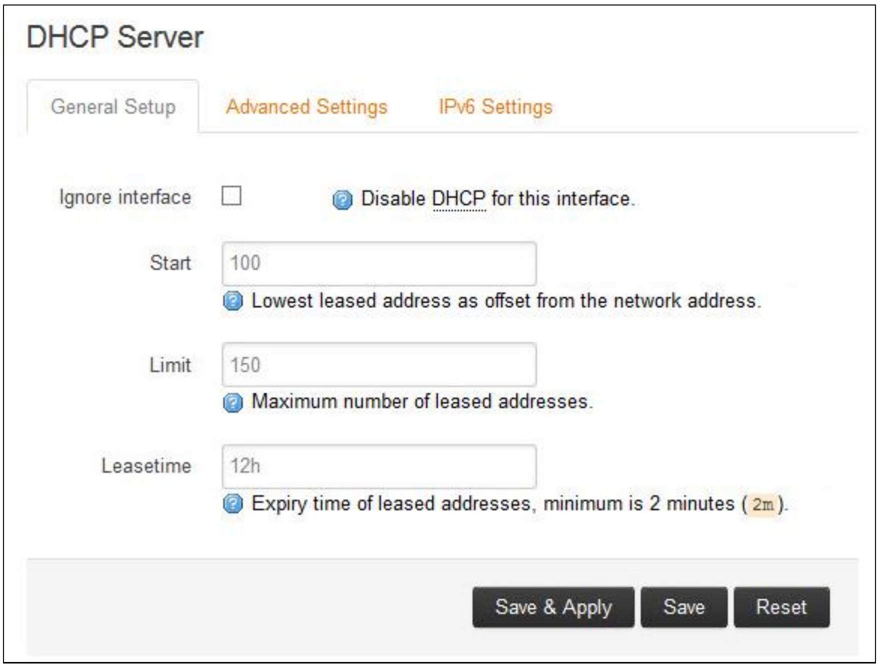
E. DHCP Server

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



DHCP Server

Ignore interface □ Disable DHCP for this interface.

Start: 100
Lowest leased address as offset from the network address.

Limit: 150
Maximum number of leased addresses.

Leasetime: 12h
Expiry time of leased addresses, minimum is 2 minutes (2m).

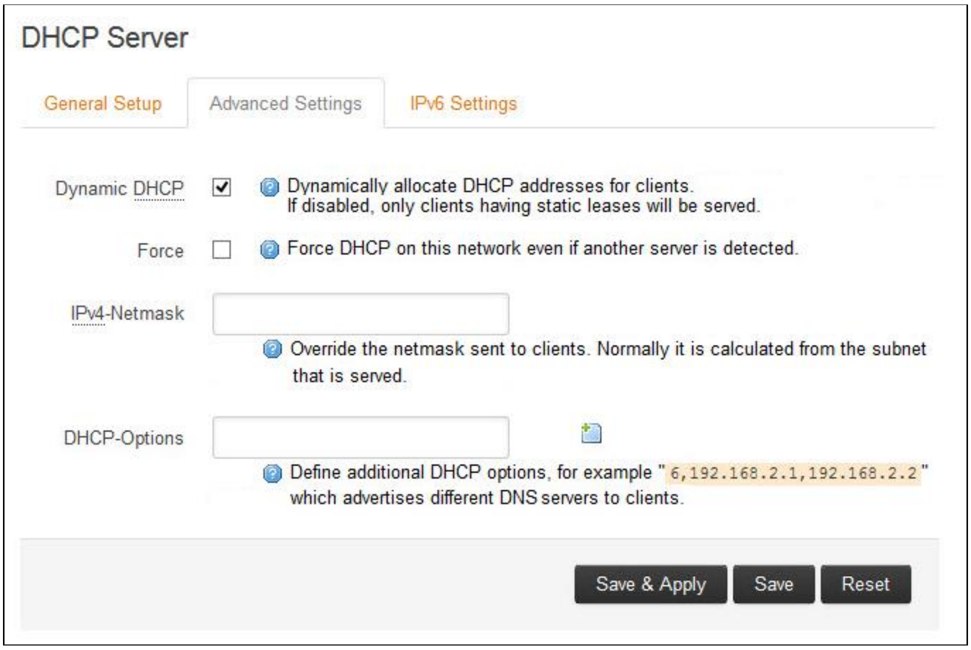
Screen 11.1-23: General Configurations for DHCP Server

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 and the parameter Start is configured as 100, and parameter Limit is configured as 150, the leased IP Address range is 192.168.1.100 to 192.168.1.249. This means a total of 150 devices can be configured.
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 11.1-23: General Configurations for DHCP Server

b. Advanced Settings



DHCP Server

Dynamic DHCP ☑ Dynamically allocate DHCP addresses for clients.
If disabled, only clients having static leases will be served.

Force □ Force DHCP on this network even if another server is detected.

IPv4-Netmask Override the netmask sent to clients. Normally it is calculated from the subnet that is served.

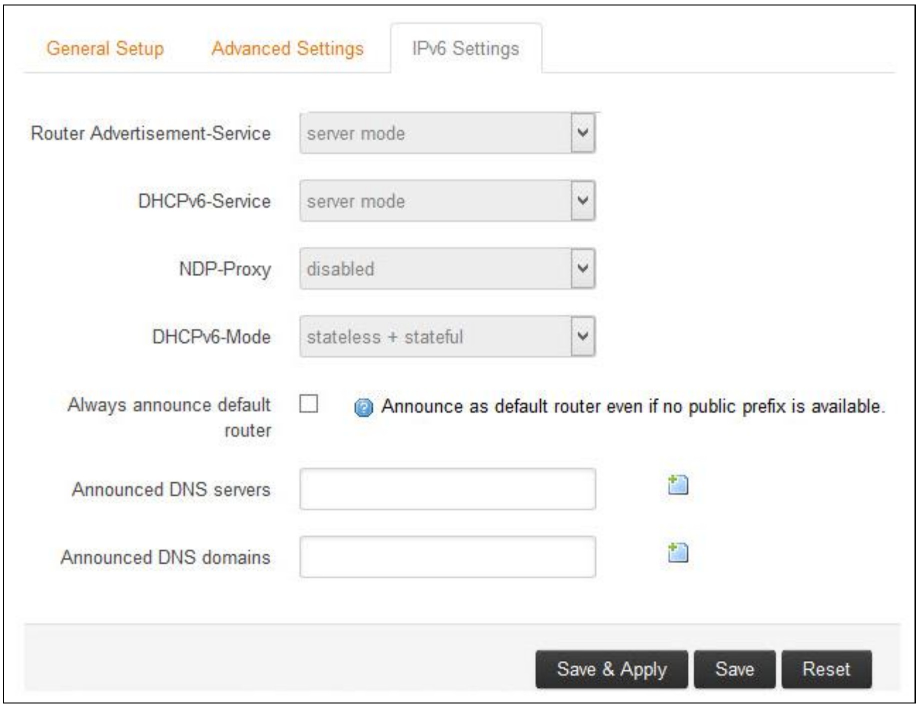
DHCP-Options Define additional DHCP options, for example "`6,192.168.2.1,192.168.2.2`" which advertises different DNS servers to clients.

Screen 11.1-24: 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 11.1-24: Advance Configurations for DHCP Server

c. IPv6 Settings



Router Advertisement-Service: server mode

DHCPv6-Service: server mode

NDP-Proxy: disabled

DHCPv6-Mode: stateless + stateful

Always announce default router: □ Announce as default router even if no public prefix is available.

Announced DNS servers:

Announced DNS domains:

Screen 11.1-25: IPv6 Configuration of DHCP Server

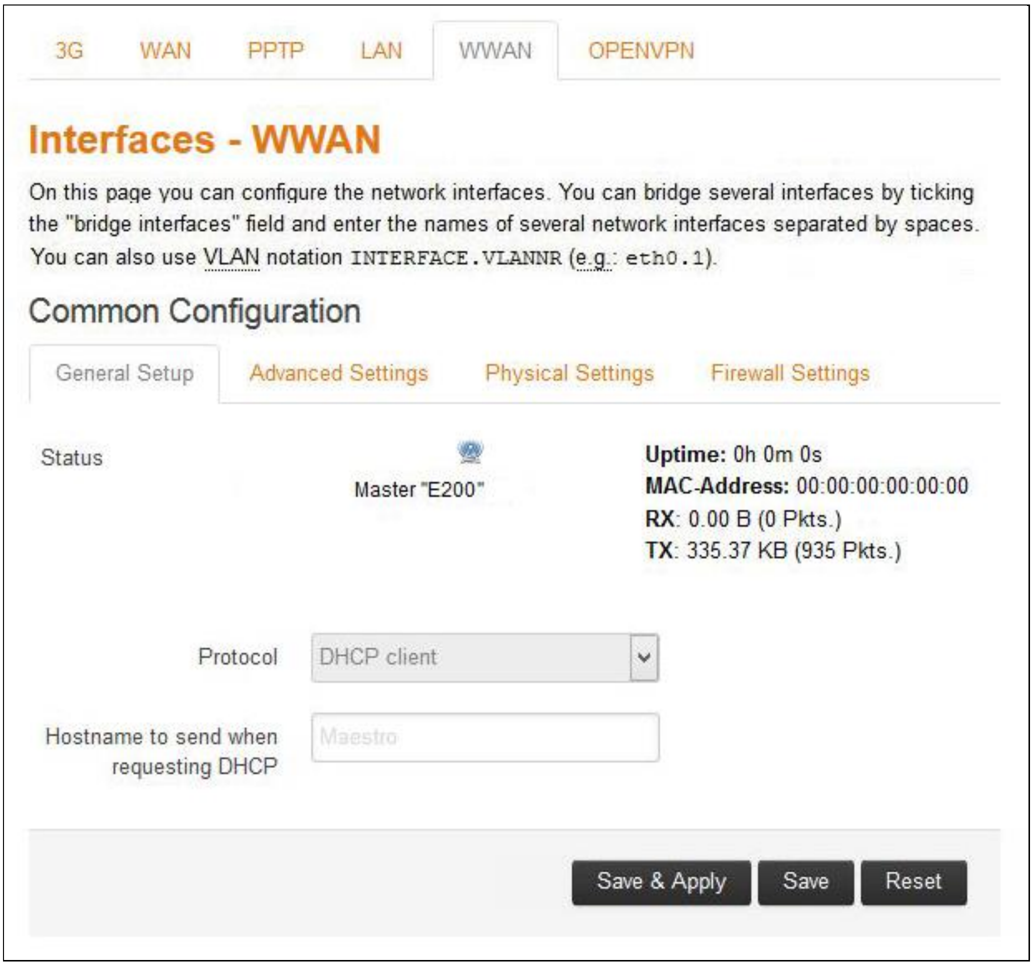
Parameters	Description
Router Advertisement-Service	Select the Router Advertisement-Service mode; disabled, server mode, relay mode, hybrid mode.
DHCPv6-Service	Select the DHCPv6-Service mode; disabled, server mode, relay mode, hybrid mode.
NDP-Proxy	Select the NDP mode; disabled, server mode, relay 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 11.1-25: IPv6 Configuration of DHCP Server

11.1.8 WWAN

Network > Interface > WWAN

A. General Setup



Interfaces - WWAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Status: Master "E200"

Uptime: 0h 0m 0s
MAC-Address: 00:00:00:00:00:00
RX: 0.00 B (0 Pkts.)
TX: 335.37 KB (935 Pkts.)

Protocol: DHCP client

Hostname to send when requesting DHCP: Maestro

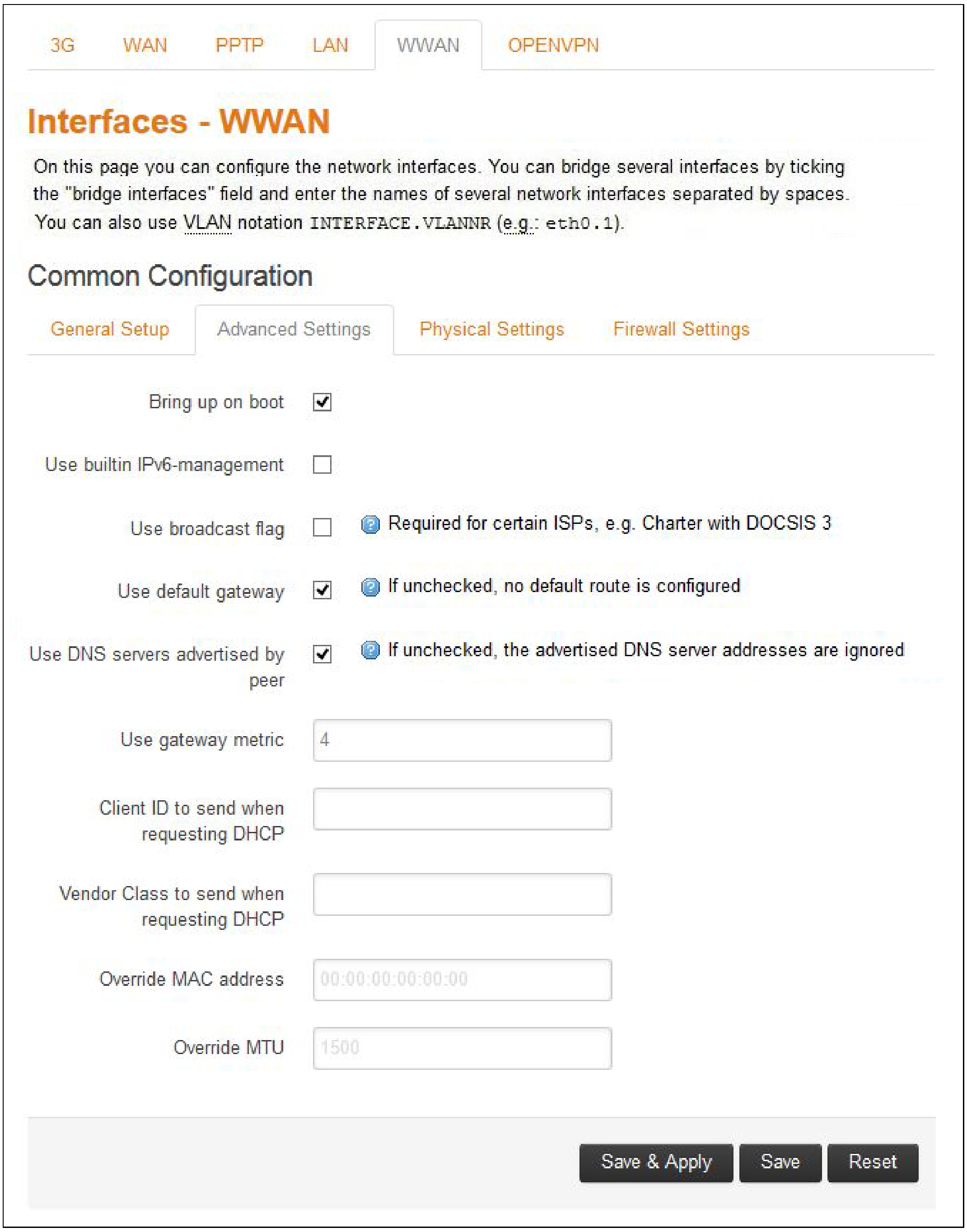
Screen 11.1-26: General Configuration for WWAN Interface

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 11.1-26: General Configuration for WWAN Interface

B. Advanced Settings



Interfaces - WWAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Bring up on boot ☑

Use builtin IPv6-management □

Use broadcast flag □ Required for certain ISPs, e.g. Charter with DOCSIS 3

Use default gateway ☑ If unchecked, no default route is configured

Use DNS servers advertised by peer ☑ If unchecked, the advertised DNS server addresses are ignored

Use gateway metric: 4

Client ID to send when requesting DHCP:

Vendor Class to send when requesting DHCP:

Override MAC address: 00:00:00:00:00:00

Override MTU: 1500

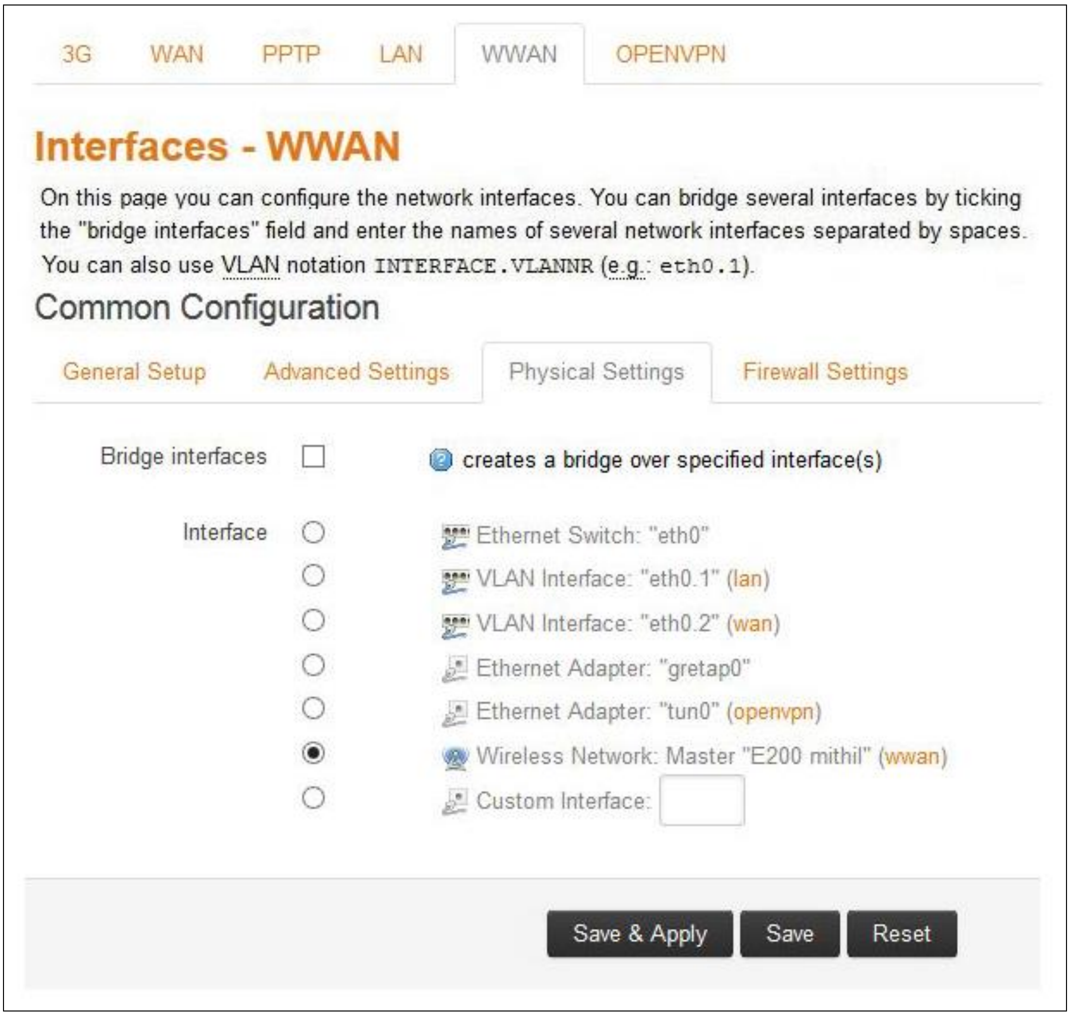
Screen 11.1-27: Advanced Configuration for WWAN Interface

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 -	Allows to use the built in IPv6 management

management	configuration.
Use broadcast flag	Check to use the broadcast flag. This flag is generally used by the ISP's.
Use default gateway	Click to configure a default gateway route. None of the gateway routes are configured by default.
Use DNS server advertised by peer	Allows advertising the DNS server address. Use DNS server advertised by peer for WAN interface is checked by default. If unchecked, the advertised DNS server addresses are ignored.
Use gateway metric	Enter the gateway metric. The Load Balancer uses these Metric values to determine priority of a WAN. The default metric is 4.
Client ID to send when requesting DHCP	Enter the Client ID that shall be sent when requesting DHCP.
Vendor Class to send when requesting DHCP	To allocate DHCP IP Addresses based on Vendor Class.
Override MAC address	Click to override the default MAC Address for the WAN Interface. On factory reset, it will be set to default MAC address.
Overrride MTU	Click to override the default MTU value (Maximum Transmission Unit) The default MTU is 1500.

Table 11.1-27: Advanced Configuration for WWAN Interface

C. Physical Settings



Interfaces - WWAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Bridge interfaces □ creates a bridge over specified interface(s)

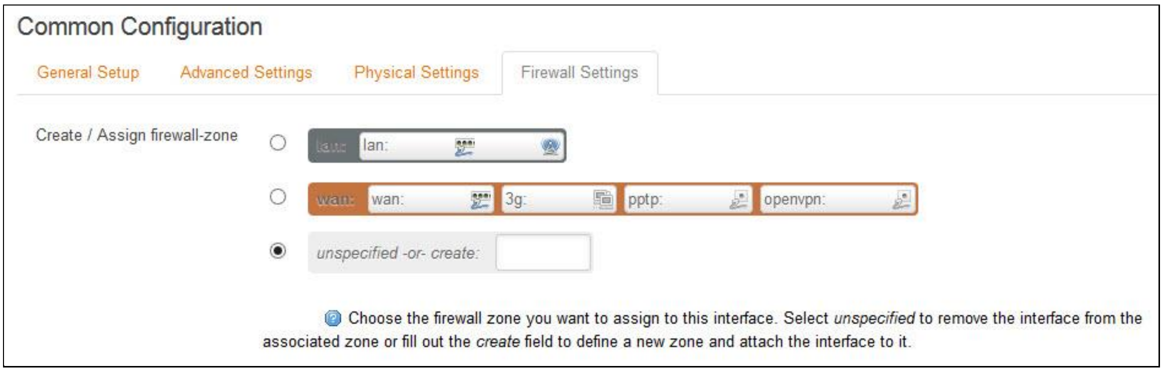
Interface
○ Ethernet Switch: "eth0"
○ VLAN Interface: "eth0.1" (lan)
○ VLAN Interface: "eth0.2" (wan)
○ Ethernet Adapter: "gretap0"
○ Ethernet Adapter: "tun0" (openvpn)
● Wireless Network: Master "E200 mithil" (wwan)
○ Custom Interface:

Screen 11.1-28: 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 11.1-28: Physical Configuration for WWAN Interface

D. Firewall Settings



Common Configuration

Create / Assign firewall-zone

○ lan: lan:

○ wan: wan: 3g: pptp: openvpn:

● unspecified -or- create:

Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

Screen 11.1-29: 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 11.1-29: Firewall Configuration for WWAN Interface

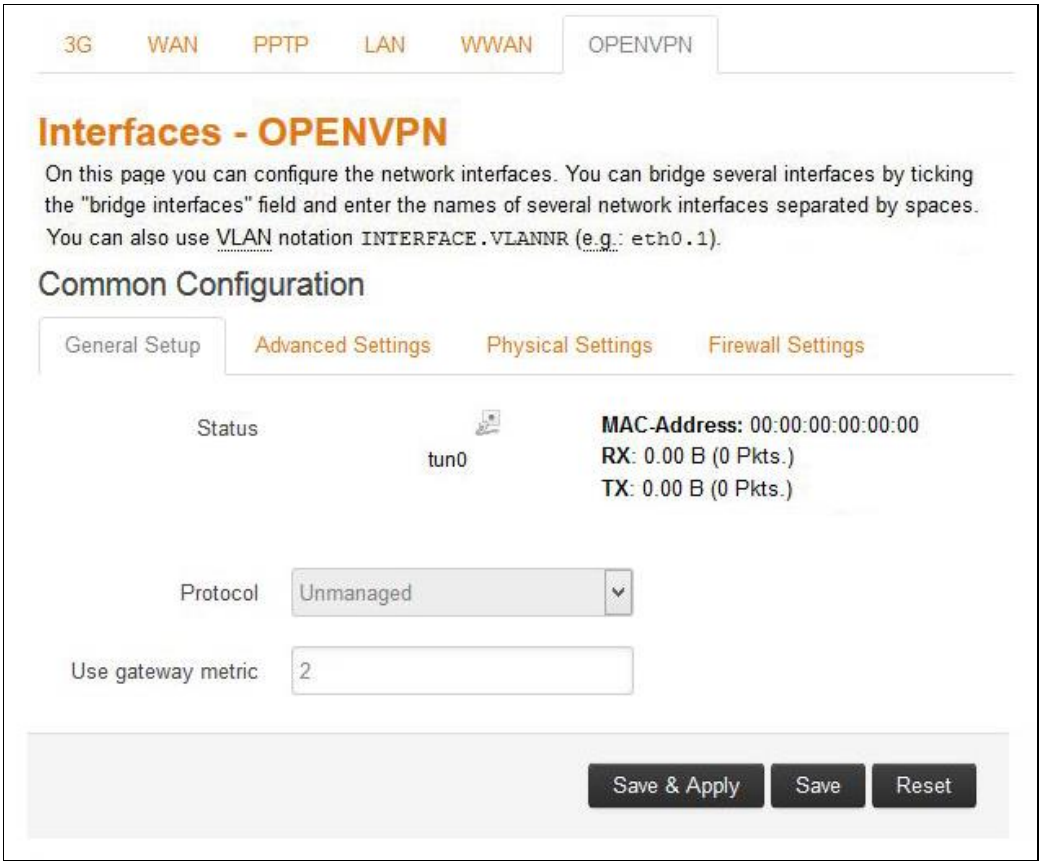
11.1.9 Open VPN

Network > Interface > 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

E200 series supports Open VPN client, Server and Pass Through.

A. General Setup



Interfaces - OPENVPN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Status: tun0 — **MAC-Address:** 00:00:00:00:00:00 **RX:** 0.00 B (0 Pkts.) **TX:** 0.00 B (0 Pkts.)

Protocol: Unmanaged

Use gateway metric: 2

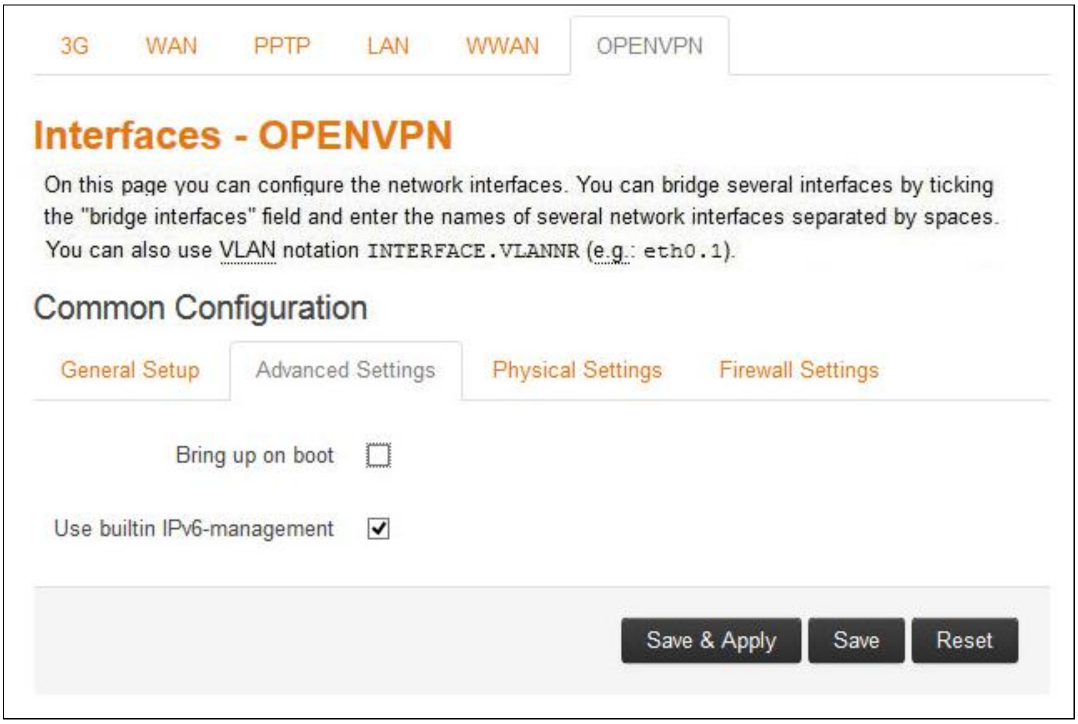
Screen 11.1-30: General Configuration of OpenVPN Interface

Parameters	Description
Status	Enter the following Interface details

	- MAC–Address - RX - TX
Protocol	Select the protocol with respect to the router model number. To update the WAN protocol, select the protocol and click Switch Protocol button. Unmanaged is the default protocol
Use gateway metric	Enter the gateway metric. The Load Balancer uses these Metric values to determine priority of a WAN. The default metric is 2

Table 11.1-30: General Configuration of OpenVPN Interface

B. Advanced Settings



Interfaces - OPENVPN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Bring up on boot □

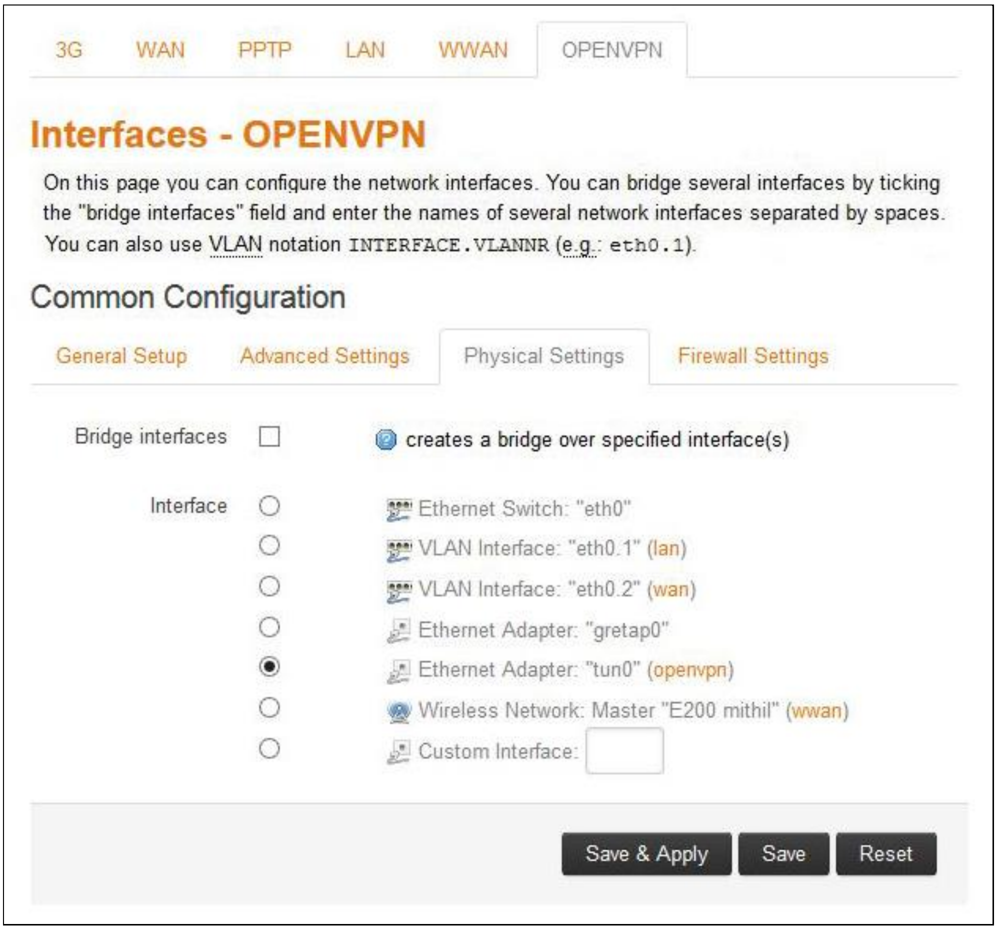
Use builtin IPv6-management ☑

Screen 11.1-31: Advance Configuration of OpenVPN 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.

Table 11.1-31: Advance Configuration of OpenVPN Interface

C. Physical Settings



Interfaces - OPENVPN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation `INTERFACE.VLANNR` (e.g.: `eth0.1`).

Common Configuration

Bridge interfaces □ creates a bridge over specified interface(s)

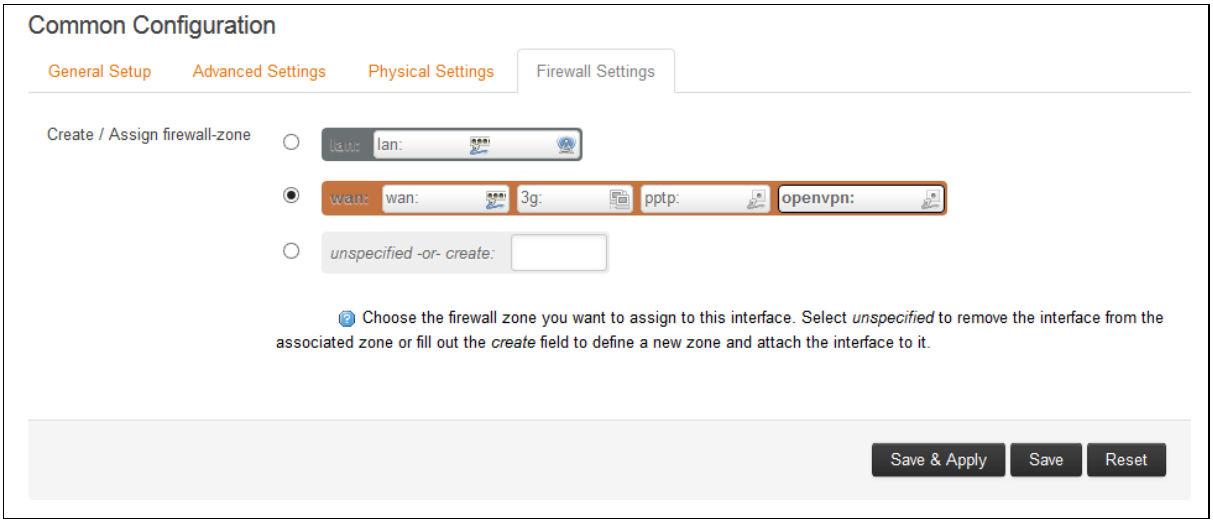
Interface
○ Ethernet Switch: "eth0"
○ VLAN Interface: "eth0.1" (lan)
○ VLAN Interface: "eth0.2" (wan)
○ Ethernet Adapter: "gretap0"
● Ethernet Adapter: "tun0" (openvpn)
○ Wireless Network: Master "E200 mithil" (wwan)
○ Custom Interface:

Screen 11.1-32: Physical Configuration of OpenVPN 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 11.1-32: Physical Configuration of OpenVPN Interface

D. Firewall Settings



Common Configuration

Create / Assign firewall-zone

○ lan: lan:

● wan: wan: 3g: pptp: openvpn:

○ unspecified -or- create:

Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

Screen 11.1-33: Firewall Configuration of OpenVPN 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 11.1-33: Firewall Configuration of OpenVPN Interface

11.2 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)

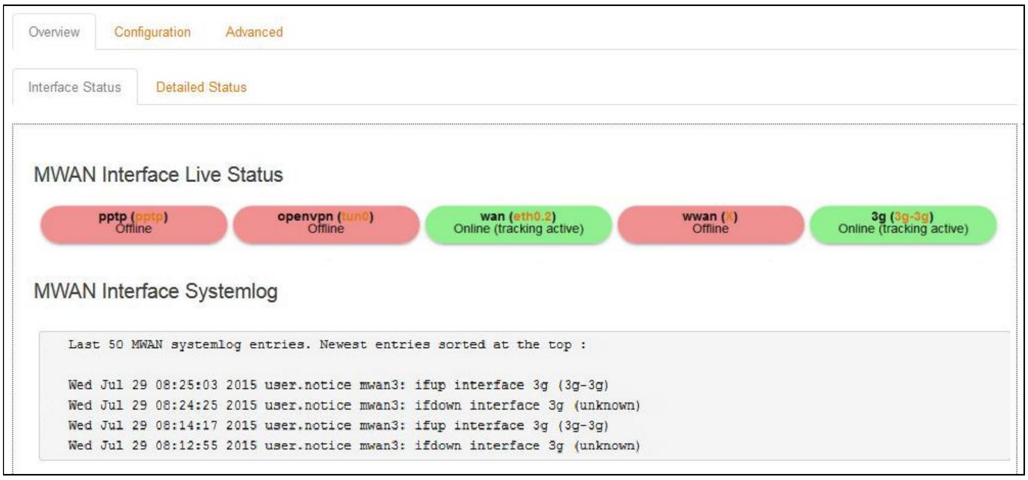
Note

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

11.2.1 Overview

Network > Load Balancing > Overview

A. Interface Status



MWAN Interface Live Status

pptp (pptp) Offline | openvpn (tun0) Offline | wan (eth0.2) Online (tracking active) | wwan (X) Offline | 3g (3g-3g) Online (tracking active)

MWAN Interface Systemlog

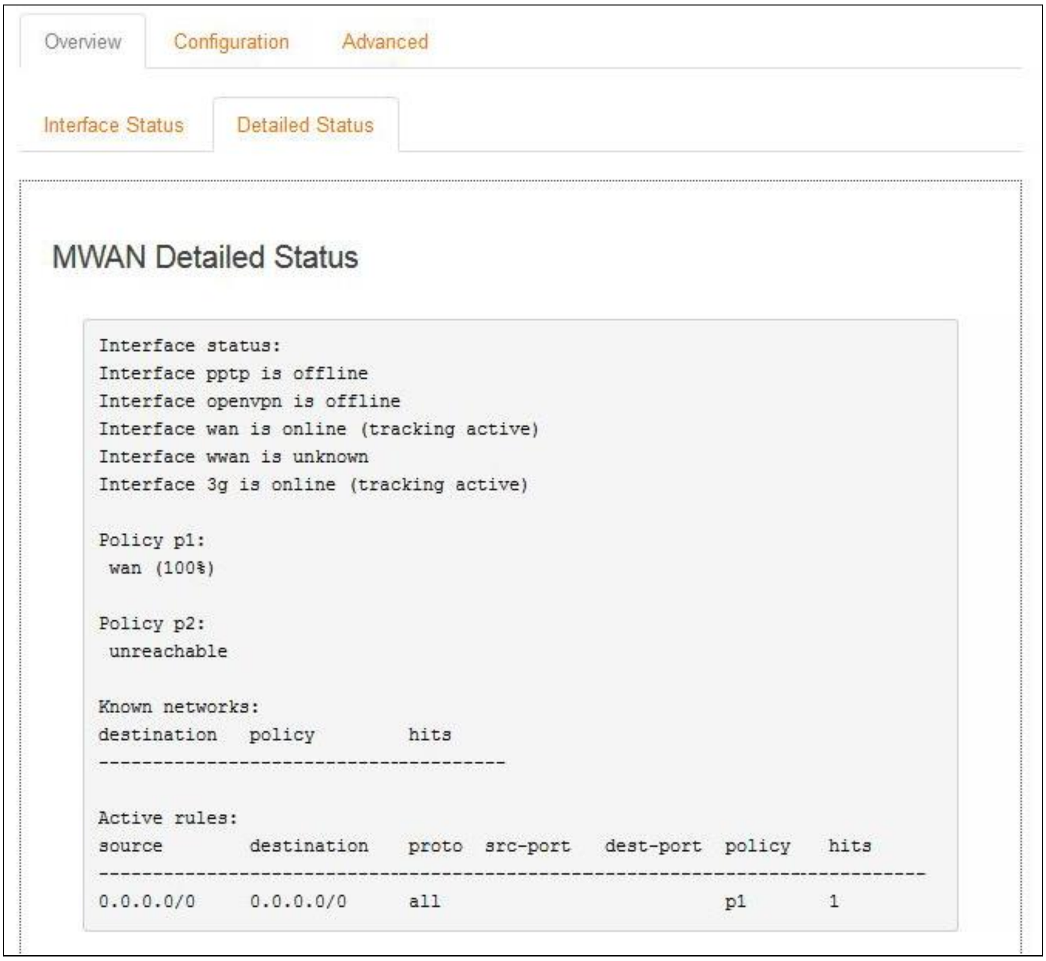
```
Last 50 MWAN systemlog entries. Newest entries sorted at the top :

Wed Jul 29 08:25:03 2015 user.notice mwan3: ifup interface 3g (3g-3g)
Wed Jul 29 08:24:25 2015 user.notice mwan3: ifdown interface 3g (unknown)
Wed Jul 29 08:14:17 2015 user.notice mwan3: ifup interface 3g (3g-3g)
Wed Jul 29 08:12:55 2015 user.notice mwan3: ifdown interface 3g (unknown)
```

Screen 11.2-1: 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 11.2-1: Live Status Overview of MWAN Interface

B. Detailed Status



MWAN Detailed Status

```
Interface status:
Interface pptp is offline
Interface openvpn is offline
Interface wan is online (tracking active)
Interface wwan is unknown
Interface 3g is online (tracking active)

Policy p1:
 wan (100%)

Policy p2:
 unreachable

Known networks:
destination   policy        hits
--------------------------------------

Active rules:
source        destination    proto  src-port   dest-port  policy    hits
-----------------------------------------------------------------------------
0.0.0.0/0     0.0.0.0/0      all                          p1        1
```

Screen 11.2-2: Detailed Status Overview of MWAN Interface

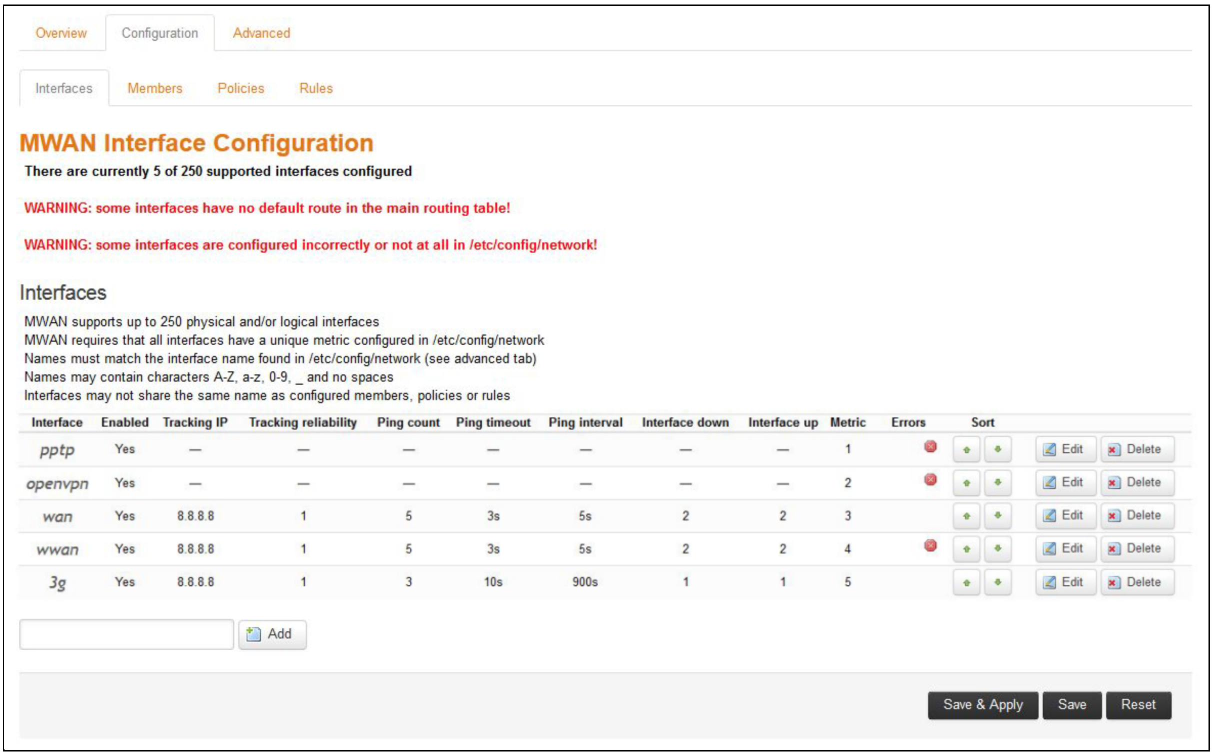
Parameters	Description
MWAN Status	Displays the detailed status for interface. These logs include the following information for all the available interfaces: - **Interface Live Status** – Online, Offline - **Each Policy Information –** Policy Name and interfaces configured for the policy - **Known Networks –** 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 11.2-2: Detailed Status Overview of MWAN Interface

11.2.2 Configuration

Network > Load Balancing > Configuration

A. Interface



MWAN Interface Configuration

There are currently 5 of 250 supported interfaces configured

WARNING: some interfaces have no default route in the main routing table!

WARNING: some interfaces are configured incorrectly or not at all in /etc/config/network!

Interfaces

MWAN supports up to 250 physical and/or logical interfaces
MWAN requires that all interfaces have a unique metric configured in /etc/config/network
Names must match the interface name found in /etc/config/network (see advanced tab)
Names may contain characters A-Z, a-z, 0-9, _ and no spaces
Interfaces may not share the same name as configured members, policies or rules

Interface	Enabled	Tracking IP	Tracking reliability	Ping count	Ping timeout	Ping interval	Interface down	Interface up	Metric	Errors	Sort	
pptp	Yes	—	—	—	—	—	—	—	1	●	↑ ↓	Edit Delete
openvpn	Yes	—	—	—	—	—	—	—	2	●	↑ ↓	Edit Delete
wan	Yes	8.8.8.8	1	5	3s	5s	2	2	3		↑ ↓	Edit Delete
wwan	Yes	8.8.8.8	1	5	3s	5s	2	2	4	●	↑ ↓	Edit Delete
3g	Yes	8.8.8.8	1	3	10s	900s	1	1	5		↑ ↓	Edit Delete

Screen 11.2-3: 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.

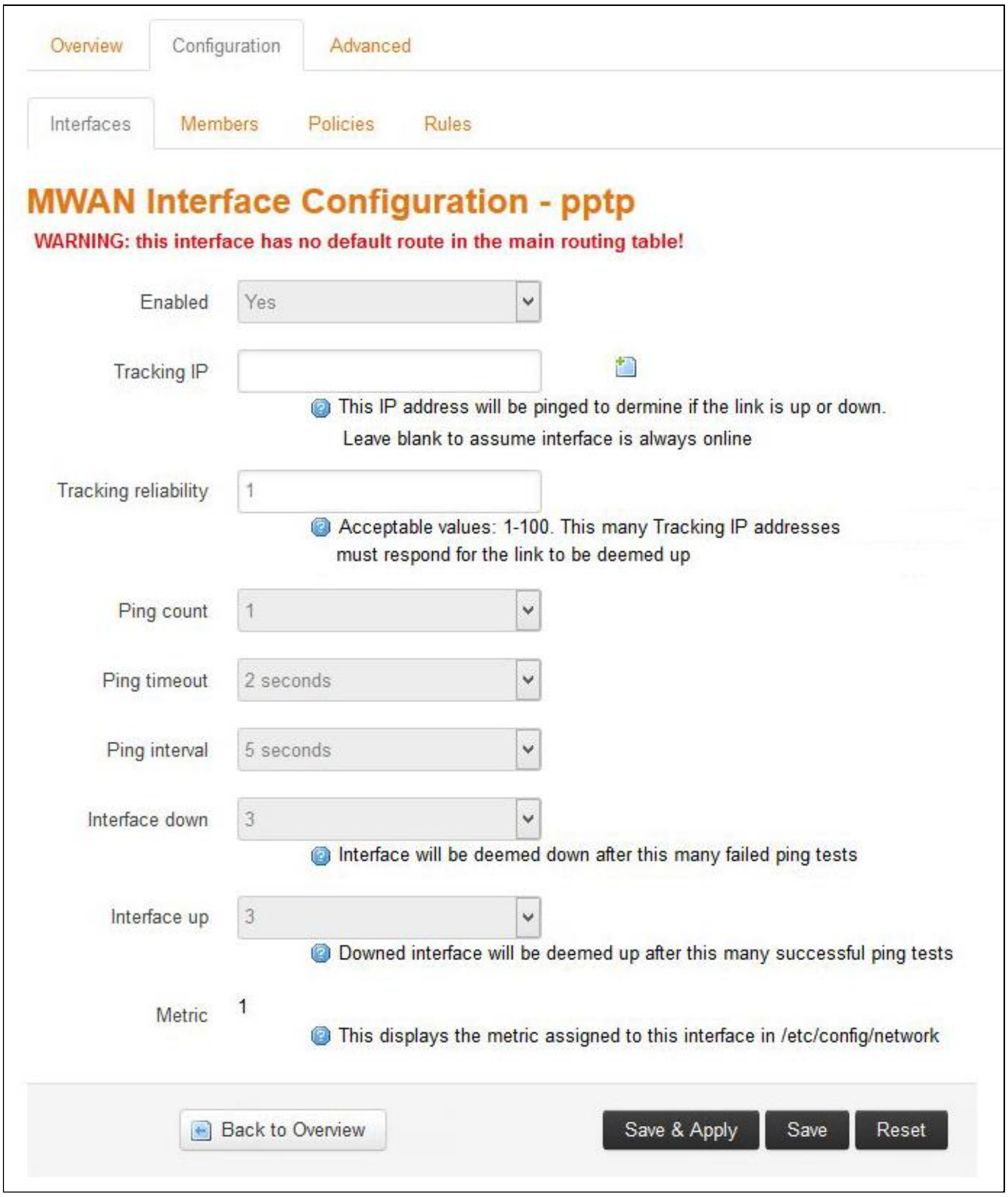
Interface down	The number of consecutive failed attempts after which the interface is declared offline
Interface up	The number of consecutive successful ping after which the interface is declared online
Metric	Metric assigned to the Interface from the Advanced Interface Configuration Settings page.
Error	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 11.2-3: Configuration details of MWAN Interface

Note

- ***More Tracking IP Address, high Ping counts and low Ping interval results in faster switchover however consumes high amount of data and vice-e-versa. We recommend you to get contact Maestro Support at support@maestro-wireless.com.***

a. Edit



MWAN Interface Configuration - pptp

WARNING: this interface has no default route in the main routing table!

Enabled: Yes

Tracking IP:

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

Tracking reliability: 1

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

Ping count: 1

Ping timeout: 2 seconds

Ping interval: 5 seconds

Interface down: 3

Interface will be deemed down after this many failed ping tests

Interface up: 3

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

Metric: 1

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

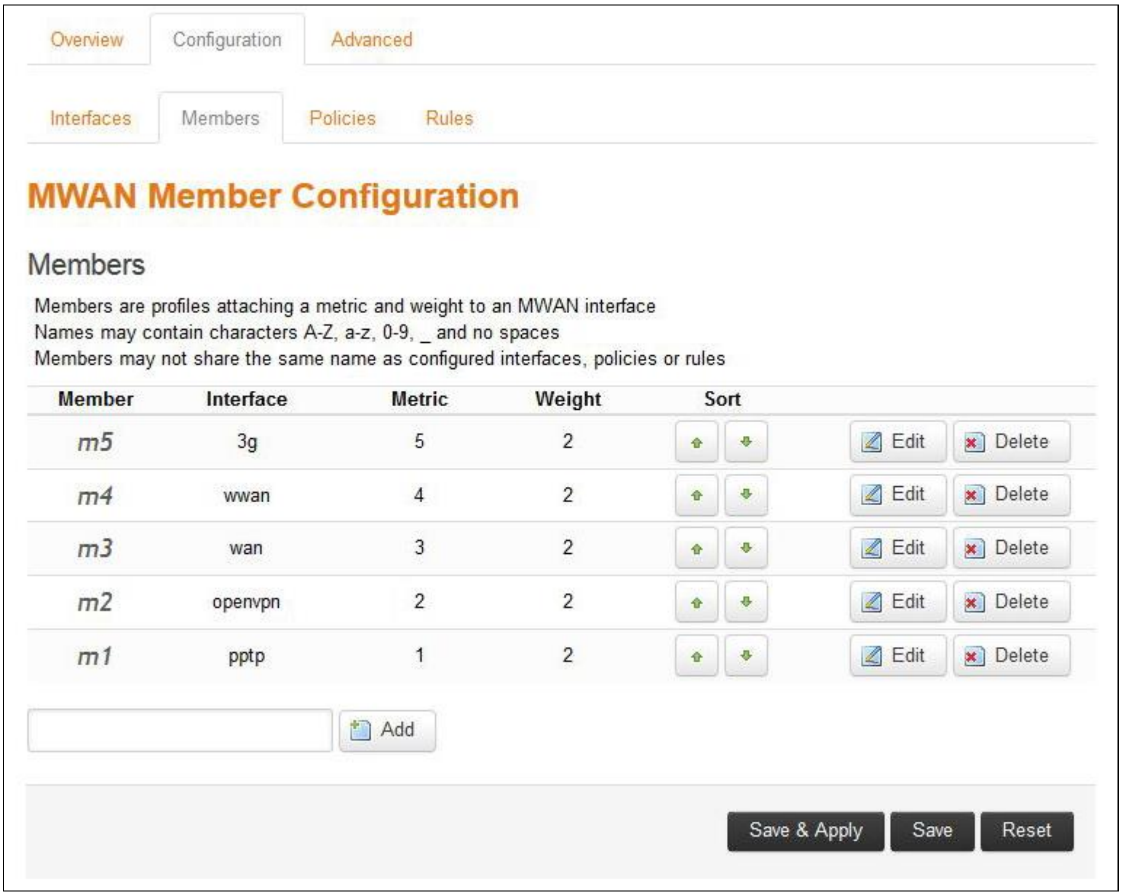
Screen 11.2-4: Modify MWAN Interface

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 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 11.2-4: Modify MWAN Interface

B. Members



MWAN Member Configuration

Members

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

Member	Interface	Metric	Weight	Sort		
m5	3g	5	2		Edit	Delete
m4	wwan	4	2		Edit	Delete
m3	wan	3	2		Edit	Delete
m2	openvpn	2	2		Edit	Delete
m1	pptp	1	2		Edit	Delete

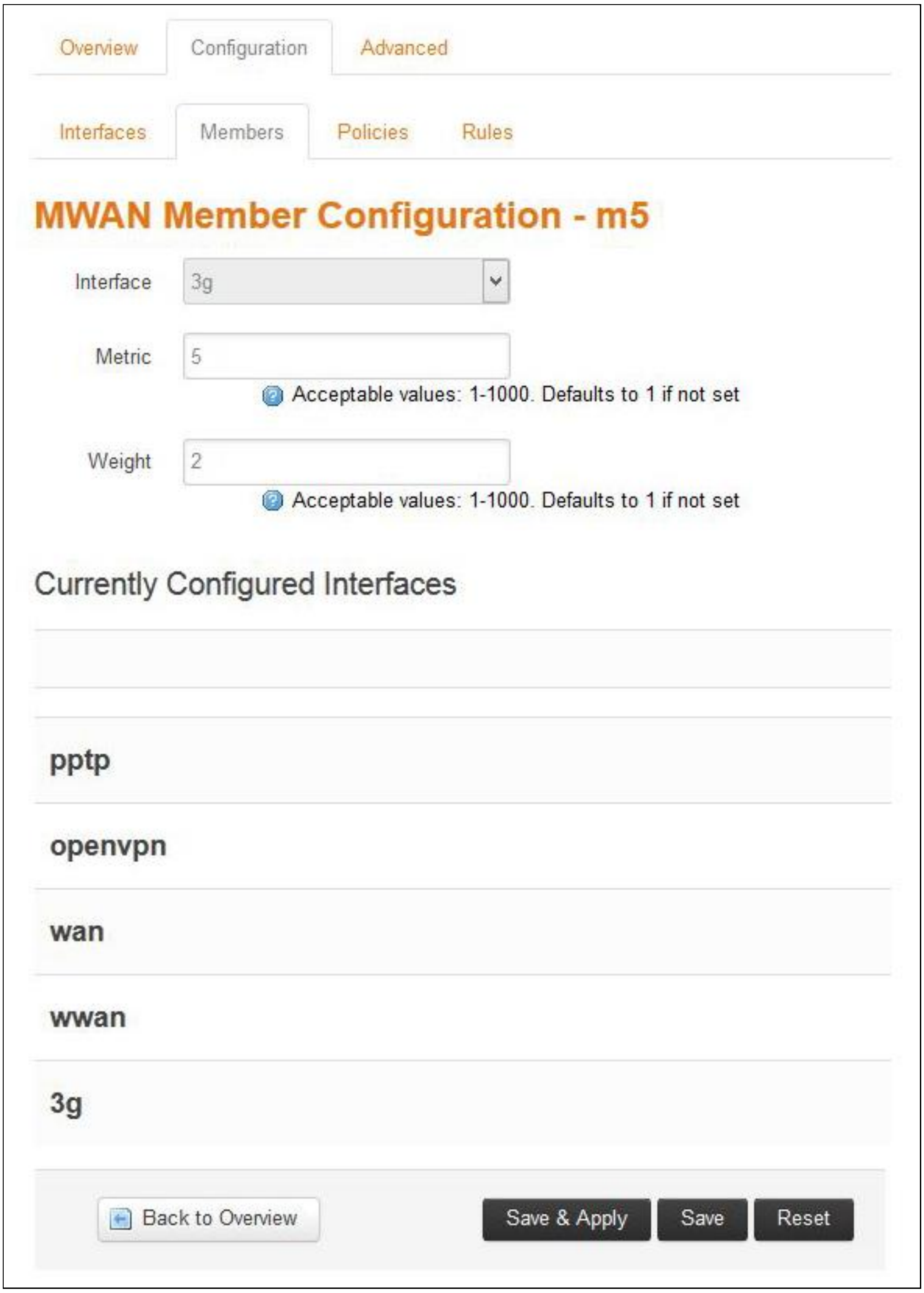
Screen 11.2-5: Member Configuration details of MWAN Interface

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 11.2-5: Member Configuration details of MWAN Interface

a. Edit



MWAN Member Configuration - m5

Interface: 3g

Metric: 5

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

Weight: 2

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

Currently Configured Interfaces

pptp

openvpn

wan

wwan

3g

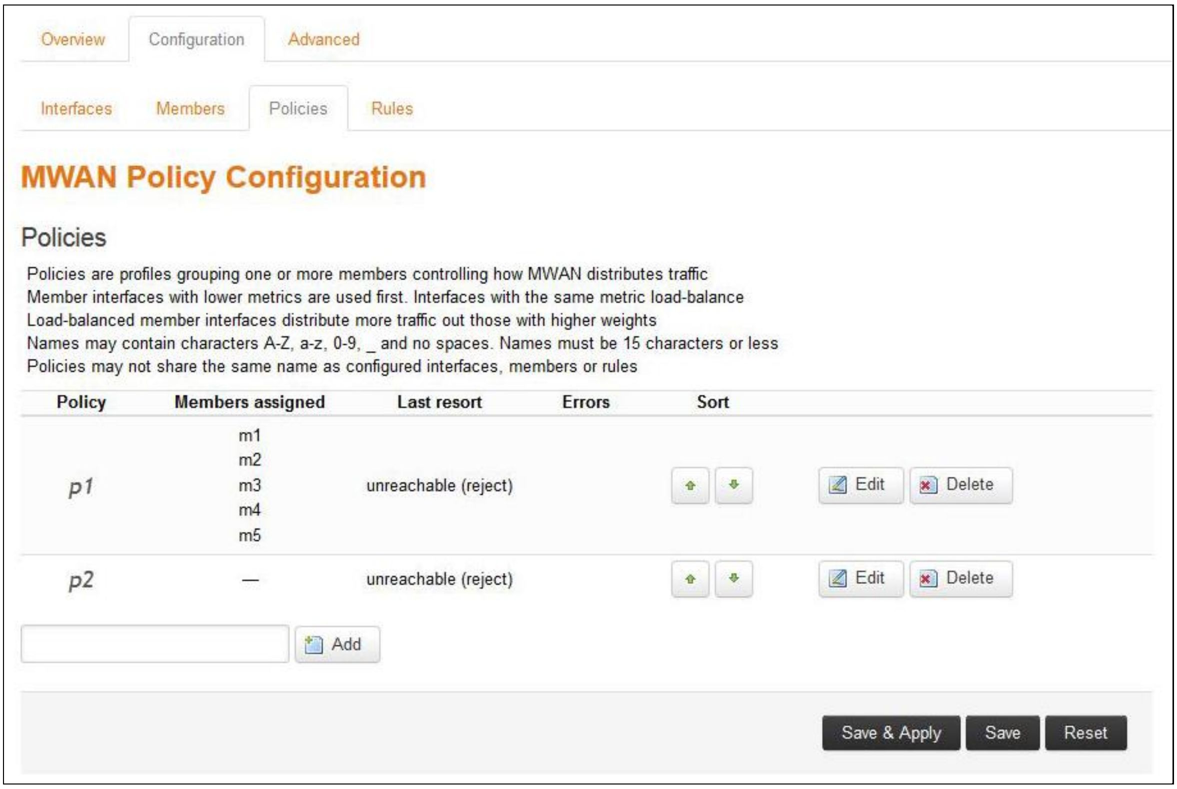
Screen 11.2-6: Modify the Member details of MWAN Interface

Parameters	Description
Interface	Displays the name of the interface.
Metric	Enter the Interface Metric. The route with least metric is considered as best route.

	The default metric assigned to the interface is 5. 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. For load balancing between two interfaces, both the interface must have the same metric value. The route with higher weight carries more traffic.
Currently Configured Interfaces	List of currently configured Interfaces.

Table 11.2-6: Modify the Member details of MWAN Interface

C. Policies



MWAN Policy Configuration

Policies

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

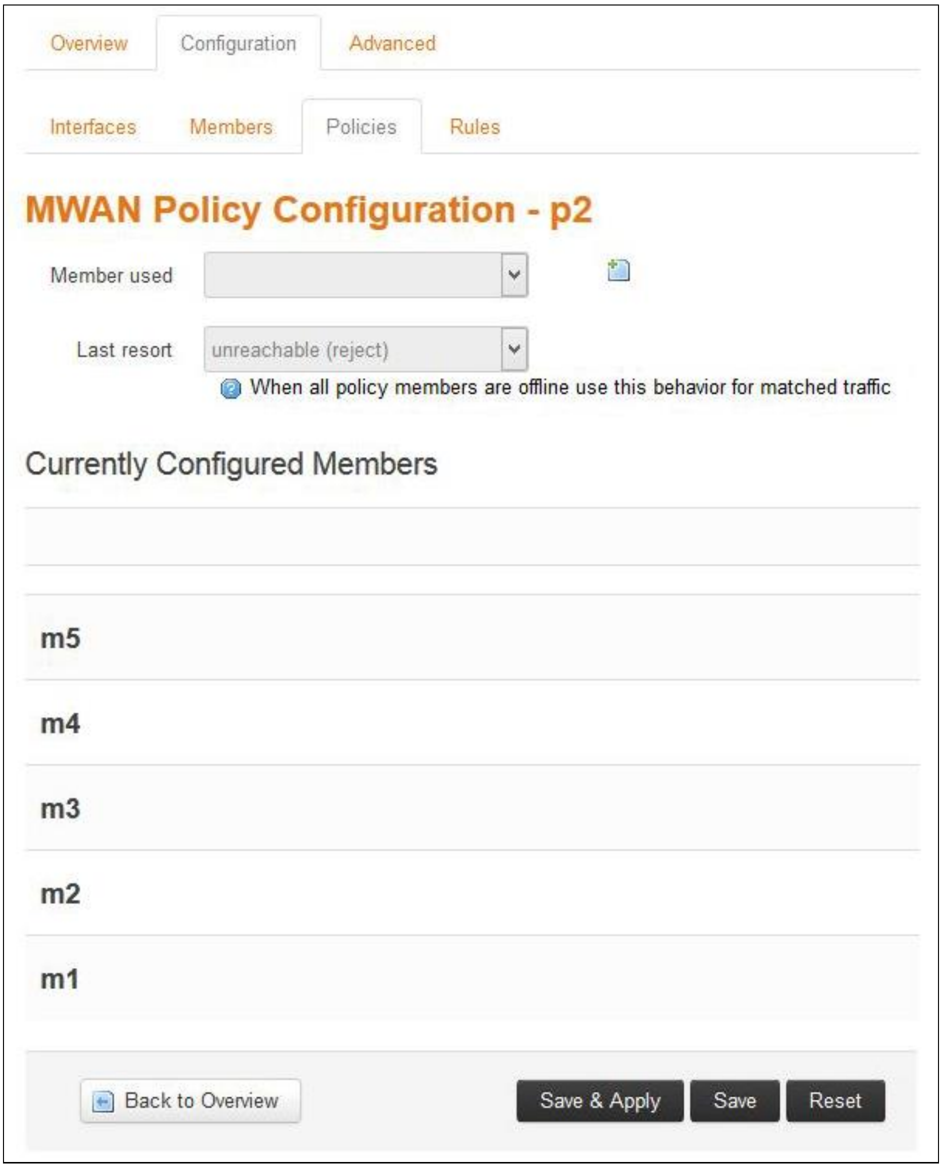
Policy	Members assigned	Last resort	Errors	Sort
p1	m1 m2 m3 m4 m5	unreachable (reject)		↑ ↓
p2	—	unreachable (reject)		↑ ↓

Screen 11.2-7: 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 11.2-7: Policy Configuration details of MWAN Interface

a. Edit



MWAN Policy Configuration - p2

Member used

Last resort: unreachable (reject)

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

Currently Configured Members

m5

m4

m3

m2

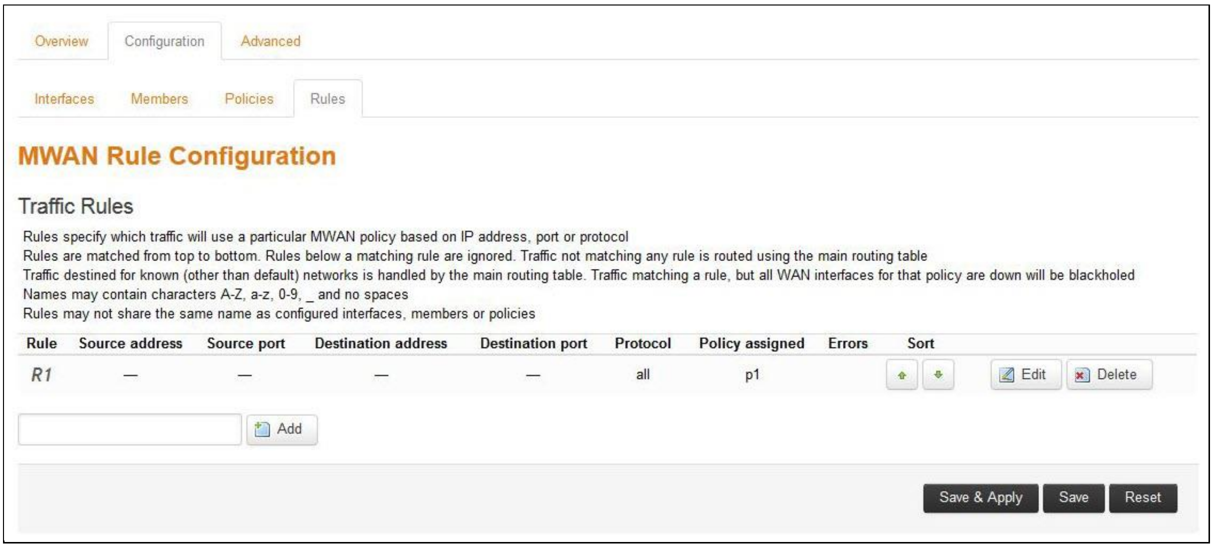
m1

Screen 11.2-8: 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 11.2-8: Modify Policy of MWAN Interface

D. Rules



MWAN Rule Configuration

Traffic Rules

Rules specify which traffic will use a particular MWAN policy based on IP address, port or protocol
Rules are matched from top to bottom. Rules below a matching rule are ignored. Traffic not matching any rule is routed using the main routing table
Traffic destined for known (other than default) networks is handled by the main routing table. Traffic matching a rule, but all WAN interfaces for that policy are down will be blackholed
Names may contain characters A-Z, a-z, 0-9, _ and no spaces
Rules may not share the same name as configured interfaces, members or policies

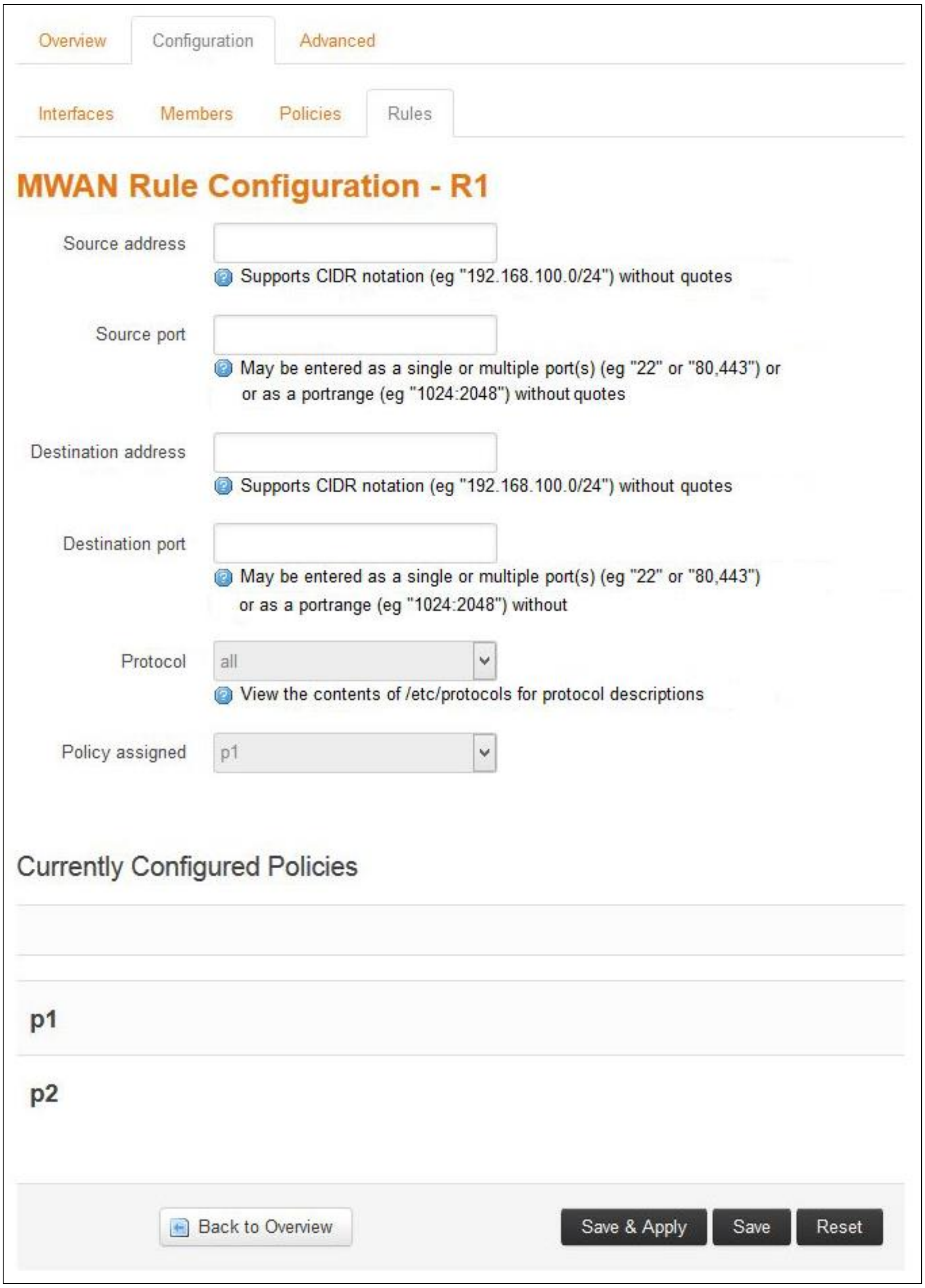
Rule	Source address	Source port	Destination address	Destination port	Protocol	Policy assigned	Errors	Sort
R1	—	—	—	—	all	p1		

Screen 11.2-9: 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 11.2-9: Rule Configuration details of MWAN Interface

a. Edit



MWAN Rule Configuration - R1

Source address

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

Source port

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

Destination address

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

Destination port

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

Protocol: all

View the contents of /etc/protocols for protocol descriptions

Policy assigned: p1

Currently Configured Policies

p1

p2

Screen 11.2-10: 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.

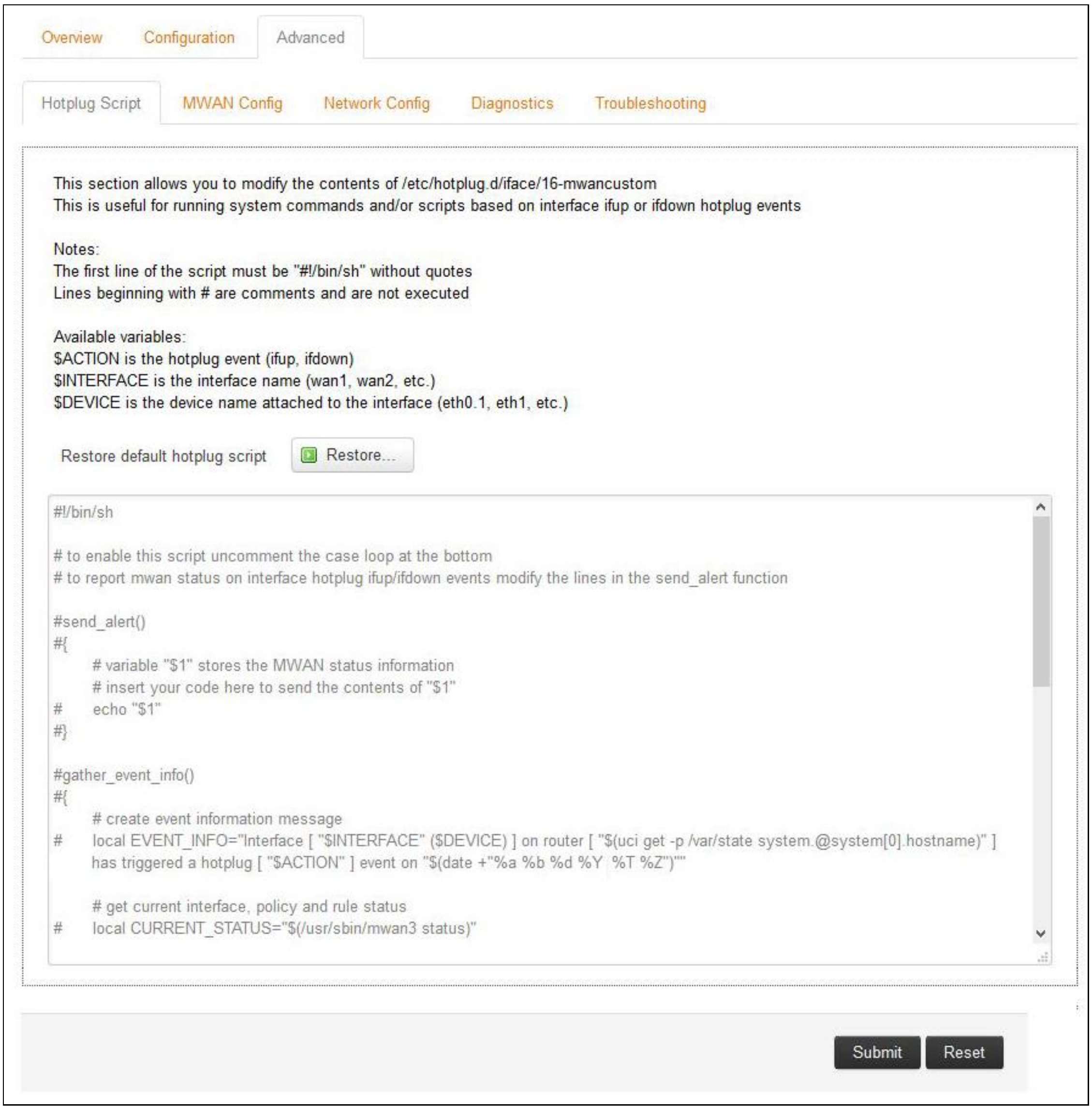
Destination port	Enter the Destination Port number.
Protocol	Select the protocols on which the rule is applicable.
Policy assigned	Policy to be applied to the rule.
Currently Configured Policies	Policy already applied to the rule.

Table 11.2-10: Edit Rule details of MWAN Interface

11.2.3 Advanced Settings

Network > Load Balancing > Advanced Settings

A. Hotplug Script



This section allows you to modify the contents of /etc/hotplug.d/iface/16-mwancustom
This is useful for running system commands and/or scripts based on interface ifup or ifdown hotplug events

Notes:
The first line of the script must be "#!/bin/sh" without quotes
Lines beginning with # are comments and are not executed

Available variables:
$ACTION is the hotplug event (ifup, ifdown)
$INTERFACE is the interface name (wan1, wan2, etc.)
$DEVICE is the device name attached to the interface (eth0.1, eth1, etc.)

Restore default hotplug script Restore...

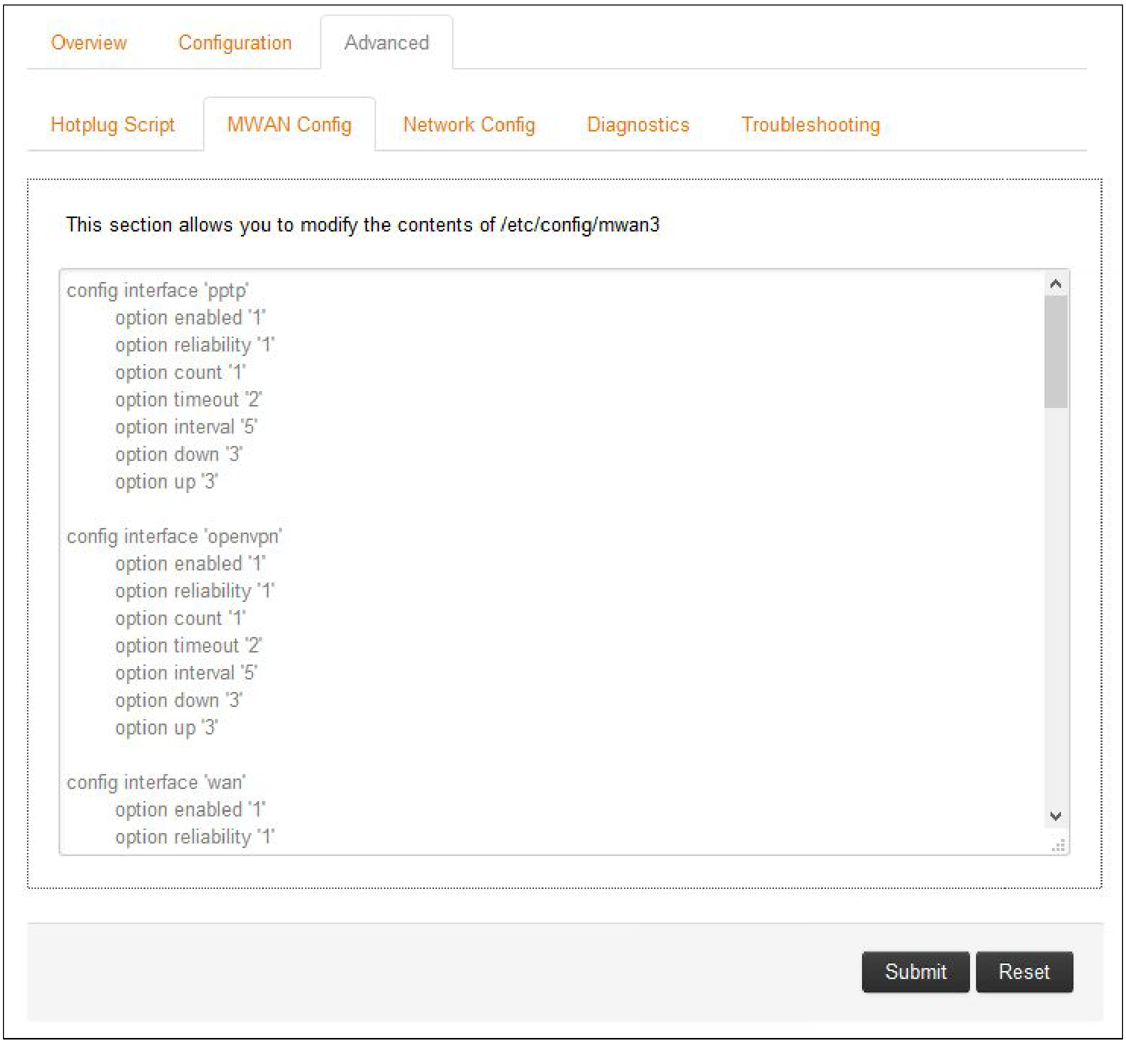
```
#!/bin/sh

# to enable this script uncomment the case loop at the bottom
# to report mwan status on interface hotplug ifup/ifdown events modify the lines in the send_alert function

#send_alert()
#{
	# variable "$1" stores the MWAN status information
	# insert your code here to send the contents of "$1"
#	echo "$1"
#}

#gather_event_info()
#{
	# create event information message
#	local EVENT_INFO="Interface [ "$INTERFACE" ($DEVICE) ] on router [ "$(uci get -p /var/state system.@system[0].hostname)" ]
	has triggered a hotplug [ "$ACTION" ] event on "$(date +"%a %b %d %Y  %T %Z")""

	# get current interface, policy and rule status
#	local CURRENT_STATUS="$(/usr/sbin/mwan3 status)"
```

Screen 11.2-11: 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 11.2-11: Advance Configuration for Hotplug Script

B. MWAN Configuration



This section allows you to modify the contents of /etc/config/mwan3

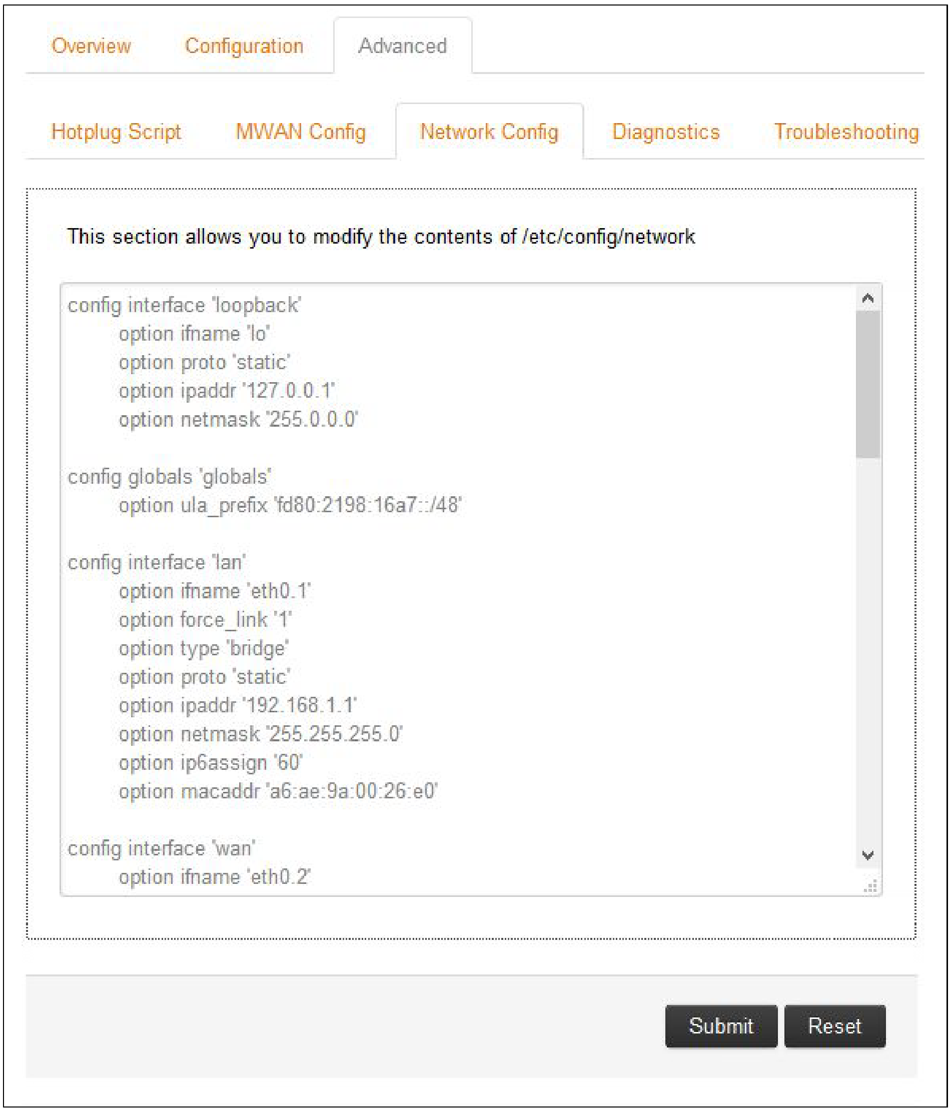
```
config interface 'pptp'
        option enabled '1'
        option reliability '1'
        option count '1'
        option timeout '2'
        option interval '5'
        option down '3'
        option up '3'

config interface 'openvpn'
        option enabled '1'
        option reliability '1'
        option count '1'
        option timeout '2'
        option interval '5'
        option down '3'
        option up '3'

config interface 'wan'
        option enabled '1'
        option reliability '1'
```

Screen 11.2-12: 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 11.2-12: Advance Configuration for MWAN Interfaces

C. Network Configuration



This section allows you to modify the contents of /etc/config/network

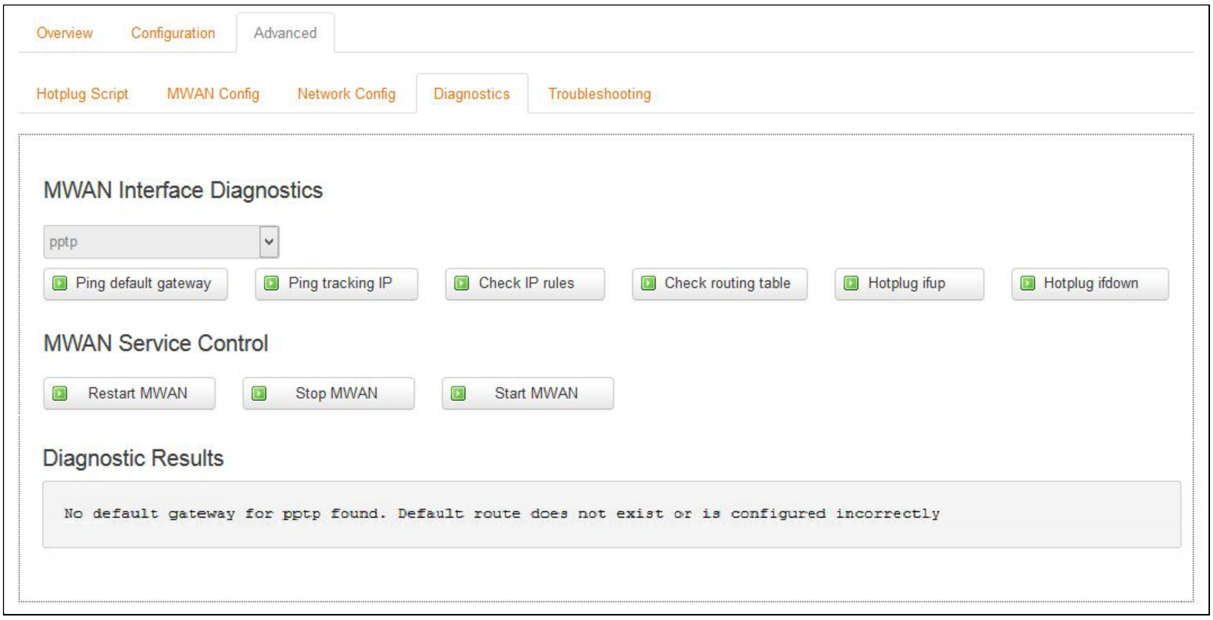
```
config interface 'loopback'
        option ifname 'lo'
        option proto 'static'
        option ipaddr '127.0.0.1'
        option netmask '255.0.0.0'

config globals 'globals'
        option ula_prefix 'fd80:2198:16a7::/48'

config interface 'lan'
        option ifname 'eth0.1'
        option force_link '1'
        option type 'bridge'
        option proto 'static'
        option ipaddr '192.168.1.1'
        option netmask '255.255.255.0'
        option ip6assign '60'
        option macaddr 'a6:ae:9a:00:26:e0'

config interface 'wan'
        option ifname 'eth0.2'
```

Screen 11.2-13: 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 11.2-13: Advance Configuration for MWAN Network

D. Diagnostics



```
No default gateway for pptp found. Default route does not exist or is configured incorrectly
```

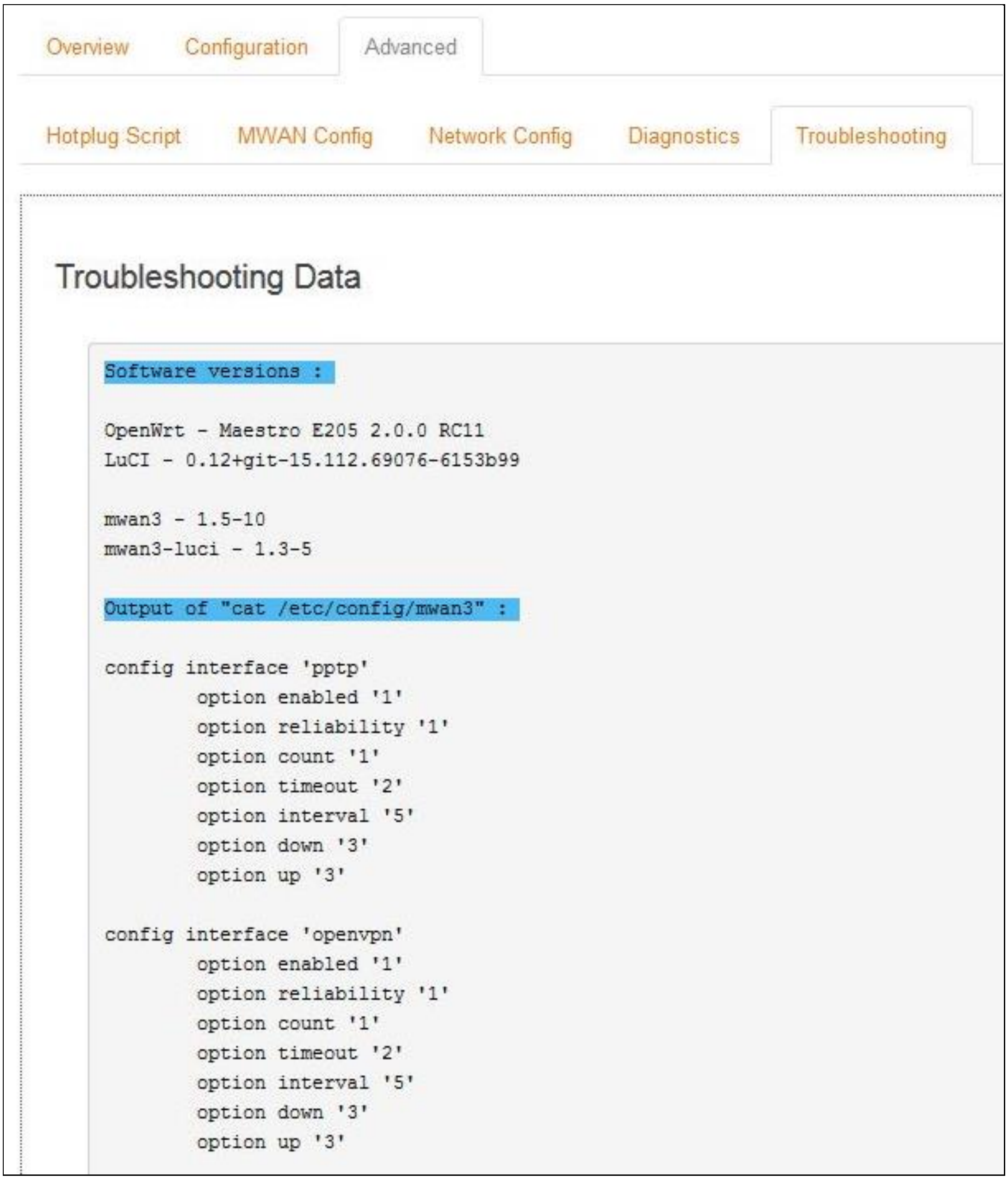
Screen 11.2-14: MWAN Interface and Service Diagnostics

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 11.2-14: MWAN Interface and Service Diagnostics

E. Troubleshooting



Troubleshooting Data

```
Software versions :

OpenWrt - Maestro E205 2.0.0 RC11
LuCI - 0.12+git-15.112.69076-6153b99

mwan3 - 1.5-10
mwan3-luci - 1.3-5

Output of "cat /etc/config/mwan3" :

config interface 'pptp'
        option enabled '1'
        option reliability '1'
        option count '1'
        option timeout '2'
        option interval '5'
        option down '3'
        option up '3'

config interface 'openvpn'
        option enabled '1'
        option reliability '1'
        option count '1'
        option timeout '2'
        option interval '5'
        option down '3'
        option up '3'
```

Screen 11.2-15: Data for Troubleshooting

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

Table 11.2-15: Data for Troubleshooting

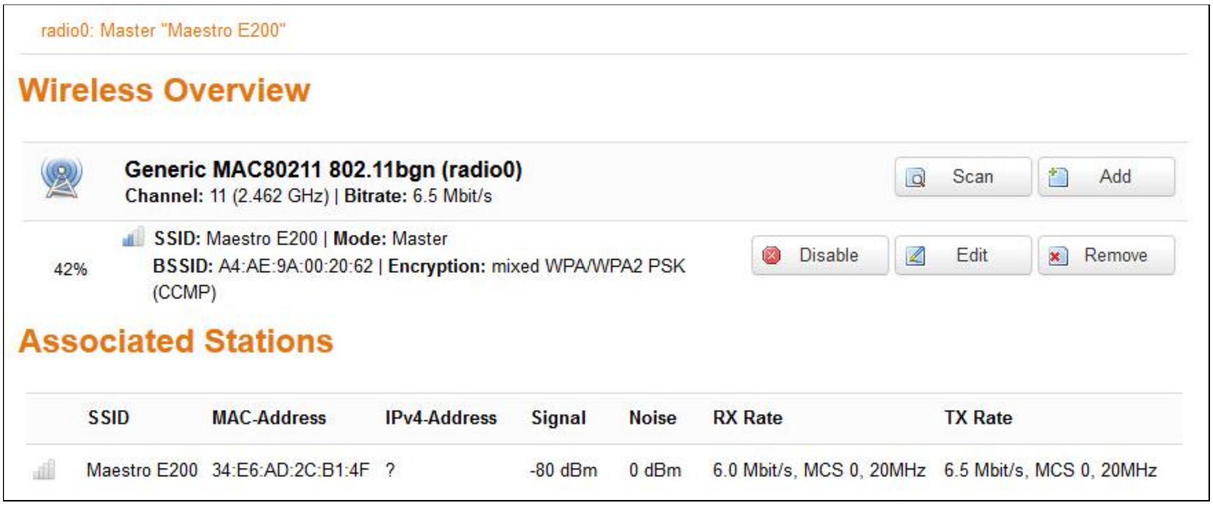
11.3 Wi-Fi

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).



radio0: Master "Maestro E200"

Wireless Overview

Generic MAC80211 802.11bgn (radio0)
Channel: 11 (2.462 GHz) | **Bitrate:** 6.5 Mbit/s

42%
SSID: Maestro E200 | **Mode:** Master
BSSID: A4:AE:9A:00:20:62 | **Encryption:** mixed WPA/WPA2 PSK (CCMP)

Associated Stations

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
Maestro E200	34:E6:AD:2C:B1:4F	?	-80 dBm	0 dBm	6.0 Mbit/s, MCS 0, 20MHz	6.5 Mbit/s, MCS 0, 20MHz

Screen 11.3-1: 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.
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 11.3-1: Wireless Connection and Associated Stations Overview

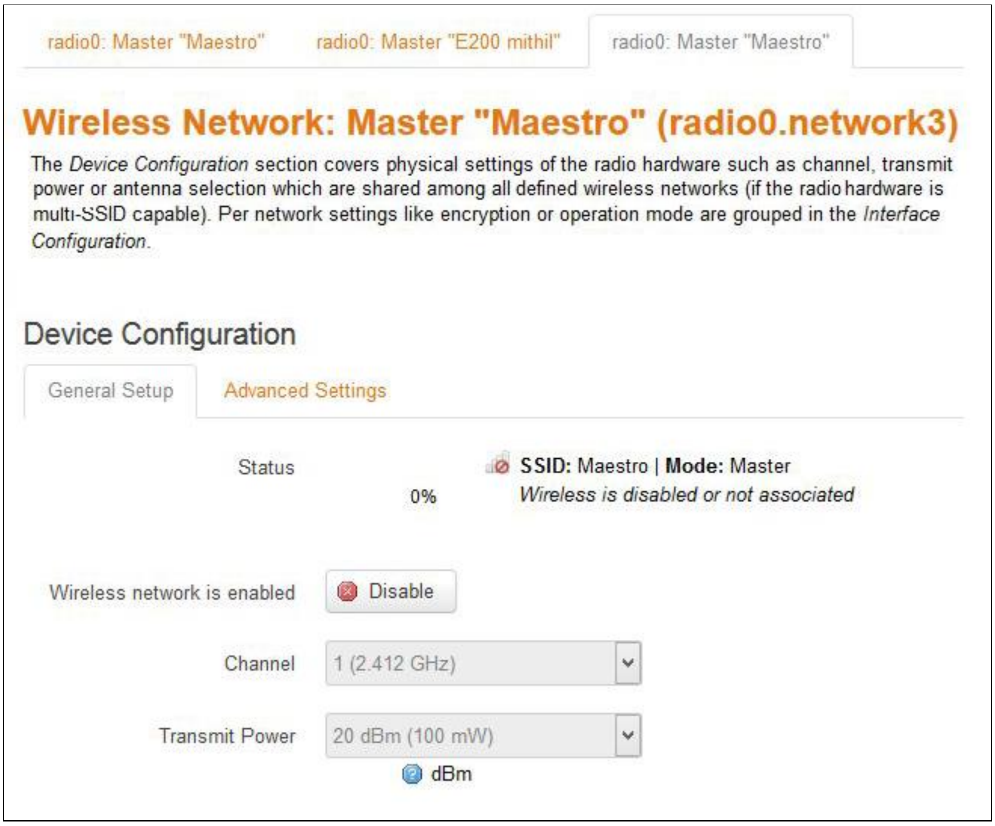
11.3.1 Add

Network > Wi-Fi > Add

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

A. Device Configuration

a. General Settings



Wireless Network: Master "Maestro" (radio0.network3)

The *Device Configuration* section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the *Interface Configuration*.

Device Configuration

Status: 0% **SSID:** Maestro | **Mode:** Master *Wireless is disabled or not associated*

Wireless network is enabled: Disable

Channel: 1 (2.412 GHz)

Transmit Power: 20 dBm (100 mW) dBm

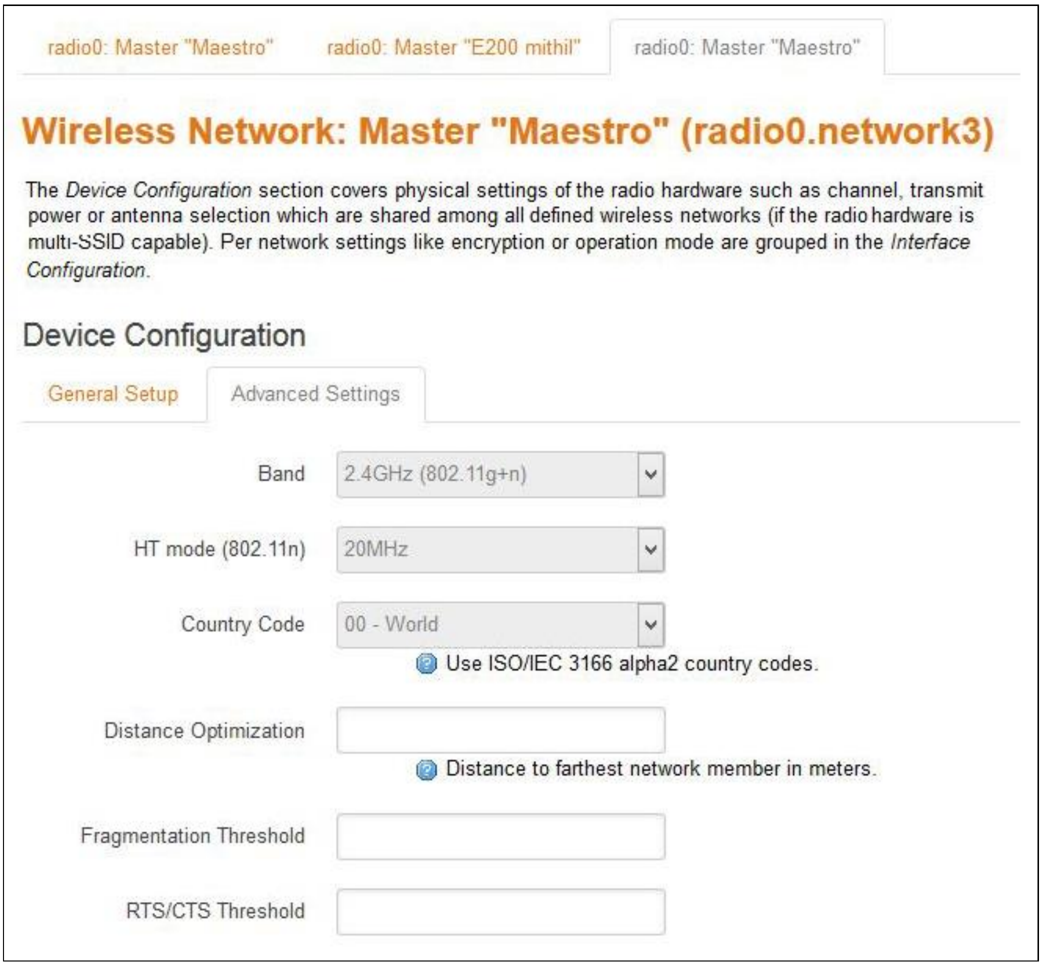
Screen 11.3-2: General Wireless Connection Configurations for a New Device

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. The default selection is 20dBm or 100mW.

Table 11.3-2: General Wireless Connection Configurations for a New Device

b. Advanced Settings



Wireless Network: Master "Maestro" (radio0.network3)

The *Device Configuration* section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the *Interface Configuration*.

Device Configuration

Band: 2.4GHz (802.11g+n)

HT mode (802.11n): 20MHz

Country Code: 00 - World
Use ISO/IEC 3166 alpha2 country codes.

Distance Optimization:
Distance to farthest network member in meters.

Fragmentation Threshold:

RTS/CTS Threshold:

Screen 11.3-3: Advance Wireless Connection Configurations for a New Device

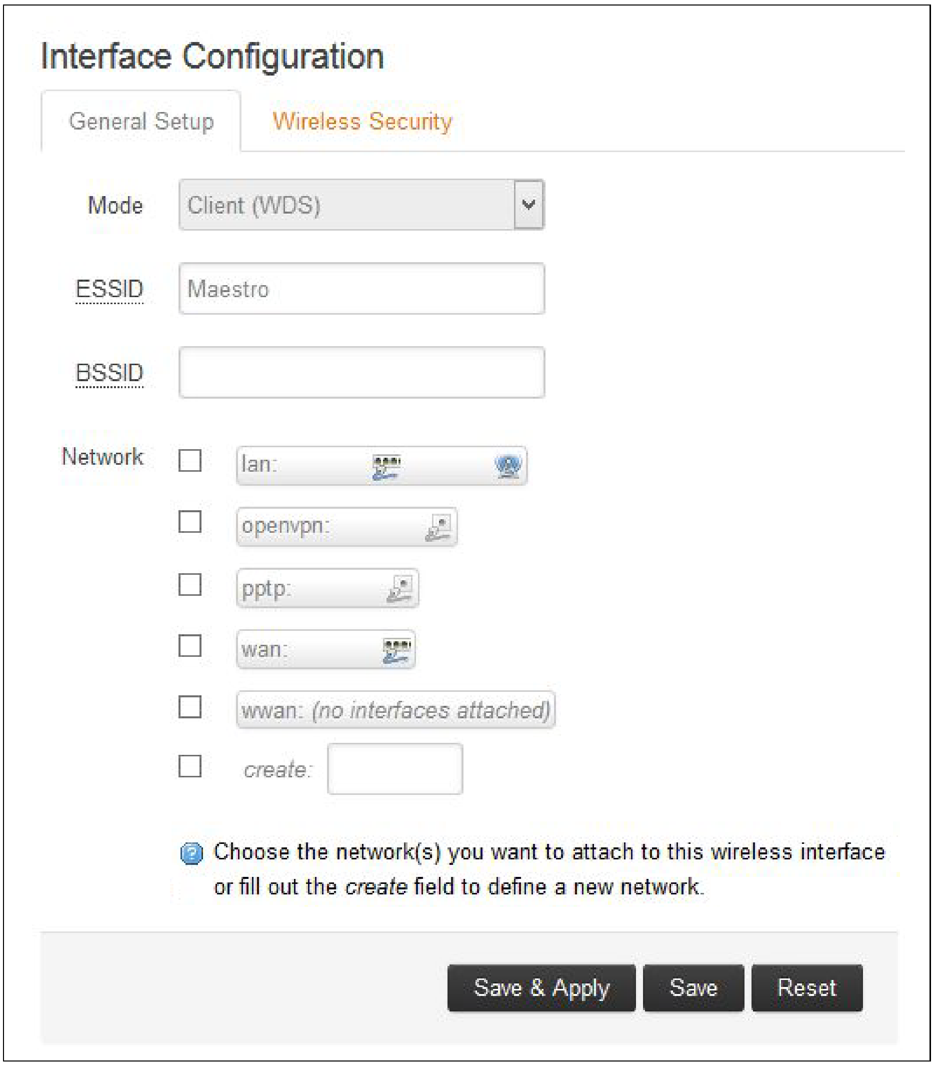
Parameters	Description
Band	Select the Wi-Fi band. The default band is 2.4GHz (802.11g+n).
HT mode (802.11n)	Select the HT mode for Wi-Fi connection. **Available Options** - 20 Mhz - 40Mhz - Disable The default HT mode value is 20Mhz
Country Code	Choose the country code corresponding to the country where 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-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 11.3-3: Advance Wireless Connection Configurations for a New Device

B. Interface Configuration

a. General Setup



Interface Configuration

Mode: Client (WDS)

ESSID: Maestro

BSSID:

Network:
- □ lan:
- □ openvpn:
- □ pptp:
- □ wan:
- □ wwan: *(no interfaces attached)*
- □ *create:*

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

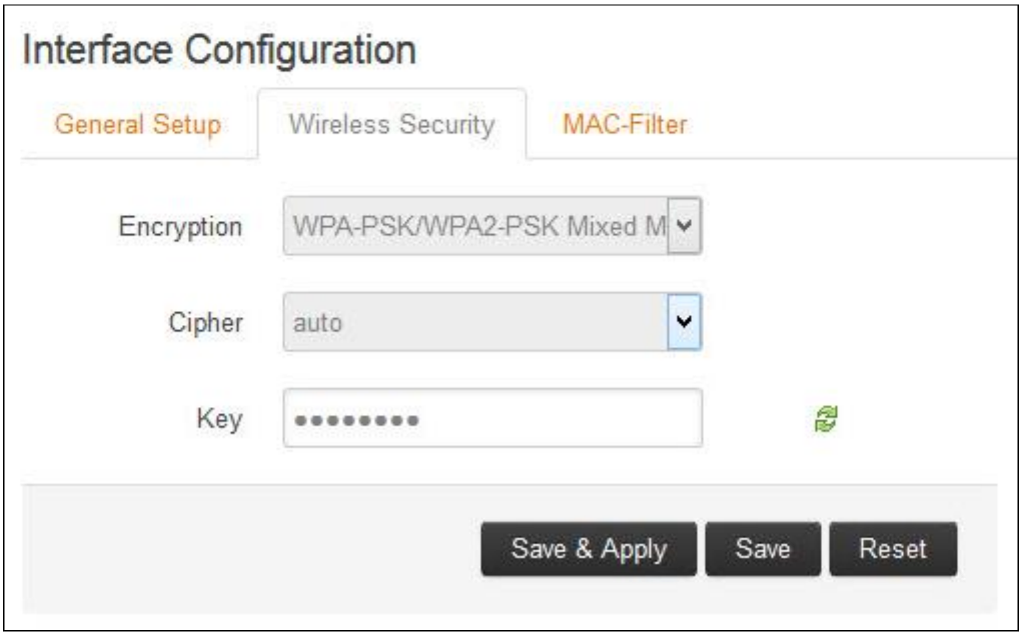
Screen 11.3-4: General Wireless Connection Configurations for a New Interface

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. 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	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 11.3-4: General Wireless Connection Configurations for a New Interface

b. Wireless Security



Interface Configuration

Encryption: WPA-PSK/WPA2-PSK Mixed M

Cipher: auto

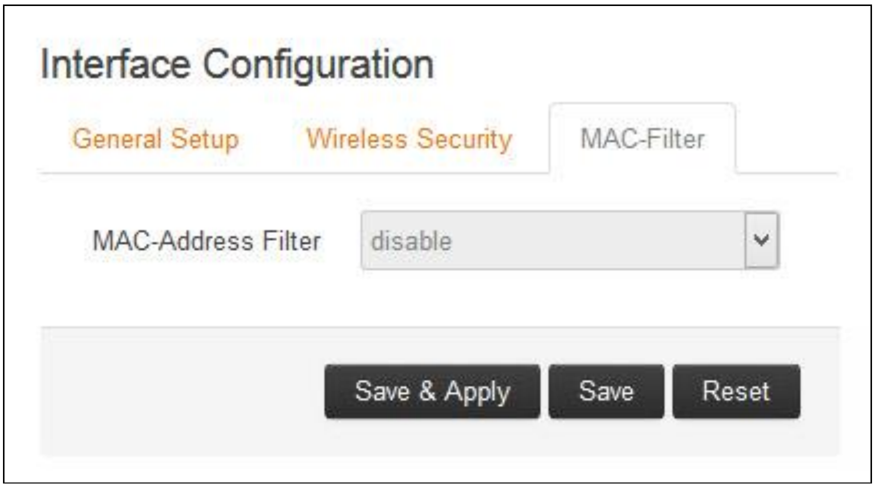
Key: ●●●●●●●●●

Screen 11.3-5: 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 11.3-5: Wireless Security Configurations for a New Interface

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



Interface Configuration

MAC-Address Filter: disable

Screen 11.3-6: 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 11.3-6: MAC Filter Configurations for a New Interface

11.4 DHCP and DNS

Network > DHCP and DNS

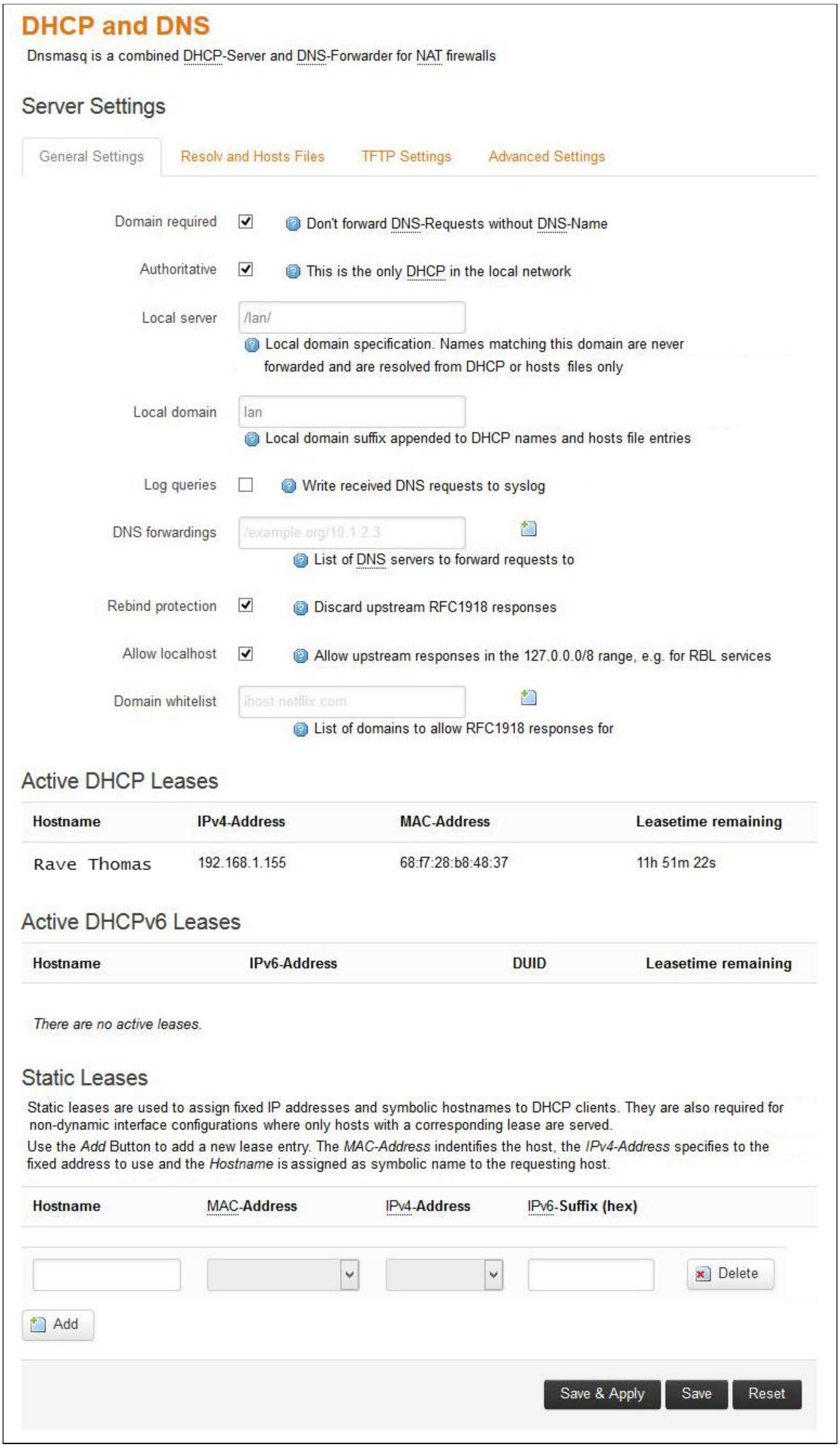
Dynamic Host Configuration Protocol (DHCP) is a network protocol that is used to configure network devices to communicate on an IP network. A DHCP client uses the DHCP protocol to acquire configuration information, such as an IP address, a default route, and one or more DNS server addresses from a DHCP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

11.4.1 General Settings

Network > DHCP and DNS > General Settings



DHCP and DNS

Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls

Server Settings

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

Domain required ☑ Don't forward DNS-Requests without DNS-Name

Authoritative ☑ This is the only DHCP in the local network

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

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

Log queries □ Write received DNS requests to syslog

DNS forwardings /example.org/10.1.2.3
List of DNS servers to forward requests to

Rebind protection ☑ Discard upstream RFC1918 responses

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

Domain whitelist ihost.netflix.com
List of domains to allow RFC1918 responses for

Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
Rave Thomas	192.168.1.155	68:f7:28:b8:48:37	11h 51m 22s

Active DHCPv6 Leases

Hostname	IPv6-Address	DUID	Leasetime remaining

There are no active leases.

Static Leases

Static leases are used to assign fixed IP addresses and symbolic hostnames to DHCP clients. They are also required for non-dynamic interface configurations where only hosts with a corresponding lease are served.
Use the *Add* Button to add a new lease entry. The *MAC-Address* indentifies the host, the *IPv4-Address* specifies to the fixed address to use and the *Hostname* is assigned as symbolic name to the requesting host.

Hostname	MAC-Address	IPv4-Address	IPv6-Suffix (hex)	
				Delete

Add

Save & Apply | Save | Reset

Screen 11.4-1: General Configuration of DHCP Server and DNS-Forwarder

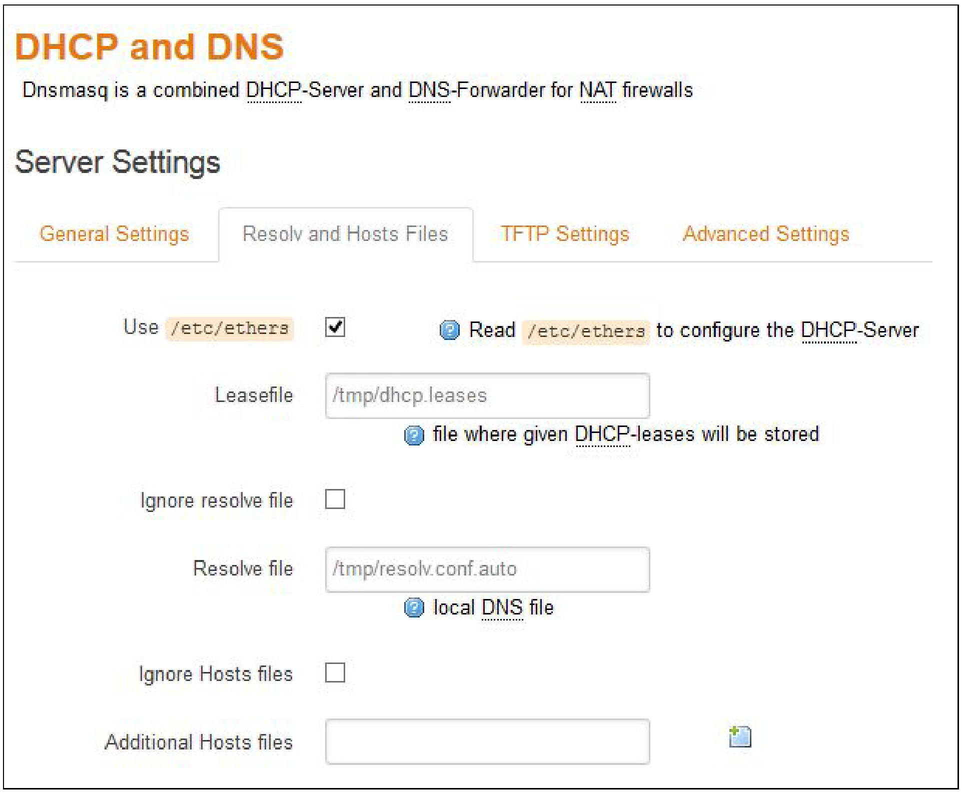
Parameters	Description
Server Settings	
Domain required	Check to allow forwarding of DNS request only if they have domain name.
Authoritative	Check to authorize the DHCP in the local network.
Local server	Enter the local server domain specification. These domain names are only resoled using DHCP or host 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 11.4-1: General Configuration of DHCP Server and DNS-Forwarder

11.4.2 Resolv and Host file

Network > DHCP and DNS > Resolv and Host File



DHCP and DNS

Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls

Server Settings

Use /etc/ethers ☑ Read /etc/ethers to configure the DHCP-Server

Leasefile /tmp/dhcp.leases — file where given DHCP-leases will be stored

Ignore resolve file □

Resolve file /tmp/resolv.conf.auto — local DNS file

Ignore Hosts files □

Additional Hosts files

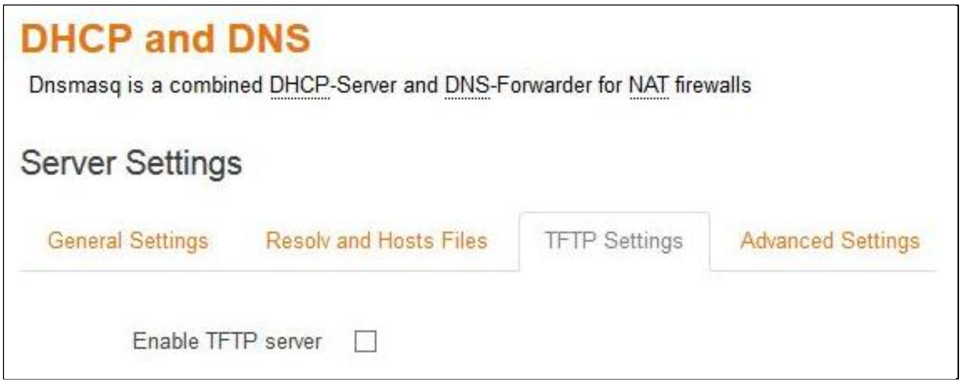
Screen 11.4-2: Resolv and Host File Configuration for DHCP and DNS

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 11.4-2: Resolv and Host File Configuration for DHCP and DNS

11.4.3 TFTP Settings

Network > DHCP and DNS > TFTP Settings



DHCP and DNS

Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls

Server Settings

Enable TFTP server □

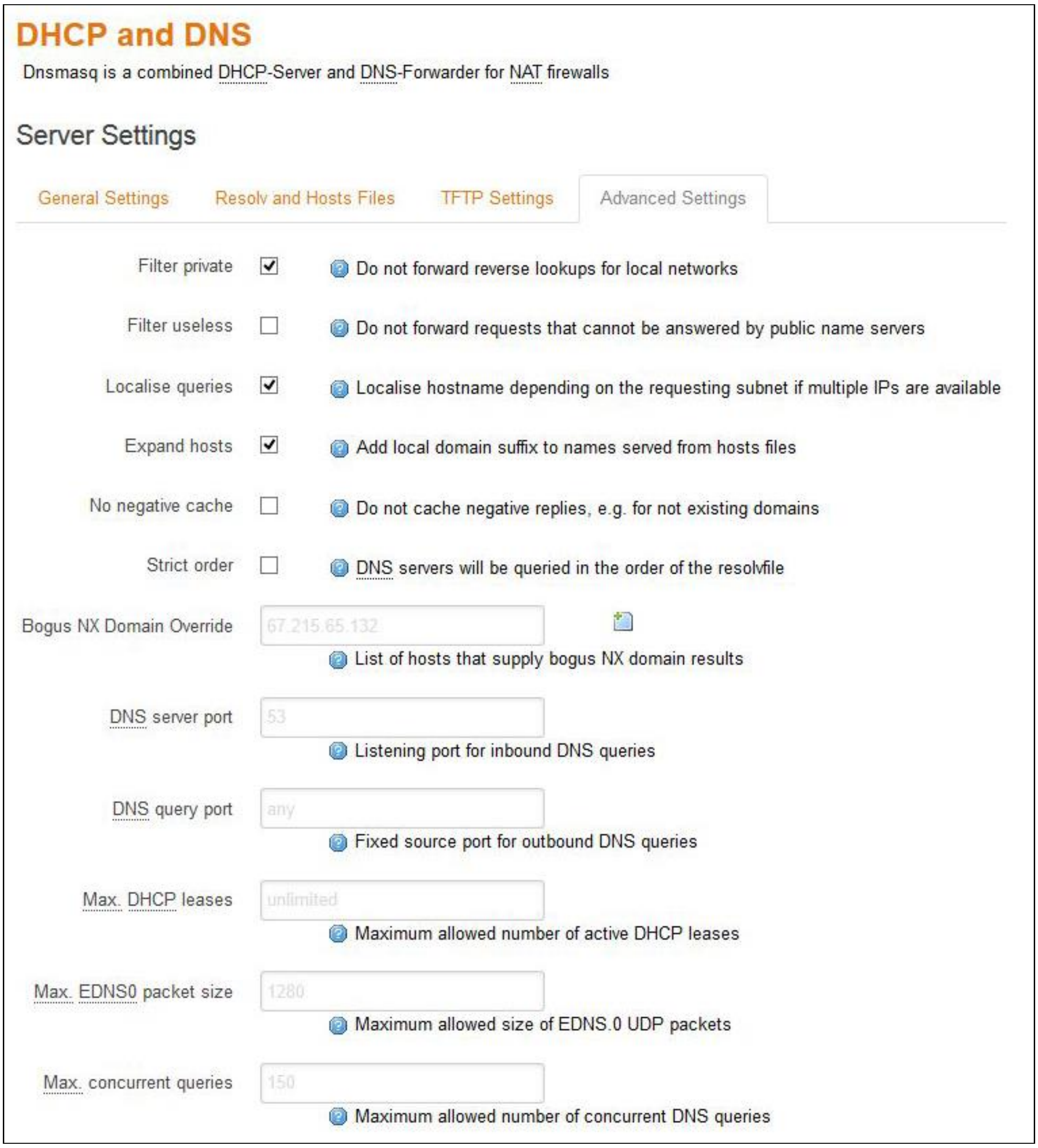
Screen 11.4-3: TFTP Configuration for DHCP and DNS

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 11.4-3: TFTP Configuration for DHCP and DNS

11.4.4 Advanced Settings

Network > DHCP and DNS > Advanced Settings



DHCP and DNS

Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls

Server Settings

Filter private ☑ Do not forward reverse lookups for local networks

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

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

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

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

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

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

DNS server port: 53 — Listening port for inbound DNS queries

DNS query port: any — Fixed source port for outbound DNS queries

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

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

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

Screen 11.4-4: Advanced Configuration for DHCP and DNS

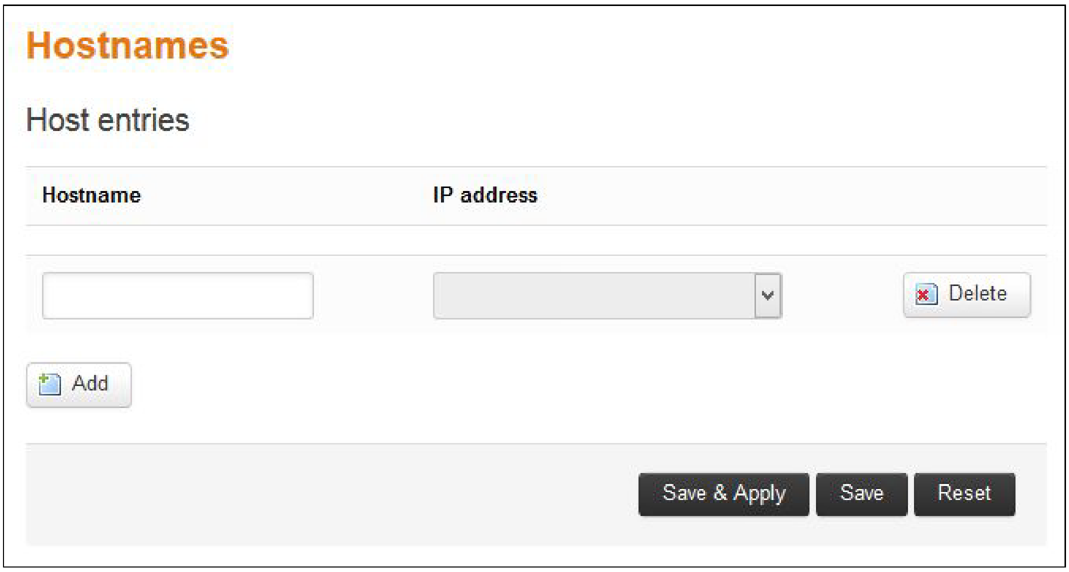
Parameters	Description
Server Settings	
Filter private	Check to deny the reverse lookups for local networks.
Filter useless	Check to deny the requests that cannot be answered by public name servers. By default the request are forwarded.

Localise queries	Check to localize hostname depending on the requesting subnet if multiple IP Addresses are available.
Expand hosts	Check to add local domain suffix to names served from hosts files.
No negative cache	Check to deny caching the negative replies, e.g. for non-existing domains.
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 11.4-4: Advanced Configuration for DHCP and DNS

11.5 Hostnames

Network > Hostnames



Screen 11.5-1: Hostnames Configuration

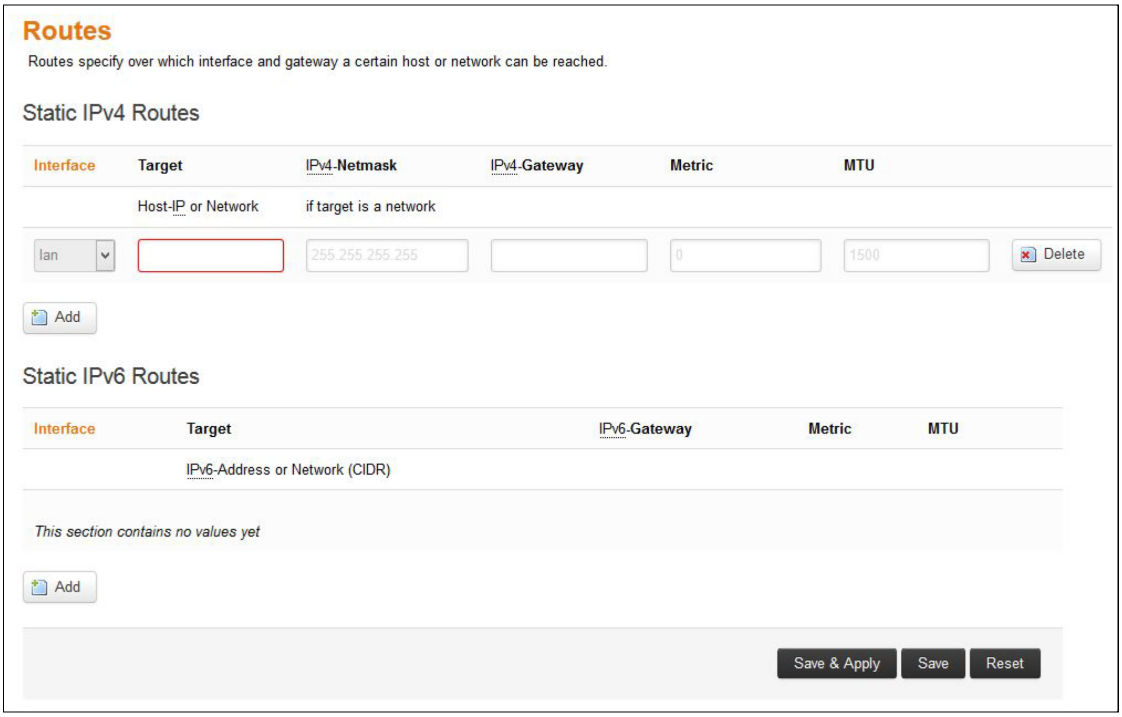
Parameters	Description
Host entries	
Hostname	Enter the Hostname.
IP address	Enter the IP Address of the host.

Table 11.5-1: Hostnames Configuration

11.6 Static Routes

Network > Static Routes

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



Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU	
	Host-IP or Network	if target is a network				
lan		255.255.255.255		0	1500	Delete

Static IPv6 Routes

Interface	Target	IPv6-Gateway	Metric	MTU
	IPv6-Address or Network (CIDR)			

This section contains no values yet

Screen 11.6-1: Static Routes Configuration

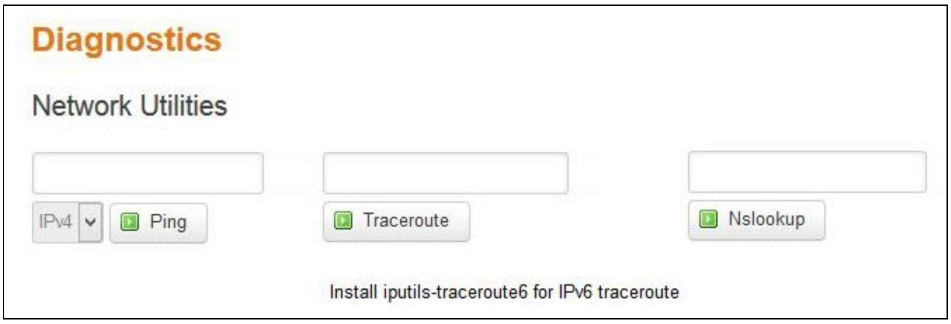
Parameters	Description
Static IPv4 Routes	
Interface	Displays the name of the interface assigned the static IPv4 Address.
Target	Displays the target host IPv4 Address or Network if the target is a network.
IPv4-Netmask	Displays the IPv4 Netmask of the static route.
IPv4-Gateway	Displays the IPv4 Gateway 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 11.6-1: Static Routes Configuration

11.7 Diagnostics

Network > Diagnostics



Diagnostics

Network Utilities

Install iputils-traceroute6 for IPv6 traceroute

Screen 11.7-1: 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 11.7-1: Diagnostics Configuration

11.8 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.

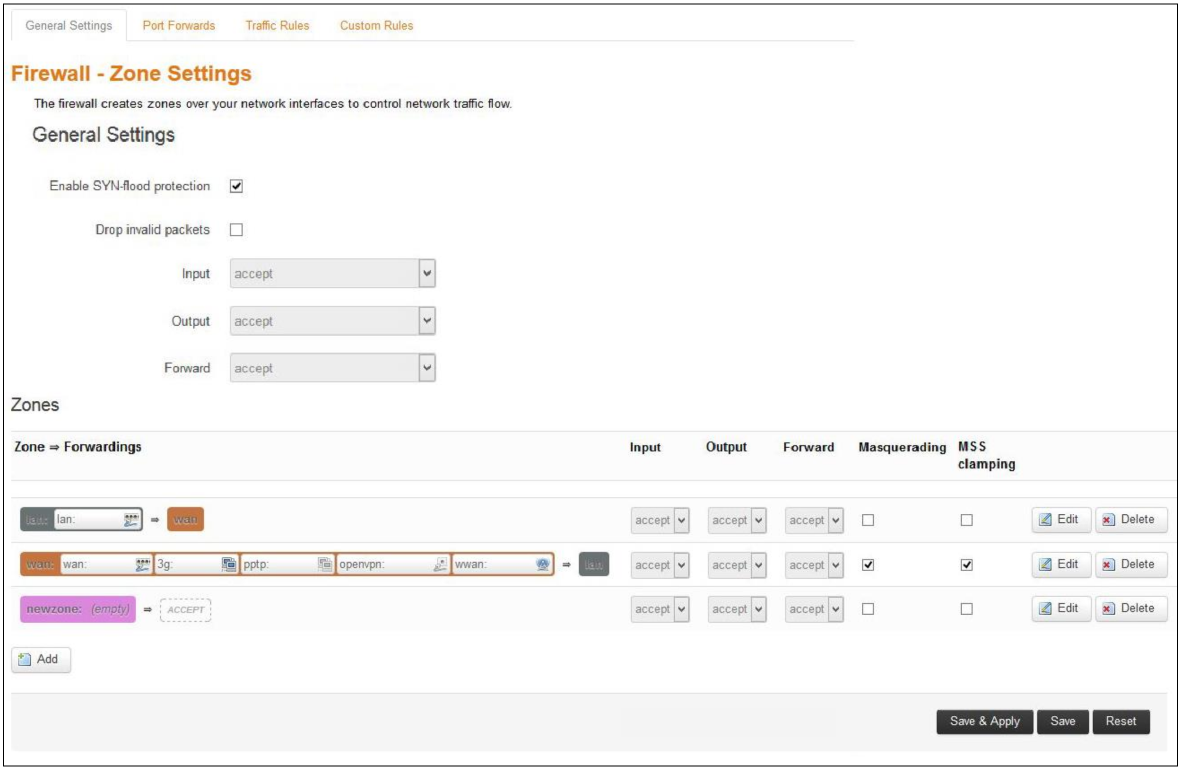
By default, there exist two zones. They are LAN zone and WAN zone as shown in the screenshot below.

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.

11.8.1 General Setting

Network > Firewall > General Settings



Firewall - Zone Settings

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

General Settings

Enable SYN-flood protection ☑

Drop invalid packets ☐

Input: accept

Output: accept

Forward: accept

Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping		
lan: lan: ⇒ wan	accept	accept	accept	☐	☐	Edit	Delete
wan: wan: 3g: pptp: openvpn: wwan: ⇒ lan	accept	accept	accept	☑	☑	Edit	Delete
newzone: (empty) ⇒ ACCEPT	accept	accept	accept	☐	☐	Edit	Delete

Screen 11.8-1: General Configuration for Firewall Zone

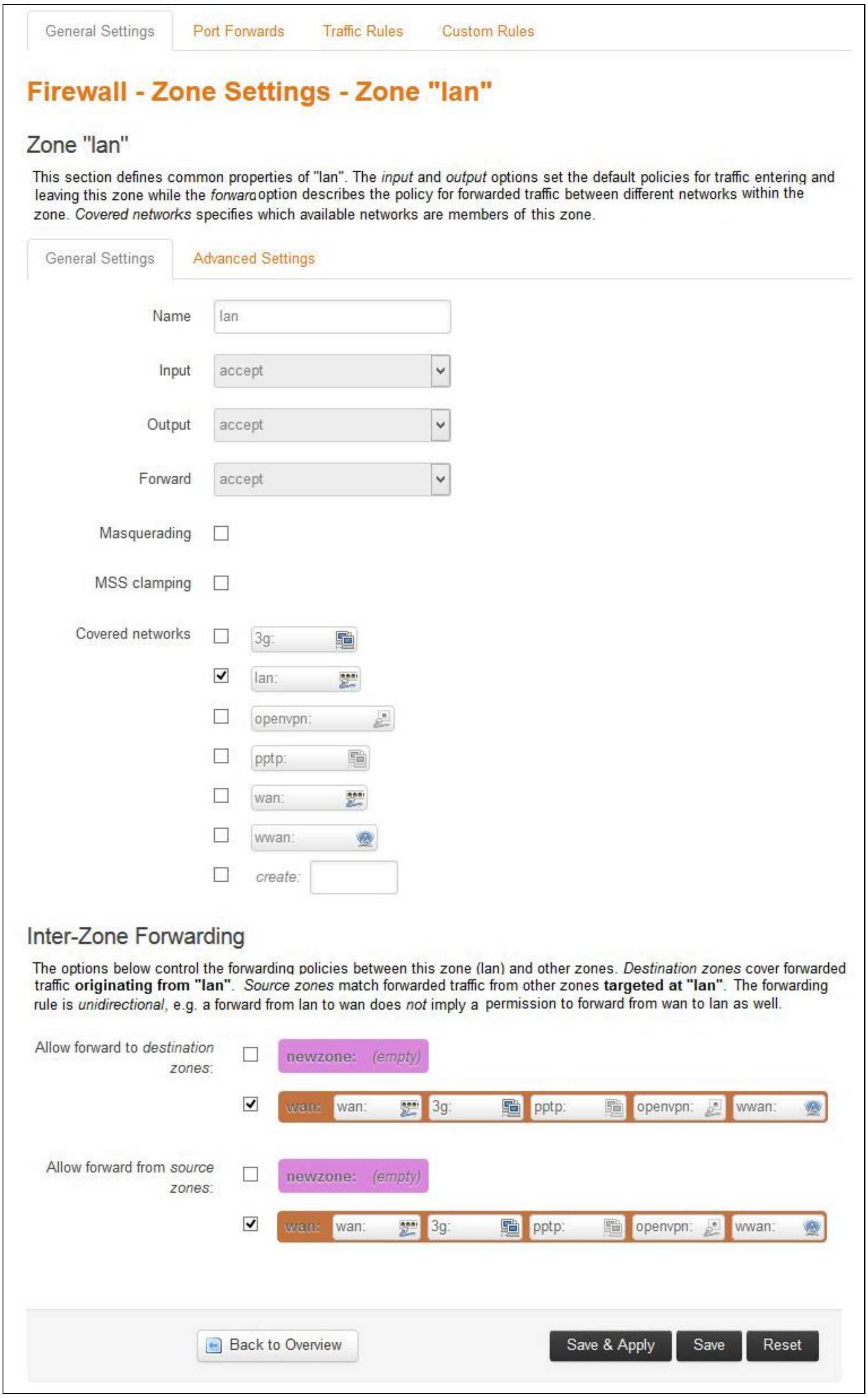
Parameters	Description
General Settings	
Enable SYN-flood protection	Check to enable SYN-flood protection.
Drop invalid packet	Check to drop the invalid packets that are not matching any active connection.

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)	
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 11.8-1: General Configuration for Firewall Zone

A. Add

a. General Settings



Firewall - Zone Settings - Zone "lan"

Zone "lan"

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

Name	lan
Input	accept
Output	accept
Forward	accept
Masquerading	□
MSS clamping	□
Covered networks	□ 3g: ☑ lan: □ openvpn: □ pptp: □ wan: □ wwan: □ *create:*

Inter-Zone Forwarding

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

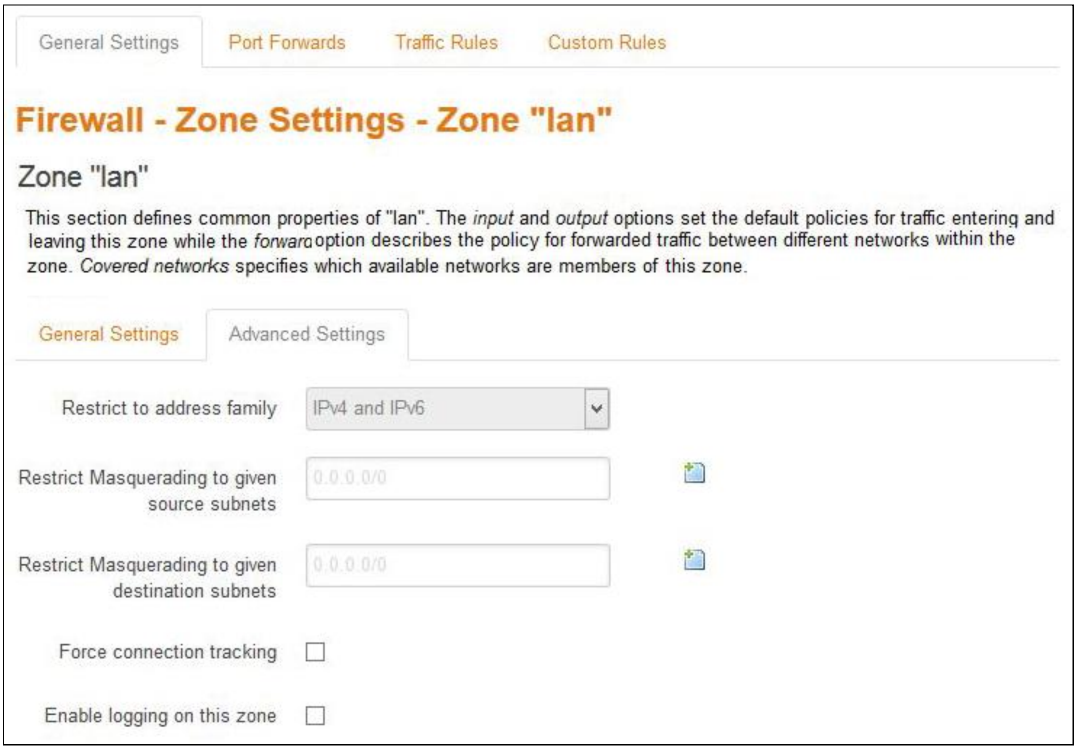
Allow forward to *destination zones*:	□ newzone: *(empty)* ☑ wan: wan: 3g: pptp: openvpn: wwan:
Allow forward from *source zones*:	□ newzone: *(empty)* ☑ wan: wan: 3g: pptp: openvpn: wwan:

Screen 11.8-2: 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 zone.
Output	Select to accept or reject the outbound traffic from all the configured zone.
Forward	Select to accept or reject the forwarded traffic from all the configured zone.
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 11.8-2: General Configuration for Firewall Zone (LAN)

b. Advanced Settings



Firewall - Zone Settings - Zone "lan"

Zone "lan"

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

Restrict to address family: IPv4 and IPv6

Restrict Masquerading to given source subnets: 0.0.0.0/0

Restrict Masquerading to given destination subnets: 0.0.0.0/0

Force connection tracking ☐

Enable logging on this zone ☐

Screen 11.8-3: 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 11.8-3: Advance Configuration for Firewall Zone (LAN)

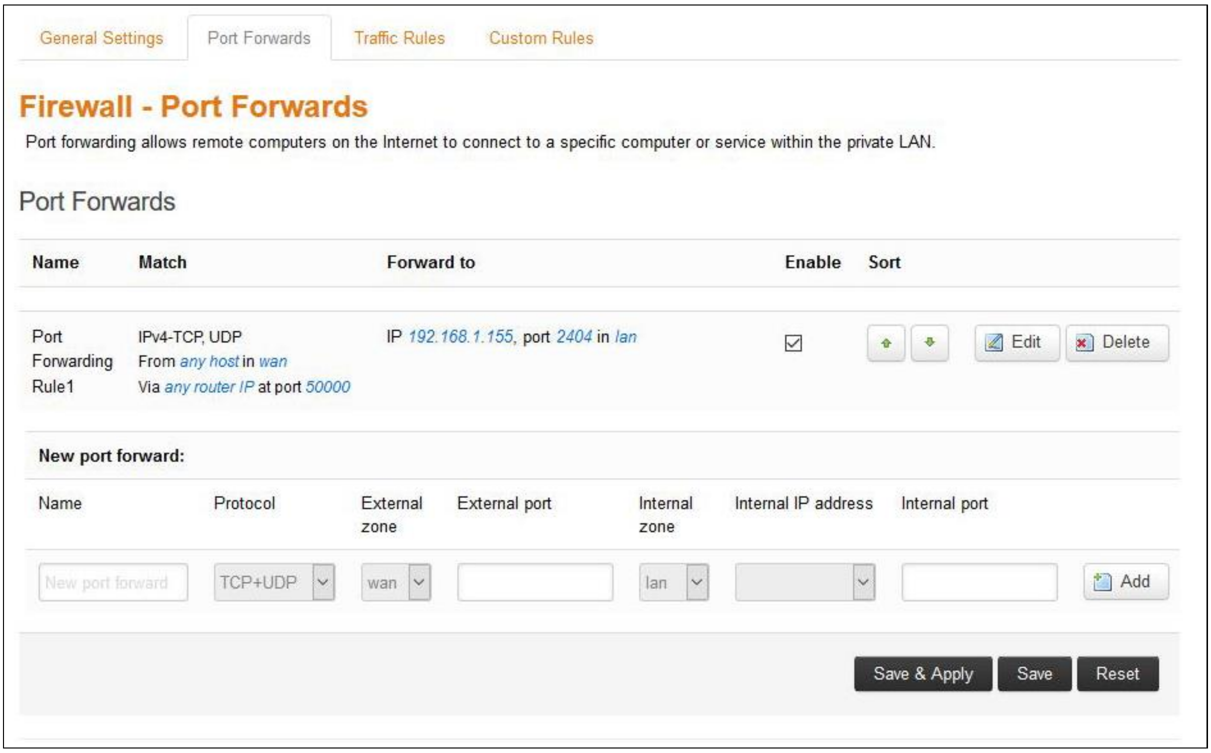
11.8.2 Port Forwarding

Network > Firewall > Port Forwarding

Port forwarding allows public access to services on network devices on the LAN by opening a specific port or port range for a service, such as FTP. Port triggering opens a port range for services such as Internet gaming that uses alternate ports to communicate between the server and the LAN host.

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.



Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Forward to	Enable	Sort
Port Forwarding Rule1	IPv4-TCP, UDP From *any host* in *wan* Via *any router IP* at port *50000*	IP *192.168.1.155*, port *2404* in *lan*	☑	

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port
New port forward	TCP+UDP	wan		lan		

Screen 11.8-4: Port Forwarding Configuration for Firewall Zone

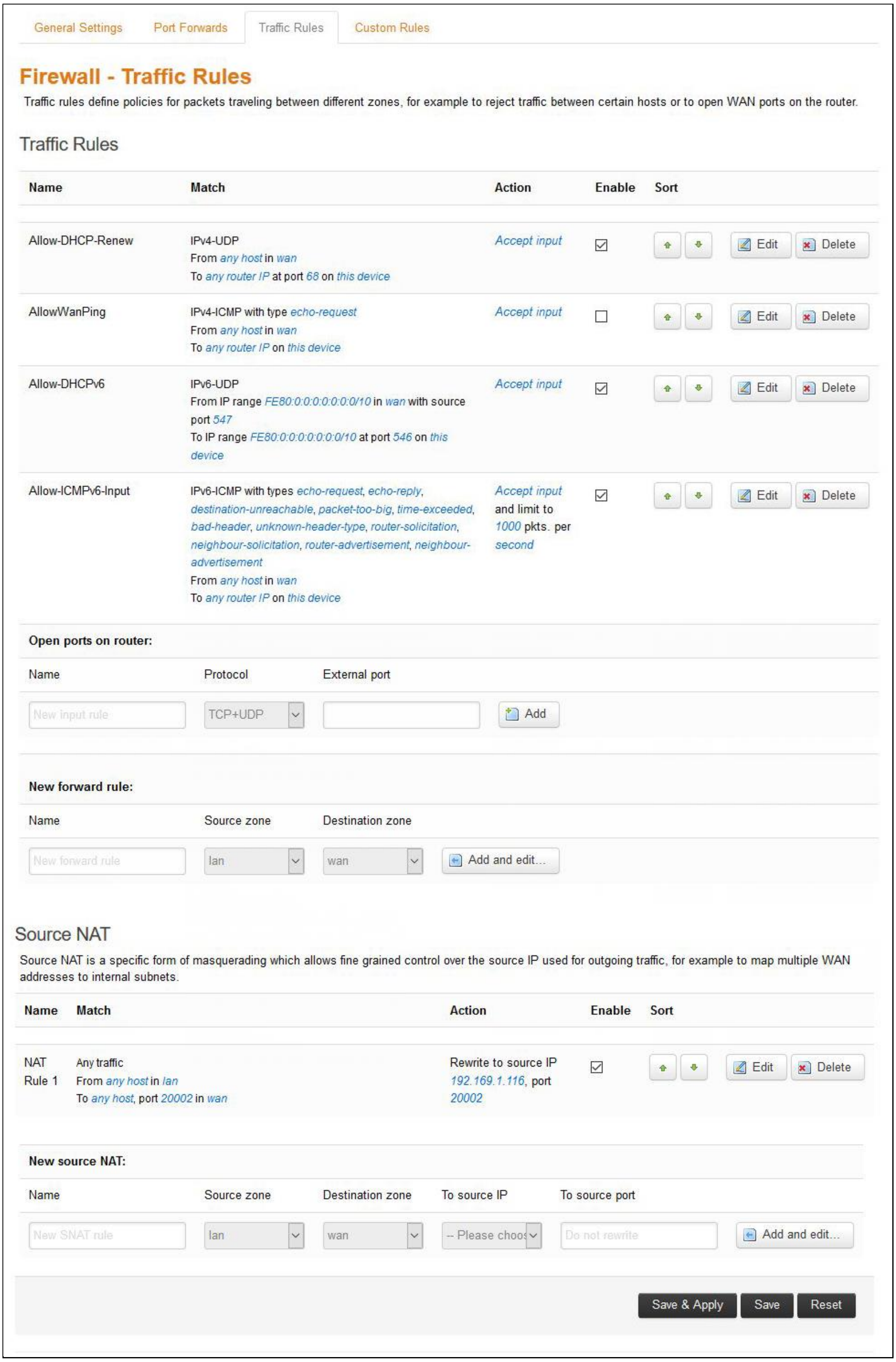
Parameters	Description
Port Forwards	
Name	Displays the name of the Port Forwarding Rule.
Match	Displays the WAN TCP/UDP ports for matching the conditions before forwarding it to LAN device.
Forward to	The destination IP Address to which the traffic must be forwarded.
Enable	Check to enable the Port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

Sort	Click ↑ ↓ to sort the configured Port Forwarding Rule.

Table 11.8-4: Port Forwarding Configuration for Firewall Zone

11.8.3 Traffic Rules

Network > Firewall > Traffic Rules



Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Traffic Rules

Name	Match	Action	Enable	Sort		
Allow-DHCP-Renew	IPv4-UDP From *any host* in *wan* To *any router IP* at port *68* on *this device*	*Accept input*	☑	↑ ↓	Edit	Delete
AllowWanPing	IPv4-ICMP with type *echo-request* From *any host* in *wan* To *any router IP* on *this device*	*Accept input*	☐	↑ ↓	Edit	Delete
Allow-DHCPv6	IPv6-UDP From IP range *FE80:0:0:0:0:0:0:0/10* in *wan* with source port *547* To IP range *FE80:0:0:0:0:0:0:0/10* at port *546* on *this device*	*Accept input*	☑	↑ ↓	Edit	Delete
Allow-ICMPv6-Input	IPv6-ICMP with types *echo-request*, *echo-reply*, *destination-unreachable*, *packet-too-big*, *time-exceeded*, *bad-header*, *unknown-header-type*, *router-solicitation*, *neighbour-solicitation*, *router-advertisement*, *neighbour-advertisement* From *any host* in *wan* To *any router IP* on *this device*	*Accept input* and limit to *1000* pkts. per *second*	☑	↑ ↓	Edit	Delete

Open ports on router:

Name	Protocol	External port	
New input rule	TCP+UDP		Add

New forward rule:

Name	Source zone	Destination zone	
New forward rule	lan	wan	Add and edit...

Source NAT

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used for outgoing traffic, for example to map multiple WAN addresses to internal subnets.

Name	Match	Action	Enable	Sort		
NAT Rule 1	Any traffic From *any host* in *lan* To *any host*, port *20002* in *wan*	Rewrite to source IP *192.169.1.116*, port *20002*	☑	↑ ↓	Edit	Delete

New source NAT:

Name	Source zone	Destination zone	To source IP	To source port	
New SNAT rule	lan	wan	-- Please choos	Do not rewrite	Add and edit...

Screen 11.8-5: Traffic Rule Overview for Firewall Zone

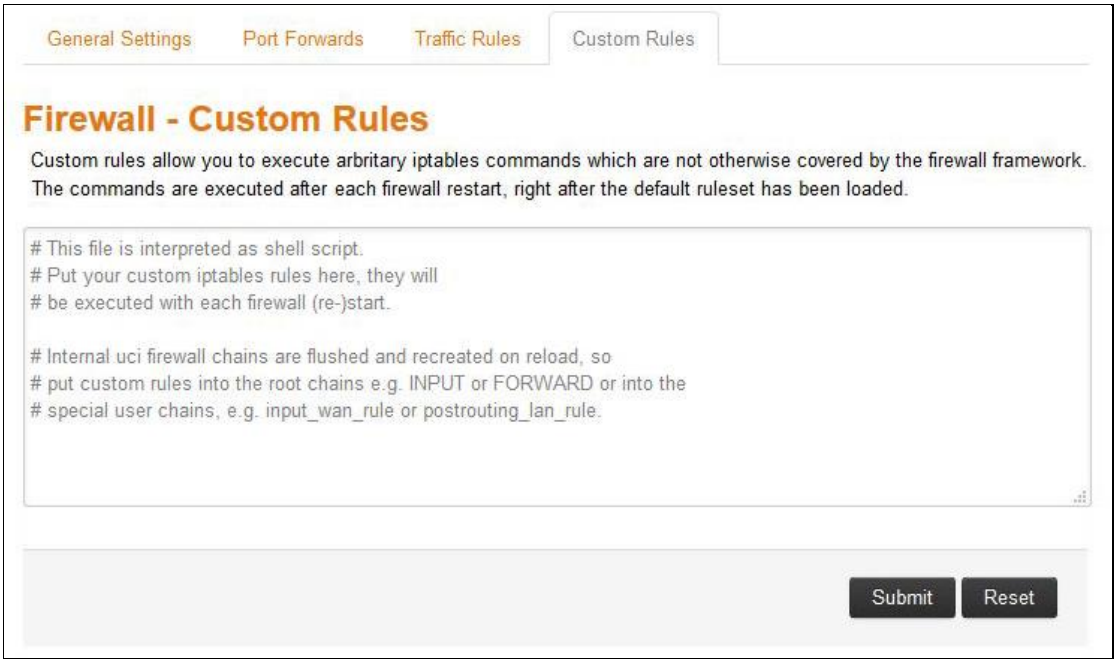
Parameters	Description
Traffic Rules **These rules define policies for traffic communication between the different zones, primarily used for traffic shaping.**	
Name	Displays the name of the Traffic Rule.
Match	Displays the details of the Traffic Rule configuration and the conditions in which the rule 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. ***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 11.8-5: Traffic Rule Overview for Firewall Zone

11.8.4 Custom Rules

Network > Firewall > Custom Rules



Firewall - Custom Rules

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

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

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

Screen 11.8-6: Custom Rules Configuration for Firewall Zone

You can configure customized rules for Firewall using shell script.

12.Services

E200 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:

- Dynamic DNS
- Agents
- SMS
- DOTA
- GPS
- Events
- OpenVPN

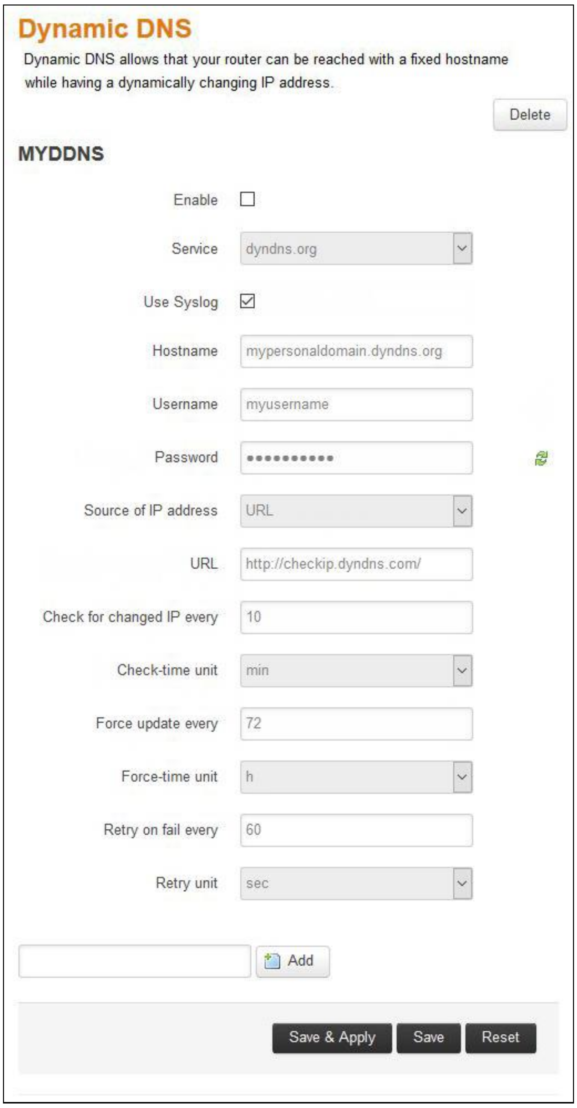
12.1 Dynamic DNS

Services > Dynamic DNS

Dynamic DNS (Domain Name System) is a method of keeping a static domain/host name linked to a dynamically assigned 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 routr server by the domain name, not the dynamic IP address. DDNS will tie a domain name (e.g. mymaestro.com, or maestro.wireless.com) to your dynamic IP address.

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



Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

Delete

MYDDNS

Enable □

Service: dyndns.org

Use Syslog ☑

Hostname: mypersonaldomain.dyndns.org

Username: myusername

Password: ••••••••••

Source of IP address: URL

URL: http://checkip.dyndns.com/

Check for changed IP every: 10

Check-time unit: min

Force update every: 72

Force-time unit: h

Retry on fail every: 60

Retry unit: sec

Screen 12.1-1: Dynamic DNS Configurations

Parameters	Description

MYDDNS	
Enable	Dynamic DNS allows the router to be reached with a fixed hostname 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 for example, maestro.com. 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. 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.

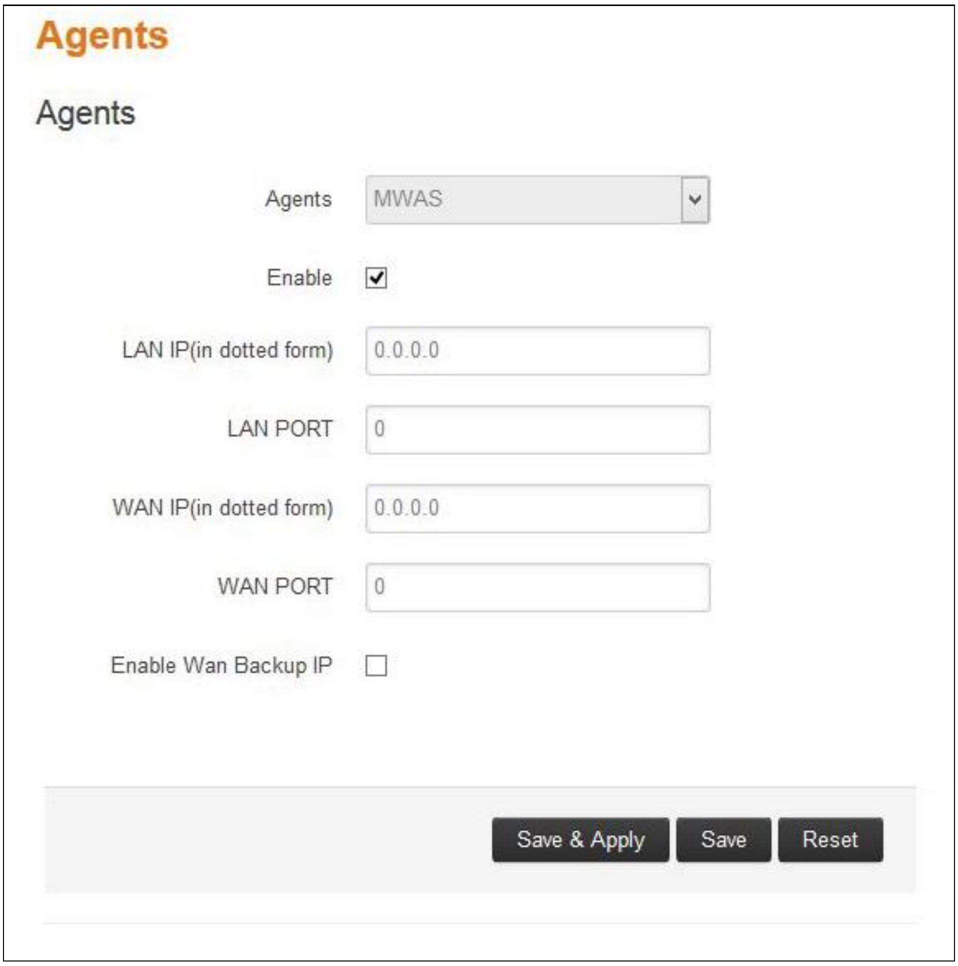
Table 12.1-1: Dynamic DNS Configurations

12.2 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, Maestro 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.



Agents

Agents

Agents: MWAS

Enable: ☑

LAN IP(in dotted form): 0.0.0.0

LAN PORT: 0

WAN IP(in dotted form): 0.0.0.0

WAN PORT: 0

Enable Wan Backup IP: □

Screen 12.2-1: Agent Configurations

Parameters	Description
Agents	
Agents	Select the Agent from the dropdown list: - MWAS – Maestro 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.

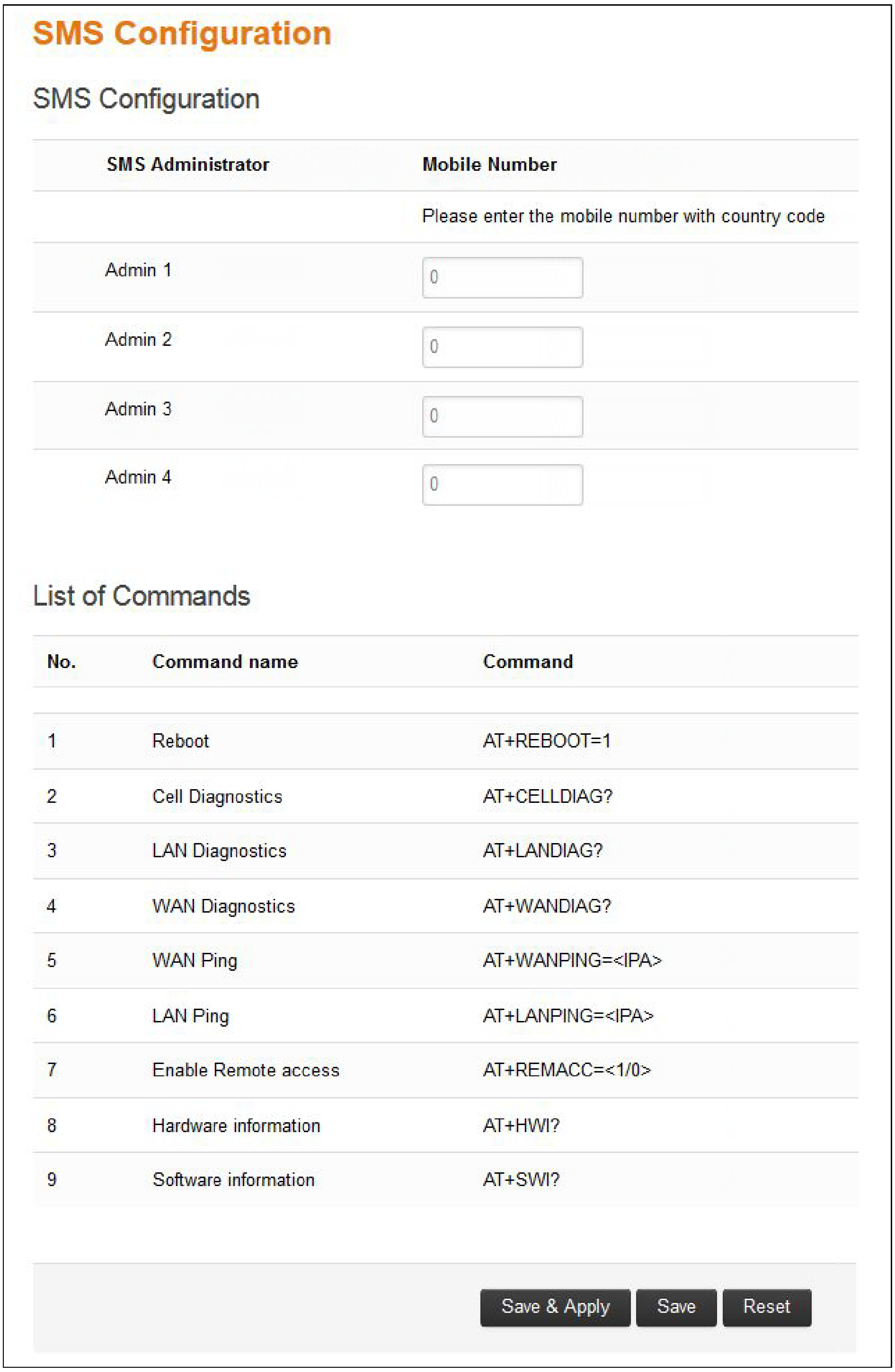
Table 12.2-1: Agent Configurations

12.3 SMS

Services > SMS

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>



SMS Configuration

SMS Configuration

SMS Administrator	Mobile Number
	Please enter the mobile number with country code
Admin 1	0
Admin 2	0
Admin 3	0
Admin 4	0

List of Commands

No.	Command name	Command
1	Reboot	AT+REBOOT=1
2	Cell Diagnostics	AT+CELLDIAG?
3	LAN Diagnostics	AT+LANDIAG?
4	WAN Diagnostics	AT+WANDIAG?
5	WAN Ping	AT+WANPING=<IPA>
6	LAN Ping	AT+LANPING=<IPA>
7	Enable Remote access	AT+REMACC=<1/0>
8	Hardware information	AT+HWI?
9	Software information	AT+SWI?

Screen 12.3-1: SMS Service Configurations

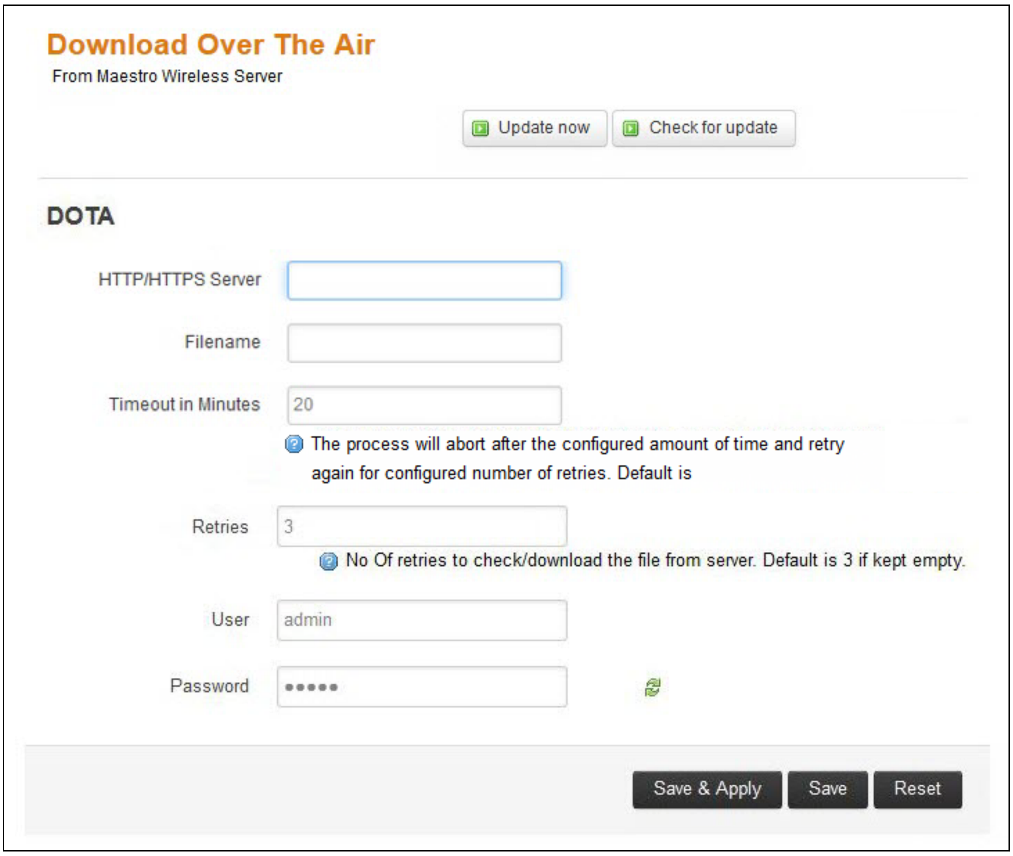
Parameters	Description
SMS Configuration	
SMS Administrator	Displays the number of Administrators configured to receive the diagnostics information of the router after they send the command using SMS. Maximum 4 SMS Administrator can be configured. ***Note*** - ***If no number is configured than the router will accept SMS from any number.***
Mobile Number	Enter the mobile number. The format of mobile number must be: - <countrycode><phonenumber>
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 12.3-1: SMS Service Configurations

12.4 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.



Download Over The Air

From Maestro Wireless Server

DOTA

HTTP/HTTPS Server:

Filename:

Timeout in Minutes: 20

The process will abort after the configured amount of time and retry again for configured number of retries. Default is

Retries: 3

No Of retries to check/download the file from server. Default is 3 if kept empty.

User admin

Password: •••••

Screen 12.4-1: 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 a configured custom server or from Maestro Wireless server.
Check for update	Click to check for available updates from Maestro server.
DOTA	
HTTP/HTTPS Server	Enter the name of the HTTP/HTTPS server to be accessed for updates. ***Note*** • ***If this field is left blank, the Router by***

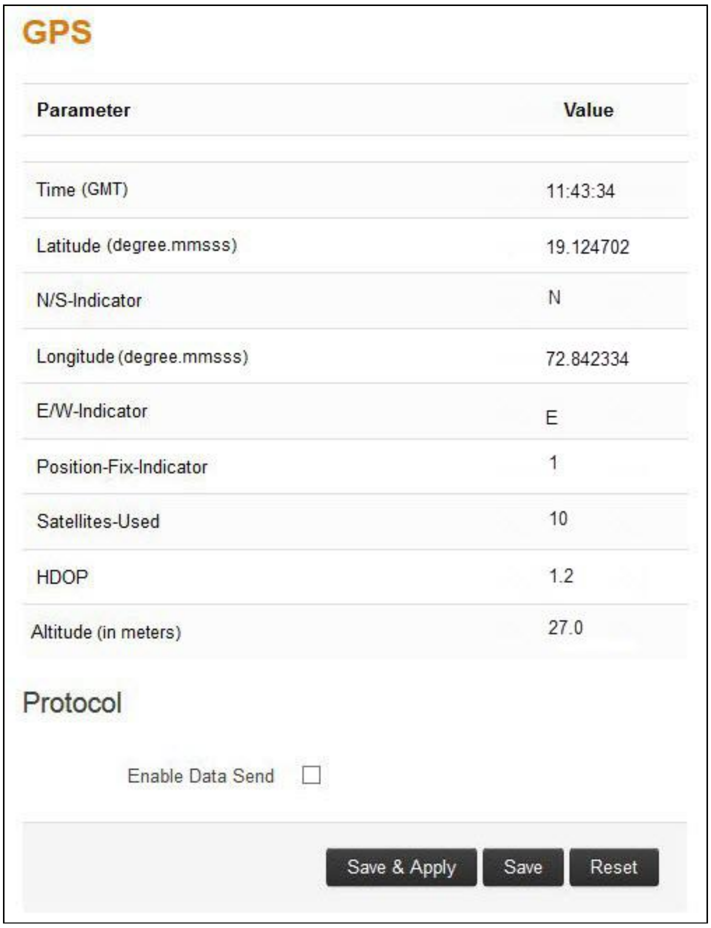
	default will use Maestro Wireless Sever for firmware updates.
Filename	Enter the name of the File to be accessed for updates.
Timeout in Minutes	Enter the time in minutes expected to download the latest firmware file. The download process will automatically get aborted after the configured time. The default Expected time is 20 minutes.
Retries	Enter the number of retries to check and download the latest firmware file from the server. The default number of retries is 3.
User	Enter the Username.
Password	Enter the Password.

Table 12.4-1: DOTA Service Configuration

12.5 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.



GPS

Parameter	Value
Time (GMT)	11:43:34
Latitude (degree.mmsss)	19.124702
N/S-Indicator	N
Longitude (degree.mmsss)	72.842334
E/W-Indicator	E
Position-Fix-Indicator	1
Satellites-Used	10
HDOP	1.2
Altitude (in meters)	27.0

Protocol

Enable Data Send ☐

Screen 12.5-1: 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. 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 12.5-1: 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

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 12.5-2: 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 12.5-3: 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 12.5-4: 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 12.5-5: 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 12.5-6: GSA Data Format

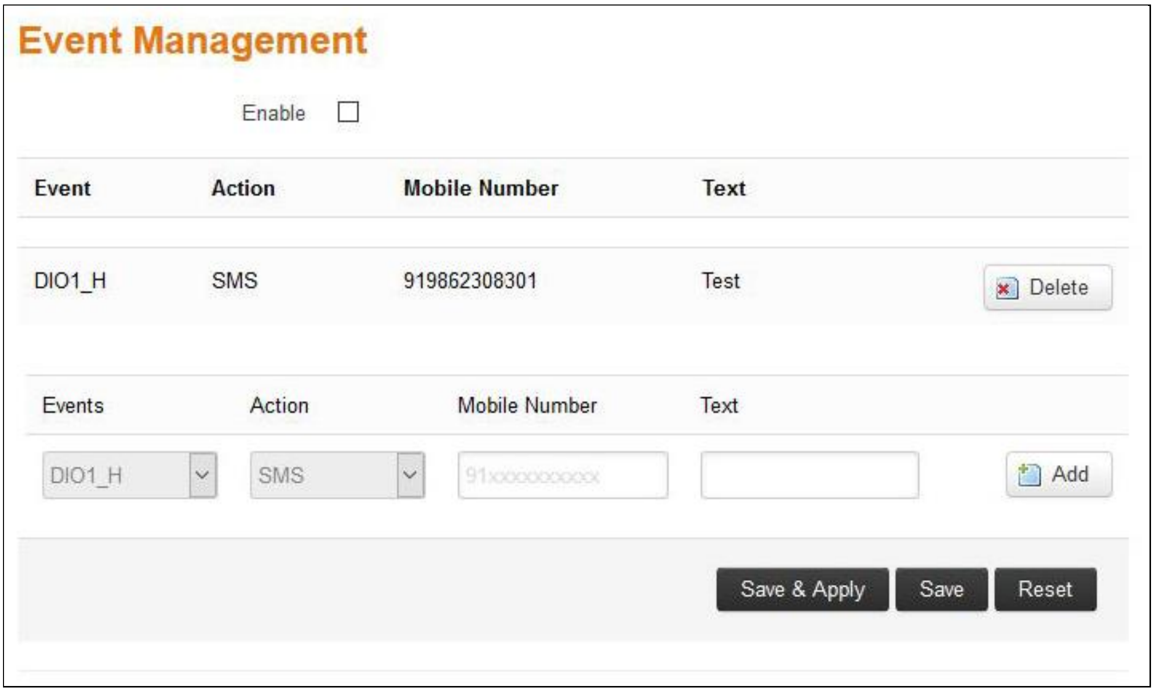
[1] Satellite used in solution.

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

12.6 Events

Services > Events

E200 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.



Event Management

Enable □

Event	Action	Mobile Number	Text	
DIO1_H	SMS	919862308301	Test	Delete

Events	Action	Mobile Number	Text	
DIO1_H	SMS	91xxxxxxxxxx		Add

Screen 12.6-1: Event Service Configuration

Parameters	Description
EVENT	
Enable	Click to enable the events
Event	Select the event from the available options DIO_H - A high to low voltage transition DIO_L – A low to high voltage transition NA DIO is by default set to a low level that means the high voltage level, pulled up. ***Note*** • ***Only one DIO (Digital input) is available.*** • ***This input pin is accessible on 4 pin Micro-fit Molex power connector. The input pin is located below the V+ pin.***

Action	Select the action from options. • SMS – to send the event details using the SMS. • 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 12.6-1: Event Service Configuration

12.7 OpenVPN

Services > 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.

E200 series supports Open VPN client, Server and Pass Through.

a. Open VPN Client

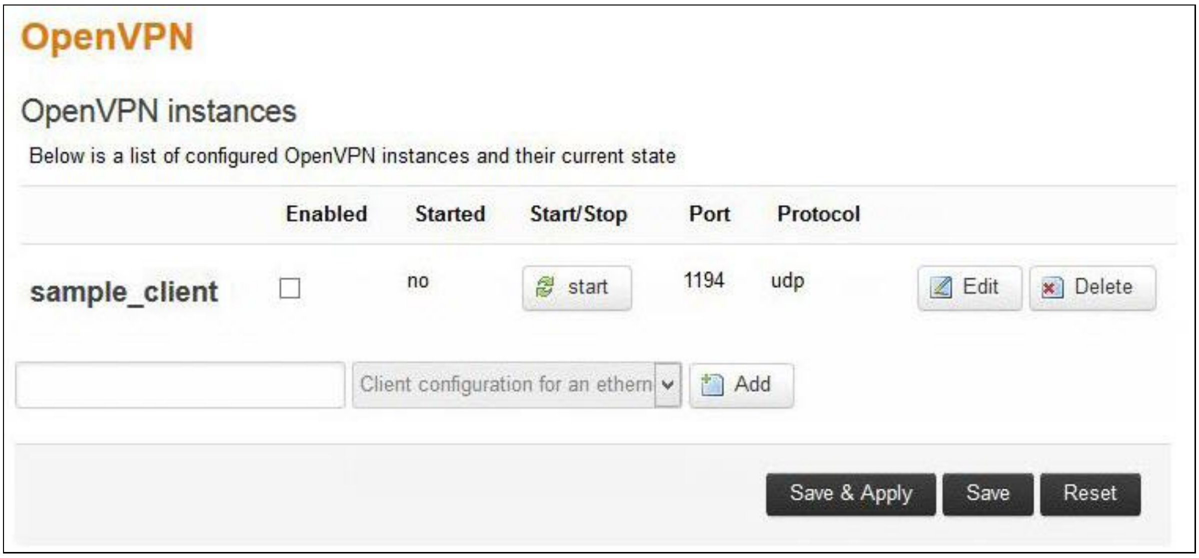
You can access the Open VPN client in Services / Open VPN.

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.***



OpenVPN

OpenVPN instances

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

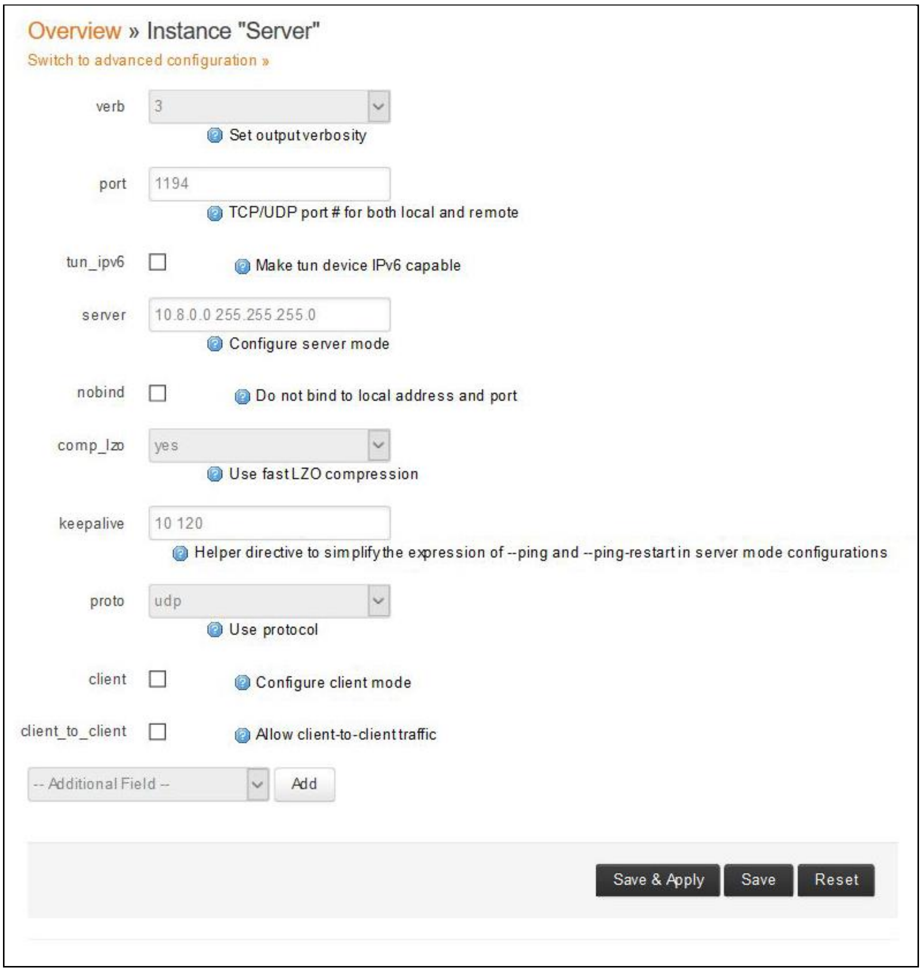
	Enabled	Started	Start/Stop	Port	Protocol		
sample_client	□	no	start	1194	udp	Edit	Delete

Screen 12.7-1: OpenVPN Service Configuration

Parameters	Description
OpenVPN instances	
Enabled	Click Enabled to allow restarting of OpenVPN in case the router is rebooted.
Started	Displays the status of OpenVPN instance, whether the instance is running or not. If the status is running, Yes is displayed along with Process ID (PID), else No.
Start/Stop	Click to start or stop the OpenVPN instance.
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 12.7-1: OpenVPN Service Configuration

b. Edit



Overview » Instance "Server"

Switch to advanced configuration »

verb: 3 — Set output verbosity

port: 1194 — TCP/UDP port # for both local and remote

tun_ipv6: □ — Make tun device IPv6 capable

server: 10.8.0.0 255.255.255.0 — Configure server mode

nobind: □ — Do not bind to local address and port

comp_lzo: yes — Use fast LZO compression

keepalive: 10 120 — Helper directive to simplify the expression of --ping and --ping-restart in server mode configurations

proto: udp — Use protocol

client: □ — Configure client mode

client_to_client: □ — Allow client-to-client traffic

Screen 12.7-2: 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 Maestro E205 2.0.0 and Maestro E206 2.0.0***
client_to_client	Check to facilitate communication between the Clients connected over the same VPN.

Table 12.7-2: OpenVPN Service Configuration

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 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 12.7-1: List of Acronyms

14.Table of Figure/Screen

15.Tables Details