PEPWAVE
Broadband Possibilities

Pepwave MAX and Surf User Manual

Pepwave Products:
MAX 700/HD2/HD2 IP67/HD2 mini/HD4/Transit/Hotspot/BR1/BR1 MK2/ BR1 Mini/BR1 Slim/BR1 ENT/BR1 Pro LTE/BR1 IP55/BR2 IP55/On-The-Go/MAX HD2/HD4 with MediaFast/Device Connector/ Surf SOHO

Pepwave Firmware 6.3
September 2017

COPYRIGHT & TRADEMARKS
Specifications are subject to change without notice. Copyright © 2017 Pepwave Ltd. All Rights Reserved. Pepwave and the Pepwave logo are trademarks of Pepwave Ltd. Other brands or products mentioned may be trademarks or registered trademarks of their respective owners.

Table of Contents

1 INTRODUCTION AND SCOPE 6

2 GLOSSARY 7

3 PRODUCT FEATURES 8

3.1 SUPPORTED NETWORK FEATURES 8
3.2 OTHER SUPPORTED FEATURES 10

4 PEPWAVE MAX MOBILE ROUTER OVERVIEW 11

4.1 MAX 700 11
4.2 MAX HD2 13
4.3 MAX HD2 IP67 15
4.4 MAX HD2 MINI 16
4.5 MAX TRANSIT 18
4.6 MAX HOTSPOT 19
4.7 MAX HD4 20
4.8 MAX BR1 (MK2) 22
4.9 MAX BR1 MINI 24
4.10 MAX BR1 SLIM 26
4.11 MAX BR1 ENT 28
4.12 MAX BR1 PRO LTE 29
4.13 MAX BR1/2 IP55 30
4.14 MAX ON-THE-GO 32
4.15 SURF SOHO 33

5 ADVANCED FEATURE SUMMARY 34

5.1 DROP-IN MODE AND LAN BYPASS: TRANSPARENT DEPLOYMENT 34
5.2 QOS: CLEARER VOIP 34
5.3 PER-USER BANDWIDTH CONTROL 35
5.4 HIGH AVAILABILITY VIA VRRP 35
5.5 USB MODEM AND ANDROID TETHERING 36
5.6 BUILT-IN REMOTE USER VPN SUPPORT 36
5.7 SIM-CARD USSD SUPPORT 37

6 INSTALLATION 38

6.1 PREPARATION 38
6.2 CONSTRUCTING THE NETWORK 39
6.3 CONFIGURING THE NETWORK ENVIRONMENT 40

7 MOUNTING THE UNIT 41

7.1 WALL MOUNT 41
7.2 CAR MOUNT 41

 Copyright @ 2017 Pepwave

7.3 IP67 Installation Guide 41

8 CONNECTING TO THE WEB ADMIN INTERFACE 42

9 CONFIGURING THE LAN INTERFACE(S) 44

9.1 Basic Settings 44
9.2 Captive Portal 54

10 CONFIGURING THE WAN INTERFACE(S) 56

10.1 Ethernet WAN 57
10.2 Cellular WAN 65
10.3 Wi-Fi WAN 70
10.4 WAN Health Check 76
10.5 Dynamic DNS Settings 78

11 ADVANCED WI-FI SETTINGS 81

12 MEDIAFAST CONFIGURATION 84

12.1 Setting Up MediaFast Content Caching 84
12.2 Scheduling Content Prefetching 85
12.3 Viewing MediaFast Statistics 86

13 BANDWIDTH BONDING SPEEDFUSION™ / PEPVPN 88

13.1 PepVPN 89
13.2 The Pepwave Router Behind a NAT Router 95
13.3 SpeedFusion™ Status 96

14 IPSEC VPN 97

14.1 IPsec VPN Settings 97

15 OUTBOUND POLICY MANAGEMENT 101

15.1 Outbound Policy 101
15.2 Custom Rules for Outbound Policy 102

16 INBOUND ACCESS 111

16.1 Port Forwarding Service 111

17 NAT MAPPINGS 114

18 QOS 116

18.1 User Groups 116
18.2 Bandwidth Control 117
18.3 Application 117

19 FIREWALL 119

19.1 Outbound and Inbound Firewall Rules 119
19.2 Content Blocking 124

 Copyright @ 2017 Pepwave

19.3 OSPF & RIPv2 125
19.4 REMOTE USER ACCESS 127

MISCELLANEOUS SETTINGS 129

19.5 HIGH AVAILABILITY 129
19.6 PPTP SERVER 132
19.7 CERTIFICATE MANAGER 133
19.8 SERVICE FORWARDING 133
19.9 SERVICE PASSTHROUGH 136
19.10 GPS FORWARDING 137

20 AP CONTROLLER 138

20.1 WIRELESS SSID 138
20.2 SETTINGS 142
20.3 TOOLBOX 146

21 SYSTEM SETTINGS 147

21.1 ADMIN SECURITY 147
21.2 FIRMWARE 152
21.3 TIME 153
21.4 SCHEDULE 153
21.5 EMAIL NOTIFICATION 154
21.6 EVENT LOG 156
21.7 SNMP 158
21.8 INCONTROL 160
21.9 CONFIGURATION 160
21.10 FEATURE ADD-ONS 162
21.11 REBOOT 162
21.12 PING 163
21.13 TRACEROUTE TEST 164
21.14 PEPVPN TEST 164
21.15 WAKE-ON-LAN 165
21.16 CLI (COMMAND LINE INTERFACE SUPPORT) 165

22 STATUS 166

22.1 DEVICE 166
22.2 ACTIVE SESSIONS 168
22.3 CLIENT LIST 170
22.4 WINS CLIENT 170
22.5 UPNP / NAT-PMP 171
22.6 SPEEDFUSION STATUS 171
22.7 EVENT LOG 175
22.8 BANDWIDTH 175

APPENDIX A. RESTORATION OF FACTORY DEFAULTS 181

APPENDIX B: DECLARATION.....182

1 Introduction and Scope

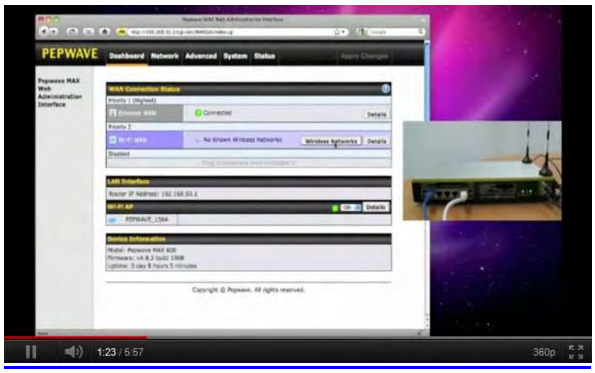
Pepwave routers provide link aggregation and load balancing across multiple WAN connections, allowing a combination of technologies like 3G HSDPA, EVDO, 4G LTE, Wi-Fi, external WiMAX dongle, and satellite to be utilized to connect to the Internet.

The MAX wireless SD-WAN router series has a wide range of products suitable for many different deployments and markets. Entry level SD-WAN models such as the MAX BR1 are suitable for SMEs or branch offices. High-capacity SD-WAN routers such as the MAX HD2 are suitable for larger organizations and head offices.

This manual covers setting up Pepwave routers and provides an introduction to their features and usage.

Tips

Want to know more about Pepwave routers? Visit our YouTube Channel for a video introduction!



http://youtu.be/UCkVQThLKO4

 Copyright @ 2017 Pepwave

2 Glossary

The following terms, acronyms, and abbreviations are frequently used in this manual:

Term	Definition
3G	3rd Generation standards for wireless communications
4G	4th Generation standards for wireless communications
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EVDO	Evolution-Data Optimized
HSDPA	High-Speed Downlink Packet Access
HTTP	Hyper-Text Transfer Protocol
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LAN	Local Area Network
MAC Address	Media Access Control Address
MTU	Maximum Transmission Unit
MSS	Maximum Segment Size
NAT	Network Address Translation
PPPoE	Point to Point Protocol over Ethernet
QoS	Quality of Service
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WINS	Windows Internet Name Service
WLAN	Wireless Local Area Network

 Copyright @ 2017 Pepwave

3 Product Features

Pepwave routers enable all LAN users to share broadband Internet connections, and they provide advanced features to enhance Internet access. Our Max BR wireless routers support multiple SIM cards. They can be configured to switch from using one SIM card to another SIM card according to different criteria, including wireless network reliability and data usage.

Our MAX HD series wireless routers are embedded with multiple 4G LTE modems, and allow simultaneous wireless Internet connections through multiple wireless networks. The wireless Internet connections can be bonded together using our SpeedFusion technology. This allows better reliability, larger bandwidth, and increased wireless coverage are comparing to use only one 4G LTE modem.

Below is a list of supported features on Pepwave routers. Features vary by model. For more information, please see peplink.com/products.

3.1 Supported Network Features

3.1.1 WAN

- Ethernet WAN connection in full/half duplex
- Static IP support for PPPoE
- Built-in HSPA and EVDO cellular modems
- USB mobile connection(s)
- Wi-Fi WAN connection
- Network address translation (NAT)/port address translation (PAT)
- Inbound and outbound NAT mapping
- IPsec NAT-T and PPTP packet passthrough
- MAC address clone and passthrough
- Customizable MTU and MSS values
- WAN connection health check
- Dynamic DNS (supported service providers: changeip.com, dyndns.org, no-ip.org, tzo.com and DNS-O-Matic)
- Ping, DNS lookup, and HTTP-based health check

3.1.2 LAN

- Wi-Fi AP
- Ethernet LAN ports
- DHCP server on LAN
- Extended DHCP option support
- Static routing rules
- VLAN on LAN support

 Copyright @ 2017 Pepwave

3.1.3 VPN

- PepVPN with SpeedFusion™
- PepVPN performance analyzer
- X.509 certificate support
- VPN load balancing and failover among selected WAN connections
- Bandwidth bonding and failover among selected WAN connections
- IPsec VPN for network-to-network connections (works with Cisco and Juniper only)
- Ability to route Internet traffic to a remote VPN peer
- Optional pre-shared key setting
- SpeedFusion™ throughput, ping, and traceroute tests
- PPTP server
- PPTP and IPsec passthrough

3.1.4 Firewall

- Outbound (LAN to WAN) firewall rules
- Inbound (WAN to LAN) firewall rules per WAN connection
- Intrusion detection and prevention
- Specification of NAT mappings
- Outbound firewall rules can be defined by destination domain name

3.1.5 Captive Portal

- Splash screen of open networks, login page for secure networks
- Customizable built-in captive portal
- Supports linking to outside page for captive portal

3.1.6 Outbound Policy

- Link load distribution per TCP/UDP service
- Persistent routing for specified source and/or destination IP addresses per TCP/UDP service
- Traffic prioritization and DSL optimization
- Prioritize and route traffic to VPN tunnels with Priority and Enforced algorithms

3.1.7 AP Controller

- Configure and manage Pepwave AP devices

 Copyright @ 2017 Pepwave

- Review the status of connected APs

3.1.8 QoS

- Quality of service for different applications and custom protocols
- User group classification for different service levels
- Bandwidth usage control and monitoring on group- and user-level
- Application prioritization for custom protocols and DSL/cable optimization

3.2 Other Supported Features

- User-friendly web-based administration interface
- HTTP and HTTPS support for web admin interface
- Configurable web administration port and administrator password
- Firmware upgrades, configuration backups, ping, and traceroute via web admin interface
- Remote web-based configuration (via WAN and LAN interfaces)
- Time server synchronization
- SNMP
- Email notification
- Read-only user for web admin
- Shared IP drop-in mode
- Authentication and accounting by RADIUS server for web admin
- Built-in WINS servers*
- Syslog
- SIP passthrough
- PPTP packet passthrough
- Event log
- Active sessions
- Client list
- WINS client list *
- UPnP / NAT-PMP
- Real-time, hourly, daily, and monthly bandwidth usage reports and charts
- IPv6 support
- Support USB tethering on Android 2.2+ phones

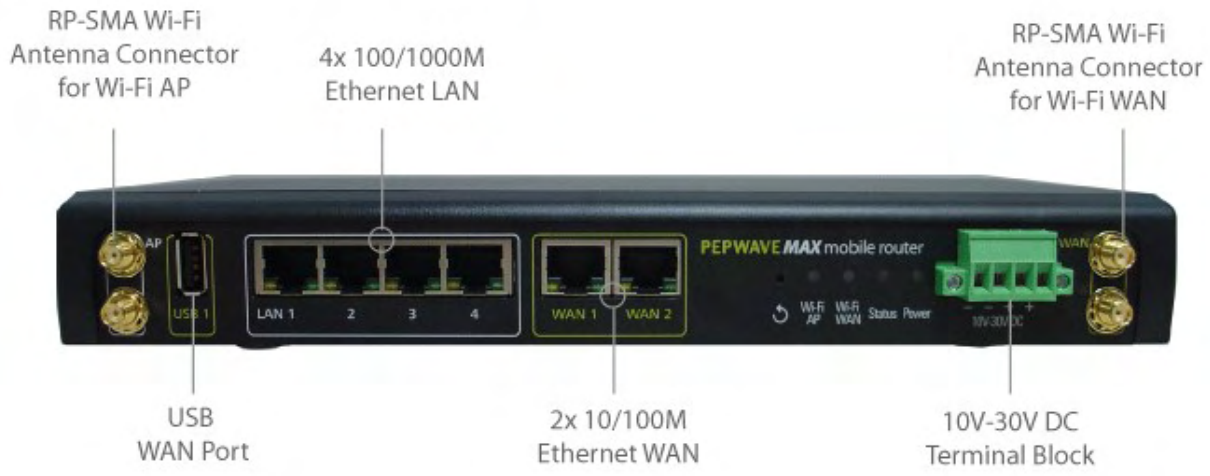
* Not supported on MAX Surf-On-The-Go, Surf SOHO, and BR1 variants

 Copyright @ 2017 Pepwave

4 Pepwave MAX Mobile Router Overview

4.1 MAX 700

4.1.1 Panel Appearance



4.1.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

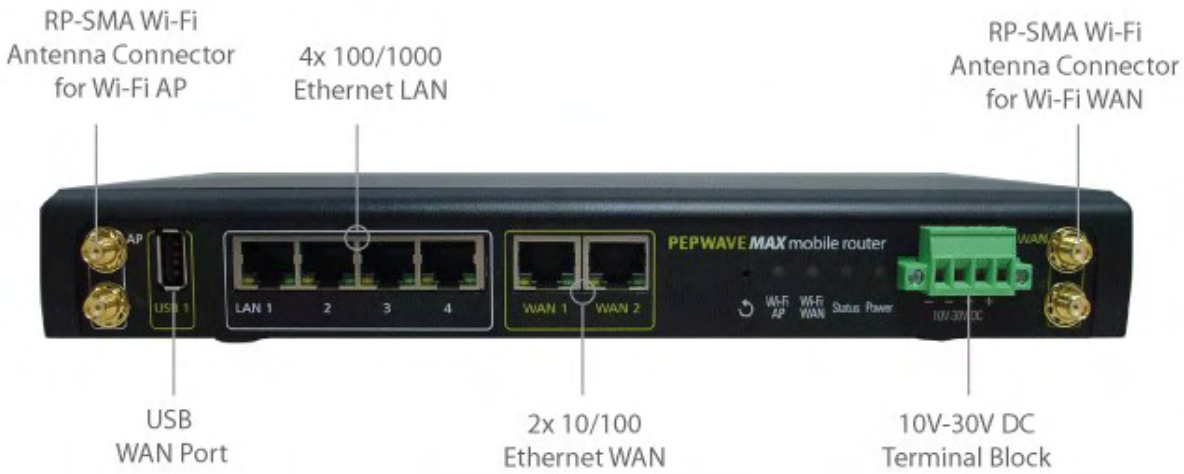
Wi-Fi AP and Wi-Fi WAN Indicators		
Wi-Fi WAN	OFF	Disconnected
	Blinking slowly	Connecting to network
	Blinking	Connected to network with traffic
	ON	Connected to network without traffic
Wi-Fi AP	OFF	Disabled
	Blinking slowly	Enabled but no client connected
	Blinking	Connected to network with traffic
	ON	Client(s) connected to wireless network

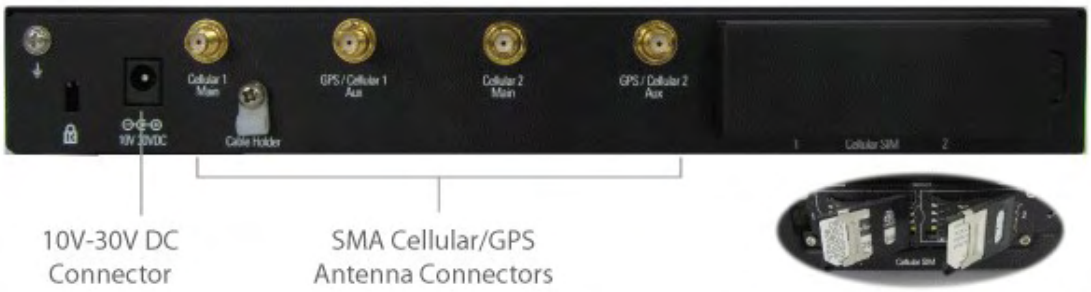
LAN and Ethernet WAN Ports		
Green LED	ON	10 / 100/ 1000 Mbps
Orange LED	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

 Copyright @ 2017 Pepwave

4.2 MAX HD2

4.2.1 Panel Appearance





2x Embedded 4G LTE/3G Modems

 Copyright @ 2017 Pepwave

4.2.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Wi-Fi AP and Wi-Fi WAN Indicators		
Wi-Fi WAN / Cellular 1 / Cellular 2	OFF	Disabled Intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

LAN and Ethernet WAN Ports		
Green LED	ON	10 / 100 / 1000 Mbps
Orange LED	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

 Copyright @ 2017 Pepwave

4.3 MAX HD2 IP67

4.3.1 Panel Appearance

The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

 Copyright @ 2017 Pepwave

4.4 MAX HD2 mini

4.4.1 Panel Appearance

* With 48V DC power, all 3 Ethernet ports can act as 802.3af PoeE or 24V Passive PoE outputs

4.4.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Cellular WAN Indicators		
Cellular 1 / Cellular 2	OFF	Disabled intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

LAN and Ethernet WAN Ports		
Green LED	ON	10 / 100 / 1000 Mbps
Orange LED	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

 Copyright @ 2017 Pepwave

4.5 MAX Transit

4.5.1 Panel Appearance

4.5.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Cellular WAN Indicators		
Cellular 1 / Cellular 2*	OFF	Disabled intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

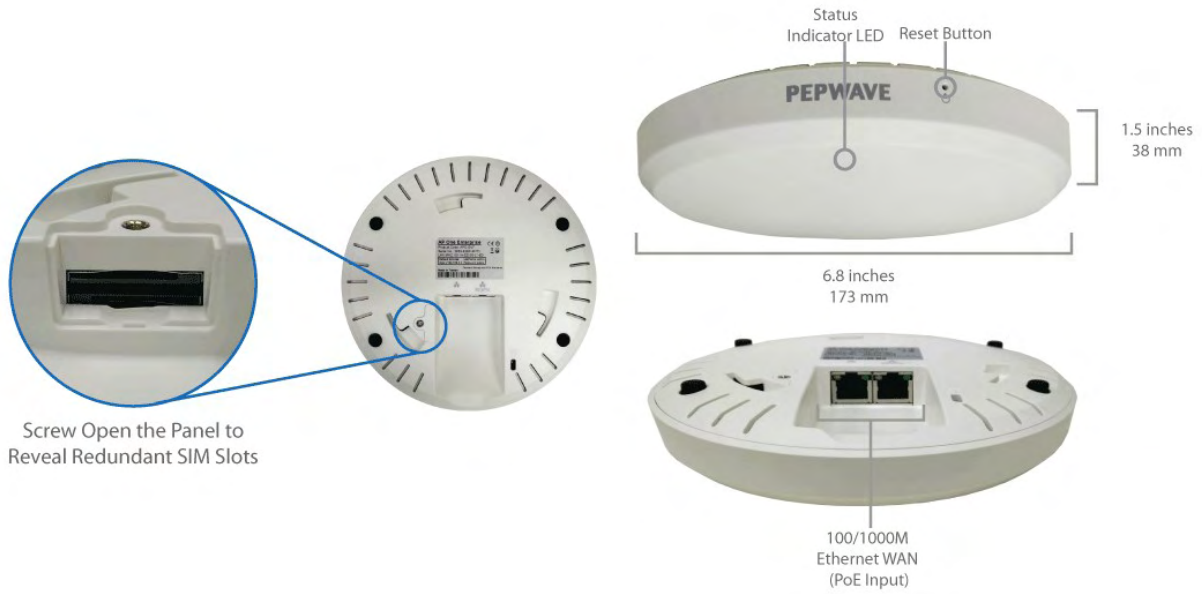
* For MAX-TST_DUO

LAN and Ethernet WAN Ports		
Green LED	ON	10 / 100 / 1000 Mbps
Orange LED	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

 Copyright @ 2017 Pepwave

4.6 MAX Hotspot

4.6.1 Panel Appearance



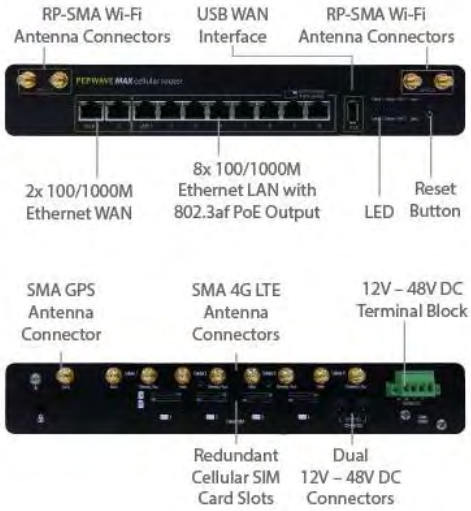
4.6.2 LED Indications

LED Indicators		
Status	RED – Access point initializing GREEN – Access point ready	
LAN and Ethernet WAN Ports		
Green LED	ON	100 Mbps
	OFF	10 Mbps
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

 Copyright @ 2017 Pepwave

4.7 MAX HD4

4.7.1 Panel Appearance



4.7.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Wi-Fi AP and Wi-Fi WAN Indicators		
Wi-Fi WAN / Cellular 1 / Cellular 2	OFF	Disabled Intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

LAN and Ethernet WAN Ports		
Green LED	ON	10 / 100 / 1000 Mbps
Orange LED	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected

 Copyright @ 2017 Pepwave

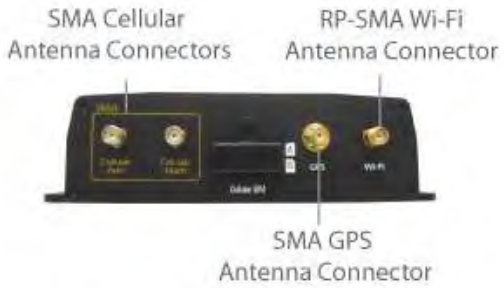
Port Type	Auto MDI/MDI-X ports

 Copyright @ 2017 Pepwave

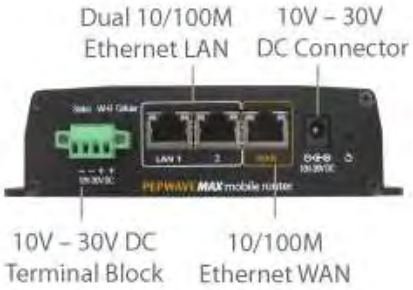
4.8 MAX BR1 / MAX BR1 MK2

4.8.1 Panel Appearance

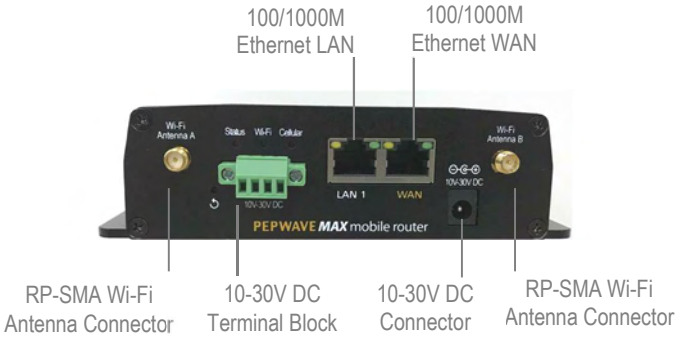
MAX-BR1-LTE Version



MAX-BR1 Version



MAX BR1 MK2



 Copyright @ 2017 Pepwave

4.8.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Wi-Fi Indicators		
Wi-Fi	OFF	Disabled intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

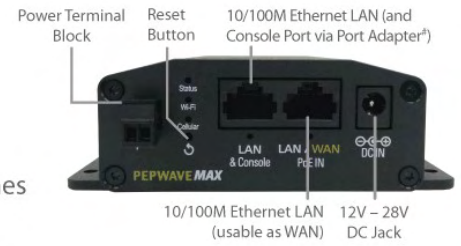
Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	ON	Connecting or connected to network(s)

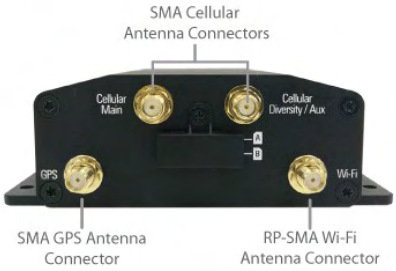
LAN and Ethernet WAN Ports		
Green LED	ON	100 Mbps / 1000Mbps (MK2)
	OFF	10 Mbps / 100Mbps (MK2)
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

 Copyright @ 2017 Pepwave

4.9 MAX BR1 Mini

4.9.1 Panel Appearance





4.9.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Wi-Fi Indicators		
Wi-Fi	OFF	Disabled intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	ON	Connecting or connected to network(s)

 Copyright @ 2017 Pepwave

Specifications

	MAX BR1 Mini
WAN Interface	1x 10/100M Ethernet Port 1x Embedded LTE Modem with Redundant SIM Slot
LAN Interface	1x 10/100M Ethernet Port
Wi-Fi Interface	802.11b/g/n Wi-Fi WAN or AP
Router Throughput	100Mbps
Recommended Users	1-60
Cellular and GPS Antenna Connector	2x SMA Antenna Connectors 1x SMA GPS Antenna Connector 1x Wi-Fi Connector
Power Input	DC Jack/Terminal Block: 12V – 28V DC Passive PoE Input (WAN Port)
Power Consumption	12W (max.)
Dimensions	4.1 x 4.3 x 1.2 inches 105 x 110 x 30 mm
Weight	0.54 pound 244 grams
Operating Temperature	40°C - 50°C
Humidity	15% – 95% (non-condensing)

A torque requirement of hex connection:

- **GPS - Torque requirement is 7.5+/-0.2kg f-cm**
- **Cellular Main - Torque requirement is 7.5+/-0.2kg f-cm**
- **Cellular Diversity/AUX - Torque requirement is 7.5+/-0.2kg f-cm**

 Copyright @ 2017 Pepwave

4.10 MAX BR1 Slim

4.10.1 Panel Appearance

4.10.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Wi-Fi Indicators		
Wi-Fi	OFF	Disabled intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	ON	Connecting or connected to network(s)

 Copyright @ 2017 Pepwave

-

LAN and Ethernet WAN Ports		
Green LED	ON	100 Mbps
	OFF	10 Mbps
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

-

 Copyright @ 2017 Pepwave

4.11 MAX BR1 ENT

4.11.1 Panel Appearance

4.11.2 LED Indicators

- The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

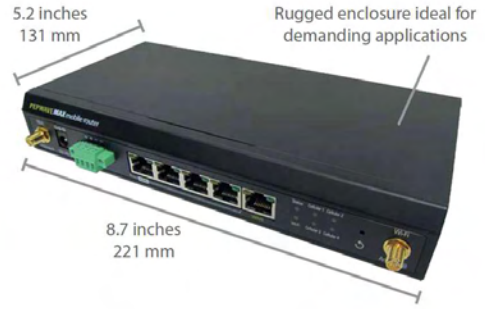
Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	ON	Connecting or connected to network(s)

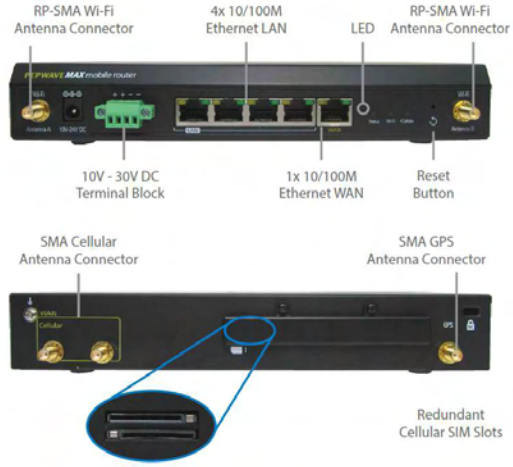
LAN and Ethernet WAN Ports		
Green LED	ON	100 Mbps
	OFF	10 Mbps
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

 Copyright @ 2017 Pepwave

4.12 MAX BR1 Pro LTE

4.12.1 Panel Appearence





4.12.2 LED Indicators

- The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	ON	Connecting or connected to network(s)

LAN and Ethernet WAN Ports		
Green LED	ON	100 Mbps
	OFF	10 Mbps
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

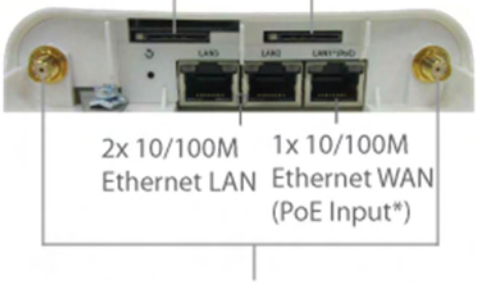
 Copyright @ 2017 Pepwave

4.13 MAX BR1/2 IP55

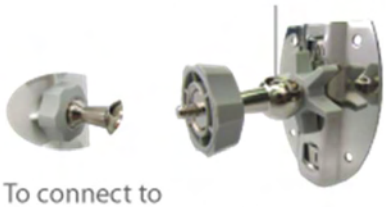
4.13.1 Panel Appearance

Built-In, Software-Selectable 10dBi MIMO Directional and 4dBi Omni Wi-Fi antennas

Screw-Holes for Wall Mounting (screws not included)



Accessory – Wall/Pole Mount with Ball Joint for IP55 Outdoor Products ^



* Requires 48V Pepwave Passive PoE input. Available separately.

^ Available separately.

4.13.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

 Copyright @ 2017 Pepwave

Wi-Fi Indicators		
Wi-Fi	OFF	Disabled Intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	ON	Connecting or connected to network(s)

LAN and Ethernet WAN Ports		
Green LED	ON	100 Mbps
	OFF	10 Mbps
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

 Copyright @ 2017 Pepwave

4.14 MAX On-The-Go

4.14.1 Panel Appearance

4.14.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Cellular Indicators		
WAN	OFF	Modem is not attached to the port
	Green	Modem is attached to the port

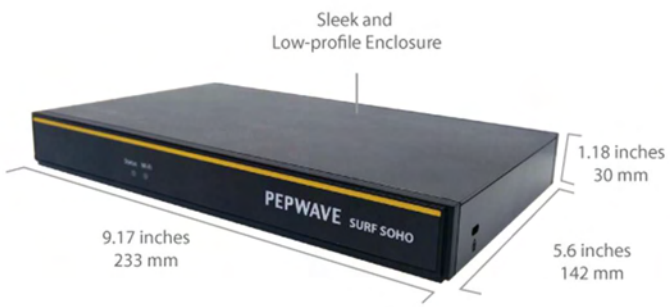
Wi-Fi Indicators		
Wi-Fi	OFF	Disconnected from AP
	Green	Connected to AP

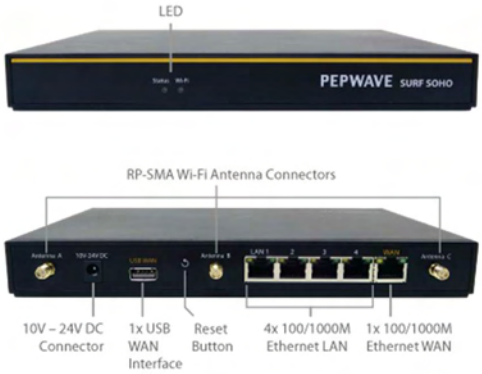
Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Green	Ready

LAN and Ethernet WAN Ports		
Green LED	ON	100 Mbps
	OFF	10 Mbps
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
Port Type	Auto MDI/MDI-X ports	

4.15 Surf SOHO

4.15.1 Panel Appearance





4.15.2 LED Indicators

The statuses indicated by the front panel LEDs are as follows:

Wi-Fi and Status Indicators		
Wi-Fi	OFF	Disabled Intermittent
	Blinking	Enabled but no client connected
	ON	Client(s) connected to wireless network
	Continuous blinking	Transferring data to wireless network
Status	OFF	System initializing
	Red	Booting up or busy
	Green	Ready state

LAN and Ethernet WAN Ports		
Green LED	ON	100/1000 Mbps
Orange LED	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
Port type	Auto MDI/MDI-X ports	

Wi-Fi Signal	
Off	No connection
Signal strength	Wi-Fi signal strength (low, medium, and high)

 Copyright @ 2017 Pepwave

5 Advanced Feature Summary

5.1 Drop-in Mode and LAN Bypass: Transparent Deployment

As your organization grows, it needs more bandwidth. But modifying your network would require effort better spent elsewhere. In **Drop-in Mode**, you can conveniently install your Peplink router without making any changes to your network. And if the Peplink router loses power for any reason, **LAN Bypass** will safely and automatically bypass the Peplink router to resume your original network connection.

Compatible with: MAX 700, MAX HD2 (All variants), HD4 (All Variants)

5.2 QoS: Clearer VoIP

VoIP and videoconferencing are highly sensitive to latency. With QoS, Peplink routers can detect VoIP traffic and assign it the highest priority, giving you crystal-clear calls.

 Copyright @ 2017 Pepwave

5.3 Per-User Bandwidth Control

With per-user bandwidth control, you can define bandwidth control policies for up to 3 groups of users to prevent network congestion. Define groups by IP address and subnet, and set bandwidth limits for every user in the group.

5.4 High Availability via VRRP

When your organization has a corporate requirement demanding the highest availability with no single point of failure, you can deploy two Peplink routers in **High Availability mode**. With High Availability mode, the second device will take over when needed.

Compatible with: MAX 700, MAX HD2 (All variants), HD4 (All Variants)

 Copyright @ 2017 Pepwave

5.5 USB Modem and Android Tethering

For increased WAN diversity, plug in a USB LTE modem as backup. Peplink routers are compatible with over 200 modem types. You can also tether to smartphones running Android 4.1.X and above.

Compatible with: MAX 700, HD2 (all variants except IP67), HD4 (All variants)

5.6 Built-In Remote User VPN Support

Use L2TP with IPsec to safely and conveniently connect remote clients to your private network. L2TP with IPsec is supported by most devices, but legacy devices can also connect using PPTP.

Click here for full instructions on setting up L2TP with IPsec.

 Copyright @ 2017 Pepwave

5.7 SIM-card USSD support

Cellular-enabled routers can now use USSD to check their SIM card's balance, process pre-paid cards, and configure carrier-specific services. Click here for full instructions on using USSD.

 Copyright @ 2017 Pepwave

6 Installation

The following section details connecting Pepwave routers to your network.

6.1 Preparation

Before installing your Pepwave router, please prepare the following as appropriate for your installation:

- At least one Internet/WAN access account and/or Wi-Fi access information
- Depending on network connection type(s), one or more of the following:
  - **Ethernet WAN**: A 10/100/1000BaseT UTP cable with RJ45 connector
  - **USB**: A USB modem
  - **Embedded modem**: A SIM card for GSM/HSPA service
  - **Wi-Fi WAN**: Wi-Fi antennas
  - **PC Card/Express Card WAN:** A PC Card/ExpressCard for the corresponding card slot
- A computer installed with the TCP/IP network protocol and a supported web browser. Supported browsers include Microsoft Internet Explorer 8.0 or above, Mozilla Firefox 10.0 or above, Apple Safari 5.1 or above, and Google Chrome 18 or above.

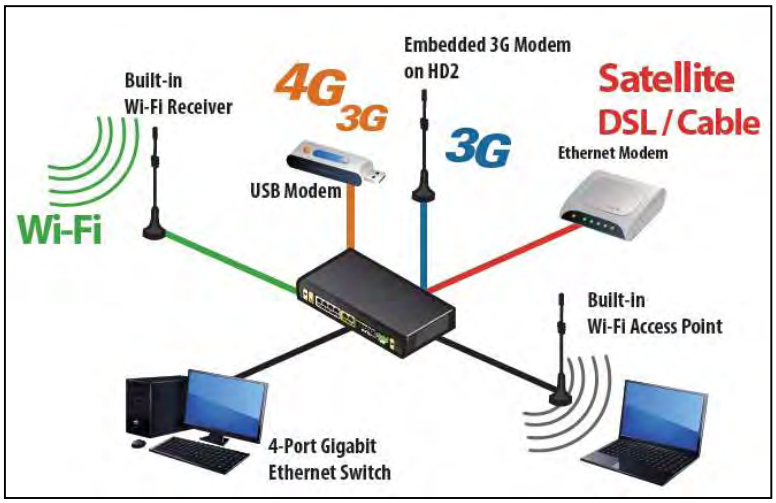
 Copyright @ 2017 Pepwave

6.2 Constructing the Network

At a high level, construct the network according to the following steps:

1. With an Ethernet cable, connect a computer to one of the LAN ports on the Pepwave router. Repeat with different cables for up to 4 computers to be connected.
2. With another Ethernet cable or a USB modem/Wi-Fi antenna/PC Card/Express Card, connect to one of the WAN ports on the Pepwave router. Repeat the same procedure for other WAN ports.
3. Connect the power adapter to the power connector on the rear panel of the Pepwave router, and then plug it into a power outlet.

The following figure schematically illustrates the resulting configuration:



6.3 Configuring the Network Environment

To ensure that the Pepwave router works properly in the LAN environment and can access the Internet via WAN connections, please refer to the following setup procedures:

- LAN configuration

  For basic configuration, refer to **Section** 8**, Connecting to the Web Admin Interface**.

  For advanced configuration, go to **Section** 9**, Configuring the LAN Interface(s)**.

- WAN configuration

  For basic configuration, refer to **Section** 8**, Connecting to the Web Admin Interface**.

  For advanced configuration, go to **Section 9.2, Captive Portal**.

 Copyright @ 2017 Pepwave

7 Mounting the Unit

7.1 Wall Mount

The Pepwave MAX 700/HD2/On-The-Go can be wall mounted using screws. After adding the screw on the wall, slide the MAX in the screw hole socket as indicated below. Recommeneded screw specification: M3.5 x 20mm, head diameter 6mm, head thickness 2.4mm.

The Pepwave MAX BR1 requires four screws for wall mounting.

7.2 Car Mount

The Pepwave MAX700/HD2 can be mounted in a vehicle using the included mounting brackets. Place the mounting brackets by the two sides and screw them onto the device.

7.3 IP67 Installation Guide

Installation instructions for IP67 devices can be found here:
http://download.peplink.com/manual/IP67_Installation_Guide.pdf

 Copyright @ 2017 Pepwave

8 Connecting to the Web Admin Interface

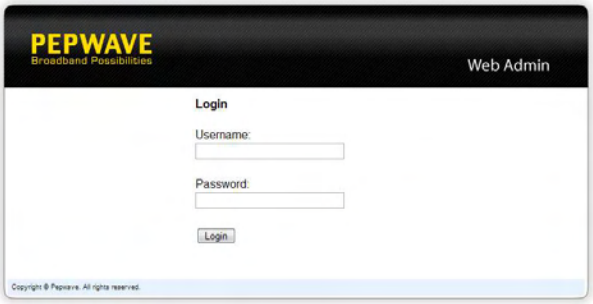
1. Start a web browser on a computer that is connected with the Pepwave router through the LAN.
2. To connect to the router's web admin interface, enter the following LAN IP address in the address field of the web browser:

   http://192.168.50.1

   (This is the default LAN IP address for Pepwave routers.)
3. Enter the following to access the web admin interface.

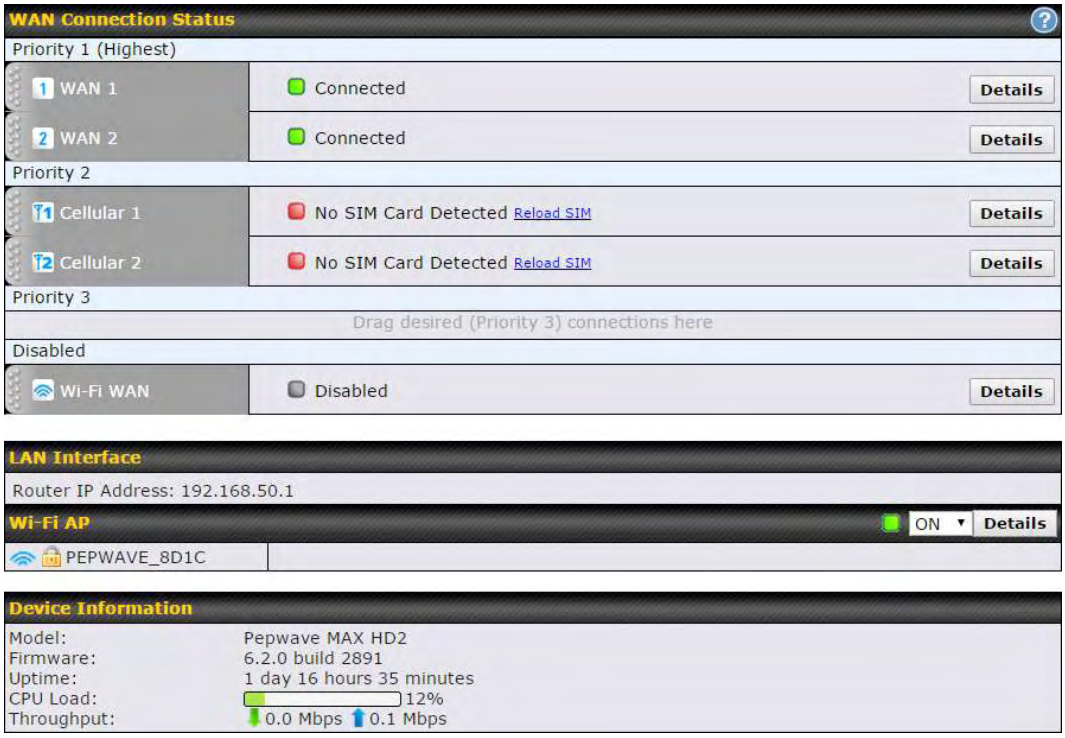
   Username: admin

   Password: admin



(This is the default username and password for Pepwave routers. The admin and read-only user passwords can be changed at **System>Admin Security**.)

4. After successful login, the **Dashboard** will be displayed.



The **Dashboard** shows current WAN, LAN, and Wi-Fi AP statuses. Here, you can change WAN connection priority and switch on/off the Wi-Fi AP. For further information on setting up these connections, please refer to **Sections 8** and **9.**

Device Information displays details about the device, including model name, firmware version, and uptime. For further information, please refer to **Section 22.**

Important Note
Configuration changes (e.g. WAN, LAN, admin settings, etc.) will take effect only after clicking the **Save** button at the bottom of each page. The **Apply Changes** button causes the changes to be saved and applied.

 Copyright @ 2017 Pepwave

9 Configuring the LAN Interface(s)

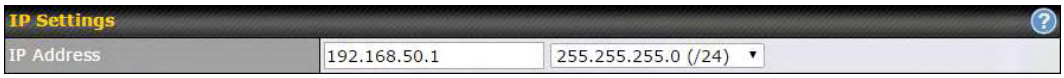
9.1 Basic Settings

LAN interface settings are located at **Network>LAN>Basic Settings**. Navigating to that page will result in the following dashboard:

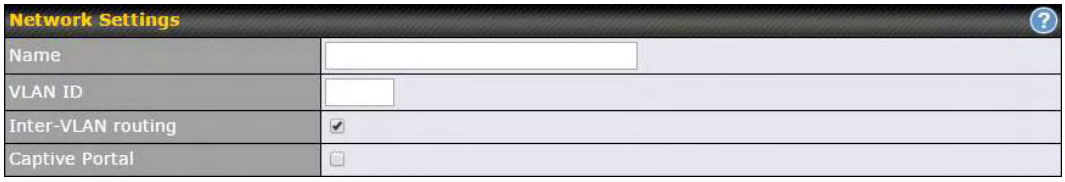
This represents the LAN interfaces that are active on your router (including VLAN). A grey “X” means that the VLAN is used in other settings and cannot be deleted. You can find which settings are using the VLAN by hovering over the grey “X”.

Alternatively, a red “X” means that there are no settings using the VLAN. You can delete that VLAN by clicking the red “X”

Clicking any of the existing LAN interfaces (or creating a new one) will result in the following

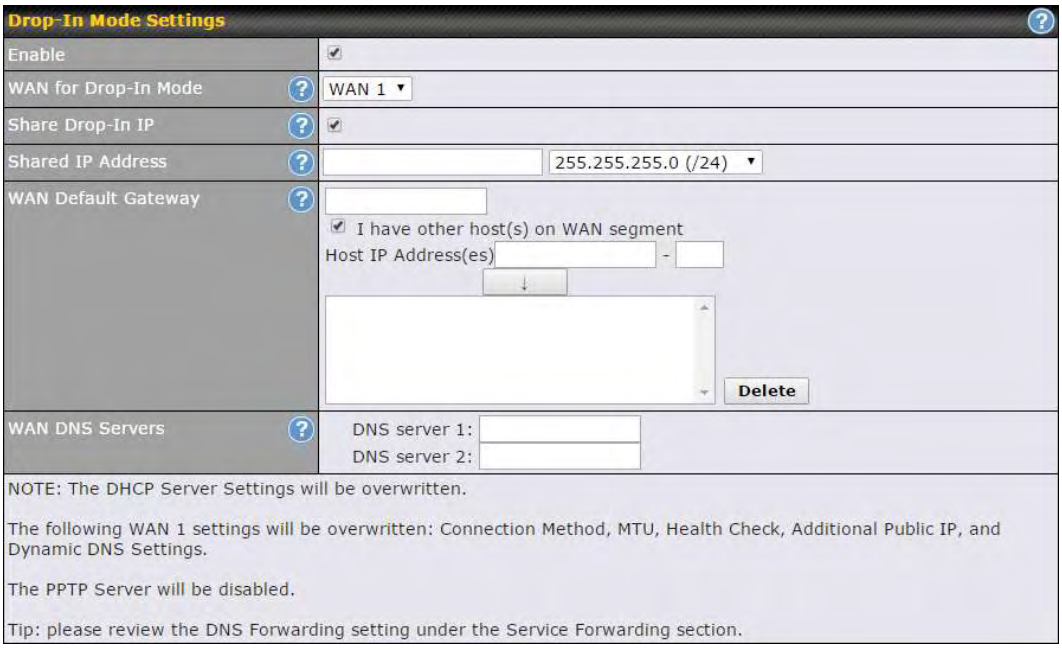


IP Settings	
IP Address	The IP address and subnet mask of the Pepwave router on the LAN.



Network Settings	
Name	Enter a name for the LAN.
VLAN ID	Enter a number for your VLAN.
Inter-VLAN routing	Check this box to enable routing between virtual LANs.

Captive Portal	Check this box to turn on captive portals.

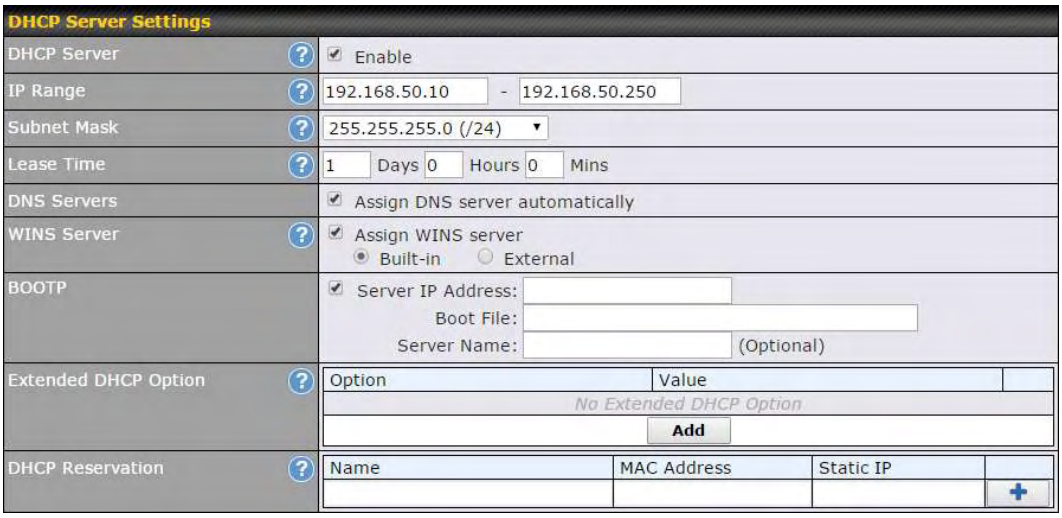


Drop-in Mode Settings	
Enable	Drop-in mode eases the installation of Peplink routers on a live network between the existing firewall and router, such that no configuration changes are required on existing equipment. Check the box to enable the drop-in mode feature, if available on your model.
WAN for Drop-In Mode	Select the WAN port to be used for drop-in mode. If **WAN 1 with LAN Bypass** is selected, the high availability feature will be disabled automatically.
Share Drop-In IP[A]	When this option is enabled, the passthrough IP address will be used to connect to WAN hosts (email notification, remote syslog, etc.). The Pepwave router will listen for this IP address when WAN hosts access services provided by the Pepwave router (web admin access from the WAN, DNS server requests, etc.). To connect to hosts on the LAN (email notification, remote syslog, etc.), the default gateway address will be used. The Pepwave router will listen for this IP address when LAN hosts access services provided by the Pepwave router (web admin access from the WAN, DNS proxy, etc.).
Shared IP Address[A]	Access to this IP address will be passed through to the LAN port if this device is not serving the service being accessed. The shared IP address will be used in connecting to hosts on the WAN (email notification, remote syslog, etc.) The device will also listen on the IP address when hosts on the WAN access services served on this device (web admin access from the WAN, DNS server, etc.)
WAN Default Gateway	Enter the WAN router's IP address in this field. If there are more hosts in addition to the router on the WAN segment, check the I **have other host(s) on WAN segment** box and enter the IP address of the hosts that need to access LAN devices or be accessed by others.
WAN DNS Servers	Enter the selected WAN's corresponding DNS server IP addresses.

[A] - Advanced feature, please click the button on the top right-hand corner to activate.

Layer 2 PepVPN Bridging	
PepVPN Profiles to Bridge	The remote network of the selected PepVPN profiles will be bridged with this local LAN, creating a Layer 2 PepVPN, they will be connected and operate like a single LAN, and any broadcast or multicast packets will be sent over the VPN.
Spanning Tree Protocol	Click the box will enable STP for this layer 2 profile bridge.
Override IP	Select "Do not override" if the LAN IP address and local DHCP server should remain unchanged after the Layer 2 PepVPN is up.

Address when bridge connected	If you choose to override IP address when the VPN is connected, the device will not act as a router, and most Layer 3 routing functions will cease to work.

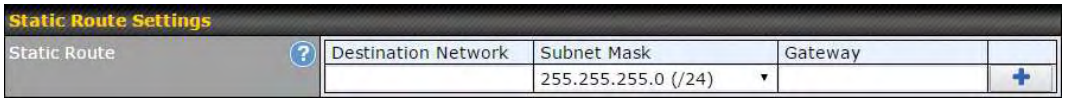


DHCP Server Settings

DHCP Server	When this setting is enabled, the DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Pepwave router's DHCP server can prevent IP address collision on the LAN.
IP Range & Subnet Mask	These settings allocate a range of IP addresses that will be assigned to LAN computers by the Pepwave router's DHCP server.
Lease Time	This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of the lease time, the assigned IP address will no longer be valid and renewal of the IP address assignment will be required.
DNS Servers	This option allows you to input the DNS server addresses to be offered to DHCP clients. If **Assign DNS server automatically** is selected, the Pepwave router's built-in DNS server address (i.e., LAN IP address) will be offered.
WINS Server	This option allows you to optionally specify a Windows Internet Name Service (WINS) server. You may choose to use the **built-in WINS server** or **external WINS servers**. When this unit is connected using SpeedFusion™, other VPN peers can share this unit's built-in WINS server by entering this unit's LAN IP address in their DHCP **WINS Server** setting. Afterward, all PC clients in the VPN can resolve the NetBIOS names of other clients in remote peers. If you have enabled this option, a list of WINS clients will be displayed at **Status>WINS Clients**.
BOOTP	Check this box to enable BOOTP on older networks that still require it.
Extended DHCP Option	In addition to standard DHCP options (e.g., DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts. To define an extended DHCP option, click the **Add** button, choose the option to define and

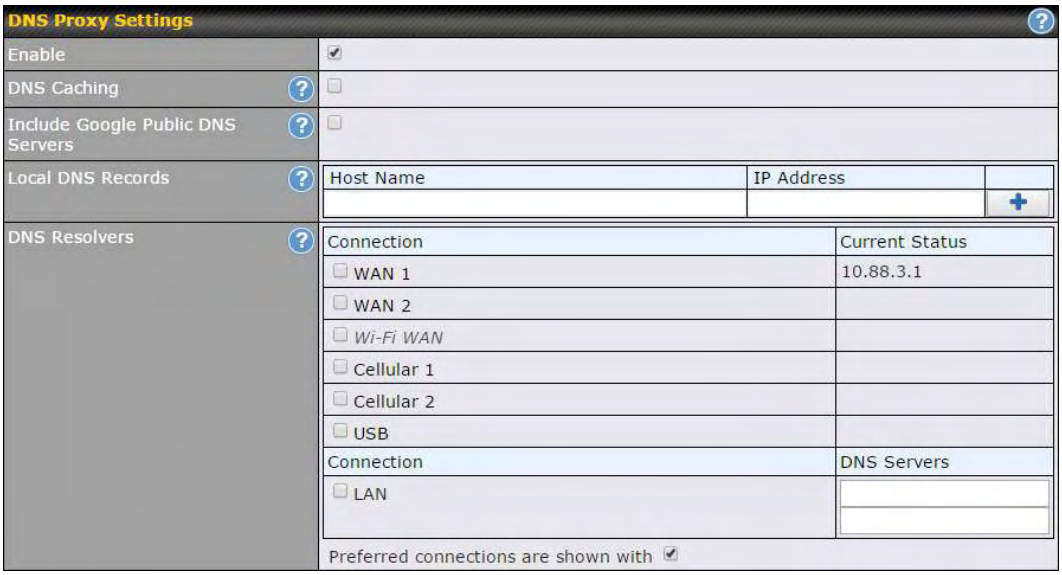
	enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only.
DHCP Reservation	This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses. The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses. **Name** (an optional field) allows you to specify a name to represent the device. MAC addresses should be in the format of **00:AA:BB:CC:DD:EE**. Press + to create a new record. Press ✖ to remove a record. Reserved client information can be imported from the **Client List**, located at **Status>Client List**. For more details, please refer to **Section 22.3.**

LAN Physical Settings	
Speed	This is the port speed of the LAN interface. It should be set to the same speed as the connected device to avoid port negotiation problems. When a static speed is set, you may choose whether to advertise its speed to the peer device. **Auto** is selected by default. You can choose not to advertise the port speed if the port has difficulty negotiating with the peer device.



Static Route Settings	
Static Route	This table is for defining static routing rules for the LAN segment. A static route consists of the network address, subnet mask, and gateway address. The address and subnet mask values are in *w.x.y.z* format. The local LAN subnet and subnets behind the LAN will be advertised to the VPN. Remote routes sent over the VPN will also be accepted. Any VPN member will be able to route to the local subnets. Press + to create a new route. Press ✖ to remove a route.

WINS Server Settings	
Enable	Check the box to enable the WINS server. A list of WINS clients will be displayed at **Status>WINS Clients**.

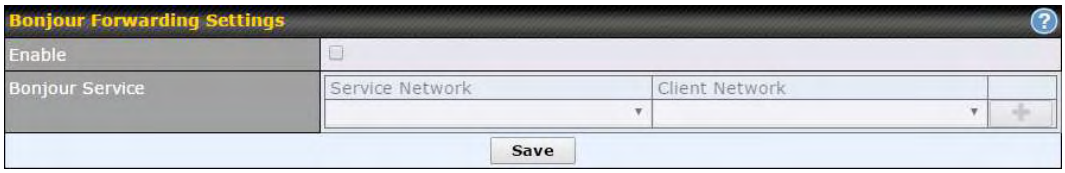


DNS Proxy Settings	
Enable	To enable the DNS proxy feature, check this box, and then set up the feature at **Network>LAN>DNS Proxy Settings**. A DNS proxy server can be enabled to serve DNS requests originating from LAN/PPTP/SpeedFusion™ peers. Requests are forwarded to the **DNS servers/resolvers** defined for each WAN connection.
DNS Caching	This field is to enable DNS caching on the built-in DNS proxy server. When the option is enabled, queried DNS replies will be cached until the records' TTL has been reached. This feature can help improve DNS lookup time. However, it cannot return the most up-to-date result for those frequently updated DNS records. By default, **DNS Caching** is disabled.
Include Google Public DNS Servers	When this option is **enabled**, the DNS proxy server will also forward DNS requests to Google's Public DNS Servers, in addition to the DNS servers defined in each WAN. This could increase the DNS service's availability. This setting is disabled by default.
Local DNS Records	This table is for defining custom local DNS records. A static local DNS record consists of a host name and IP address. When looking up the host name from the LAN to LAN IP of the Pepwave router, the corresponding IP address will be returned. Press + to create a new record. Press ✖ to remove a record.
DNS Resolvers [A]	Check the box to enable the WINS server. A list of WINS clients will be displayed at **Network>LAN>DNS Proxy Settings>DNS Resolvers**. This field specifies which DNS resolvers will receive forwarded DNS requests. If no WAN/VPN/LAN DNS resolver is selected, all of the WAN's DNS resolvers will be selected. If a SpeedFusion™ peer is selected, you may enter the VPN peer's DNS resolver IP address(es). Queries will be forwarded to the selected connections' resolvers. If all of the selected connections are down, queries will be forwarded to all resolvers on healthy WAN connections.

[A] - Advanced feature, please click the button on the top right hand corner to activate.

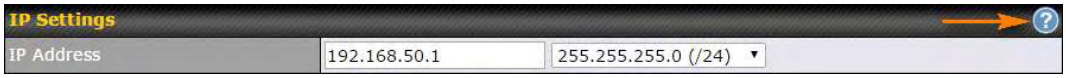
Finally, if needed, configure Bonjour forwarding, Apple's zero configuration networking

protocol. Once VLAN configuration is complete, click **Save** to store your changes.



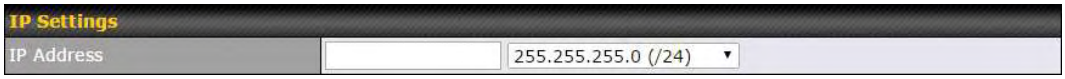
Bonjour Forwarding Settings	
Enable	Check this box to turn on Bonjour forwarding.
Bonjour Service	Choose **Service** and **Client** networks from the drop-down menus, and then click + to add the networks. To delete an existing Bonjour listing, click ✖.

To enable VLAN configuration, click the button in the **IP Settings** section.

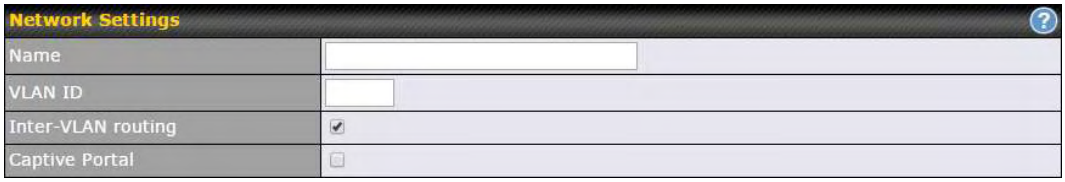


To add a new LAN, click the **New LAN** button. To change LAN settings, click the name of the LAN to change under the **LAN** heading.

The following settings are displayed when creating a new LAN or editing an existing LAN.

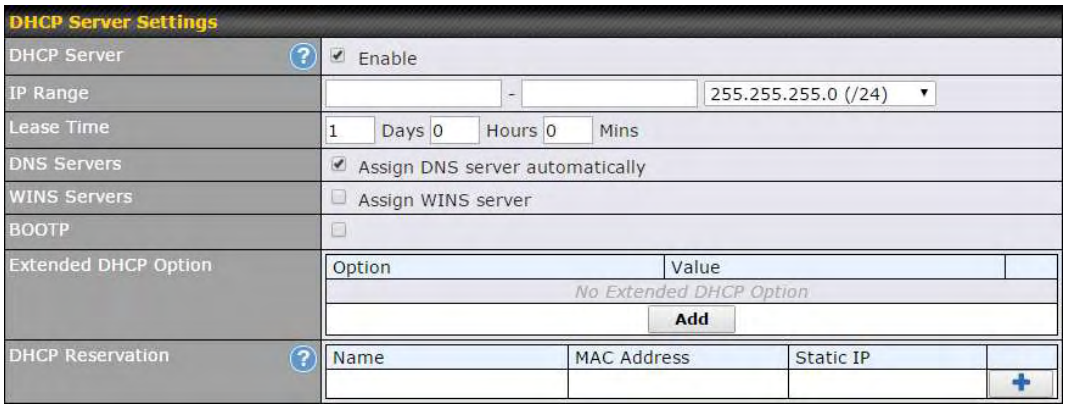


IP Settings	
IP Address & Subnet Mask	Enter the Pepwave router's IP address and subnet mask values to be used on the LAN.



Network Settings	
Name	Enter a name for the LAN.
VLAN ID	Enter a number for your VLAN.
Inter-VLAN routing	Check this box to enable routing between virtual LANs.
Captive Portal	Check this box to turn on captive portals.

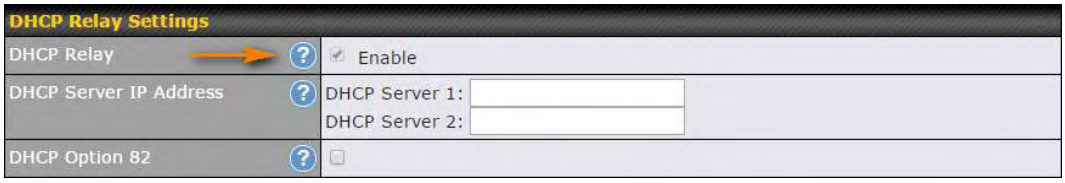
 Copyright @ 2017 Pepwave



DHCP Server Settings	
DHCP Server	When this setting is enabled, the Pepwave router's DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Pepwave router's DHCP server can prevent IP address collisions on the LAN. To enable DHCP bridge relay, please click the icon on this menu item.
IP Range & Subnet Mask	These settings allocate a range of IP address that will be assigned to LAN computers by the Pepwave router's DHCP server.
Lease Time	This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of **Lease Time**, the assigned IP address will no longer be valid and the IP address assignment must be renewed.
DNS Servers	This option allows you to input the DNS server addresses to be offered to DHCP clients. If **Assign DNS server automatically** is selected, the Pepwave router's built-in DNS server address (i.e., LAN IP address) will be offered.
WINS Servers	This option allows you to specify the Windows Internet Name Service (WINS) server. You may choose to use the built-in WINS server or external WINS servers. When this unit is connected using SpeedFusion™, other VPN peers can share this unit's built-in WINS server by entering this unit's LAN IP address in their **DHCP WINS Servers** setting. Therefore, all PC clients in the VPN can resolve the NetBIOS names of other clients in remote peers. If you have enabled this option, a list of WINS clients will be displayed at **Status>WINS Clients**.
BOOTP	Check this box to enable BOOTP on older networks that still require it.
Extended DHCP Option	In addition to standard DHCP options (e.g. DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts. To define an extended DHCP option, click the **Add** button, choose the option to define, and then enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only.
DHCP Reservation	This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses. The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses. **Name** (an optional field) allows you to specify a name to represent the device. MAC addresses should be in the format of **00:AA:BB:CC:DD:EE**. Press to create a new record. Press to remove a record. Reserved clients information can be imported from the **Client List**, located at **Status>Client List**. For more details, please refer to **Section**

22.3.

To configure DHCP relay, first click the button found next to the **DHCP Server** option to display the settings.

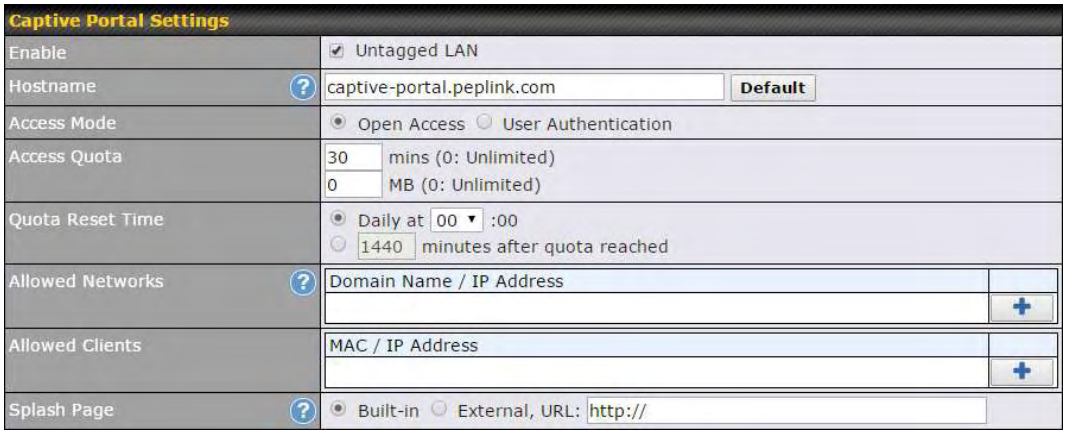


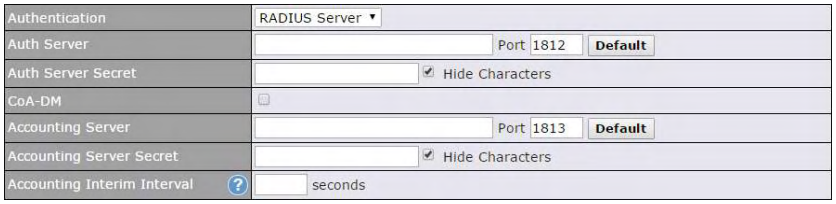
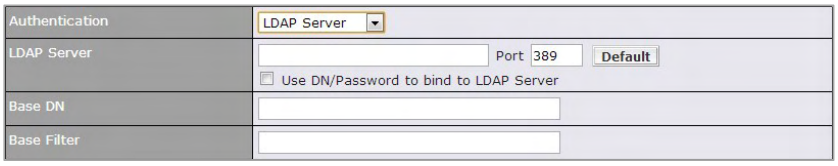
DHCP Relay Settings	
Enable	Check this box to turn on DHCP relay. Click the icon to disable DHCP relay.
DHCP Server IP Address	Enter the IP addresses of one or two DHCP servers in the provided fields. The DHCP servers entered here will receive relayed DHCP requests from the LAN. For active-passive DHCP server configurations, enter active and passive DHCP server relay IP addresses in **DHCP Server 1** and **DHCP Server 2.**
DHCP Option 82	DCHP Option 82 includes device information as relay agent for the attached client when forwarding DHCP requests from client to server. This option also embeds the device's MAC address and network name in circuit and remote IDs. Check this box to enable DHCP Option 82.

Once DHCP is set up, configure **LAN Physical Settings**, **Static Route Settings**, **WINS Server Settings**, and **DNS Proxy Settings** as noted above.

9.2 Captive Portal

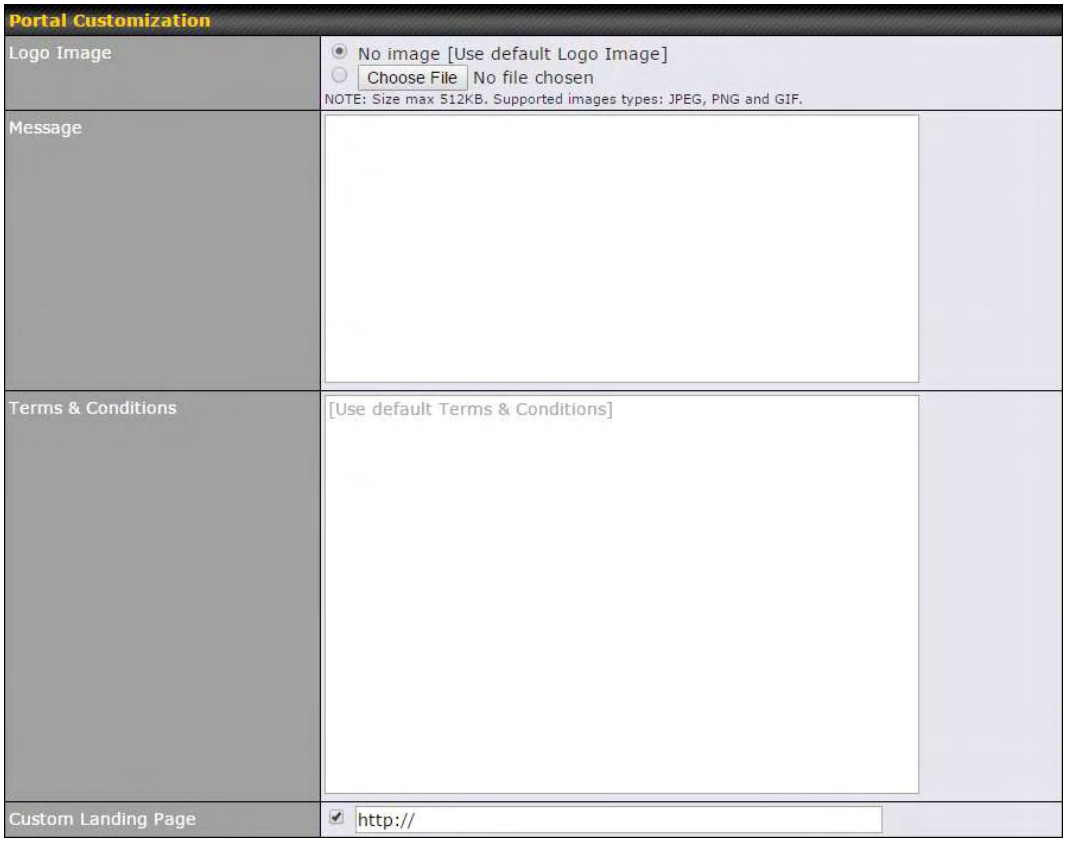
The captive portal serves as gateway that clients have to pass if they wish to access the internet using your router. To configure, navigate to **Network>LAN>Captive Portal**.



Captive Portal Settings	
Enable	Check **Enable** and then, optionally, select the LANs/VLANs that will use the captive portal.
Hostname	To customize the portal's form submission and redirection URL, enter a new URL in this field. To reset the URL to factory settings, click **Default**.
Access Mode	Click **Open Access** to allow clients to freely access your router. Click **User Authentication** to force your clients to authenticate before accessing your router.
RADIUS Server	This authenticates your clients through a RADIUS server. After selecting this option, you will see the following fields:  Fill in the necessary information to complete your connection to the server and enable authentication.
LDAP Server	This authenticates your clients through a LDAP server. Upon selecting this option, you will see the following fields:  Fill in the necessary information to complete your connection to the server and enable authentication.

Access Quota	Set a time and data cap to each user's Internet usage.
Quota Reset Time	This menu determines how your usage quota resets. Setting it to **Daily** will reset it at a specified time every day. Setting a number of **minutes after quota reached** establish a timer for each user that begins after the quota has been reached.
Allowed Networks	To whitelist a network, enter the domain name / IP address here and click [+]. To delete an existing network from the list of allowed networks, click the [✖] button next to the listing.
Splash Page	Here, you can choose between using the Pepwave router's built-in captive portal and redirecting clients to a URL you define.

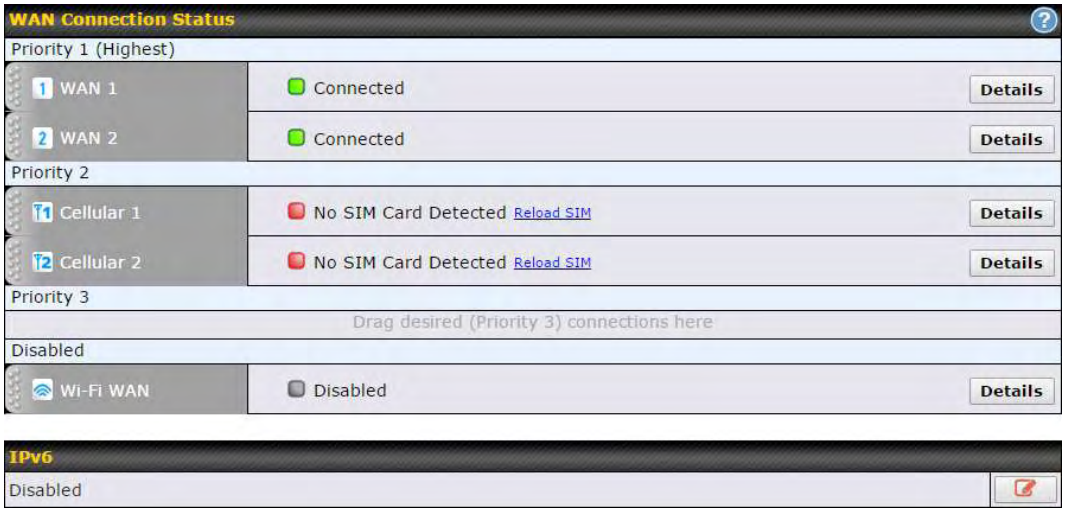
The **Portal Customization** menu has two options: [Preview] and [✎]. Clicking [Preview] displays a pop-up previewing the captive portal that your clients will see. Clicking [✎] displays the following menu:



Portal Customization	
Logo Image	Click the **Choose File** button to select a logo to use for the built-in portal.
Message	If you have any additional messages for your users, enter them in this field.
Terms & Conditions	If you would like to use your own set of terms and conditions, please enter them here. If left empty, the built-in portal will display the default terms and conditions.
Custom Landing Page	Fill in this field to redirect clients to an external URL.

10 Configuring the WAN Interface(s)

WAN Interface settings are located at **Network>WAN**. To reorder WAN priority, drag on the appropriate WAN by holding the left mouse button, move it to the desired priority (the first one would be the highest priority, the second one would be lower priority, and so on), and drop it by releasing the mouse button.

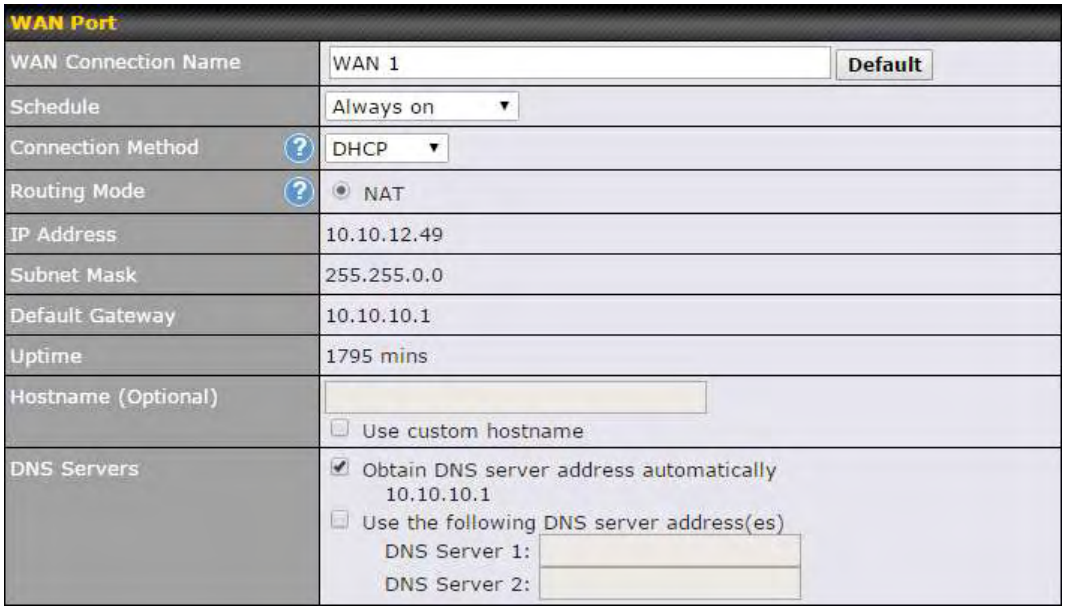


To disable a particular WAN connection, drag on the appropriate WAN by holding the left mouse button, move it the **Disabled** row, and drop it by releasing the mouse button. You can also set priorities on the **Dashboard**. Click the **Details** button in the corresponding row to modify the connection setting.

Important Note
Connection details will be changed and become effective immediately after clicking the **Save and Apply** button.

10.1 Ethernet WAN

From **Network>WAN,** choose a WAN connection and then click **Details**.



WAN Port (Section 1)	
WAN Connection Name	Enter a name to represent this WAN connection.
Schedule	Click the drop-down menu to apply a time schedule to this interface
Connection Method	There are three possible connection methods for Ethernet WAN: • **DHCP** • **Static IP** • **PPPoE** The connection method and details are determined by, and can be obtained from, the ISP. See the following sections for details on each connection method.
Routing Mode	This field shows that **NAT** (network address translation) will be applied to the traffic routed over this WAN connection. **IP Forwarding** is available when you click the link in the help text.
IP Address/Subnet Mask/Default Gateway	Enter the WAN IP address and subnet mask, as well as the IP address of the default gateway, in these fields.

 Copyright @ 2017 Pepwave

Hostname	Enter a hostname for this WAN port if needed.
DNS Servers	Select a DNS server for this port to use. This port can either be automatically selected or manually designated.

Standby State	Remain connected / Disconnect
Upstream Bandwidth	1 Gbps
Downstream Bandwidth	1 Gbps
Health Check Settings	
Health Check Method	PING
PING Hosts	Host 1: 8.8.8.8 Host 2: Use first two DNS servers as PING Hosts
Timeout	5 second(s)
Health Check Interval	5 second(s)
Health Check Retries	3
Recovery Retries	3

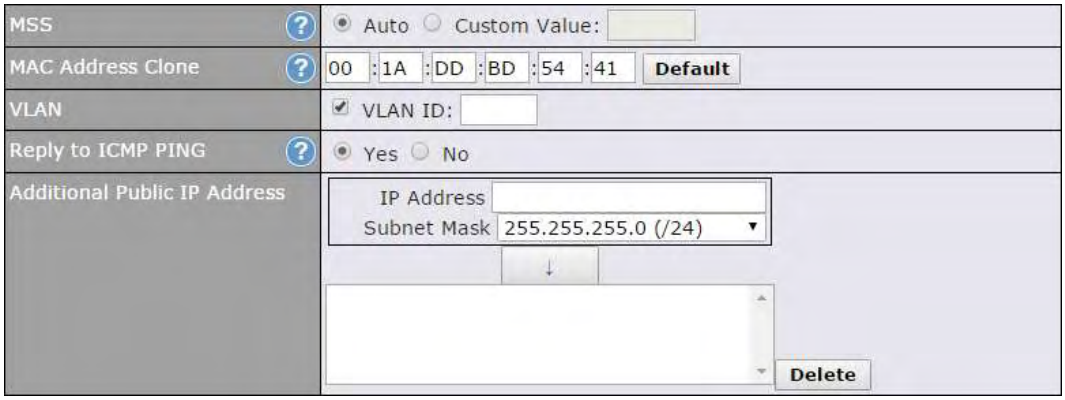
WAN Port (Section 2)	
Standby State	This setting specifies the standby state of the WAN connection. The available options are **Remain connected** and **Disconnect**. The default state is **Remain Connected**.
Upstream Bandwidth	This setting specifies the data bandwidth in the outbound direction from the LAN through the WAN interface.
Downstream Bandwidth	This setting specifies the data bandwidth in the inbound direction from the WAN interface to the LAN. This value is referenced as the default weight value when using the algorithm **Least Used** or the algorithm **Persistence (Auto)** in outbound policy with **Managed by Custom Rules** chosen (see **Section 15.2**).
Health Check Method	This setting specifies the health check method for the WAN connection. The value of method can be configured as **Disabled**, **Ping**, **DNS Lookup**, or **HTTP**. The default method is **Disabled**. See **Section 10.4** for configuration details.
PING Hosts	These fields are for specifying the target DNS servers where DNS lookups will be sent to for health check. If the box Use first two DNS servers as Health Check DNS Servers is checked, the first two DNS servers will be the DNS lookup targets for checking the connection healthiness. If the box is not checked, the field Host 1 must be filled and the field Host 2 is optional. The connection is considered to be up if DNS responses are received from any one of the

 Copyright @ 2017 Pepwave

	health check DNS servers, regardless of whether the result is positive or negative.
Timeout	If a health check test cannot be completed within the specified amount of time, the test will be treated as failed.
Health Check Interval	This is the number of consecutive check failures before treating a connection as down.
Health Check Retries	This is the number of consecutive check failures before treating a connection as down.
Recovery Retries	This is the number of responses required after a health check failure before treating a connection as up again.

WAN Port (Section 3)	
Dynamic DNS Service Provider	This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers: • changeip.com • dyndns.org • no-ip.org • tzo.com • DNS-O-Matic Select **Disabled** to disable this feature. See **Section 9.5** for configuration details.
Bandwidth Allowance Monitor	This option enables bandwidth usage monitoring on this WAN connection for each billing cycle. When this setting is not enabled, each month's bandwidth usage is tracked, but no action will be taken.
Port Speed	This setting specifies port speed and duplex configurations of the WAN port. By default, **Auto** is selected and the appropriate data speed is automatically detected by the Pepwave router. In the event of negotiation issues, the port speed can be manually specified. You can also choose whether or not to advertise the speed to the peer by selecting the **Advertise Speed** checkbox.
MTU	This setting specifies the maximum transmission unit. By default, MTU is set to **Custom 1440**. You may adjust the MTU value by editing the text field. Click **Default** to restore the

	default MTU value. Select **Auto** and the appropriate MTU value will be automatically detected. Auto-detection will run each time the WAN connection establishes.



WAN Port (Section 4)	
MSS	This setting should be configured based on the maximum payload size that the local system can handle. The MSS (maximum segment size) is computed from the MTU minus 40 bytes for TCP over IPv4. If MTU is set to **Auto**, the MSS will also be set automatically. By default, MSS is set to **Auto**.
MAC Address Clone	Some service providers (e.g., cable providers) identify the client's MAC address and require the client to always use the same MAC address to connect to the network. In such cases, change the WAN interface's MAC address to the original client PC's MAC address via this field. The default MAC address is a unique value assigned at the factory. In most cases, the default value is sufficient. Clicking **Default** restores the MAC address to the default value.
VLAN	Click the square if you wish to enable VLAN functionality and enable multiple broadcast domains. Once you enable VLAN, you will be able to enter a name for your network.
Reply to ICMP PING	If this field is disabled, the WAN connection will not respond to ICMP ping requests. By default, this is **enabled**.
Additional Public IP Address	The **IP Address** list represents the list of fixed Internet IP addresses assigned by the ISP, in the event that more than one Internet IP address is assigned to this WAN connection. Enter the fixed Internet IP addresses and the corresponding subnet mask, and then click the **Down Arrow** button to populate IP address entries to the **IP Address** List.

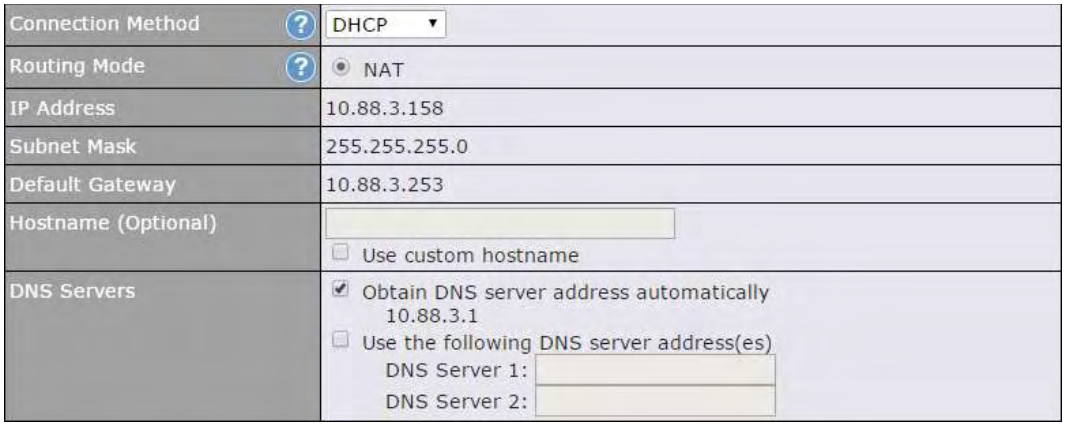
IPv6	
IPv6	IPv6 support can be enabled on one of the available Ethernet WAN ports. On this screen, you can choose which WAN will support IPv6. To enable IPv6 support on a WAN, the WAN router must respond to stateless address auto configuration advertisements and DHCPv6 requests. IPv6 clients on the LAN will acquire their IPv6, gateway, and DNS server addresses from it. The device will also acquire an IPv6 address for performing ping/traceroute checks and accepting web admin accesses. Note: This feature is only available on the Pepwave MAX 700, HD2, and HD2 IP67.

10.1.1 DHCP Connection

There are four possible connection methods:

1. DHCP
2. Static IP
3. PPPoE
4. L2TP

The DHCP connection method is suitable if the ISP provides an IP address automatically using DHCP (e.g., satellite modem, WiMAX modem, cable, Metro Ethernet, etc.).

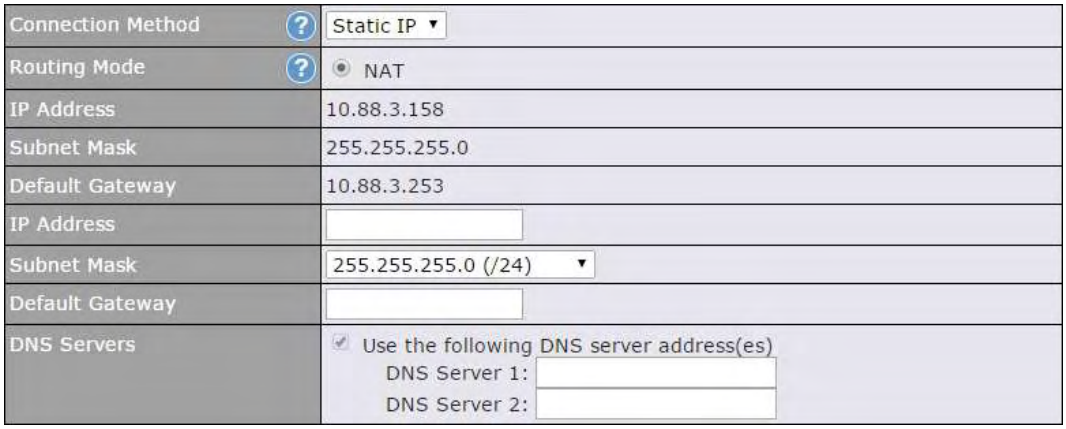


DHCP Connection Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.

IP Address/ Subnet Mask/ Default Gateway	This information is obtained from the ISP automatically.
Hostname (Optional)	If your service provider's DHCP server requires you to supply a hostname value upon acquiring an IP address, you may enter the value here. If your service provider does not provide you with the value, you can safely bypass this option.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers being assigned by the WAN DHCP server to be used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned from the DHCP server.) When **Use the following DNS server address(es)** is selected, you may enter custom DNS server addresses for this WAN connection into the **DNS Server 1** and **DNS Server 2** fields.

10.1.2 Static IP Connection

The static IP connection method is suitable if your ISP provides a static IP address to connect directly.



Static IP Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.
IP Address / Subnet Mask / Default Gateway	These settings allow you to specify the information required in order to communicate on the Internet via a fixed Internet IP address. The information is typically determined by and can be obtained from the ISP.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers being assigned by the WAN DHCP server to be used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned from the DHCP server.) When **Use the following DNS server address(es)** is

	selected, you may enter custom DNS server addresses for this WAN connection into the **DNS Server 1** and **DNS Server 2** fields.

10.1.3 PPPoE Connection

This connection method is suitable if your ISP provides a login ID/password to connect via PPPoE.

Connection Method	PPPoE
Routing Mode	NAT
IP Address	10.88.3.158
Subnet Mask	255.255.255.0
Default Gateway	10.88.3.253
PPPoE User Name	
PPPoE Password	
Confirm PPPoE Password	
Service Name (Optional)	Leave it blank unless it is provided by ISP
IP Address (Optional)	Leave it blank unless it is provided by ISP
DNS Servers	Obtain DNS server address automatically 10.88.3.1 Use the following DNS server address(es) DNS Server 1: DNS Server 2:

PPPoE Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.
IP Address / Subnet Mask / Default Gateway	This information is obtained from the ISP automatically.
PPPoE User Name / Password	Enter the required information in these fields in order to connect via PPPoE to the ISP. The parameter values are determined by and can be obtained from the ISP.
Confirm PPPoE Password	Verify your password by entering it again in this field.
Service Name (Optional)	Service name is provided by the ISP. **Note: Leave this field blank unless it is provided by your ISP.**
IP Address (Optional)	If your ISP provides a PPPoE IP address, enter it here. **Note: Leave this field blank unless it is provided by your ISP.**
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results

	in the DNS servers being assigned by the WAN DHCP server to be used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned from the DHCP server.) When **Use the following DNS server address(es)** is selected, you may enter custom DNS server addresses for this WAN connection into the **DNS Server 1** and **DNS Server 2** fields.

10.1.4 L2TP Connection

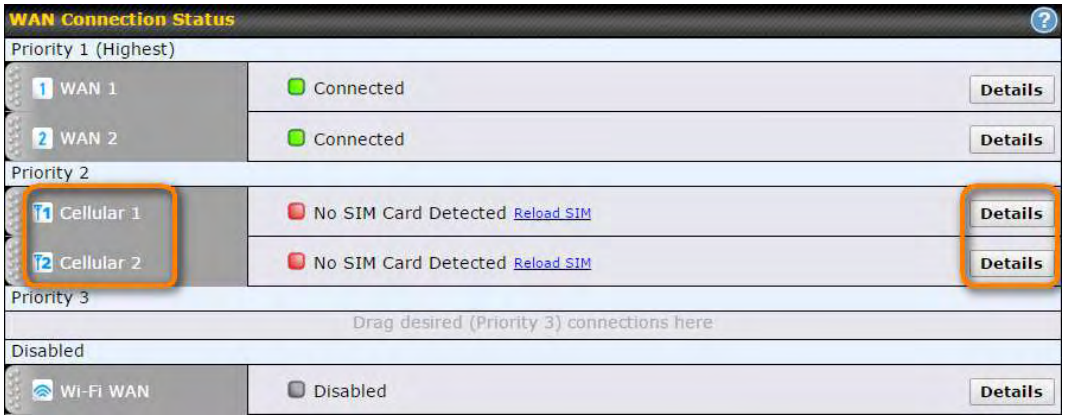
L2TP has all the compatibility and convenience of PPTP with greater security. Combine this with IPsec for a good balance between ease of use and security.

Connection Method	L2TP
Routing Mode	NAT
IP Address	10.88.3.158
Subnet Mask	255.255.255.0
Default Gateway	10.88.3.253
L2TP User Name	
L2TP Password	
Confirm L2TP Password	
Server IP Address / Host	
Address Type	Dynamic IP Static IP
DNS Servers	Obtain DNS server address automatically 10.88.3.1 Use the following DNS server address(es) DNS Server 1: DNS Server 2:

L2TP Settings	
L2TP User Name / Password	Enter the required information in these fields in order to connect via L2TP to your ISP. The parameter values are determined by and can be obtained from your ISP.
Confirm L2TP Password	Verify your password by entering it again in this field.
Server IP Address / Host	L2TP server address is a parameter which is provided by your ISP. Note: Leave this field blank unless it is provided by your ISP.
Address Type	Your ISP will also indicate whether the server IP address is Dynamic or Static. Please click the appropriate value.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers assigned by the PPPoE server to be used for outbound DNS lookups over the WAN connection. (The DNS servers are obtained along with the WAN IP address assigned from the PPPoE server.)

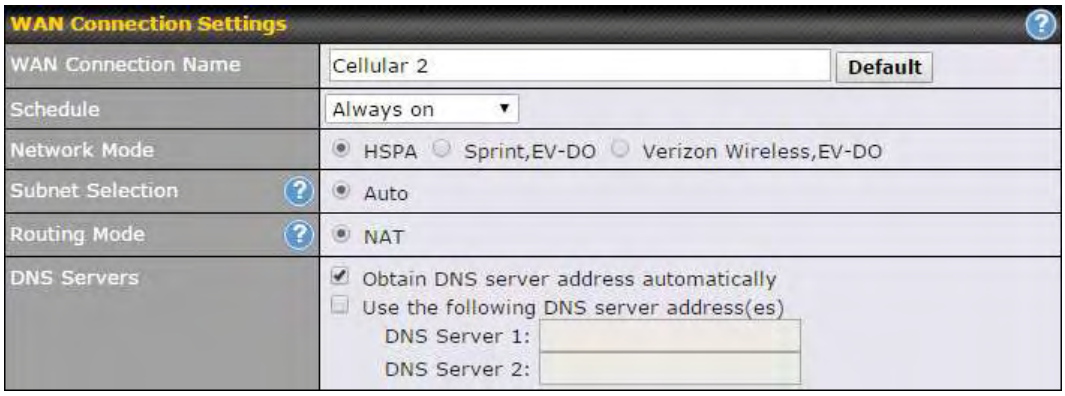
When **Use the following DNS server address(es)** is selected, you can enter custom DNS server addresses for this WAN connection into the **DNS server 1** and **DNS server 2** fields.

10.2 Cellular WAN



To access cellular WAN settings, click **Network>WAN>Details**.
(**Available on the Pepwave MAX BR1, HD2, and HD2 IP67 only)**

Cellular Status	
IMSI	This is the International Mobile Subscriber Identity which uniquely identifies the SIM card. This is applicable to 3G modems only.
MEID	Some Pepwave routers support both HSPA and EV-DO. For Sprint or Verizon Wireless EV-DO users, a unique MEID identifier code (in hexadecimal format) is used by the carrier to associate the EV-DO device with the user. This information is presented in hex and decimal format.
ESN	This serves the same purpose as MEID HEX but uses an older format.
IMEI	This is the unique ID for identifying the modem in GSM/HSPA mode.



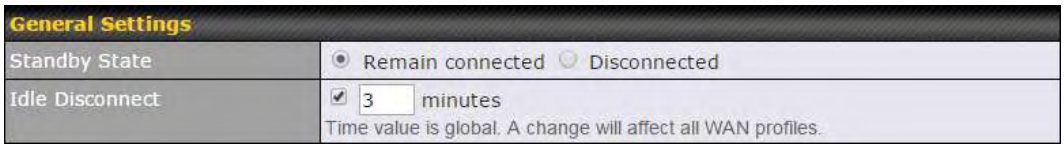
WAN Connection Settings	
WAN Connection Name	Enter a name to represent this WAN connection.
Schedule	Click the drop-down menu to apply a time schedule to this interface if needed.
Network Mode	Users have to specify the network they are on accordingly.
Subnet Selection	Auto: The subnet mask will be set automatically. Force /31 Subnet: The subnet mask will be set as 255.255.255.254(/31), and the gateway IP address will be recalculated.
Routing Mode	This option allows you to select the routing method to be used in routing IP frames via the WAN connection. The mode can be either **NAT** (network address translation) or **IP Forwarding**. Click the button to enable IP forwarding.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers assigned by the PPPoE server to be used for outbound DNS lookups over the WAN connection. (The DNS servers are obtained along with the WAN IP address assigned from the PPPoE server.) When **Use the following DNS server address(es)** is selected, you can enter custom DNS server addresses for this WAN connection into the **DNS server 1** and **DNS server 2** fields.

Cellular Settings	
Network Selection	Auto Manual
3G/2G	Auto
Authentication	Auto
Band Selection	WCDMA / HSDPA / HSUPA / HSPA+ (800 MHz) WCDMA / HSDPA / HSUPA / HSPA+ (850 MHz) WCDMA / HSDPA / HSUPA / HSPA+ (900 MHz) WCDMA / HSDPA / HSUPA / HSPA+ (1700 MHz) WCDMA / HSDPA / HSUPA / HSPA+ (1900 MHz) WCDMA / HSDPA / HSUPA / HSPA+ (2100 MHz) GSM / GPRS / EDGE (850 MHz) GSM / GPRS / EDGE (900 MHz) GSM / GPRS / EDGE (1800 MHz) GSM / GPRS / EDGE (1900 MHz)
Data Roaming	
Operator Settings	Auto Custom
APN	
Username	
Password	
SIM PIN (Optional)	
Bandwidth Allowance Monitor	Enable
Action	Disconnect when usage hits 100% Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification.
Start Day	On 1st of each month
Monthly Allowance	GB

Cellular Settings	
Network Selection	By default, the MAX router will automatically choose a network to connect to. If you wish to use only certain networks, click the button beside the menu item.
3G/2G	This drop-down menu allows restricting cellular to particular band. Click the button to enable the selection of specific bands.
Authentication	Choose from **PAP Only** or **CHAP Only** to use those authentication methods exclusively. Select **Auto** to automatically choose an authentication method.
Data Roaming	This checkbox enables data roaming on this particular SIM card. Please check your service provider's data roaming policy before proceeding.

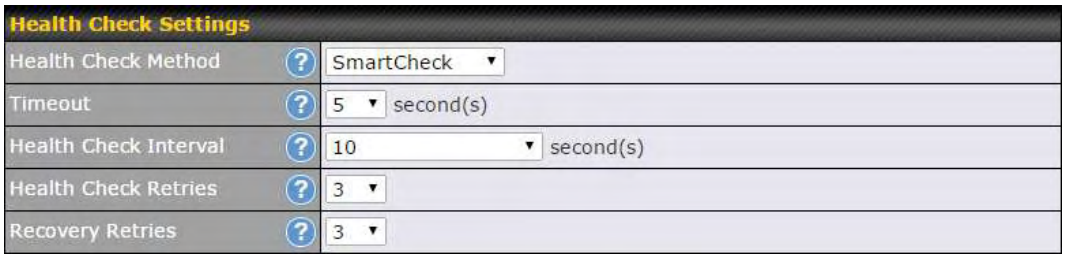
 Copyright @ 2017 Pepwave

Operator Settings	This setting applies to 3G/EDGE/GPRS modems only. It does not apply to EVDO/EVDO Rev. A modems. This allows you to configure the APN settings of your connection. If **Auto** is selected, the mobile operator should be detected automatically. The connected device will be configured and connection will be made automatically. If there is any difficulty in making connection, you may select **Custom** to enter your carrier's **APN**, **Login**, **Password**, and **Dial Number** settings manually. The correct values can be obtained from your carrier. The default and recommended setting is **Auto**.
APN / Login / Password / SIM PIN	When **Auto** is selected, the information in these fields will be filled automatically. Select **Custom** to customize these parameters. The parameter values are determined by and can be obtained from the ISP.
Bandwidth Allowance Monitor	Check the box Enable to enable bandwidth usage monitoring on this WAN connection for each billing cycle. When this option is not enabled, bandwidth usage of each month is still being tracked but no action will be taken.
Action	If email notification is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance. If **Disconnect when usage hits 100% of monthly allowance** is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume connection unless this option has been turned off or the usage has been reset when a new billing cycle starts.
Start Day	This option allows you to define which day of the month each billing cycle begins.
Monthly Allowance	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

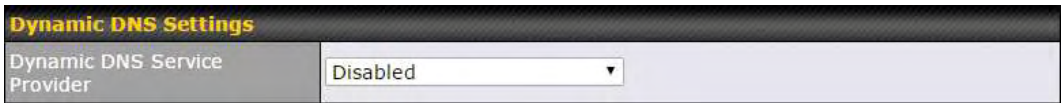


General Settings	
Standby State	This option allows you to choose whether to remain connected or disconnected when this WAN connection is no longer in the highest priority and has entered the standby state. When **Remain connected** is chosen, bringing up this WAN connection to active makes it immediately available for use.
Idle Disconnect	When Internet traffic is not detected within the user-specified timeframe, the modem will automatically disconnect. Once the traffic is resumed by the LAN host, the connection will be re-activated.

 Copyright @ 2017 Pepwave



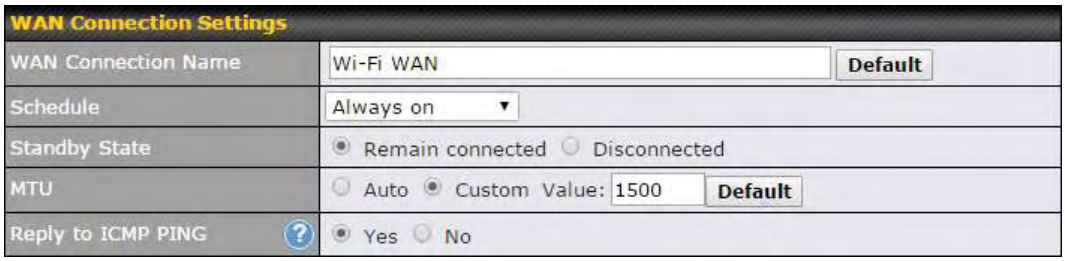
Health Check Settings	
Heath Check Method	This setting allows you to specify the health check method for the cellular connection. Available options are **Disabled, Ping, DNS Lookup, HTTP,** and **SmartCheck**. The default method is **DNS Lookup**. See **Section 10.4** for configuration details.
Timeout	If a health check test cannot be completed within the specified amount of time, the test will be treated as failed.
Health Check Interval	This is the time interval between each health check test.
Health Check Retries	This is the number of consecutive check failures before treating a connection as down.
Recovery Retries	This is the number of responses required after a health check failure before treating a connection as up again.



Dynamic DNS Settings	
Dynamic DNS Service Provider	This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers: • changeip.com • dyndns.org • no-ip.org • tzo.com • DNS-O-Matic Select **Disabled** to disable this feature. See **Section 9.5** for configuration details.

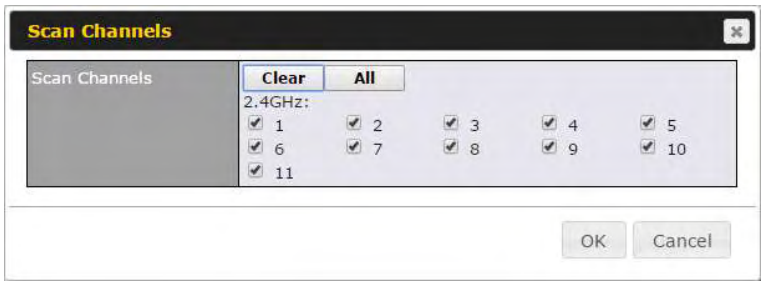
10.3 Wi-Fi WAN

To access Wi-Fi WAN settings, click **Network>WAN>Details**.

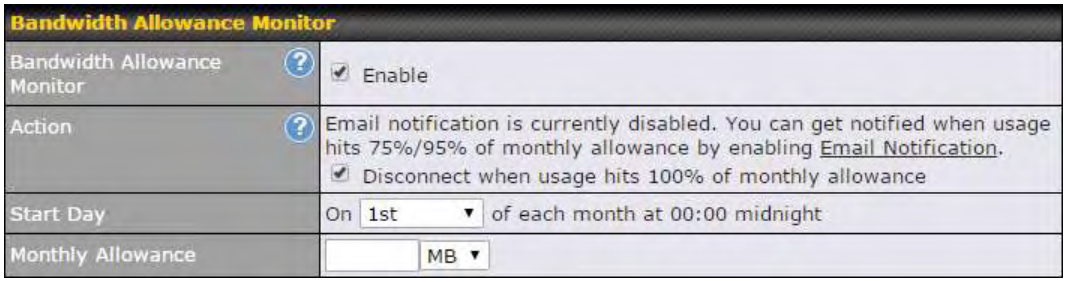


Wi-Fi Connection Settings	
WAN Connection Name	Enter a name to represent this WAN connection.
Schedule	Click the drop-down menu to apply a time schedule to this interface.
Standby State	This setting specifies the state of the WAN connection while in standby. The available options are **Remain Connected** (hot standby) and **Disconnect** (cold standby).
MTU	This setting specifies the maximum transmission unit. By default, MTU is set to **Custom 1440**. You may adjust the MTU value by editing the text field. Click **Default** to restore the default MTU value. Select **Auto** and the appropriate MTU value will be automatically detected. The auto-detection will run each time the WAN connection establishes
Reply to ICMP PING	If this setting is disabled, the WAN connection will not respond to ICMP ping requests. By default, this setting is enabled.

Wi-Fi WAN Settings	
Channel Selection	Determine whether the channel will be automatically selected. If you select custom, the following table will appear:

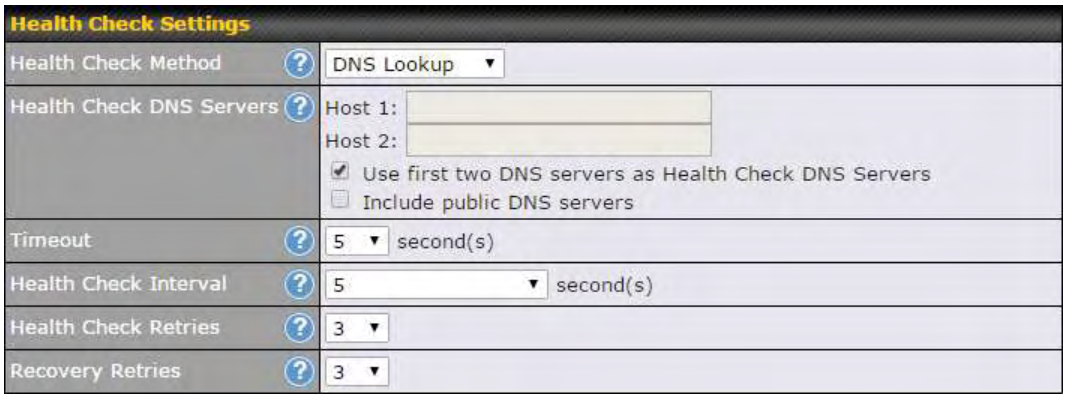


Roaming	Checking this box will enable Wi-Fi roaming. Click the icon for additional options.
Connect to Any Open Mode AP	This option is to specify whether the Wi-Fi WAN will connect to any open mode access points it finds.



Bandwidth Allowance Monitor	
Action	If **Error! Reference source not found.** is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance. If **Disconnect when usage hits 100% of monthly allowance** is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume connection unless this option has been turned off or the usage has been reset when a new billing cycle starts.
Start Day	This option allows you to define which day of the month each billing cycle begins.
Monthly Allowance	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

 Copyright @ 2017 Pepwave



Health Check Settings

Method

This setting specifies the health check method for the WAN connection. This value can be configured as **Disabled**, **PING**, **DNS Lookup**, or **HTTP**. The default method is **DNS Lookup**. For mobile Internet connections, the value of **Method** can be configured as **Disabled** or **SmartCheck**.

Health Check Disabled

When **Disabled** is chosen in the **Method** field, the WAN connection will always be considered as up. The connection will **NOT** be treated as down in the event of IP routing errors.

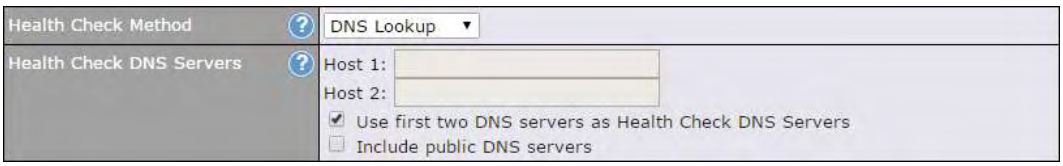
Health Check Method: PING

ICMP ping packets will be issued to test the connectivity with a configurable target IP address or hostname. A WAN connection is considered as up if ping responses are received from either one or both of the ping hosts.

PING Hosts

This setting specifies IP addresses or hostnames with which connectivity is to be tested via ICMP ping. If **Use first two DNS servers as Ping Hosts** is checked, the target ping host will be the first DNS server for the corresponding WAN connection. Reliable ping hosts with a high uptime should be considered. By default, the first two DNS servers of the WAN connection are used as the ping hosts.

Health Check Method: DNS Lookup



DNS lookups will be issued to test connectivity with target DNS servers. The connection will be treated as up if DNS responses are received from one or both of the servers, regardless of whether the result was positive or negative.

 Copyright @ 2017 Pepwave

Health Check DNS Servers	This field allows you to specify two DNS hosts' IP addresses with which connectivity is to be tested via DNS Lookup. If **Use first two DNS servers as Health Check DNS Servers** is checked, the first two DNS servers will be the DNS lookup targets for checking a connection's health. If the box is not checked, **Host 1** must be filled, while a value for **Host 2** is optional. If **Include public DNS servers** is selected and no response is received from all specified DNS servers, DNS lookups will also be issued to some public DNS servers. A WAN connection will be treated as down only if there is also no response received from the public DNS servers. Connections will be considered as up if DNS responses are received from any one of the health check DNS servers, regardless of a positive or negative result. By default, the first two DNS servers of the WAN connection are used as the health check DNS servers.

Health Check Method: HTTP

HTTP connections will be issued to test connectivity with configurable URLs and strings to match.

URL1	**WAN Settings>WAN Edit>Health Check Settings>URL1** The URL will be retrieved when performing an HTTP health check. When **String to Match** is left blank, a health check will pass if the HTTP return code is between 200 and 299 (Note: HTTP redirection codes 301 or 302 are treated as failures). When **String to Match** is filled, a health check will pass if the HTTP return code is between 200 and 299 and if the HTTP response content contains the string.
URL 2	**WAN Settings>WAN Edit>Health Check Settings>URL2** If **URL2** is also provided, a health check will pass if either one of the tests passed.

 Copyright @ 2017 Pepwave

Other Health Check Settings

Timeout	5 second(s)
Health Check Interval	5 second(s)
Health Check Retries	3
Recovery Retries	3

Timeout	This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is **5 seconds**.
Health Check Interval	This setting specifies the time interval in seconds between ping or DNS lookup requests. The default health check interval is **5 seconds**.
Health Check Retries	This setting specifies the number of consecutive ping/DNS lookup timeouts after which the Peplink Balance will treat the corresponding WAN connection as down. Default health retries is set to **3**. Using the default **Health Retries** setting of **3**, the corresponding WAN connection will be treated as down after three consecutive timeouts.
Recovery Retries	This setting specifies the number of consecutive successful ping/DNS lookup responses that must be received before the Peplink Balance treats a previously down WAN connection as up again. By default, **Recover Retries** is set to **3**. Using the default setting, a WAN connection that is treated as down will be considered as up again upon receiving three consecutive successful ping/DNS lookup responses.

Dynamic DNS Settings	
Service Provider	DNS-O-Matic
Username	
Password	
Confirm Password	
Update All Hosts	
Hosts / IDs	

Dynamic DNS Settings

Service Provider	This setting specifies the dynamic DNS service provider to be used for the WAN. Supported providers are: • changeip.com • dyndns.org • no-ip.org • tzo.com • DNS-O-Matic Select **Disabled** to disable this feature.
User ID / User / Email	This setting specifies the registered user name for the dynamic DNS service.
Password / Pass /	This setting specifies the password for the dynamic DNS service.

 Copyright @ 2017 Pepwave

TZO Key	
Update All Hosts	Check this box to automatically update all hosts.
Hosts / Domain	This setting specifies a list of hostnames or domains to be associated with the public Internet IP address of the WAN connection.

Important Note
In order to use dynamic DNS services, appropriate hostname registration(s), as well as a valid account with a supported dynamic DNS service provider, are required. A dynamic DNS update is performed whenever a WAN's IP address is changed, such as when an IP is changed after a DHCP IP refresh or reconnection. Due to dynamic DNS service providers' policies, a dynamic DNS host expires automatically when the host record has not been not updated for a long time. Therefore, the Peplink Balance performs an update every 23 days, even if a WAN's IP address did not change.

10.3.1 Creating Wi-Fi Connection Profiles

You can manually create a profile to connect to a Wi-Fi connection. This is useful for creating a profile for connecting to hidden-SSID access points. Click **Network>WAN>Details>Create Profile…** to get started.

This will open a window similar to the one shown below:

Wi-Fi Connection Profile Settings	
Type	Select whether the network will connect automatically or manually.
Network Name (SSID)	Enter a name to represent this Wi-Fi connection.
Security	This option allows you to select which security policy is used for this wireless network. Available options: • **Open** • **WEP** • **WPA/WPA2 – Personal** • **WPA/WPA2 – Enterprise**

Open

Security	Open

WEP

Security	WEP
Encryption Key	Hide Characters

WPA/WPA2 – Personal

Security	WPA/WPA2-Personal
Shared Key	Hide Characters

WPA/WPA2 – Enterprise

Security	WPA/WPA2-Enterprise
Login ID	
Password	
Confirm Password	
EAP Method	PEAP
EAP Phase 2 Method	EAP/CHAP
EAP outer authentication identity	Anonymous User Credentials Other:

10.4 WAN Health Check

To ensure traffic is routed to healthy WAN connections only, the Pepwave router can periodically check the health of each WAN connection. The health check settings for each WAN connection can be independently configured via **Network>WAN>Details**.

Health Check Settings	
Method	This setting specifies the health check method for the WAN connection. This value can be configured as **Disabled**, **PING**, **DNS Lookup**, or **HTTP**. The default method is **DNS Lookup**. For mobile Internet connections, the value of **Method** can be configured as **Disabled** or **SmartCheck**.
Health Check Disabled	

Health Check Method	Disabled Health Check disabled. Network problem cannot be detected.

When **Disabled** is chosen in the **Method** field, the WAN connection will always be considered as up. The connection will **NOT** be treated as down in the event of IP routing errors.

Health Check Method: PING

Health Check Method	PING
PING Hosts	Host 1: Host 2: ☑ Use first two DNS servers as PING Hosts

ICMP ping packets will be issued to test the connectivity with a configurable target IP address or hostname. A WAN connection is considered as up if ping responses are received from either one or both of the ping hosts.

PING Hosts	This setting specifies IP addresses or hostnames with which connectivity is to be tested via ICMP ping. If **Use first two DNS servers as Ping Hosts** is checked, the target ping host will be the first DNS server for the corresponding WAN connection. Reliable ping hosts with a high uptime should be considered. By default, the first two DNS servers of the WAN connection are used as the ping hosts.

Health Check Method: DNS Lookup

Health Check Method	DNS Lookup
Health Check DNS Servers	Host 1: Host 2: ☑ Use first two DNS servers as Health Check DNS Servers ☐ Include public DNS servers

DNS lookups will be issued to test connectivity with target DNS servers. The connection will be treated as up if DNS responses are received from one or both of the servers, regardless of whether the result was positive or negative.

Health Check DNS Servers	This field allows you to specify two DNS hosts' IP addresses with which connectivity is to be tested via DNS lookup. If **Use first two DNS servers as Health Check DNS Servers** is checked, the first two DNS servers will be the DNS lookup targets for checking a connection's health. If the box is not checked, **Host 1** must be filled, while a value for **Host 2** is optional. If **Include public DNS servers** is selected and no response is received from all specified DNS servers, DNS lookups will also be issued to some public DNS servers. A WAN connection will be treated as down only if there is also no response received from the public DNS servers. Connections will be considered as up if DNS responses are received from any one of the health check DNS servers, regardless of a positive or negative result. By default, the first two DNS servers of the WAN connection are used as the health check DNS servers.

Health Check Method: HTTP

Health Check Method	HTTP
URL 1	http:// Matching String: ☐
URL 2	http:// Matching String: ☐

HTTP connections will be issued to test connectivity with configurable URLs and strings to match.

URL1	**WAN Settings>WAN Edit>Health Check Settings>URL1** The URL will be retrieved when performing an HTTP health check. When **String to Match** is left blank, a health check will pass if the HTTP return code is between 200 and 299 (Note: HTTP redirection codes 301 or 302 are treated as failures). When **String to Match** is

 Copyright @ 2017 Pepwave

	filled, a health check will pass if the HTTP return code is between 200 and 299 and if the HTTP response content contains the string.
URL 2	**WAN Settings>WAN Edit>Health Check Settings>URL2** If **URL2** is also provided, a health check will pass if either one of the tests passed.

Timeout	10 second(s)
Health Check Interval	5 second(s)
Health Check Retries	3
Recovery Retries	3

Other Health Check Settings	
Timeout	This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is **5 seconds**.
Health Check Interval	This setting specifies the time interval in seconds between ping or DNS lookup requests. The default health check interval is **5 seconds**.
Health Check Retries	This setting specifies the number of consecutive ping/DNS lookup timeouts after which the Pepwave router will treat the corresponding WAN connection as down. Default health retries is set to **3**. Using the default **Health Retries** setting of **3**, the corresponding WAN connection will be treated as down after three consecutive timeouts.
Recovery Retries	This setting specifies the number of consecutive successful ping/DNS lookup responses that must be received before the Pepwave router treats a previously down WAN connection as up again. By default, **Recover Retries** is set to **3**. Using the default setting, a WAN connection that is treated as down will be considered as up again upon receiving three consecutive successful ping/DNS lookup responses.

Automatic Public DNS Server Check on DNS Test Failure

When the health check method is set to **DNS Lookup** and health checks fail, the Pepwave router will automatically perform DNS lookups on public DNS servers. If the tests are successful, the WAN may not be down, but rather the target DNS server malfunctioned. You will see the following warning message on the main page:

Failed to receive DNS response from the health-check DNS servers for WAN connection 3. But public DNS server lookup test via the WAN passed. So please check the DNS server settings.

10.5 Dynamic DNS Settings

Pepwave routers are capable of registering the domain name relationships to dynamic DNS service providers. Through registration with dynamic DNS service provider(s), the default public Internet IP address of each WAN connection can be associated with a host name. With dynamic DNS service enabled for a WAN connection, you can connect to your WAN's IP address from the external, even if its IP address is dynamic. You must register for an account from the listed dynamic DNS service providers before enabling this option.

If the WAN connection's IP address is a reserved private IP address (i.e., behind a NAT

router), the public IP of each WAN will be automatically reported to the DNS service provider.

Either upon a change in IP addresses or every 23 days without link reconnection, the Pepwave router will connect to the dynamic DNS service provider to perform an IP address update within the provider's records.

The settings for dynamic DNS service provider(s) and the association of hostname(s) are configured via **Network>WAN>Details>Dynamic DNS Service Provider/Dynamic DNS Settings**.

Dynamic DNS Service Provider	changeip.com
User ID	
Password	
Confirm Password	
Hosts	

Dynamic DNS Settings	
Dynamic DNS	This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers: • changeip.com • dyndns.org • no-ip.org • tzo.com • DNS-O-Matic • Others… Support custom Dynamic DNS servers by entering its URL. Works with any service compatible with DynDNS API. Select **Disabled** to disable this feature.
Account Name / Email Address	This setting specifies the registered user name for the dynamic DNS service.
Password / TZO Key	This setting specifies the password for the dynamic DNS service.
Hosts / Domain	This field allows you to specify a list of host names or domains to be associated with the public Internet IP address of the WAN connection. If you need to enter more than one host, use a carriage return to separate them.

Important Note
In order to use dynamic DNS services, appropriate host name registration(s) and a valid account with a supported dynamic DNS service provider are required. A dynamic DNS update is performed whenever a WAN's IP address changes (e.g., the IP is changed after a DHCP IP refresh, reconnection, etc.). Due to dynamic DNS service

providers' policy, a dynamic DNS host will automatically expire if the host record has not been updated for a long time. Therefore the Pepwave router performs an update every 23 days, even if a WAN's IP address has not changed.

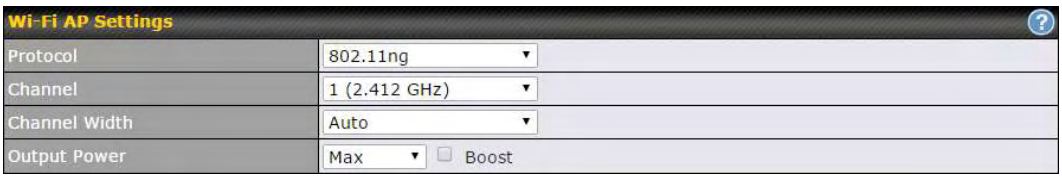
 Copyright @ 2017 Pepwave

11 Advanced Wi-Fi Settings

Wi-Fi settings can be configured at **Advanced>Wi-Fi Settings** (or **AP>Settings** on some models). Note that menus displayed can vary by model.

Wi-Fi Radio Settings

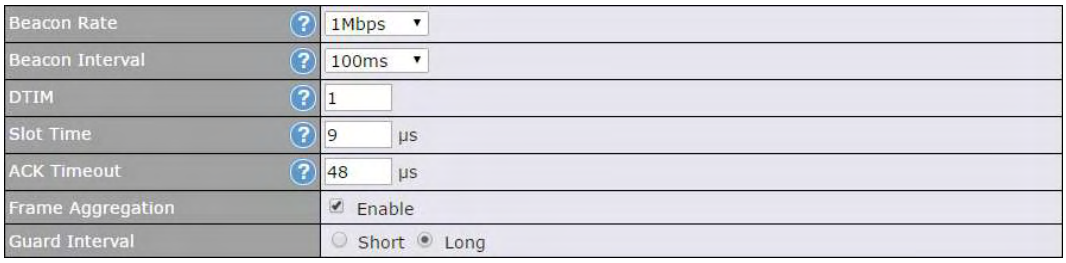
Important Note



Wi-Fi AP Settings	
Protocol	This option allows you to specify whether 802.11b and/or 802.11g client association requests will be accepted. Available options are **802.11ng** and **802.11na**. By default, **802.11ng** is selected.
Channel	This option allows you to select which 802.11 RF channel will be utilized. **Channel 1 (2.412 GHz)** is selected by default.
Channel Width	Available options are **20 MHz**, **40 MHz**, and **Auto (20/40 MHz)** . Default is **Auto (20/40 MHz),** which allows both widths to be used simultaneously.
Output Power	This option is for specifying the transmission output power for the Wi-Fi AP. There are 4 relative power levels available – **Max**, **High**, **Mid**, and **Low**. The actual output power will be bound by the regulatory limits of the selected country.

 Copyright @ 2017 Pepwave

Advanced Wi-Fi AP settings can be displayed by clicking the on the top right-hand corner of the **Wi-Fi AP Settings** section, which can be found at **AP>Settings**. Other models will display a separate section called **Wi-Fi AP Advanced Settings**, which can be found at **Advanced>Wi-Fi Settings**.

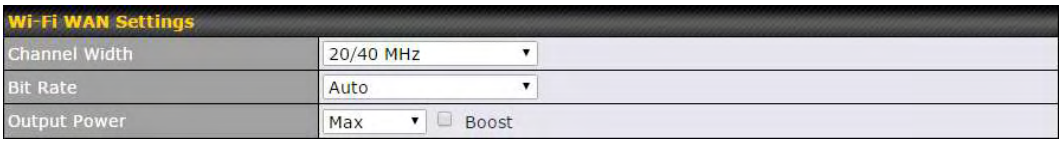


Wi-Fi AP Advanced Settings	
Beacon Rate [A]	This option is for setting the transmit bit rate for sending a beacon. By default, **1Mbps** is selected.
Beacon Interval [A]	This option is for setting the time interval between each beacon. By default, **100ms** is selected.
DTIM [A]	This field allows you to set the frequency for the beacon to include delivery traffic indication messages. The interval is measured in milliseconds. The default value is set to **1 ms**.
Slot Time [A]	This field is for specifying the unit wait time before transmitting a packet. By default, this field is set to **9 µs**.
ACK Timeout [A]	This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to **48 µs**.
Frame Aggregation [A]	This option allows you to enable frame aggregation to increase transmission throughput.
Guard Interval [A]	This is where you opt for a short or long guard period interval for your transmissions.

[A] - Advanced feature, please click the button on the top right-hand corner to activate.

 Copyright @ 2017 Pepwave

Wi-Fi WAN settings can be configured at **Advanced>Wi-Fi Settings** (or **Advanced>Wi-Fi WAN** or some models).



Wi-Fi WAN Settings	
Channel Width	Available options are **20/40 MHz** and **20 MHz**. Default is **20/40 MHz,** which allows both widths to be used simultaneously.
Bit Rate	This option allows you to select a specific bit rate for data transfer over the device's Wi-Fi network. By default, **Auto** is selected.
Output Power	This option is for specifying the transmission output power for the Wi-Fi AP. There are 4 relative power levels available – **Max**, **High**, **Mid**, and **Low**. The actual output power will be bound by the regulatory limits of the selected country. Note that selecting the **Boost** option may cause the MAX's radio output to exceed local regulatory limits.

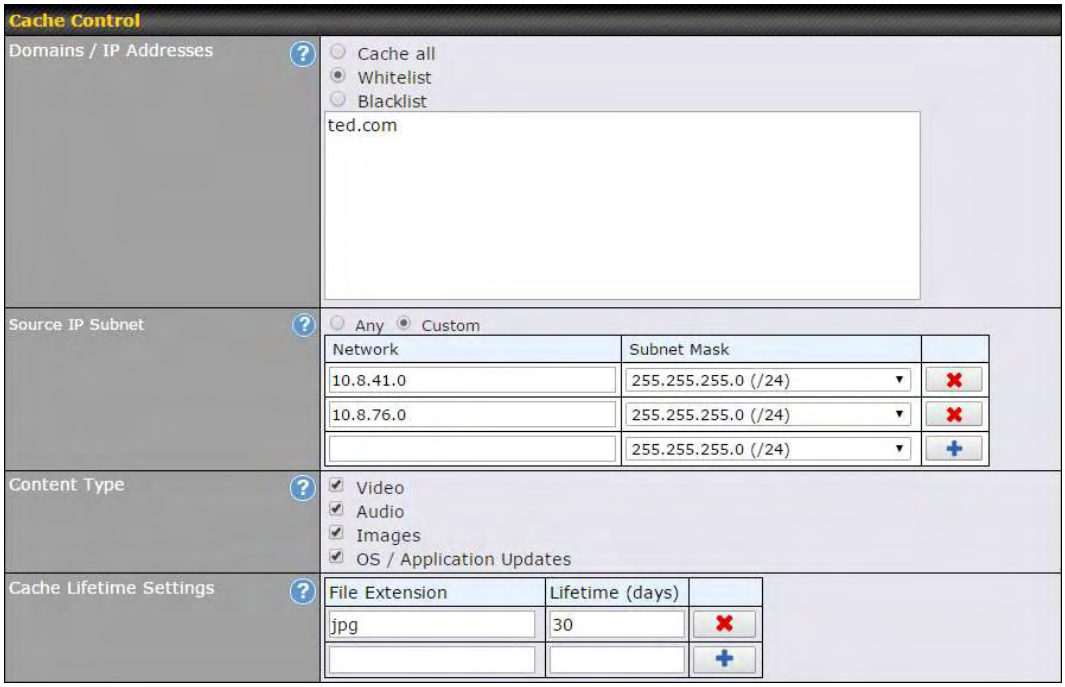
 Copyright @ 2017 Pepwave

12 MediaFast Configuration

MediaFast settings can be configured from the **Network** menu.

12.1 Setting Up MediaFast Content Caching

To access MediaFast content caching settings, select **Advanced>Cache Control**.

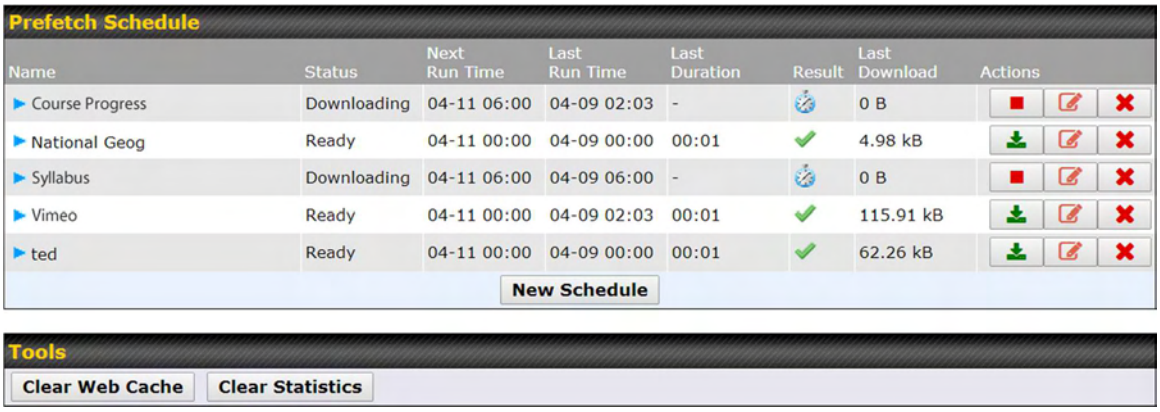


Cache Control Settings	
Domain	Choose to **Cache on all domains**, or enter domain names and then choose either **Cache the specified domains only** or **Do not cache the specified domains**.
Source IP Subnet	This setting allows caching to be applied to the user-specified IP subnets. If "Any" is selected, then caching will apply to all subnets.
Content Type	Check these boxes to cache the listed content types or leave boxes unchecked to disable caching for the listed types.
Cache Lifetime Settings	Enter a file extension, such as JPG or DOC. Then enter a lifetime in days to specify how long files with that extension will be cached. Add or delete entries using the controls on the right.

 Copyright @ 2017 Pepwave

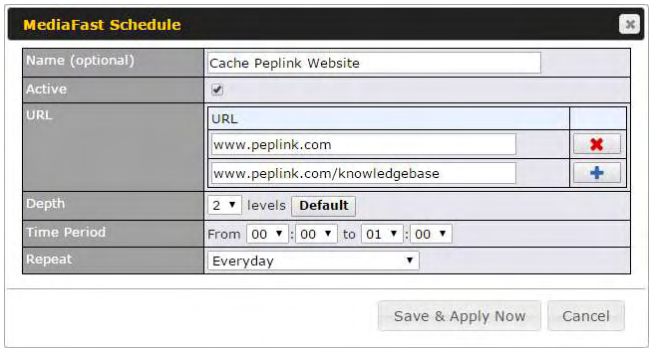
12.2 Scheduling Content Prefetching

Content prefetching allows you to download content on a schedule that you define, which can help to preserve network bandwidth during busy times and keep costs down. To access MediaFast content prefetching settings, select **Advanced >Prefetch Schedule**.



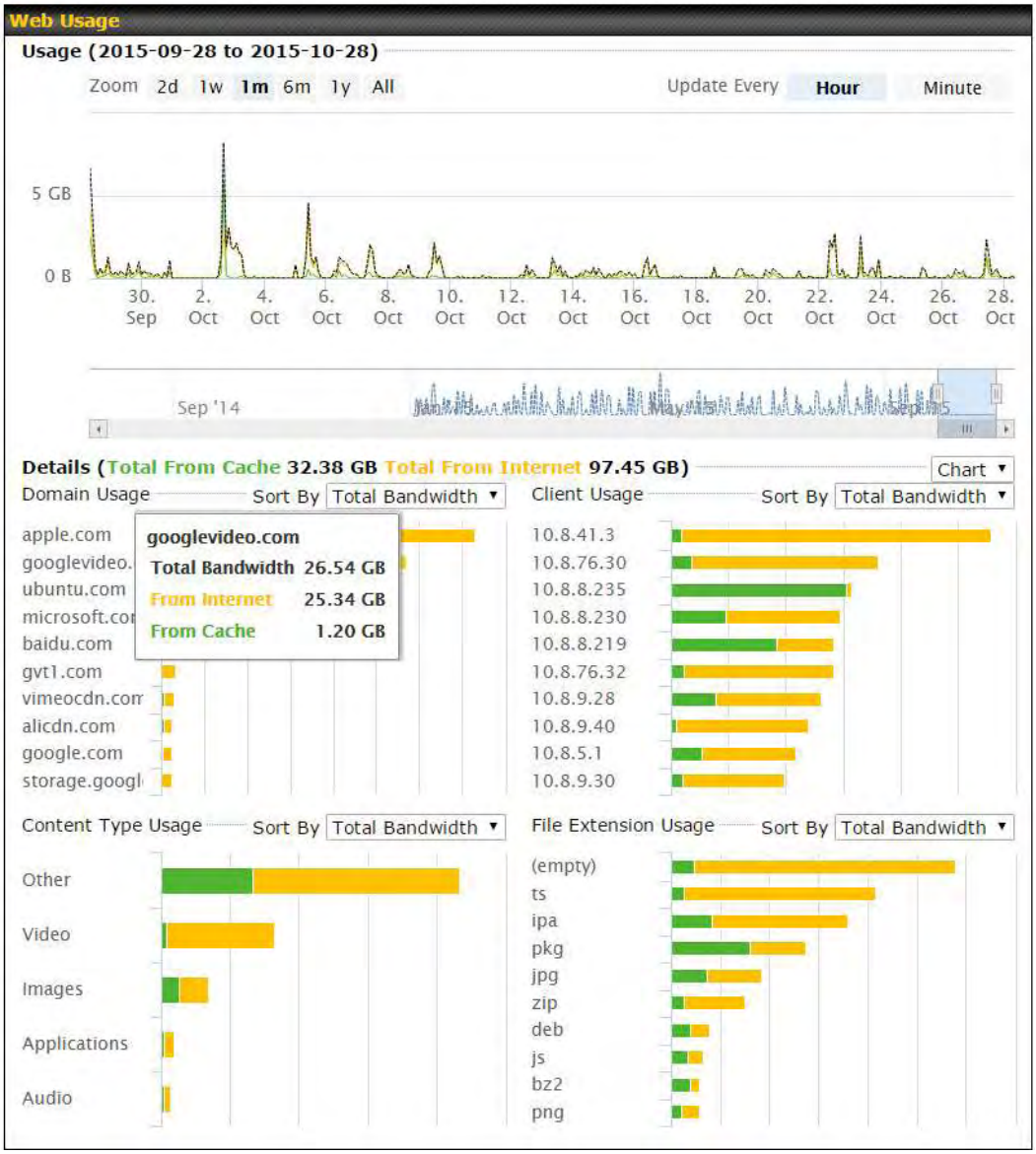
Prefetch Schedule Settings	
Name	This field displays the name given to the scheduled download.
Status	Check the status of your scheduled download here.
Next Run Time/Last Run Time	These fields display the date and time of the next and most recent occurrences of the scheduled download.
Last Duration	Check this field to ensure that the most recent download took as long as expected to complete. A value that is too low might indicate an incomplete download or incorrectly specified download target, while a value that is too long could mean a download with an incorrectly specified target or stop time.
Result	This field indicates whether downloads are in progress ( ) or complete ( ).
Last Download	Check this field to ensure that the most recent download file size is within the expected range. A value that is too low might indicate an incomplete download or incorrectly specified download target, while a value that is too long could mean a download with an incorrectly specified target or stop time. This field is also useful for quickly seeing which downloads are consuming the most storage space.

 Copyright @ 2017 Pepwave

Actions	To begin a scheduled download immediately, click . To cancel a scheduled download, click . To edit a scheduled download, click . To delete a scheduled download, click .
New Schedule	Click to begin creating a new scheduled download. Clicking the button will cause the following screen to appear:  Simply provide the requested information to create your schedule.
Clear Web Cache	To clear all cached content, click this button. Note that this action cannot be undone.
Clear Statistics	To clear all prefetch and status page statistics, click this button.

12.3 Viewing MediaFast Statistics

To get details on storage and bandwidth usage, select **Status>MediaFast**.


Web Usage
Usage (2015-09-28 to 2015-10-28)
Zoom 2d 1w 1m 6m 1y All
Update Every Hour Minute
5 GB
0 B
30. Sep
2. Oct
4. Oct
6. Oct
8. Oct
10. Oct
12. Oct
14. Oct
16. Oct
18. Oct
20. Oct
22. Oct
24. Oct
26. Oct
28. Oct
Sep '14
Details (Total From Cache 32.38 GB Total From Internet 97.45 GB)
Chart
Domain Usage
Sort By Total Bandwidth
apple.com
googlevideo.com
ubuntu.com
microsoft.com
baidu.com
gvt1.com
vimeocdn.com
alicdn.com
google.com
storage.google
googlevideo.com
Total Bandwidth 26.54 GB
From Internet 25.34 GB
From Cache 1.20 GB
Client Usage
Sort By Total Bandwidth
10.8.41.3
10.8.76.30
10.8.8.235
10.8.8.230
10.8.8.219
10.8.76.32
10.8.9.28
10.8.9.40
10.8.5.1
10.8.9.30
Content Type Usage
Sort By Total Bandwidth
Other
Video
Images
Applications
Audio
File Extension Usage
Sort By Total Bandwidth
(empty)
ts
ipa
pkg
jpg
zip
deb
js
bz2
png

13 Bandwidth Bonding SpeedFusion™ / PepVPN

Pepwave bandwidth bonding SpeedFusionTM is our patented technology that enables our SD-WAN routers to bond multiple Internet connections to increase site-to-site bandwidth and reliability. SpeedFusion functionality securely connects your Pepwave router to another Pepwave or Peplink device (Peplink Balance 210/310/380/580/710/1350 only). Data, voice, or video communications between these locations are kept confidential across the public Internet.

Bandwidth bonding SpeedFusion™ is specifically designed for multi-WAN environments. In case of failures and network congestion at one or more WANs, other WANs can be used to continue carrying the network traffic.

Different models of our SD-WAN routers have different numbers of site-to-site connections allowed. End-users who need to have more site-to-site connections can purchase a SpeedFusion license to increase the number of site-to-site connections allowed.

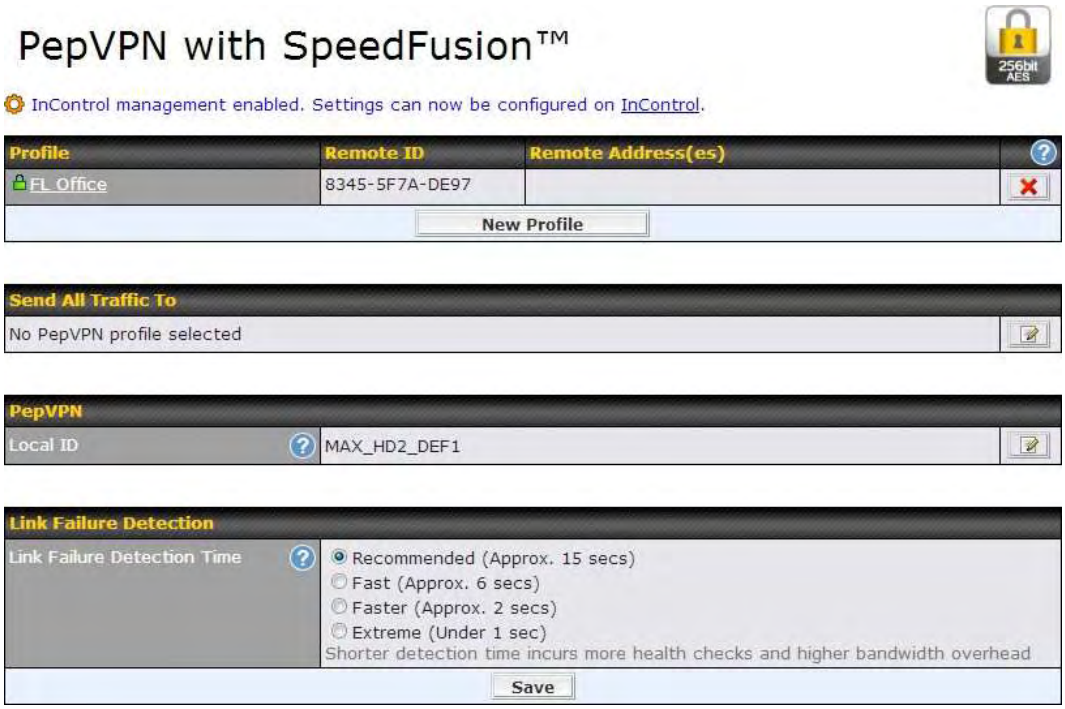
Pepwave routers can aggregate all WAN connections' bandwidth for routing SpeedFusion™ traffic. Unless all the WAN connections of one site are down, Pepwave routers can keep the VPN up and running.

VPN bandwidth bonding is supported in Firmware 5.1 or above. All available bandwidth will be utilized to establish the VPN tunnel, and all traffic will be load balanced at packet level across all links. VPN bandwidth bonding is enabled by default.

 Copyright @ 2017 Pepwave

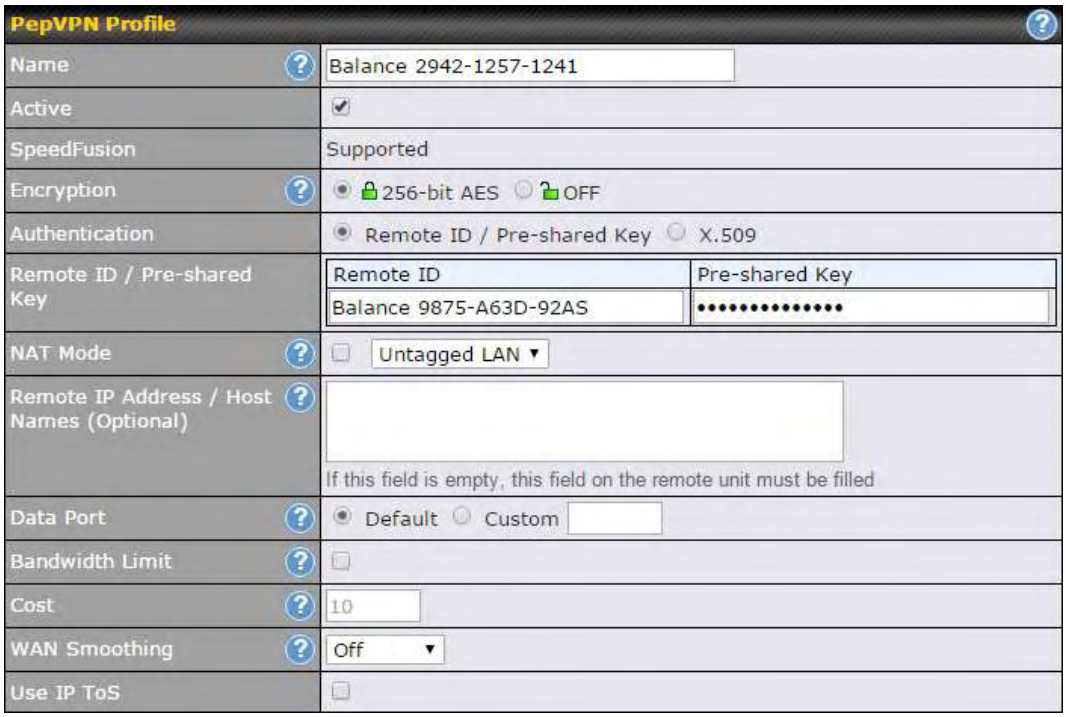
13.1 PepVPN

To configure PepVPN and SpeedFusion, navigate to **Advanced>SpeedFusion™** or **Advanced>PepVPN**.



The local LAN subnet and subnets behind the LAN (defined under **Static Route** on the LAN settings page) will be advertised to the VPN. All VPN members (branch offices and headquarters) will be able to route to local subnets.
Note that all LAN subnets and the subnets behind them must be unique. Otherwise, VPN members will not be able to access each other.

All data can be routed over the VPN using the 256-bit AES encryption standard. To configure, navigate to **Advanced>SpeedFusion™** or **Advanced>PepVPN** and click the **New Profile** button to create a new VPN profile (you may have to first save the displayed default profile in order to acesss the **New Profile** button). Each profile specifies the settings for making VPN connection with one remote Pepwave or Peplink device. Note that available settings vary by model.



A list of defined SpeedFusion connection profiles and a **Link Failure Detection Time** option will be shown. Click the **New Profile** button to create a new VPN connection profile for making a VPN connection to a remote Peplink Balance via the available WAN connections. Each profile is for making a VPN connection with one remote Peplink Balance.

PepVPN Profile Settings	
Name	This field is for specifying a name to represent this profile. The name can be any combination of alphanumeric characters (0-9, A-Z, a-z), underscores (_), dashes (-), and/or non-leading/trailing spaces ( ).
Active	When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled.
Encryption	By default, VPN traffic is encrypted with **256-bit AES**. If **Off** is selected on both sides of a VPN connection, no encryption will be applied.
Authentication	Select from **By Remote ID Only**, **Preshared Key**, or **X.509** to specify the method the Peplink Balance will use to authenticate peers. When selecting **By Remote ID Only**, be sure to enter a unique peer ID number in the **Remote ID** field.
Remote ID / Pre-shared Key	This optional field becomes available when **Remote ID / Pre-shared Key** is selected as the Peplink Balance's VPN **Authentication** method, as explained above. **Pre-shared Key** defines the pre-shared key used for this particular VPN connection. The VPN connection's session key will be further protected by the pre-shared key. The connection will be up only if the pre-shared keys on each side match. When the peer is running firmware 5.0+, this setting will be ignored.

	Enter Remote IDs either by typing out each Remote ID and Pre-shared Key, or by pasting a CSV. If you wish to paste a CSV, click the icon next to the "Remote ID / Preshared Key" setting.
Remote ID/Remote Certificate	These optional fields become available when **X.509** is selected as the Peplink Balance's VPN authentication method, as explained above. To authenticate VPN connections using X.509 certificates, copy and paste certificate details into these fields. To get more information on a listed X.509 certificate, click the **Show Details** link below the field.
Allow Shared Remote ID	When this option is enabled, the router will allow multiple peers to run using the same remote ID.
NAT Mode	Check this box to allow the local DHCP server to assign an IP address to the remote peer. When **NAT Mode** is enabled, all remote traffic over the VPN will be tagged with the assigned IP address using network address translation.
Remote IP Address / Host Names (Optional)	If **NAT Mode** is not enabled, you can enter a remote peer's WAN IP address or hostname(s) here. If the remote uses more than one address, enter only one of them here. Multiple hostnames are allowed and can be separated by a space character or carriage return. Dynamic-DNS host names are also accepted. This field is optional. With this field filled, the Peplink Balance will initiate connection to each of the remote IP addresses until it succeeds in making a connection. If the field is empty, the Peplink Balance will wait for connection from the remote peer. Therefore, at least one of the two VPN peers must specify this value. Otherwise, VPN connections cannot be established.
Data Port	This field is used to specify a UDP port number for transporting outgoing VPN data. If **Default** is selected, UDP port 4500 will be used. Port 32015 will be used if the remote unit uses Firmware prior to version 5.4 or if port 4500 is unavailable. If **Custom** is selected, enter an outgoing port number from 1 to 65535.
Bandwidth Limit	Define maximum download and upload speed to each individual peer. This functionality requires the peer to use PepVPN version 4.0.0 or above.
Cost	Define path cost for this profile. OSPF will determine the best route through the network using the assigned cost. Default: 10
WAN Smoothing[A]	Select the degree to which WAN Smoothing will be implemented across your WAN links.

[A] - Advanced feature, please click the button on the top right-hand corner to activate.

To enable Layer 2 Bridging between PepVPN profiles, navigate to **Network>LAN>Basic Settings>*LAN Profile Name*** and refer to instructions in section 9.1

WAN Connection Priority

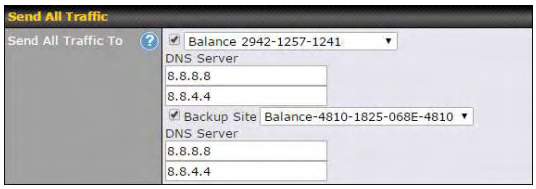
WAN Connection Priority

If your device supports it, you can specify the priority of WAN connections to be used for making VPN connections. WAN connections set to **OFF** will never be used. Only available WAN connections with the highest priority will be used.

To enable asymmetric connections, connection mapping to remote WANs, cut-off latency, and packet loss suspension time, click the button.

Send All Traffic To

This feature allows you to redirect all traffic to a specified PepVPN connection. Click the button to select your connection and the following menu will appear:



You could also specify a DNS server to resolve incoming DNS requests. Click the checkbox next to **Backup Site** to designate a backup SpeedFusion profile that will take over, should the main PepVPN connection fail.

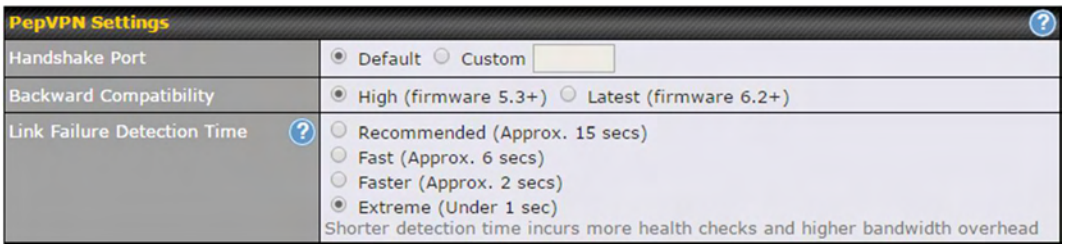
Outbound Policy/PepVPN Outbound Custom Rules

Some models allow you to set outbound policy and custom outbound rules from **Advanced>PepVPN**. See **Section 14** for more information on outbound policy settings.

 Copyright @ 2017 Pepwave

PepVPN Local ID

The local ID is a text string to identify this local unit when establishing a VPN connection. When creating a profile on a remote unit, this local ID must be entered in the remote unit's **Remote ID** field. Click the icon to edit **Local ID**.



PepVPN Settings

Handshake Port[A]	To designate a custom handshake port (TCP), click the **custom** radio button and enter the port number you wish to designate.
Backward Compatibility	Determine the level of backward compatibility needed for PepVPN tunnels. The use of the **Latest** setting is recommended as it will improve the performance and resilience of SpeedFusion connections.
Link Failure Detection Time	The bonded VPN can detect routing failures on the path between two sites over each WAN connection. Failed WAN connections will not be used to route VPN traffic. Health check packets are sent to the remote unit to detect any failure. The more frequently checks are sent, the shorter the detection time, although more bandwidth will be consumed. When **Recommended** (default) is selected, a health check packet is sent every five seconds, and the expected detection time is 15 seconds. When **Fast** is selected, a health check packet is sent every three seconds, and the expected detection time is six seconds. When **Faster** is selected, a health check packet is sent every second, and the expected detection time is two seconds. When **Extreme** is selected, a health check packet is sent every 0.1 second, and the expected detection time is less than one second.

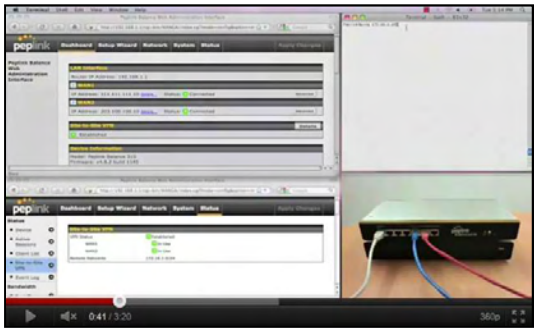
[A] - Advanced feature, please click the button on the top right-hand corner to activate.

Important Note

Peplink proprietary SpeedFusion™ uses TCP port 32015 and UDP port 4500 for establishing VPN connections. If you have a firewall in front of your Pepwave devices, you will need to add firewall rules for these ports and protocols to allow inbound and outbound traffic to pass through the firewall.

Tip

Want to know more about VPN sub-second session failover? Visit our YouTube Channel for a video tutorial!



http://youtu.be/TLQgdpPSY88

 Copyright @ 2017 Pepwave

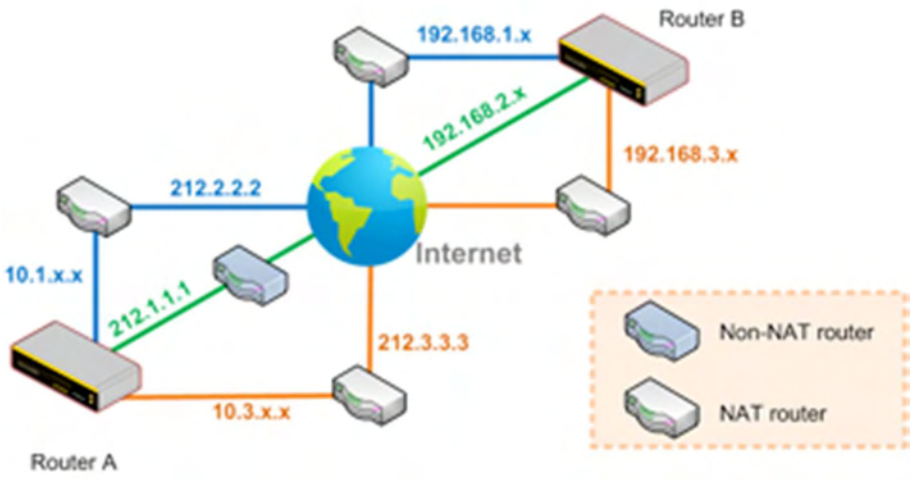
13.2 The Pepwave Router Behind a NAT Router

Pepwave routers support establishing SpeedFusion™ over WAN connections which are behind a NAT (network address translation) router.

To enable a WAN connection behind a NAT router to accept VPN connections, you can configure the NAT router in front of the WAN connection to inbound port-forward TCP port 32015 to the Pepwave router.

If one or more WAN connections on Unit A can accept VPN connections (by means of port forwarding or not), while none of the WAN connections on the peer Unit B can do so, you should enter all of Unit A's public IP addresses or hostnames into Unit B's **Remote IP Addresses / Host Names** field. Leave the field in Unit A blank. With this setting, a SpeedFusion™ connection can be set up and all WAN connections on both sides will be utilized.

See the following diagram for an example of this setup in use:

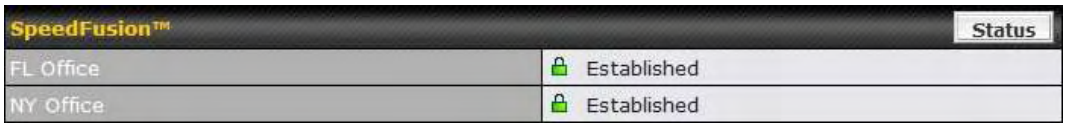


One of the WANs connected to Router A is non-NAT'd (*212.1.1.1*). The rest of the WANs connected to Router A and all WANs connected to Router B are NAT'd. In this case, the **Peer IP Addresses / Host Names** field for Router B should be filled with all of Router A's hostnames or public IP addresses (i.e., *212.1.1.1*, *212.2.2.2*, and *212.3.3.3*), and the field in Router A can be left blank. The two NAT routers on WAN1 and WAN3 connected to Router A should inbound port-forward TCP port 32015 to Router A so that all WANs will be utilized in establishing the VPN.

 Copyright @ 2017 Pepwave

13.3 SpeedFusion™ Status

SpeedFusion™ status is shown in the **Dashboard**. The connection status of each connection profile is shown as below.



After clicking the **Status** button at the top right corner of the SpeedFusion™ table, you will be forwarded to **Status>SpeedFusion™**, where you can view subnet and WAN connection information for each VPN peer. Please refer to **Section 22.6** for details.

IP Subnets Must Be Unique Among VPN Peers
The entire interconnected SpeedFusion™ network is a single non-NAT IP network. Avoid duplicating subnets in your sites to prevent connectivity problems when accessing those subnets.

14 IPsec VPN

IPsec VPN functionality securely connects one or more branch offices to your company's main headquarters or to other branches. Data, voice, and video communications between these locations are kept safe and confidential across the public Internet.

IPsec VPN on Pepwave routers is specially designed for multi-WAN environments. For instance, if a user sets up multiple IPsec profiles for a multi-WAN environment and WAN1 is connected and healthy, IPsec traffic will go through this link. However, should unforeseen problems (e.g., unplugged cables or ISP problems) cause WAN1 to go down, our IPsec implementation will make use of WAN2 and WAN3 for failover.

14.1 IPsec VPN Settings

Many Pepwave products can make multiple IPsec VPN connections with Peplink, Pepwave, Cisco, and Juniper routers. Note that all LAN subnets and the subnets behind them must be unique. Otherwise, VPN members will not be able to access each other. All data can be routed over the VPN with a selection of encryption standards, such as 3DES, AES-128, and AES-256. To configure IPsec VPN on Pepwave devices that support it, navigate to **Advanced>IPsec VPN.**

A **NAT-Traversal** option and list of defined **IPsec VPN** profiles will be shown. **NAT-Traversal** should be enabled if your system is behind a NAT router. Click the **New Profile** button to create new IPsec VPN profiles that make VPN connections to remote Pepwave, Cisco, or Juniper routers via available WAN connections. To edit any of the profiles, click on its associated connection name in the leftmost column.

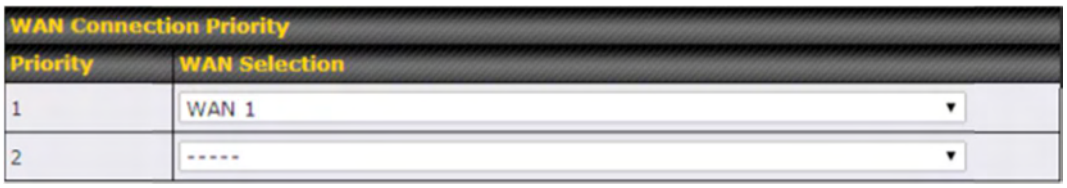
Name	Profile 1
Active	☑
Connect Upon Disconnection of	☑ WAN 2
Remote Gateway IP Address / Host Name	12.12.12.12
Local Networks	Propose the following networks to remote gateway: ☐ *172.16.1.1/24* ☐ 172.16.2.1/24 ☐ 172.16.3.1/24 ☑ 10.10.0.1/32 ☑ 192.168.10.0/24 ☑ 192.168.11.0/24 ☐
	Apply the following NAT policies: ☑ 172.16.1.0/24 → 192.168.10.0/24 ☑ 172.16.2.0/24 → 10.10.0.1/32 ☑ 172.16.3.11/32 → 192.168.11.101/32 ☑ 172.16.3.21/32 → 192.168.11.201/32 ☐ Local Network → NAT Network
Remote Networks	Network: 192.167.11.193 / Subnet Mask: 255.255.255.0 (/24) ✚
Authentication	◉ Preshared Key ○ X.509 Certificate
Mode	◉ Main Mode (All WANs need to have Static IP) ○ Aggressive Mode
Force UDP Encapsulation	☐
Preshared Key	•••••••••••• ☑ Hide Characters
Local ID	
Remote ID	
Phase 1 (IKE) Proposal	1 AES-256 & SHA1 2 -----
Phase 1 DH Group	☑ Group 2: MODP 1024 ☐ Group 5: MODP 1536
Phase 1 SA Lifetime	3600 seconds Default
Phase 2 (ESP) Proposal	1 AES-256 & SHA1 2 -----
Phase 2 PFS Group	◉ None ○ Group 2: MODP 1024 ○ Group 5: MODP 1536
Phase 2 SA Lifetime	28800 seconds Default

IPsec VPN Settings	
Name	This field is for specifying a local name to represent this connection profile.
Active	When this box is checked, this IPsec VPN connection profile will be enabled. Otherwise, it

	will be disabled.
Connect Upon Disconnection of	Check this box and select a WAN to connect to this VPN automatically when the specified WAN is disconnected.
Remote Gateway IP Address / Host Name	Enter the remote peer's public IP address. For **Aggressive Mode**, this is optional.
Local Networks	Enter the local LAN subnets here. If you have defined static routes, they will be shown here. Using NAT, you can map a specific local network / IP address to another, and the packets received by remote gateway will appear to be coming from the mapped network / IP address. This allow you to establish IPsec connection to a remote site that has one or more subnets overlapped with local site. Two types of NAT policies can be defined: One-to-One NAT policy: if the defined subnet in Local Network and NAT Network has the same size, for example, policy "192.168.50.0/24 > 172.16.1.0/24" will translate the local IP address 192.168.50.10 to 172.16.1.10 and 192.168.50.20 to 172.16.1.20. This is a bidirectional mapping which means clients in remote site can initiate connection to the local clients using the mapped address too. Many-to-One NAT policy: if the defined NAT Network on the right hand side is an IP address (or having a network prefix /32), for example, policy "192.168.1.0/24 > 172.168.50.1/32" will translate all clients in 192.168.1.0/24 network to 172.168.50.1. This is a unidirectional mapping which means clients in remote site will not be able to initiate connection to the local clients.
Remote Networks	Enter the LAN and subnets that are located at the remote site here.
Authentication	To access your VPN, clients will need to authenticate by your choice of methods. Choose between the **Preshared Key** and **X.509 Certificate** methods of authentication.
Mode	Choose **Main Mode** if both IPsec peers use static IP addresses. Choose **Aggressive Mode** if one of the IPsec peers uses dynamic IP addresses.
Force UDP Encapsulation	For forced UDP encapsulation regardless of NAT-traversal, tick this checkbox.
Pre-shared Key	This defines the peer authentication pre-shared key used to authenticate this VPN connection. The connection will be up only if the pre-shared keys on each side match.
Remote Certificate (pem encoded)	Available only when **X.509 Certificat**e is chosen as the **Authentication** method, this field allows you to paste a valid X.509 certificate.
Local ID	In **Main Mode**, this field can be left blank. In **Aggressive Mode**, if **Remote Gateway IP Address** is filled on this end and the peer end, this field can be left blank. Otherwise, this

 Copyright @ 2017 Pepwave

	field is typically a U-FQDN.
Remote ID	In **Main Mode**, this field can be left blank. In **Aggressive Mode**, if **Remote Gateway IP Address** is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.
Phase 1 (IKE) Proposal	In **Main Mode**, this allows setting up to six encryption standards, in descending order of priority, to be used in initial connection key negotiations. In **Aggressive Mode**, only one selection is permitted.
Phase 1 DH Group	This is the Diffie-Hellman group used within IKE. This allows two parties to establish a shared secret over an insecure communications channel. The larger the group number, the higher the security. **Group 2**: **1024-bit** is the default value. **Group 5**: **1536-bit** is the alternative option.
Phase 1 SA Lifetime	This setting specifies the lifetime limit of this Phase 1 Security Association. By default, it is set at **3600** seconds.
Phase 2 (ESP) Proposal	In **Main Mode**, this allows setting up to six encryption standards, in descending order of priority, to be used for the IP data that is being transferred. In **Aggressive Mode**, only one selection is permitted.
Phase 2 PFS Group	Perfect forward secrecy (PFS) ensures that if a key was compromised, the attacker will be able to access only the data protected by that key. **None** - Do not request for PFS when initiating connection. However, since there is no valid reason to refuse PFS, the system will allow the connection to use PFS if requested by the remote peer. This is the default value. **Group 2**: 1024-bit Diffie-Hellman group. The larger the group number, the higher the security. **Group 5**: **1536-bit** is the third option.
Phase 2 SA Lifetime	This setting specifies the lifetime limit of this Phase 2 Security Association. By default, it is set at **28800** seconds.



WAN Connection Priority	
WAN Connection	Select the appropriate WAN connection from the drop-down menu.

15 Outbound Policy Management

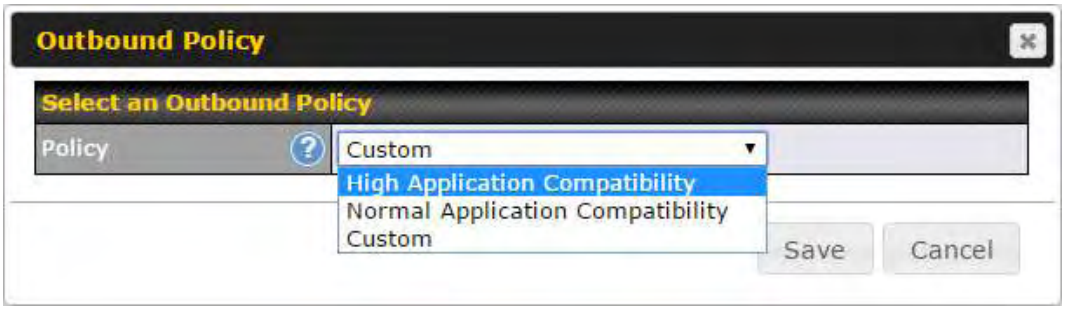
Pepwave routers can flexibly manage and load balance outbound traffic among WAN connections.

Important Note
Outbound policy is applied only when more than one WAN connection is active.

The settings for managing and load balancing outbound traffic are located at **Advanced>Outbound Policy** or **Advanced>PepVPN**, depending on the model.

15.1 Outbound Policy

Outbound policies for managing and load balancing outbound traffic are located at **Network>Outbound Policy>** or **Advanced>PepVPN>Outbound Policy.**



There are three main selections for the outbound traffic policy:

- High Application Compatibility
- Normal Application Compatibility
- Custom

Note that some Pepwave routers provide only the **Send All Traffic To** setting here. See **Section 12.1** for details.

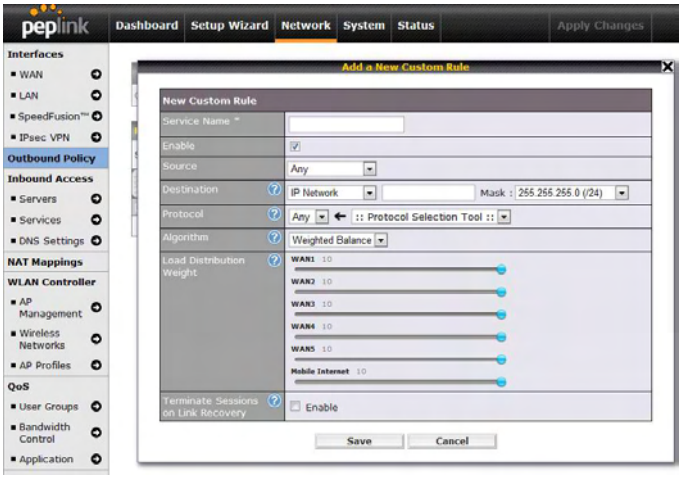
Outbound Policy Settings	
High	Outbound traffic from a source LAN device is routed through the same WAN connection regardless of the destination Internet IP address and protocol. This option provides the

Application Compatibility	highest application compatibility.
Normal Application Compatibility	Outbound traffic from a source LAN device to the same destination Internet IP address will be routed through the same WAN connection persistently, regardless of protocol. This option provides high compatibility to most applications, and users still benefit from WAN link load balancing when multiple Internet servers are accessed.
Custom	Outbound traffic behavior can be managed by defining rules in a custom rule table. A default rule can be defined for connections that cannot be matched with any of the rules.

The default policy is **Normal Application Compatibility**.

Tip

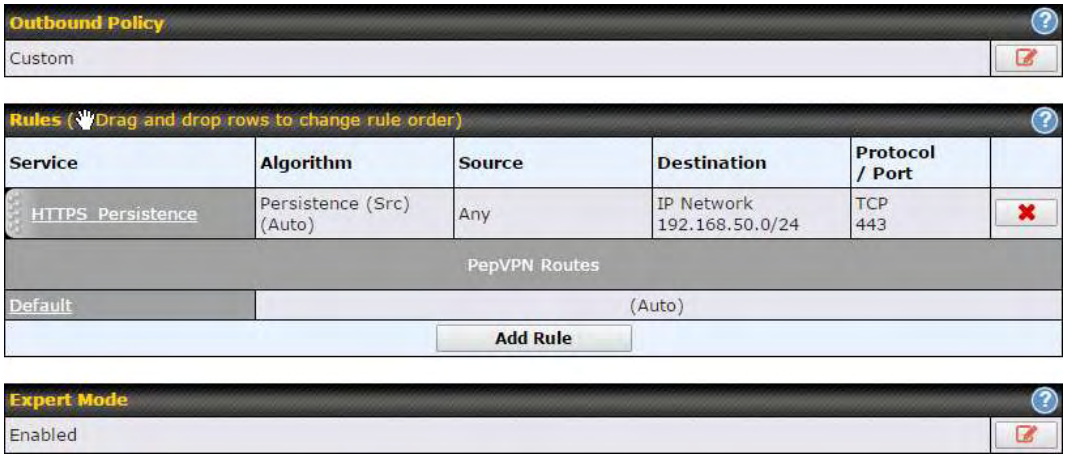
Want to know more about creating outbound rules? Visit our YouTube Channel for a video tutorial!



http://youtu.be/rKH4AS_bQnE

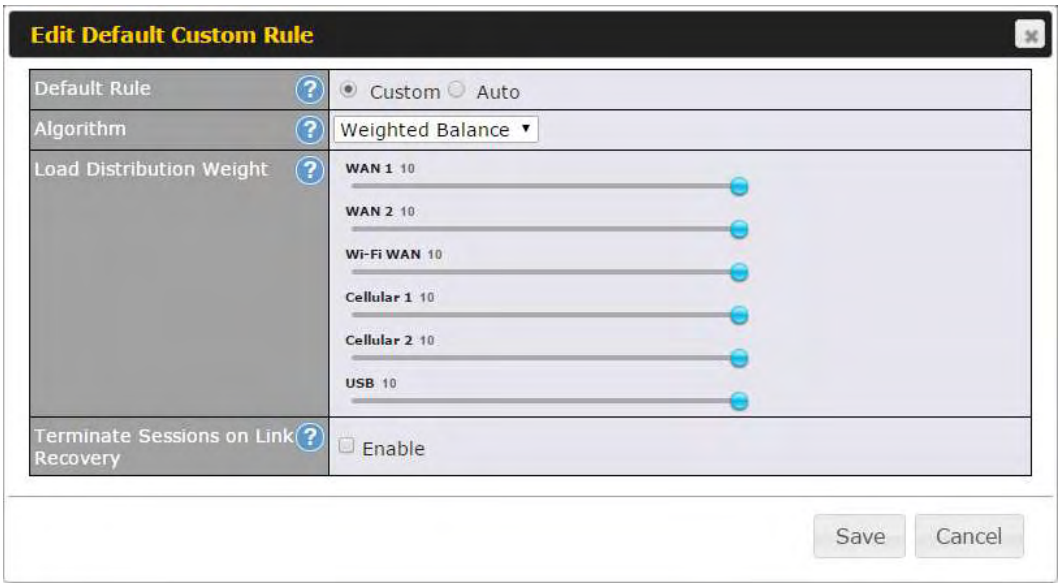
15.2 Custom Rules for Outbound Policy

Click in the **Outbound Policy** form. Choose **Custom** and press the **Save** button.



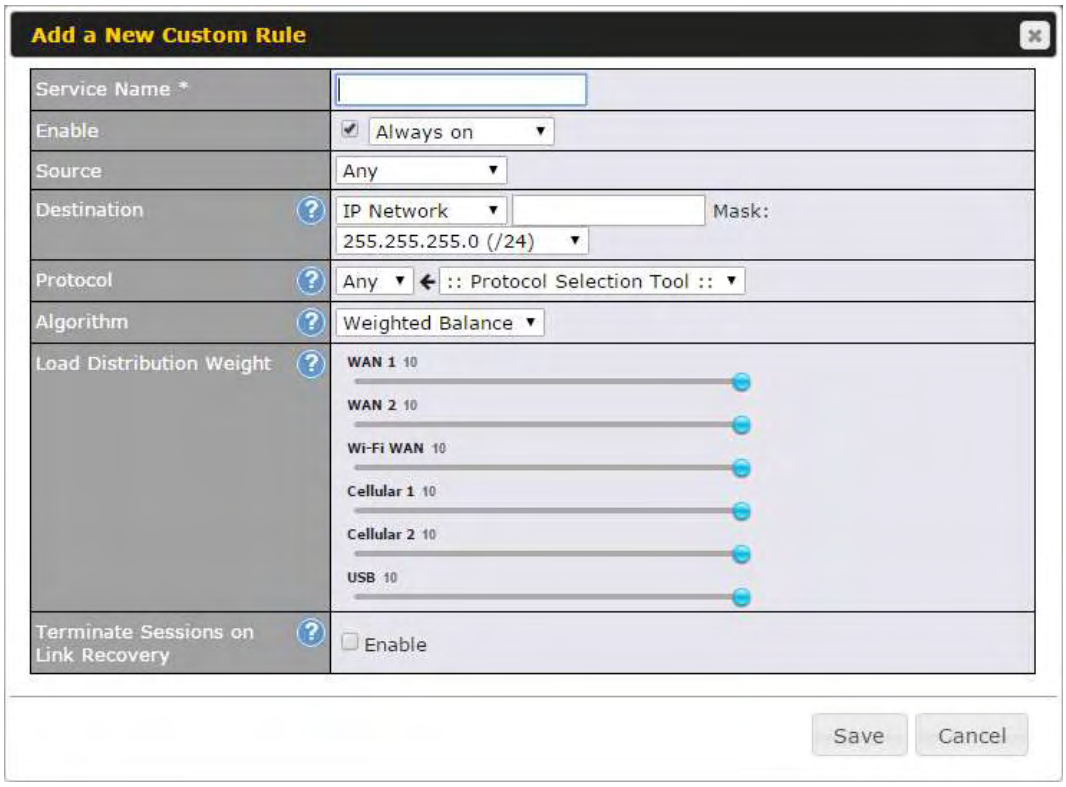
The bottom-most rule is **Default**. Edit this rule to change the device's default manner of controlling outbound traffic for all connections that do not match any of the rules above it. Under the **Service** heading, click **Default** to change these settings.

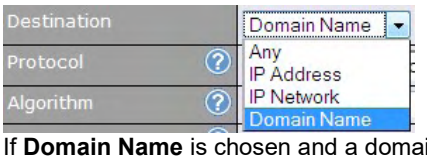
To rearrange the priority of outbound rules, drag and drop them into the desired sequence.



By default, **Auto** is selected as the **Default Rule**. You can select **Custom** to change the algorithm to be used. Please refer to the upcoming sections for the details on the available algorithms.

To create a custom rule, click **Add Rule** at the bottom of the table. Note that some Pepwave routers display this button at **Advanced>PepVPN>PepVPN Outbound Custom Rules**.



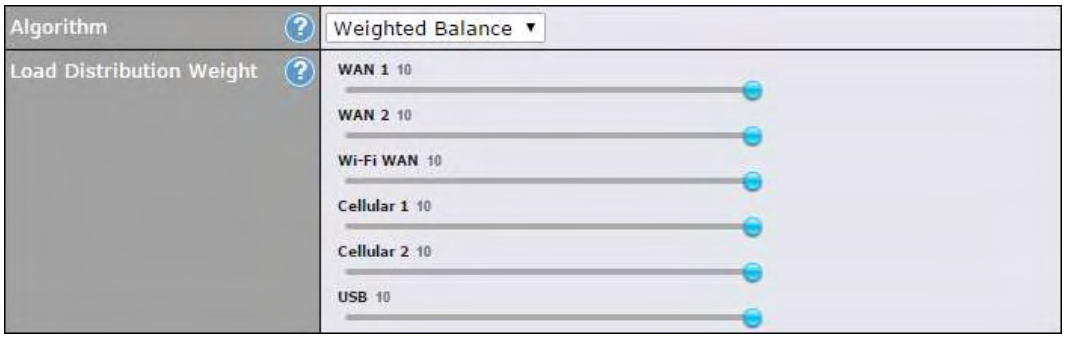
New Custom Rule Settings	
Service Name	This setting specifies the name of the outbound traffic rule.
Enable	This setting specifies whether the outbound traffic rule takes effect. When **Enable** is checked, the rule takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When **Enable** is unchecked, the rule does not take effect: the Pepwave router disregards the other parameters of the rule. Click the drop-down menu next to the checkbox to apply a time schedule to this custom rule.
Source	This setting specifies the source IP address, IP network, or MAC address for traffic that matches the rule.
Destination	This setting specifies the destination IP address, IP network, or domain name for traffic that matches the rule.  If **Domain Name** is chosen and a domain name, such as *foobar.com*, is entered, any outgoing accesses to *foobar.com* and **.foobar.com* will match this criterion. You may enter a wildcard (.*) at the end of a domain name to match any host with a name having the domain name in the middle. If you enter *foobar.**, for example, *www.foobar.com*, *www.foobar.co.jp*, or *foobar.co.uk* will also match. Placing wildcards in any other position is not supported. NOTE: if a server has one Internet IP address and multiple server names, and if one of the names is defined here, accesses to any one of the server names will also match this rule.

Protocol and Port	This setting specifies the IP protocol and port of traffic that matches this rule.
Algorithm	This setting specifies the behavior of the Pepwave router for the custom rule. One of the following values can be selected (note that some Pepwave routers provide only some of these options): • Weighted Balance • Persistence • Enforced • Priority • Overflow • Least Used • Lowest Latency The upcoming sections detail the listed algorithms.
Terminate Sessions on Link Recovery	This setting specifies whether to terminate existing IP sessions on a less preferred WAN connection in the event that a more preferred WAN connection is recovered. This setting is applicable to the **Weighted, Persistence**, and **Priority** algorithms. By default, this setting is disabled. In this case, existing IP sessions will not be terminated or affected when any other WAN connection is recovered. When this setting is enabled, existing IP sessions may be terminated when another WAN connection is recovered, such that only the preferred healthy WAN connection(s) is used at any point in time.

 Copyright @ 2017 Pepwave

15.2.1 Algorithm: Weighted Balance

This setting specifies the ratio of WAN connection usage to be applied on the specified IP protocol and port. This setting is applicable only when **Algorithm** is set to **Weighted Balance**.



The amount of matching traffic that is distributed to a WAN connection is proportional to the weight of the WAN connection relative to the total weight. Use the sliders to change each WAN's weight.

For example, with the following weight settings:

- Ethernet WAN1: 10
- Ethernet WAN2: 10
- Wi-Fi WAN: 10
- Cellular 1: 10
- Cellular 2: 10
- USB: 10

Total weight is 60 = (10 +10 + 10 + 10 + 10 + 10).

Matching traffic distributed to Ethernet WAN1 is 16.7% = (10 / 60 x 100%.

Matching traffic distributed to Ethernet WAN2 is 16.7% = (10 / 60) x 100%.

Matching traffic distributed to Wi-Fi WAN is 16.7% = (10 / 60) x 100%.

Matching traffic distributed to Cellular 1 is 16.7% = (10 / 60) x 100%.

Matching traffic distributed to Cellular 2 is 16.7% = (10 / 60) x 100%.

Matching traffic distributed to USB is 16.7% = (10 / 60) x 100%.

 Copyright @ 2017 Pepwave

15.2.2 Algorithm: Persistence

The configuration of persistent services is the solution to the few situations where link load distribution for Internet services is undesirable. For example, for security reasons, many e-banking and other secure websites terminate the session when the client computer's Internet IP address changes mid-session.

In general, different Internet IP addresses represent different computers. The security concern is that an IP address change during a session may be the result of an unauthorized intrusion attempt. Therefore, to prevent damages from the potential intrusion, the session is terminated upon the detection of an IP address change.

Pepwave routers can be configured to distribute data traffic across multiple WAN connections. Also, the Internet IP depends on the WAN connections over which communication actually takes place. As a result, a LAN client computer behind the Pepwave router may communicate using multiple Internet IP addresses. For example, a LAN client computer behind a Pepwave router with three WAN connections may communicate on the Internet using three different IP addresses.

With the persistence feature, rules can be configured to enable client computers to persistently utilize the same WAN connections for e-banking and other secure websites. As a result, a client computer will communicate using one IP address, eliminating the issues mentioned above.

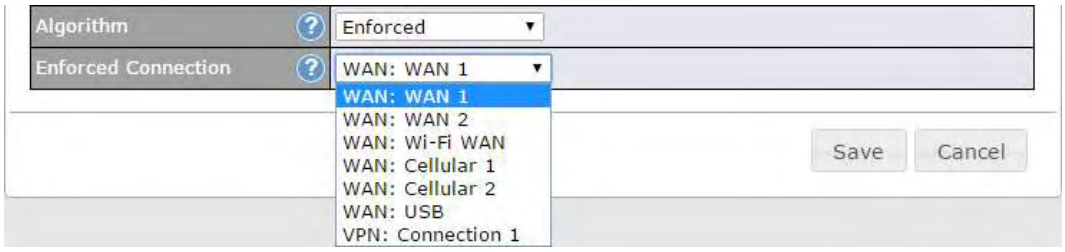
There are two persistent modes: **By Source** and **By Destination**.

By Source:	The same WAN connection will be used for traffic matching the rule and originating from the same machine, regardless of its destination. This option will provide the highest level of application compatibility.
By Destination:	The same WAN connection will be used for traffic matching the rule, originating from the same machine, and going to the same destination. This option can better distribute loads to WAN connections when there are only a few client machines.

The default mode is **By Source**. When there are multiple client requests, they can be distributed (persistently) to WAN connections with a weight. If you choose **Auto** in **Load Distribution**, the weights will be automatically adjusted according to each WAN's **Downstream Bandwidth** which is specified in the WAN settings page). If you choose **Custom**, you can customize the weight of each WAN manually by using the sliders.

15.2.3 Algorithm: Enforced

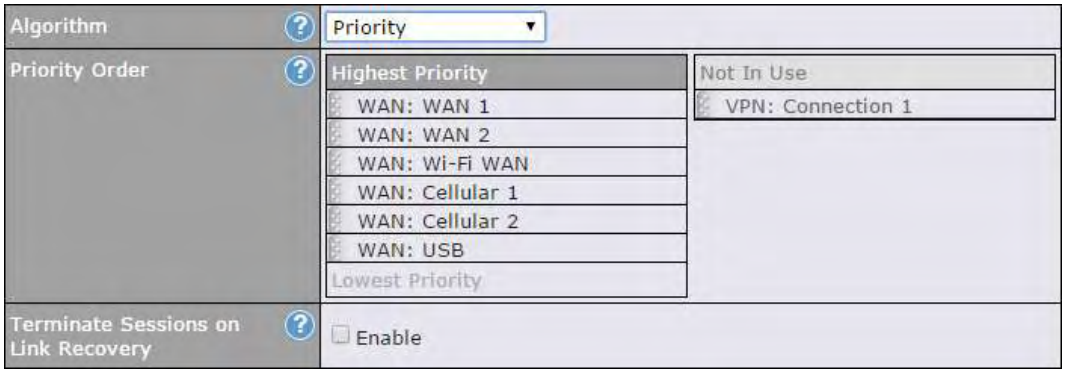
This setting specifies the WAN connection usage to be applied on the specified IP protocol and port. This setting is applicable only when **Algorithm** is set to **Enforced**.



Matching traffic will be routed through the specified WAN connection, regardless of the health check status of the WAN connection. Starting from Firmware 5.2, outbound traffic can be enforced to go through a specified SpeedFusion™ connection.

15.2.4 Algorithm: Priority

This setting specifies the priority of the WAN connections used to route the specified network service. The highest priority WAN connection available will always be used for routing the specified type of traffic. A lower priority WAN connection will be used only when all higher priority connections have become unavailable.

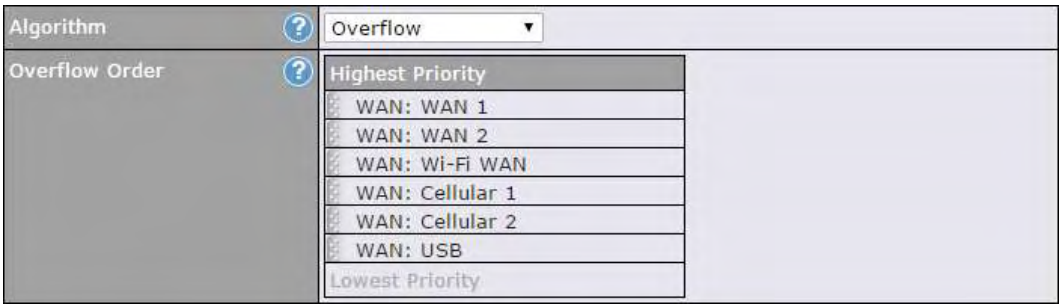


Starting from Firmware 5.2, outbound traffic can be prioritized to go through SpeedFusion™ connection(s). By default, VPN connections are not included in the priority list.

Tip
Configure multiple distribution rules to accommodate different kinds of services.

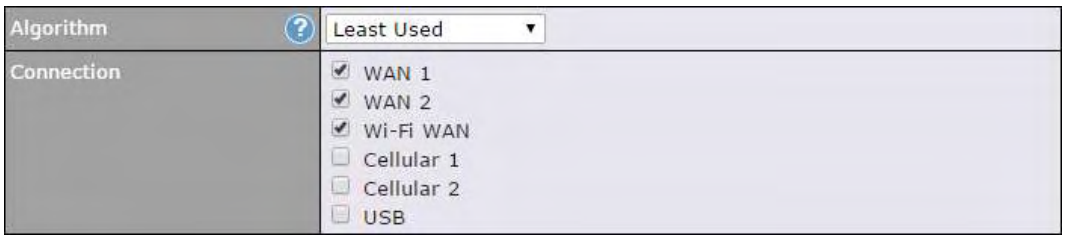
15.2.5 Algorithm: Overflow

The traffic matching this rule will be routed through the healthy WAN connection that has the highest priority and is not in full load. When this connection gets saturated, new sessions will be routed to the next healthy WAN connection that is not in full load.



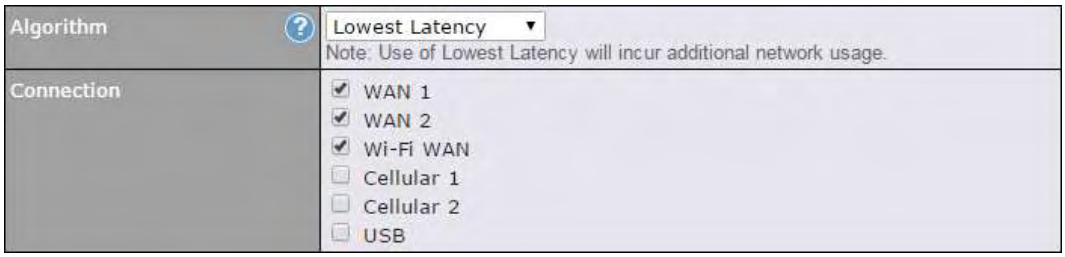
Drag and drop to specify the order of WAN connections to be used for routing traffic. Only the highest priority healthy connection that is not in full load will be used.

15.2.6 Algorithm: Least Used



The traffic matching this rule will be routed through the healthy WAN connection that is selected in **Connection** and has the most available download bandwidth. The available download bandwidth of a WAN connection is calculated from the total download bandwidth specified on the WAN settings page and the current download usage. The available bandwidth and WAN selection is determined every time an IP session is made.

15.2.7 Algorithm: Lowest Latency



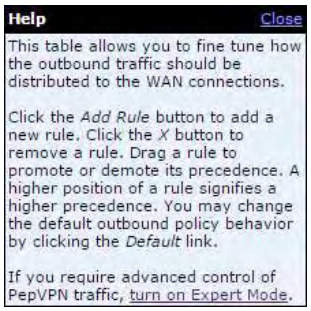
The traffic matching this rule will be routed through the healthy WAN connection that is selected in **Connection** and has the lowest latency. Latency checking packets are issued periodically to a nearby router of each WAN connection to determine its latency value. The latency of a WAN is the packet round trip time of the WAN connection. Additional network usage may be incurred as a result.

Tip
The roundtrip time of a 6M down/640k uplink can be higher than that of a 2M down/2M up link because the overall round trip time is lengthened by its slower upload bandwidth, despite its higher downlink speed. Therefore, this algorithm is good for two scenarios: • All WAN connections are symmetric; or

- A latency sensitive application must be routed through the lowest latency WAN, regardless of the WAN's available bandwidth.

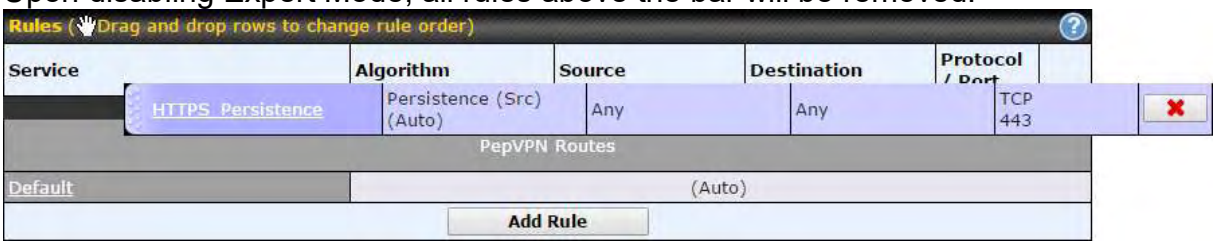
15.2.8 Expert Mode

Expert Mode is available on some Pepwave routers for use by advanced users. To enable the feature, click on the help icon and click **turn on Expert Mode**.



In Expert Mode, a new special rule, **SpeedFusion™ Routes**, is displayed in the **Custom Rules** table. This rule represents all SpeedFusion™ routes learned from remote VPN peers. By default, this bar is on the top of all custom rules. This position means that traffic for remote VPN subnets will be routed to the corresponding VPN peer. You can create custom **Priority** or **Enforced** rules and move them above the bar to override the SpeedFusion™ routes.

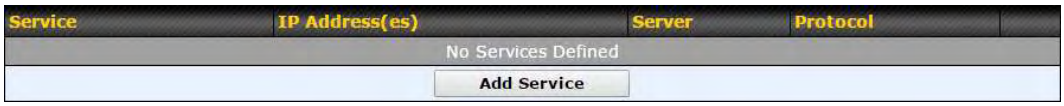
Upon disabling Expert Mode, all rules above the bar will be removed.



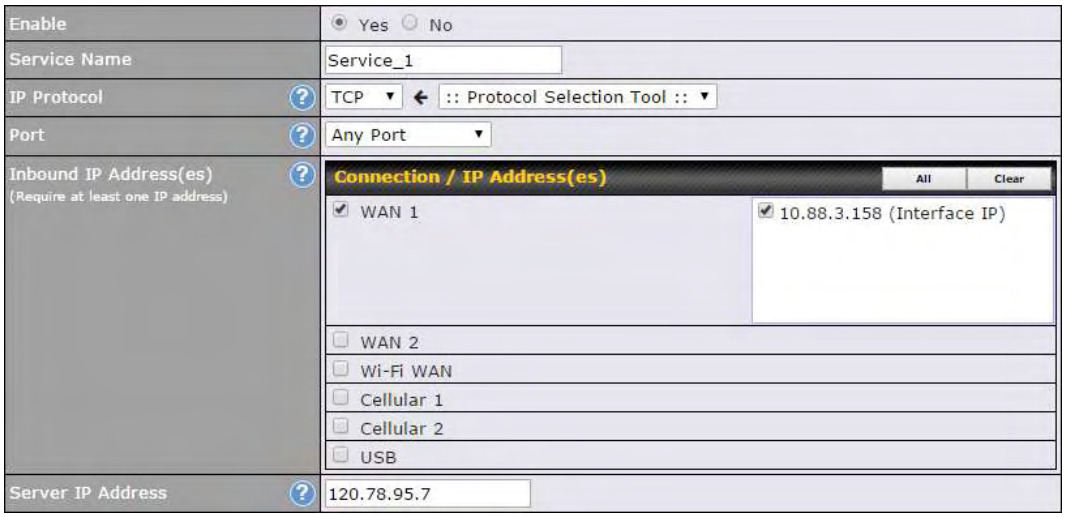
16 Inbound Access

16.1 Port Forwarding Service

Pepwave routers can act as a firewall that blocks, by default, all inbound access from the Internet. By using port forwarding, Internet users can access servers behind the Pepwave router. Inbound port forwarding rules can be defined at **Advanced>Port Forwarding**.



To define a new service, click **Add Service**.



Port Forwarding Settings	
Enable	This setting specifies whether the inbound service takes effect. When **Enable** is checked, the inbound service takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When this setting is disabled, the inbound service does not take effect: the Pepwave router disregards the other parameters of the rule.
Service Name	This setting identifies the service to the system administrator. Valid values for this setting consist of only alphanumeric and underscore "_" characters.
IP Protocol	The **IP Protocol** setting, along with the **Port** setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Traffic that is received by the Pepwave router via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the **Servers** setting. Please see below for details on the **Port** and **Servers** settings. Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and a single port number of common Internet services (e.g. HTTP, HTTPS, etc.). After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remain manually modifiable.

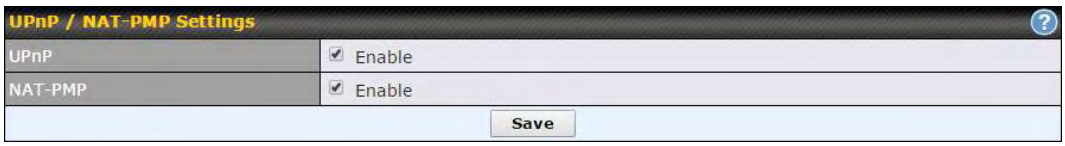
Port	The **Port** setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners: **Any Port**, **Single Port**, **Port Range**, **Port Map**, and **Range Mapping** Port ? Any Port **Any Port**: all traffic that is received by the Pepwave router via the specified protocol is forwarded to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Any Port**, all TCP traffic is forwarded to the configured servers. Port ? Single Port Service Port: 80 **Single Port**: traffic that is received by the Pepwave router via the specified protocol at the specified port is forwarded via the same port to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Single Port** and **Service Port** 80, TCP traffic received on port 80 is forwarded to the configured servers via port 80. Port ? Port Range Service Ports: 80 - 88 **Port Range**: traffic that is received by the Pepwave router via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Range** and **Service Ports** 80-88, TCP traffic received on ports 80 through 88 is forwarded to the configured servers via the respective ports. Port ? Port Mapping Service Port: 80 Map to Port: 88 **Port Mapping**: traffic that is received by Pepwave router via the specified protocol at the specified port is forwarded via a different port to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Mapping**, **Service Port** 80, and **Map to Port** 88, TCP traffic on port 80 is forwarded to the configured servers via port 88. (Please see below for details on the **Servers** setting.) Port ? Range Mapping Service Ports: 80 - 88 Map to Ports: 88 - 96 **Range Mapping**: traffic that is received by the Pepwave router via the specified protocol at the specified port range is forwarded via a different port to the servers specified by the **Servers** setting.
Inbound IP Address(es)	This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed.
Server IP Address	This setting specifies the LAN IP address of the server that handles the requests for the service.

16.1.1 UPnP / NAT-PMP Settings

UPnP and NAT-PMP are network protocols which allow a computer connected to the LAN port to automatically configure the router to allow parties on the WAN port to connect to itself. That way, the process of inbound port forwarding becomes automated.

When a computer creates a rule using these protocols, the specified TCP/UDP port of all WAN connections' default IP address will be forwarded.

Check the corresponding box(es) to enable UPnP and/or NAT-PMP. Enable these features only if you trust the computers connected to the LAN ports.

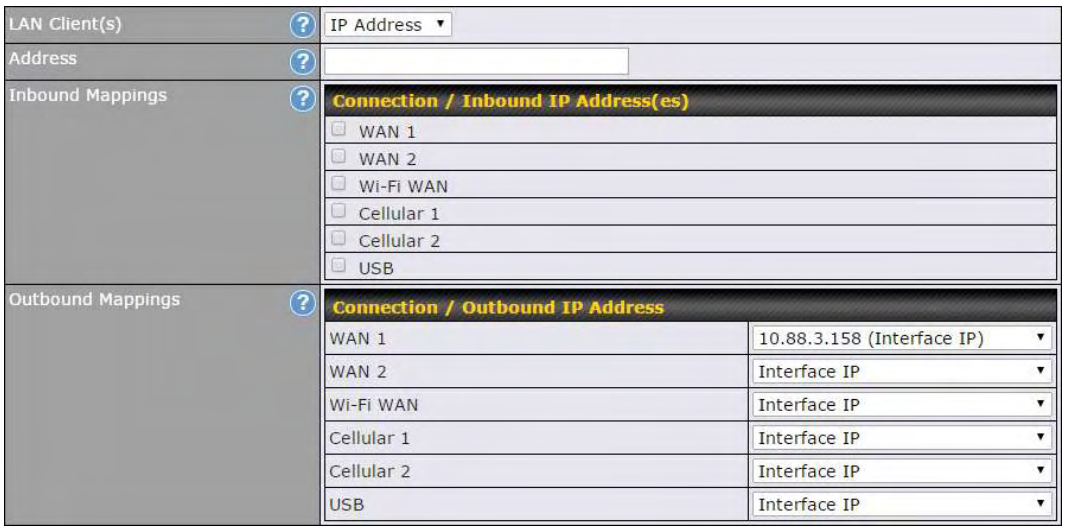


When the options are enabled, a table listing all the forwarded ports under these two protocols can be found at **Status>UPnP / NAT-PMP**.

17 NAT Mappings

NAT mappings allow IP address mapping of all inbound and outbound NAT'dt raffic to and from an internal client IP address. Settings to configure NAT mappings are located at **Advanced>NAT Mappings**.

To add a rule for NAT mappings, click **Add NAT Rule**.



NAT Mapping Settings	
LAN Client(s)	NAT mapping rules can be defined for a single LAN **IP Address**, an **IP Range**, or an **IP Network**.
Address	This refers to the LAN host's private IP address. The system maps this address to a number of public IP addresses (specified below) in order to facilitate inbound and outbound traffic. This option is only available when **IP Address** is selected.
Range	The IP range is a contiguous group of private IP addresses used by the LAN host. The system maps these addresses to a number of public IP addresses (specified below) to facilitate outbound traffic. This option is only available when **IP Range** is selected.
Network	The IP network refers to all private IP addresses and ranges managed by the LAN host. The system maps these addresses to a number of public IP addresses (specified below) to facilitate outbound traffic. This option is only available when **IP Network** is selected.

 Copyright @ 2017 Pepwave

Inbound Mappings	This setting specifies the WAN connections and corresponding WAN-specific Internet IP addresses on which the system should bind. Any access to the specified WAN connection(s) and IP address(es) will be forwarded to the LAN host. This option is only available when **IP Address** is selected in the **LAN Client(s)** field. Note that inbound mapping is not needed for WAN connections in drop-in mode or IP forwarding mode. Also note that each WAN IP address can be associated to one NAT mapping only.
Outbound Mappings	This setting specifies the WAN IP addresses that should be used when an IP connection is made from a LAN host to the Internet. Each LAN host in an IP range or IP network will be evenly mapped to one of each selected WAN's IP addresses (for better IP address utilization) in a persistent manner (for better application compatibility). Note that if you do not want to use a specific WAN for outgoing accesses, you should still choose default here, then customize the outbound access rule in the **Outbound Policy** section. Also note that WAN connections in drop-in mode or IP forwarding mode are not shown here.

Click **Save** to save the settings when configuration has been completed.

Important Note
Inbound firewall rules override the **Inbound Mappings** settings.

 Copyright @ 2017 Pepwave

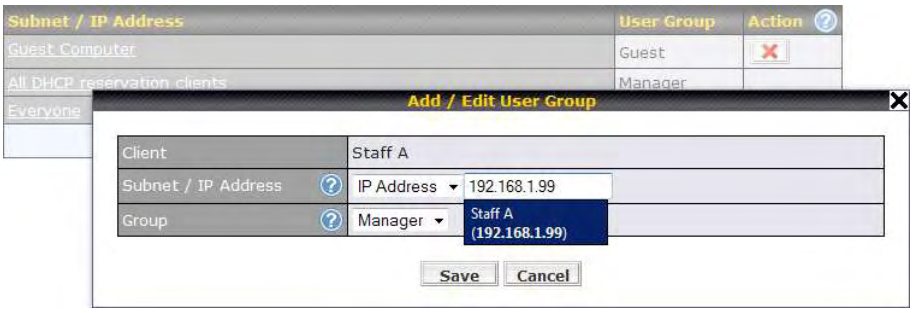
18 QoS

18.1 User Groups

LAN and PPTP clients can be categorized into three user groups: **Manager, Staff, and Guest**. This menu allows you to define rules and assign client IP addresses or subnets to a user group. You can apply different bandwidth and traffic prioritization policies on each user group in the **Bandwidth Control** and **Application** sections (note that the options available here vary by model).

The table is automatically sorted by rule precedence. The smaller and more specific subnets are put towards the top of the table and have higher precedence; larger and less specific subnets are placed towards the bottom.

Click the **Add** button to define clients and their user group. Click the ✖ button to remove the defined rule. Two default rules are pre-defined and put at the bottom. They are **All DHCP reservation clients** and **Everyone**, and they cannot be removed. The **All DHCP reservation client represents** the LAN clients defined in the DHCP Reservation table on the LAN settings page. **Everyone** represents all clients that are not defined in any rule above. Click on a rule to change its group.

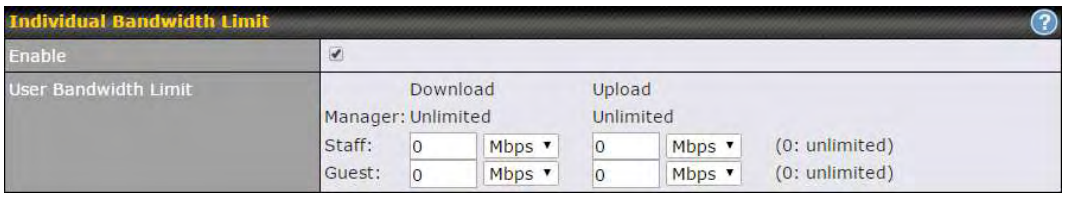


Add / Edit User Group	
Subnet / IP Address	From the drop-down menu, choose whether you are going to define the client(s) by an **IP Address** or a **Subnet**. If **IP Address** is selected, enter a name defined in DHCP reservation table or a LAN client's IP address. If **Subnet** is selected, enter a subnet address and specify its subnet mask.
Group	This field is to define which **User Group** the specified subnet / IP address belongs to.

Once users have been assigned to a user group, their internet traffic will be restricted by rules defined for that particular group. Please refer to the following two sections for details.

18.2 Bandwidth Control

You can define a maximum download speed (over all WAN connections) and upload speed (for each WAN connection) that each individual Staff and Guest member can consume. No limit can be imposed on individual Manager members. By default, download and upload bandwidth limits are set to unlimited (set as **0**).

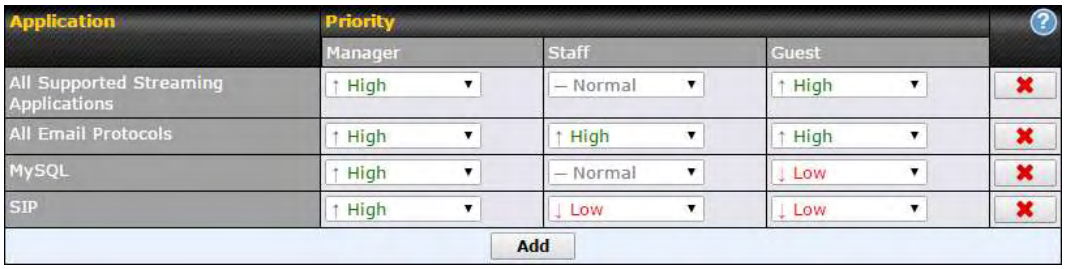


18.3 Application

18.3.1 Application Prioritization

On many Pepwave routers, you can choose whether to apply the same prioritization settings to all user groups or customize the settings for each group.

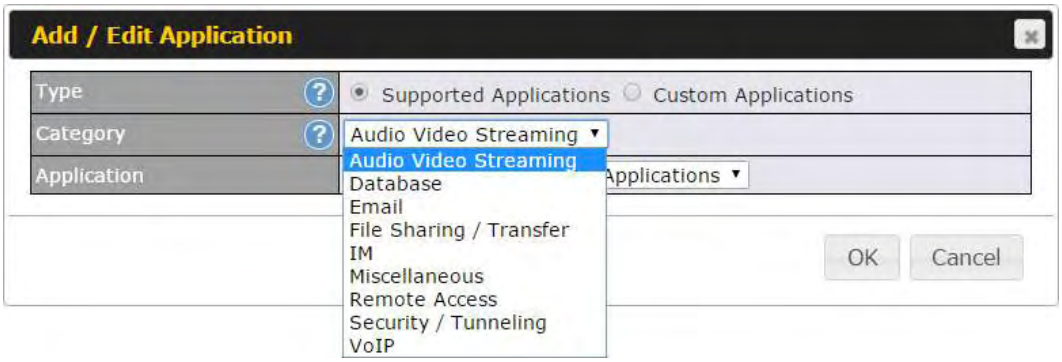
Three application priority levels can be set: ↑ **High**,— **Normal**, and ↓ **Low**. Pepwave routers can detect various application traffic types by inspecting the packet content. Select an application by choosing a supported application, or by defining a custom application manually. The priority preference of supported applications is placed at the top of the table. Custom applications are at the bottom.



18.3.2 Prioritization for Custom Applications

Click the **Add** button to define a custom application. Click the button ✖ in the **Action** column to delete the custom application in the corresponding row.

When **Supported Applications** is selected, the Pepwave router will inspect network traffic and prioritize the selected applications. Alternatively, you can select **Custom Applications** and define the application by providing the protocol, scope, port number, and DSCP value.



18.3.3 DSL/Cable Optimization

DSL/cable-based WAN connections have lower upload bandwidth and higher download bandwidth. When a DSL/cable circuit's uplink is congested, the download bandwidth will be affected. Users will not be able to download data at full speed until the uplink becomes less congested. **DSL/Cable Optimization** can relieve such an issue. When it is enabled, the download speed will become less affected by the upload traffic. By default, this feature is enabled.

19 Firewall

A firewall is a mechanism that selectively filters data traffic between the WAN side (the Internet) and the LAN side of the network. It can protect the local network from potential hacker attacks, access to offensive websites, and/or other inappropriate uses.

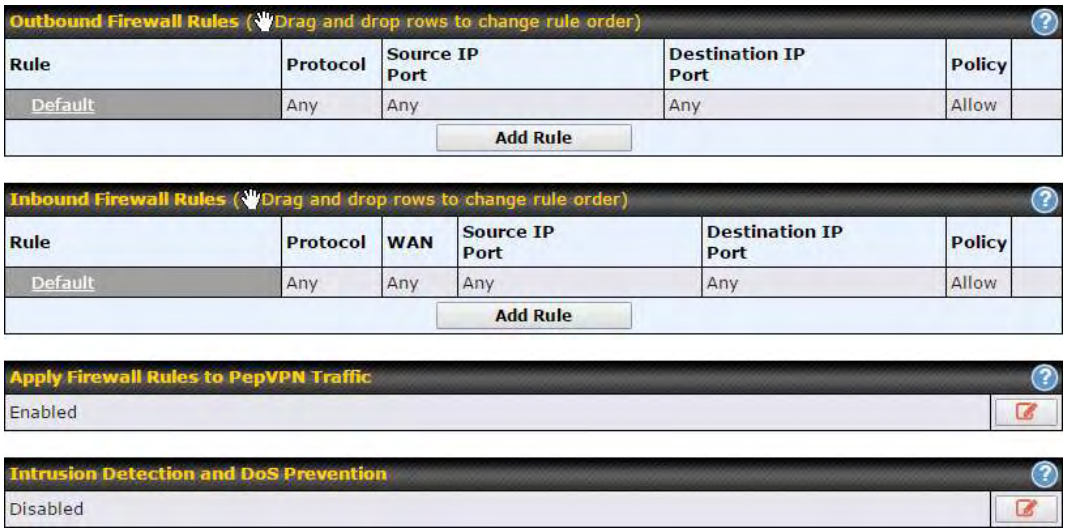
The firewall functionality of Pepwave routers supports the selective filtering of data traffic in both directions:

- Outbound (LAN to WAN)
- Inbound (WAN to LAN)

The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

With SpeedFusion™ enabled, the firewall rules also apply to VPN tunneled traffic.



19.1 Outbound and Inbound Firewall Rules

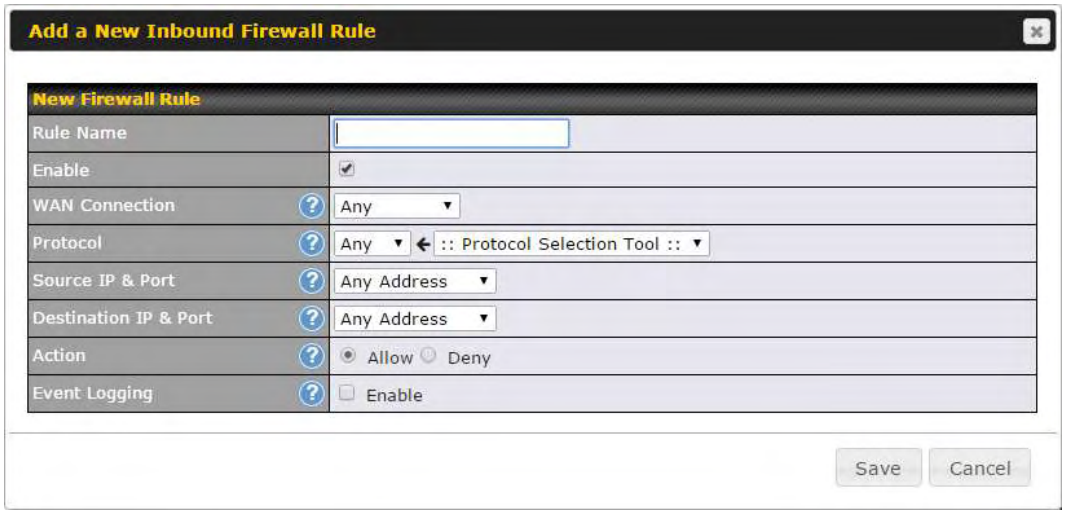
19.1.1 Access Rules

The outbound firewall settings are located at **Advanced>Firewall>Access Rules>Outbound Firewall Rules.**

Click **Add Rule** to display the following screen:

Inbound firewall settings are located at **Advanced>Firewall>Access Rules>Inbound Firewall Rules.**

Click **Add Rule** to display the following screen:



Rules are matched from top to bottom. If a connection matches any one of the upper rules, the matching process will stop. If none of the rules match, the **Default** rule will be applied. By default, the **Default** rule is set as **Allow** for both outbound and inbound access.