



# Pepwave MAX

## User Manual

### Pepwave Products:

MAX 700 / HD2 / HD2 IP67 / HD2 mini / HD2 Dome / HD4 / HD4 MBX / HD4 IP67 / Transit / Transit Mini / BR1 Classic / BR1 MK2 / BR1 Slim / BR1 ENT / BR1 M2M / BR1 Mini / BR1 Mini Core / BR1 Pro LTE / BR1 IP55 / BR1 IP67 / BR2 IP55 / On-The-Go / MAX HD2 / HD4 with MediaFast / SpeedFusion Engine / UBR LTE / PDX

Pepwave Firmware 8.1.0  
August 2020

### Copyright & Trademarks

Specifications are subject to change without notice. Copyright © 2020 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

<b>Introduction and Scope</b>	7
<b>Glossary</b>	8
<b>Product Features</b>	9
Supported Network Features	9
WAN	9
LAN	10
VPN	10
Firewall	10
Captive Portal	10
Outbound Policy	10
AP Controller	11
QoS	11
Other Supported Features	11
<b>Pepwave MAX Mobile Router Overview</b>	13
MAX 700	13
MAX HD2	15
MAX HD2 IP67	17
MAX HD2 mini	18
MAX HD2 Dome	20
MAX Transit / MAX Transit Duo (CAT-12)	22
MAX Transit (CAT-18)	23
MAX Transit Mini	25
MAX HD2 and HD4 with MediaFast	26
MAX HD4	28
MAX HD4 MBX (CAT-12)	30
MAX HD2/4 MBX (CAT-18)	32
MAX HD4 IP67	33
MAX BR1 Classic	34
MAX BR1 MK2	36
MAX BR1 Slim	38
MAX BR1 Mini	40
MAX BR1 Mini Core	42
MAX BR1 M2M	43
MAX BR1 ENT	45
MAX BR1 Pro	46

MAX Hotspot	47
MAX BR1 IP55	48
MAX BR2 IP55	50
MAX BR1 IP67	51
MAX On-The-Go	52
SpeedFusion Engine	53
UBR LTE	54
PDX	55
<b>Advanced Feature Summary</b>	56
Drop-in Mode and LAN Bypass: Transparent Deployment	56
QoS: Clearer VoIP	57
Per-User Bandwidth Control	57
High Availability via VRRP	58
USB Modem and Android Tethering	58
Built-In Remote User VPN Support	59
SIM-card USSD support	59
DPI Engine	60
<b>Installation</b>	61
Preparation	61
Constructing the Network	61
Configuring the Network Environment	62
<b>Mounting the Unit</b>	62
Wall Mount	62
Car Mount	63
IP67 Installation Guide	63
PDX Accessory Kit Installation Guide	63
<b>Connecting to the Web Admin Interface</b>	69
<b>SpeedFusion Cloud</b>	72
Activate SpeedFusion Cloud Service	72
Enable SpeedFusion Cloud	74
Connect Clients to Cloud	81
Link Wi-Fi to Cloud	82
<b>Configuring the LAN Interface(s)</b>	84
Basic Settings	84
Port Settings	95
Captive Portal	95

<b>Configuring the WAN Interface(s)</b>	98
Ethernet WAN	99
DHCP Connection	102
Static IP Connection	103
PPPoE Connection	104
L2TP Connection	105
Cellular WAN	106
Wi-Fi WAN	113
Creating Wi-Fi Connection Profiles	119
WAN Health Check	120
Dynamic DNS Settings	122
<b>Advanced Wi-Fi Settings</b>	124
<b>ContentHub Configuration</b>	129
ContentHub	129
Configuring the ContentHub	129
Configure a website to be published from the ContentHub	130
Configure an application to be published from the ContentHub	131
<b>MediaFast Configuration</b>	133
Setting Up MediaFast Content Caching	134
Scheduling Content Prefetching	135
Viewing MediaFast Statistics	138
<b>Bandwidth Bonding SpeedFusion™ / PepVPN</b>	139
PepVPN	139
The Pepwave Router Behind a NAT Router	145
<b>IPsec VPN</b>	147
IPsec VPN Settings	147
<b>Outbound Policy Management</b>	151
Outbound Policy	151
Custom Rules for Outbound Policy	153
Algorithm: Weighted Balance	153
Algorithm: Persistence	154
Algorithm: Enforced	155
Algorithm: Priority	156
Algorithm: Overflow	156
Algorithm: Least Used	157
Algorithm: Lowest Latency	157

Expert Mode	158
<b>Inbound Access</b>	158
Port Forwarding Service	158
UPnP / NAT-PMP Settings	160
<b>NAT Mappings</b>	161
User Groups	163
Bandwidth Control	164
Application	164
Application Prioritization	164
Prioritization for Custom Applications	164
DSL/Cable Optimization	165
<b>Firewall</b>	165
Outbound and Inbound Firewall Rules	166
Access Rules	166
Apply Firewall Rules to PepVpn Traffic	169
Intrusion Detection and DoS Prevention	169
Content Blocking	171
Application Blocking	171
Web Blocking	171
Customized Domains	172
Exempted User Groups	172
Exempted Subnets	172
URL Logging	172
OSPF & RIPv2	172
BGP	176
<b>Remote User Access</b>	178
L2TP with IPsec	179
OpenVPN	179
PPTP	180
Authentication Methods	180
<b>Miscellaneous Settings</b>	182
High Availability	182
Certificate Manager	185
Service Forwarding	186
SMTP Forwarding	186
Web Proxy Forwarding	187
DNS Forwarding	188

Custom Service Forwarding	188
Service Passthrough	188
UART	190
GPS Forwarding	192
Ignition Sensing	192
Ignition Sensing installation	193
GPIO Menu	195
NTP Server	196
Grouped Networks	196
SIM Toolkit	197
<b>AP - access point</b>	200
AP Controller	200
Wireless SSID	200
Settings	205
<b>AP Controller Status</b>	211
Info	211
Access Point (Usage)	213
Wireless SSID	215
Wireless Client	216
Nearby Device	217
Event Log	218
<b>Toolbox</b>	219
<b>System Settings</b>	220
Admin Security	220
Firmware	223
Web admin interface : automatically check for updates	223
Web admin interface : install updates manually	224
The InControl method	225
Time	226
Schedule	226
Email Notification	227
Event Log	229
SNMP	230
InControl	232
Configuration	232
Feature Add-ons	233
Reboot	234

<b>Tools</b>	234
Ping	234
Traceroute Test	235
PepVPN Test	236
Wake-on-LAN	237
CLI (Command Line Interface Support)	237
<b>Status</b>	238
Device	238
GPS Data	239
Active Sessions	240
Client List	241
WINS Client	242
UPnP / NAT-PMP	242
OSPF & RIPv2	243
BGP	244
SpeedFusion Status	244
Event Log	246
WAN Quality	248
Usage Reports	248
Real-Time	249
Hourly	249
Daily	250
Monthly	251
<b>Appendix A: Restoration of Factory Defaults</b>	254
<b>Appendix B: Declaration</b>	254

## 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!



<https://youtu.be/13M-JHRAICA>



## Glossary

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

Term	Definition
3G	3rd generation standards for wireless communications (e.g., HSDPA)
4G	4th generation standards for wireless communications (e.g., LTE)
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EVDO	Evolution-Data Optimized
FQDN	Fully Qualified Domain Name
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

# 1 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](http://peplink.com/products).

## 1.1 Supported Network Features

### 1.1.1 WAN

- Ethernet WAN connection in full/half duplex
- Static IP support for PPPoE
- Built-in 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](http://changeip.com), [dyndns.org](http://dyndns.org), [no-ip.org](http://no-ip.org), [tzo.com](http://tzo.com) and [DNS-O-Matic](http://DNS-O-Matic))
- Ping, DNS lookup, and HTTP-based health check

### **1.1.2 LAN**

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

### **1.1.3 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

### **1.1.4 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

### **1.1.5 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

### **1.1.6 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

### **1.1.7 AP Controller**

- Configure and manage Pepwave AP devices
- Review the status of connected APs

### **1.1.8 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

## **1.2 Other Supported Features**

- User-friendly web-based administration interface
- HTTP and HTTPS support for web admin interface (default redirection to HTTPS)
- 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

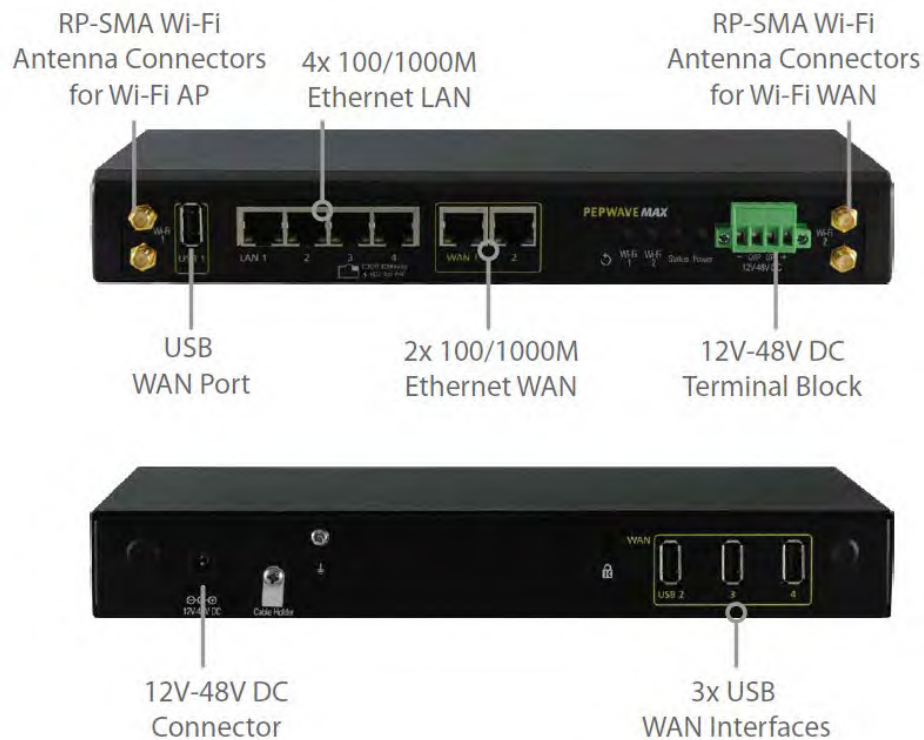
- IPv6 support
- Support USB tethering on Android 2.2+ phones

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

## 2 Pepwave MAX Mobile Router Overview

### 2.1 MAX 700

#### 2.1.1 Panel Appearance



#### 2.1.2 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

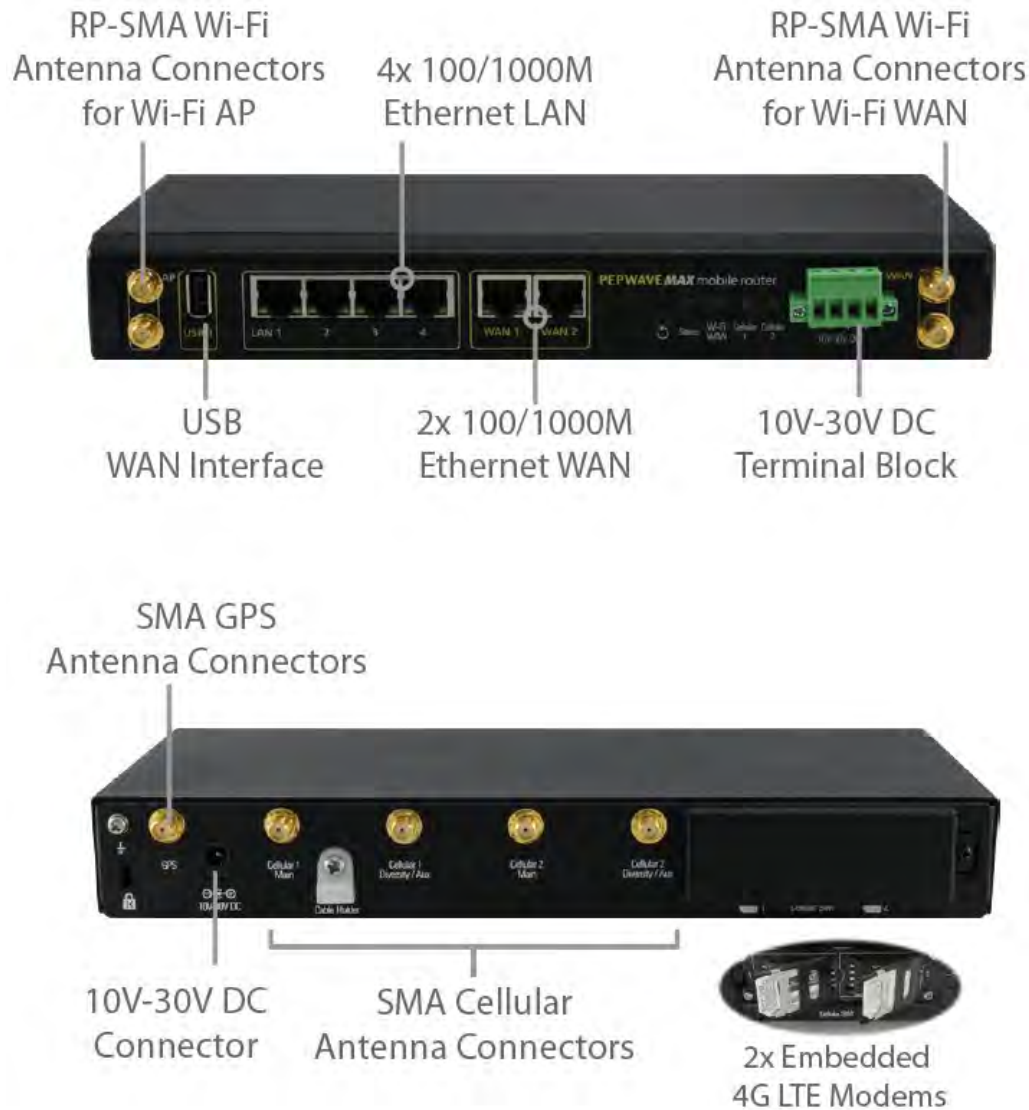
Wi-Fi AP and Wi-Fi WAN Indicators		
<b>Wi-Fi WAN</b>	OFF	Disconnected
	Blinking slowly	Connecting to network
	Blinking	Connected to network with traffic
	ON	Connected to network without traffic
<b>Wi-Fi AP</b>	OFF	Disabled
	Blinking slowly	Enabled but no client connected
	Blinking	Connected to network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

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

## 2.2 MAX HD2

2.3 For certification information, please refer to [Appendix B: Declaration](#)

### 2.3.1 Panel Appearance





### 2.3.2 LED Indicators

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

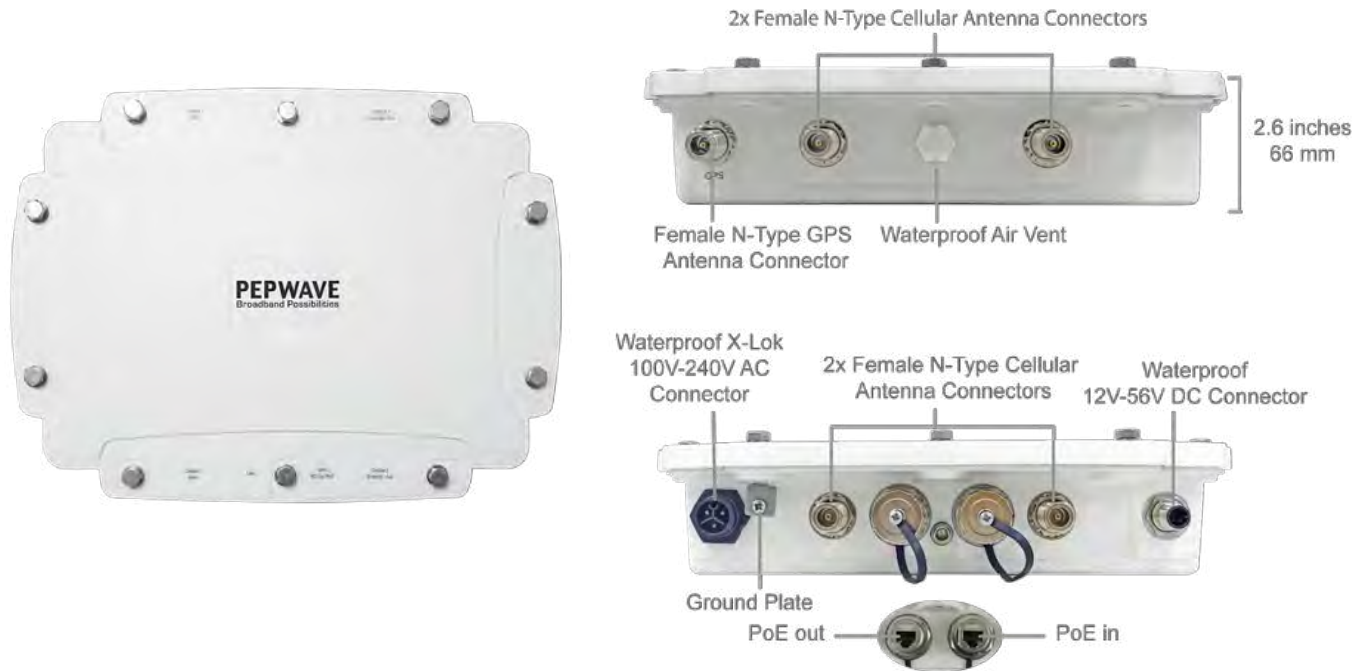
Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

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
	Blinking	Data is transferring
Orange LED	OFF	No data is being transferred or port is not connected
	ON	
Port Type	Auto MDI/MDI-X ports	

## 2.4 MAX HD2 IP67

### 2.4.1 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

## 2.5 MAX HD2 mini

### 2.5.1 Panel Appearance



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

### 2.5.2 LED Indicators

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

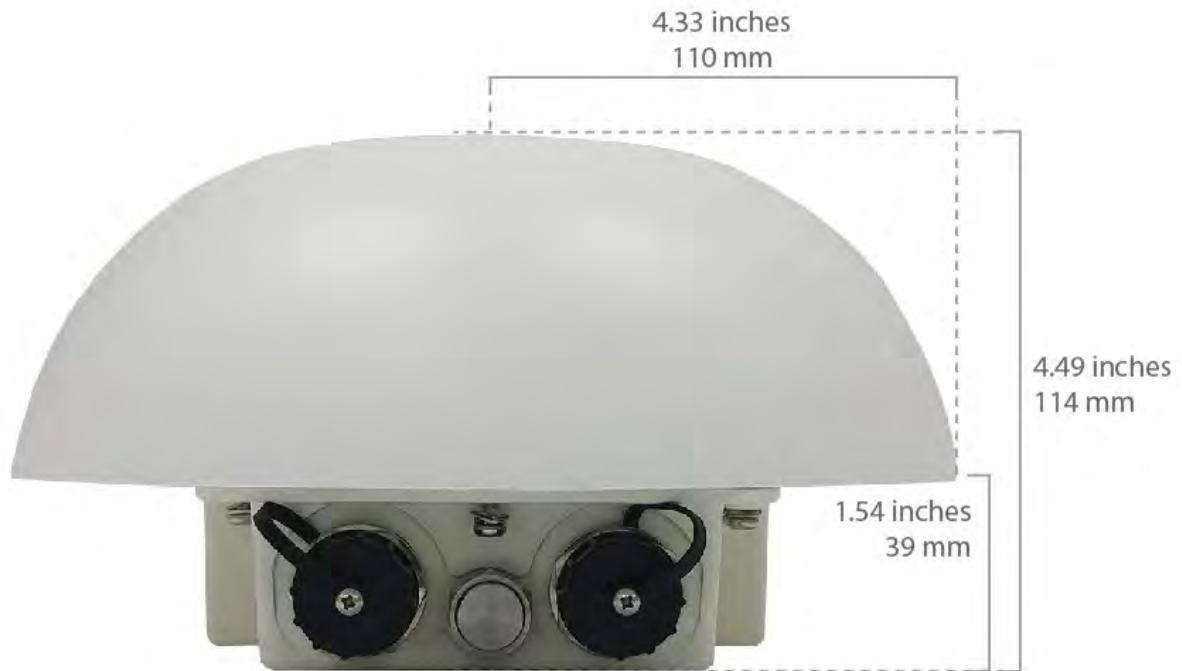
Status Indicators		
<b>Status</b>	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Cellular WAN Indicators		
<b>Cellular 1 / Cellular 2</b>	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		
<b>Green LED</b>	ON	10 / 100 / 1000 Mbps
<b>Orange LED</b>	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
<b>Port Type</b>	Auto MDI/MDI-X ports	

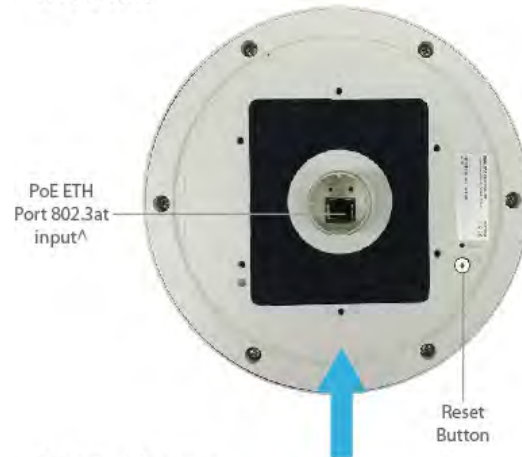
## 2.6 MAX HD2 Dome

### 2.6.1 Panel Appearance



#SIM Injector is available separately  
 ^Ethernet LAN port can be split into two LAN ports  
 using the included splitter (1x LAN 802.3af PoE out, 1x LAN PoE in)

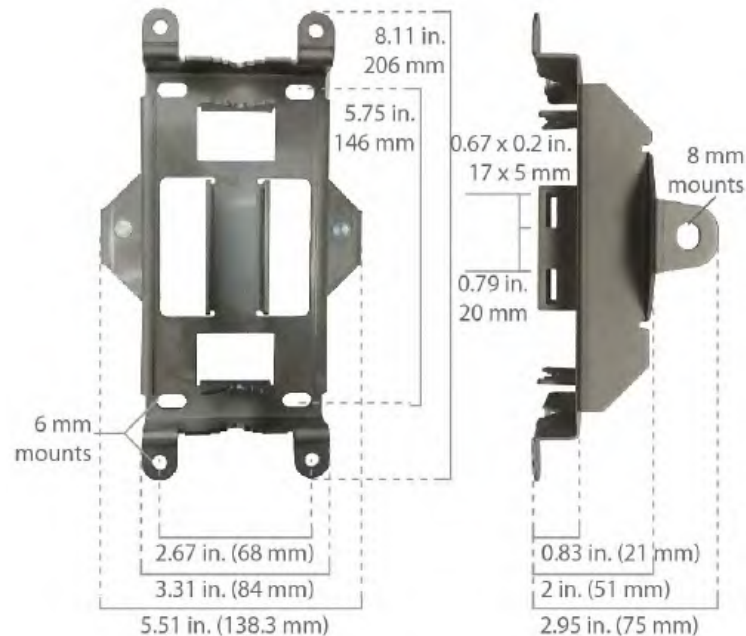
### HD2 Dome



### Ethernet Splitter



### Mounting Bracket



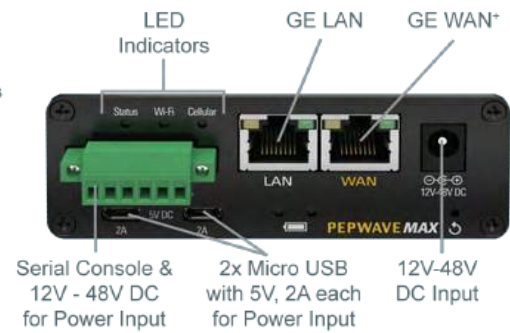
## 2.7 MAX Transit / MAX Transit Duo (CAT-12)

### 2.7.1 Panel Appearance

MAX-TST / MAX-TST-DUO (CAT-12)

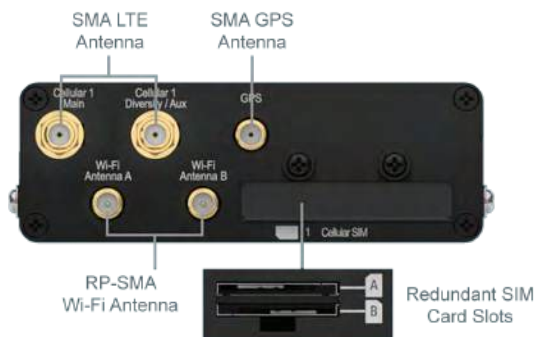


Front

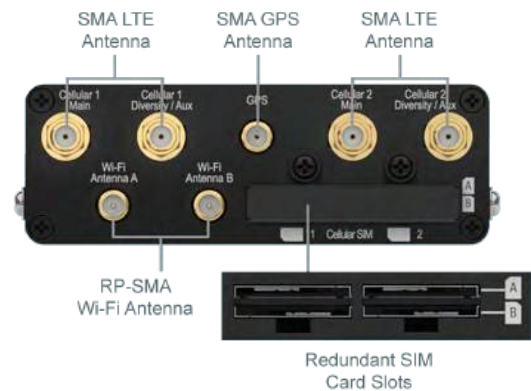


Back

MAX-TST (CAT-12)



MAX-TST-DUO (CAT-12)



### 2.7.2 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

### Cellular WAN Indicators

<b>Cellular 1 / Cellular 2*</b>	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		
<b>Green LED</b>	ON	10 / 100 / 1000 Mbps
	Blinking	Data is transferring
<b>Orange LED</b>	OFF	No data is being transferred or port is not connected
<b>Port Type</b>	Auto MDI/MDI-X ports	

## 2.8 MAX Transit (CAT-18)

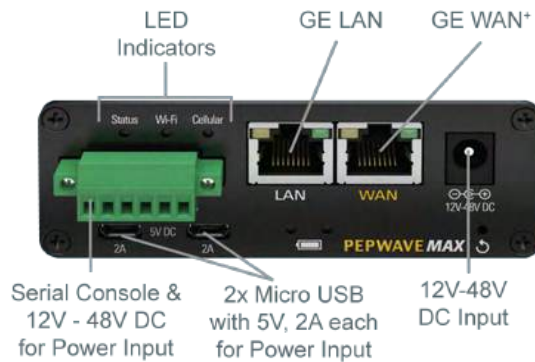
### 2.8.1 Panel Appearance



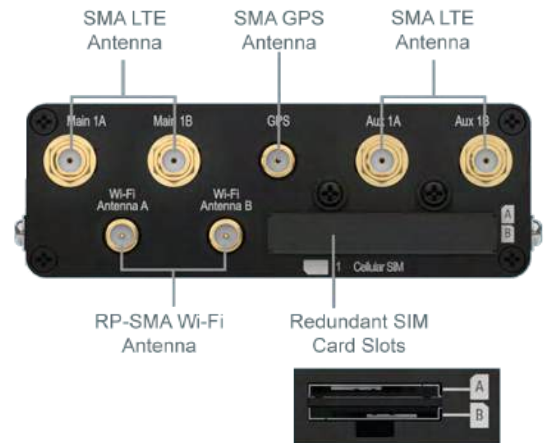
### MAX-TST (CAT-18)



#### Front



#### Back



### 2.8.2 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

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
	Blinking	Data is transferring
Orange LED	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

## 2.9 MAX Transit Mini

### 2.9.1 Panel Appearance



### 2.9.2 LED indicators

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

#### Status Indicators

<b>Status</b>	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Wi-Fi Indicators		
<b>Wi-Fi</b>	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 WAN Indicators		
<b>Cellular</b>	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

## 2.10 MAX HD2 and HD4 with MediaFast

### 2.10.1 Panel Appearance

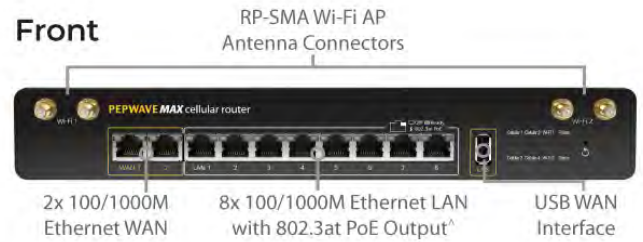


## Back

### HD4 with MediaFast



## Front



### HD2 with MediaFast



## 2.10.2 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

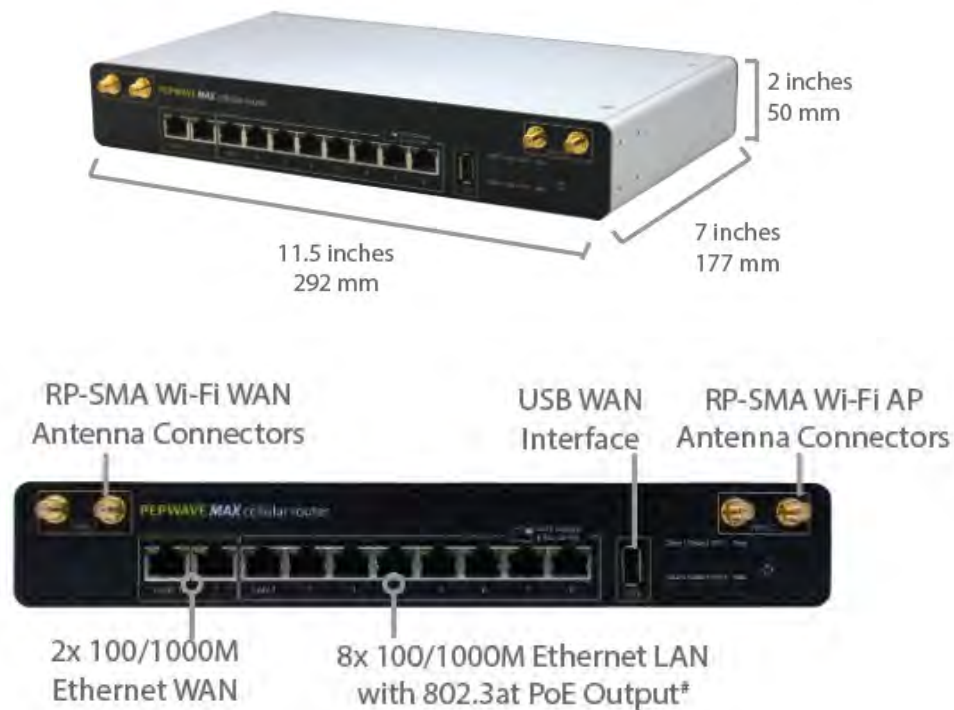
Wi-Fi AP and Wi-Fi WAN Indicators		
Wi-Fi WAN / Cellular 1 / Cellular 2	OFF	Disabled Intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

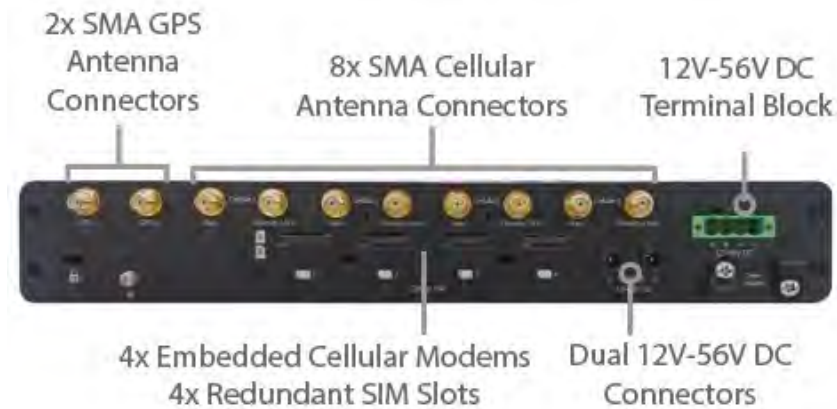
LAN and Ethernet WAN Ports		
Green LED	ON	10 / 100 / 1000 Mbps
Orange LED	Blinking	Data is transferring

	OFF	No data is being transferred or port is not connected
<b>Port Type</b>	Auto MDI/MDI-X ports	

## 2.11 MAX HD4

### 2.11.1 Panel Appearance





### 2.11.2 LED Indicators

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

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

Wi-Fi AP and Wi-Fi WAN Indicators		
<b>Wi-Fi WAN / Cellular 1 / Cellular 2</b>	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		
<b>Green LED</b>	ON	10 / 100 / 1000 Mbps
	Blinking	Data is transferring
<b>Orange LED</b>	OFF	No data is being transferred or port is not connected
<b>Port Type</b>	Auto MDI/MDI-X ports	

## 2.12 MAX HD4 MBX (CAT-12)

2.13 For certification information, please refer to [Appendix B: Declaration](#)

### 2.13.1 Panel Appearance



### 2.13.2 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



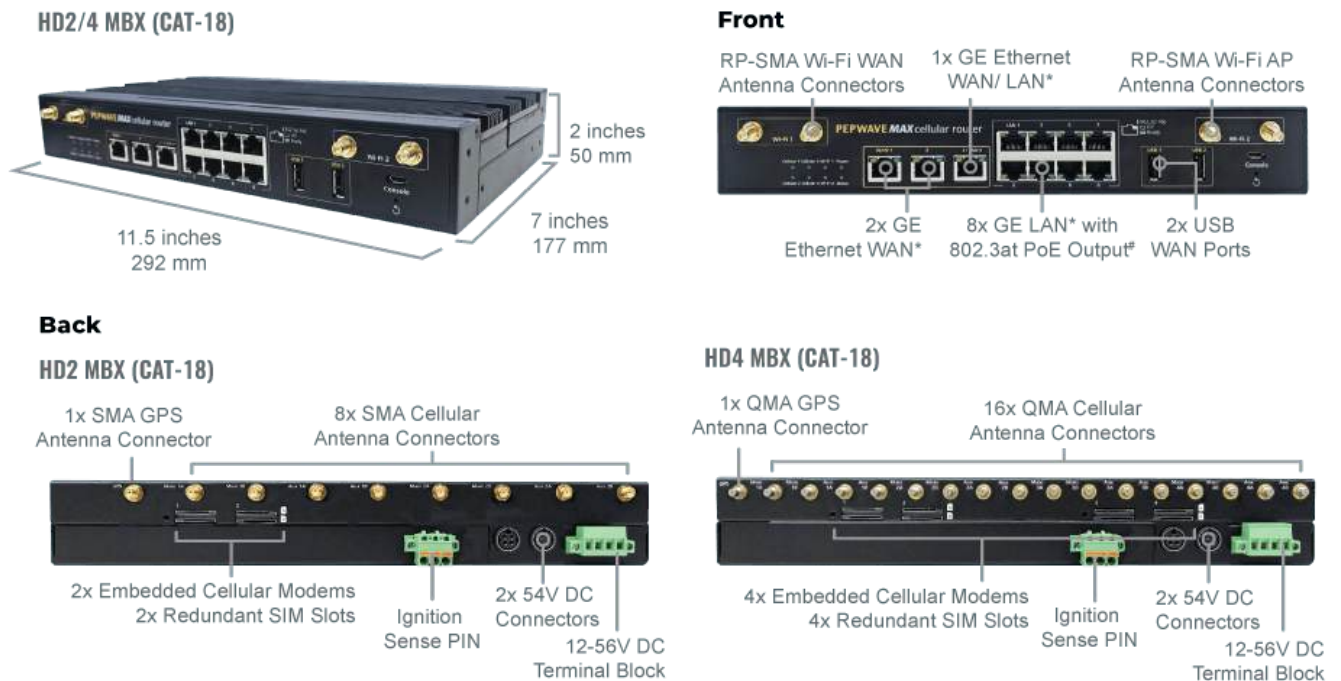
Wi-Fi AP and Wi-Fi WAN Indicators		
<b>Wi-Fi WAN / Cellular 1 / Cellular 2</b>	OFF	Disabled Intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

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



## 2.14 MAX HD2/4 MBX (CAT-18)

### 2.14.1 Panel Appearance



### 2.14.2 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

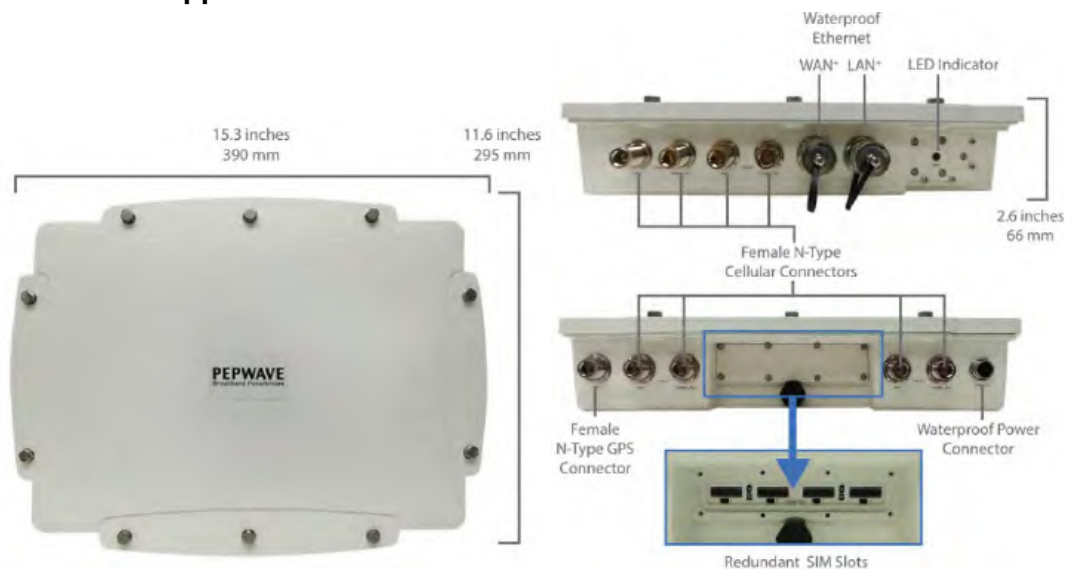
Wi-Fi AP and Wi-Fi WAN Indicators		
Wi-Fi WAN / Cellular 1 / Cellular 2	OFF	Disabled Intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic

	ON	Connected to wireless network(s) without traffic
--	----	--

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

## 2.15 MAX HD4 IP67

### 2.15.1 Panel Appearance



### 2.15.2 LED Indicators

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

## 2.16 MAX BR1 Classic

2.17 For certification information, please refer to [Appendix B: Declaration](#)

### 2.17.1 Panel Appearance



## 2.17.2 LED Indicators

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

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

Wi-Fi Indicators		
<b>Wi-Fi</b>	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

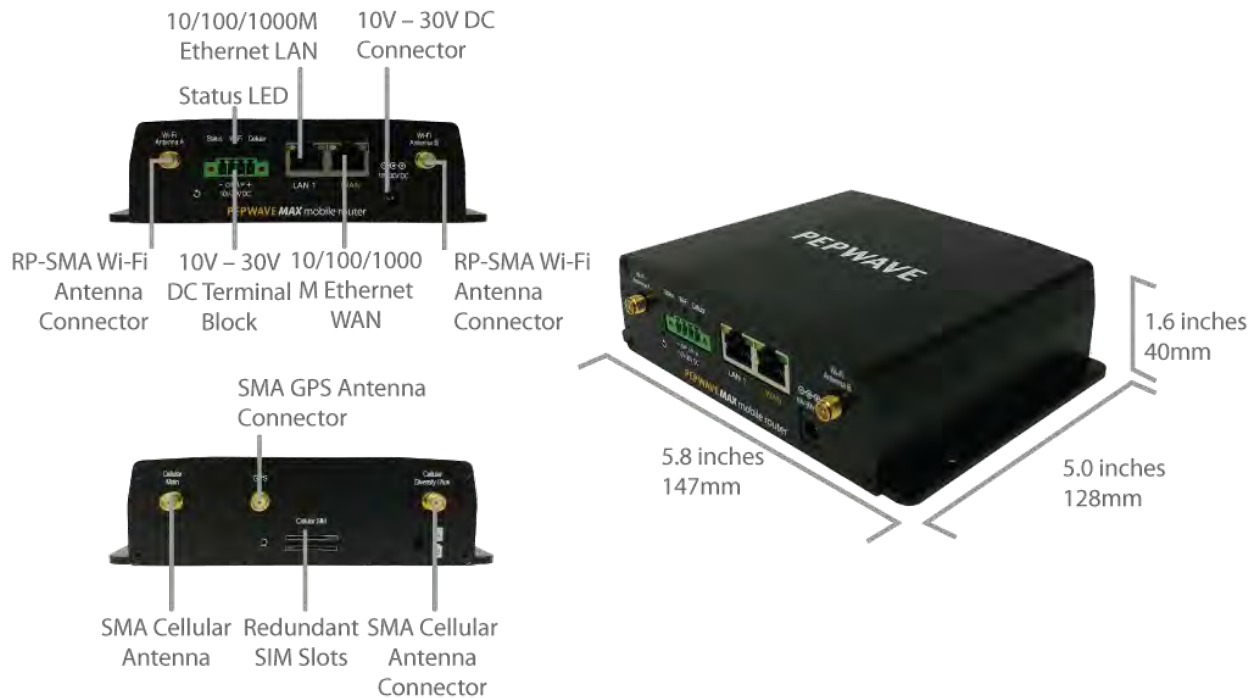
Cellular Indicators		
<b>Cellular</b>	OFF	Disabled or no SIM card inserted
	ON	Connecting or connected to network(s)

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

## 2.18 MAX BR1 MK2

2.19 For certification information, please refer to [Appendix B: Declaration](#)

### 2.19.1 Panel Appearance



### 2.19.2 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

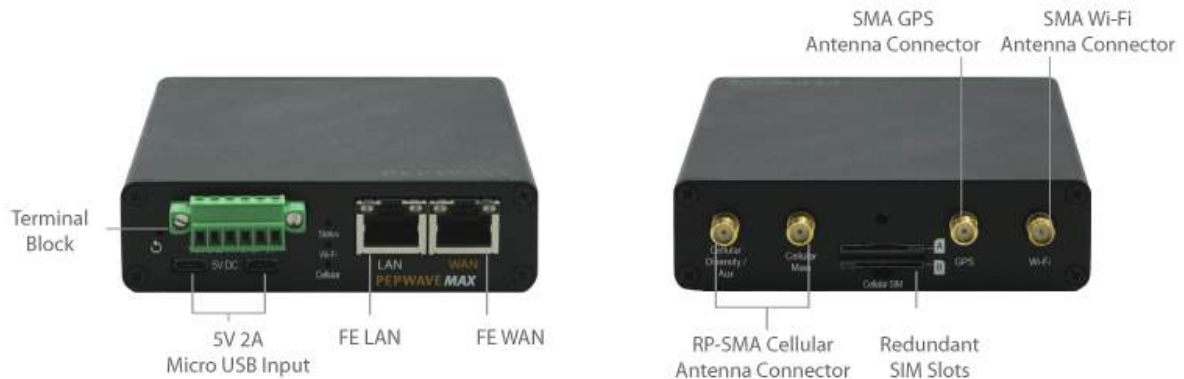
Wi-Fi Indicators		
<b>Wi-Fi</b>	OFF	Disabled intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

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

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

## 2.20 MAX BR1 Slim

### 2.20.1 Panel Appearance



### 2.20.2 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		
<b>Cellular</b>	OFF	Disabled or no SIM card inserted
	ON	Connecting or connected to network(s)

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



## 2.21 MAX BR1 Mini

2.22 For certification information, please refer to [Appendix B: Declaration](#)

### 2.22.1 Panel Appearance



### 2.22.2 LED Indicators

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	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

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

## 2.23 MAX BR1 Mini Core

### 2.23.1 Panel Appearance



### 2.23.2 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	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

## 2.24 MAX BR1 M2M

### 2.24.1 Panel Appearance



### 2.24.2 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	

## 2.25 MAX BR1 ENT

### 2.25.1 Panel Appearance



### 2.25.2 LED Indicators

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

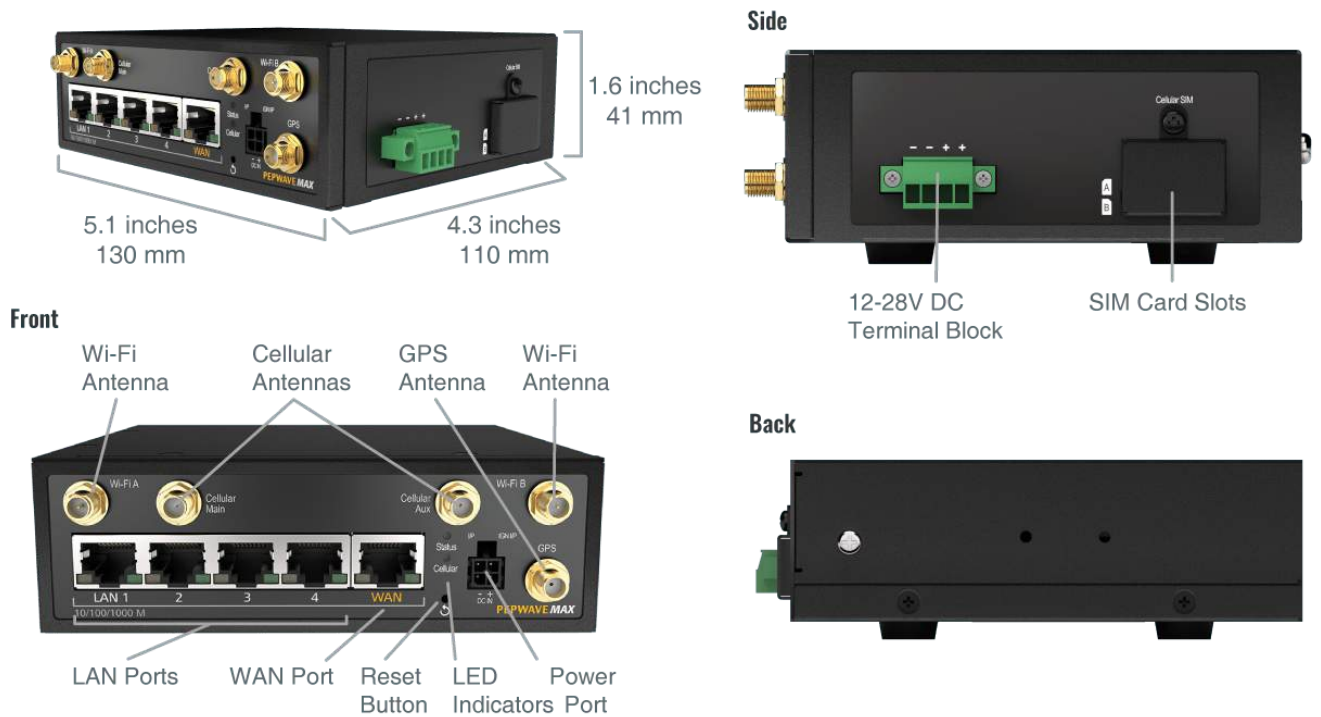
Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

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	

## 2.26 MAX BR1 Pro

### 2.26.1 Panel Appearance



### 2.26.2 LED Indicators

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

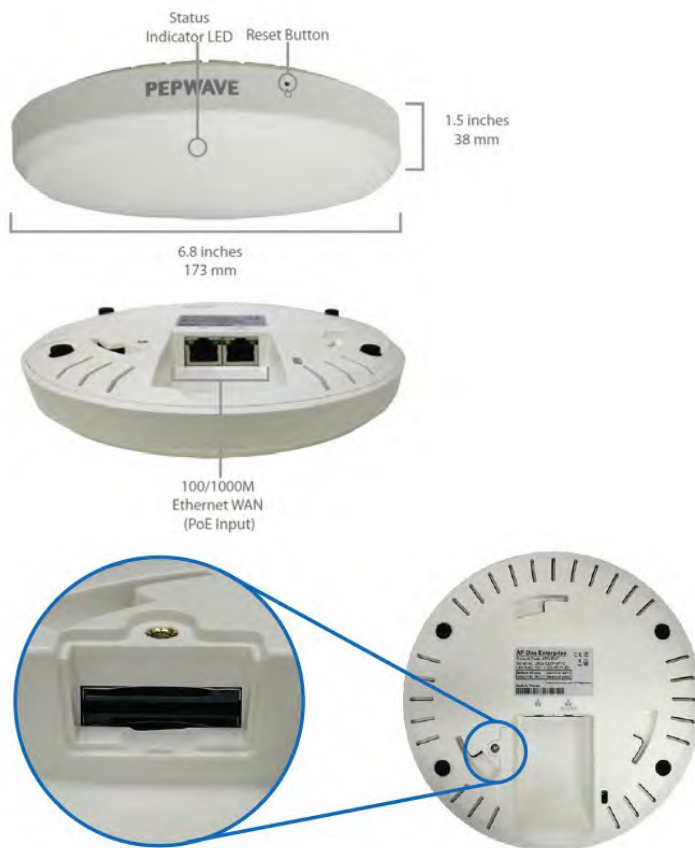
Status Indicators		
<b>Status</b>	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Cellular Indicators		
<b>Cellular</b>	OFF	Disabled or no SIM card inserted
	Blinking Slowly	Connecting to network(s)
	ON	Connected to network(s)

LAN and Ethernet WAN Ports		
Green LED	ON	1000 Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

## 2.27 MAX Hotspot

### 2.27.1 Panel Appearance



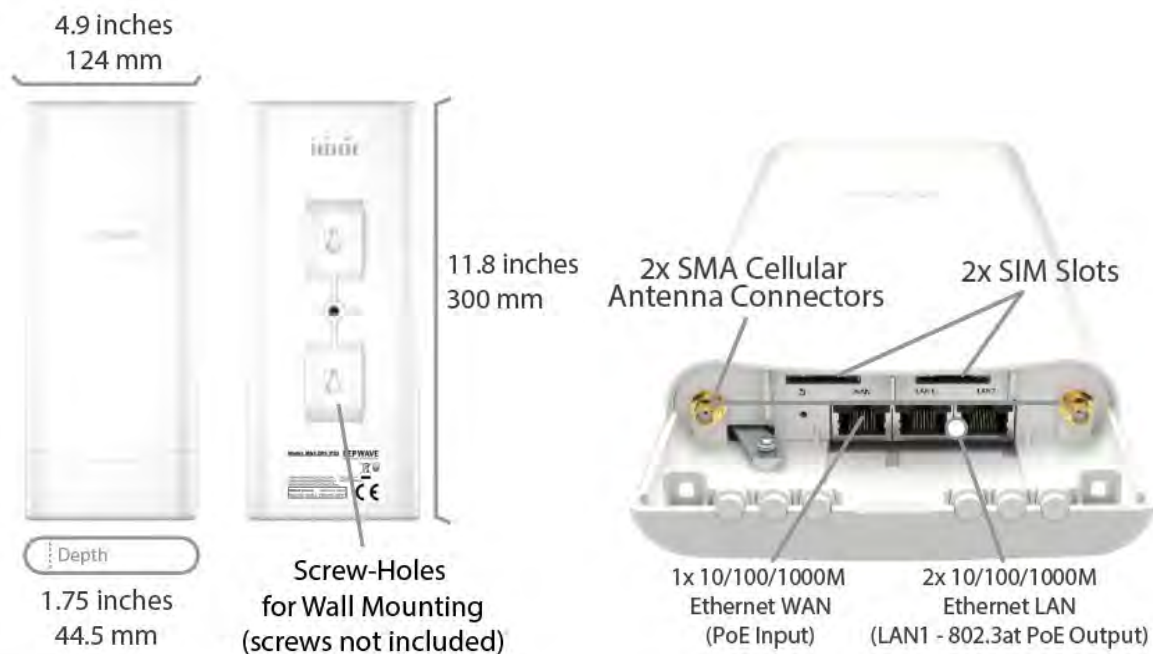


## 2.27.2 LED Indicators

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

## 2.28 MAX BR1 IP55

### 2.28.1 Panel Appearance




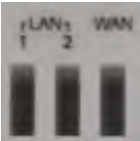
## 2.28.2 LED Indicators

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

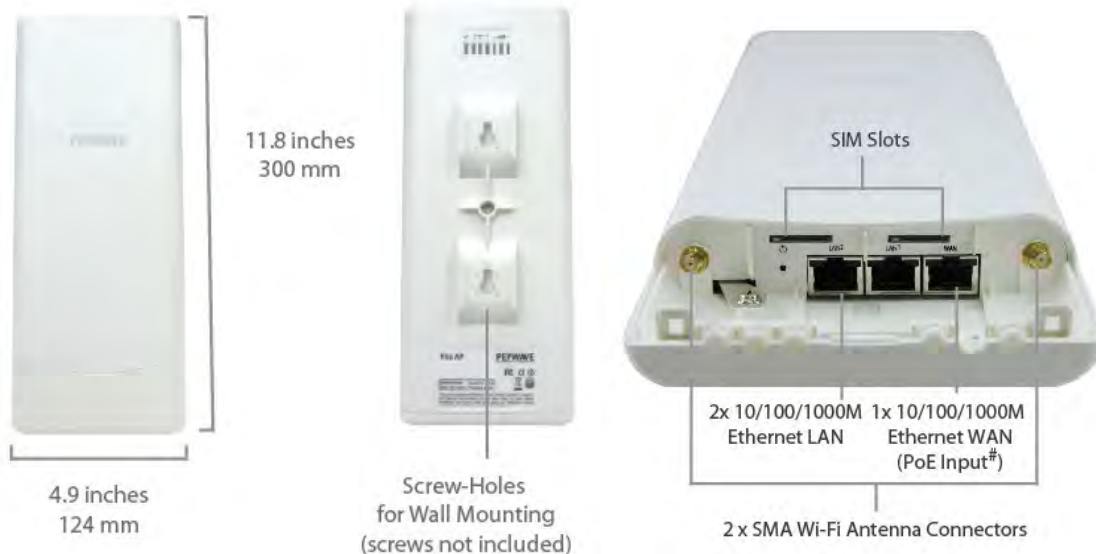
LAN and Ethernet WAN Ports		
Green LED	ON	1000Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

Cellular Indicators		
<b>Cellular</b> 	OFF	Disabled or no SIM card inserted
	Blinking	Connecting to network(s) in Standby Mode
	Green	Connected to network(s) in Priority 1 (Active)

LAN and WAN Indicators		
	Green	Powered-on device connected to Ethernet port
	OFF	No device connected to Ethernet port

## 2.29 MAX BR2 IP55

### 2.29.1 Panel Appearance



### 2.29.2 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

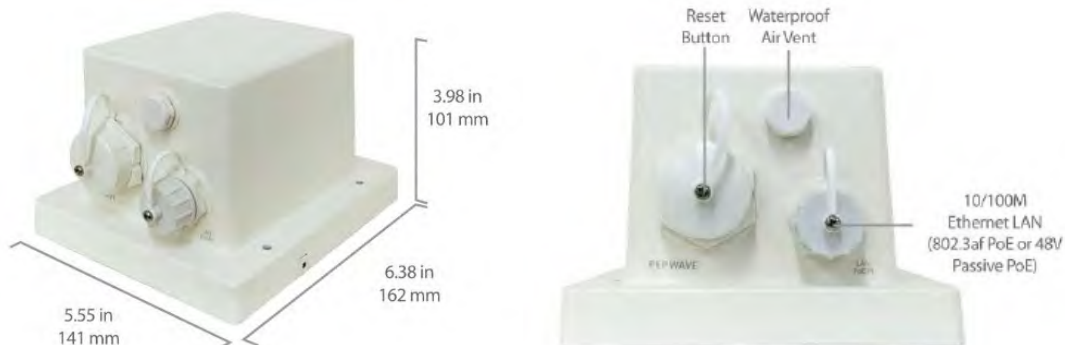
Wi-Fi Indicators		
Wi-Fi	OFF	Disabled Intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

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
	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	

## MAX BR1 IP67

### 2.29.3 Panel Appearance



## 2.30 MAX On-The-Go

### 2.30.1 Panel Appearance



### 2.30.2 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

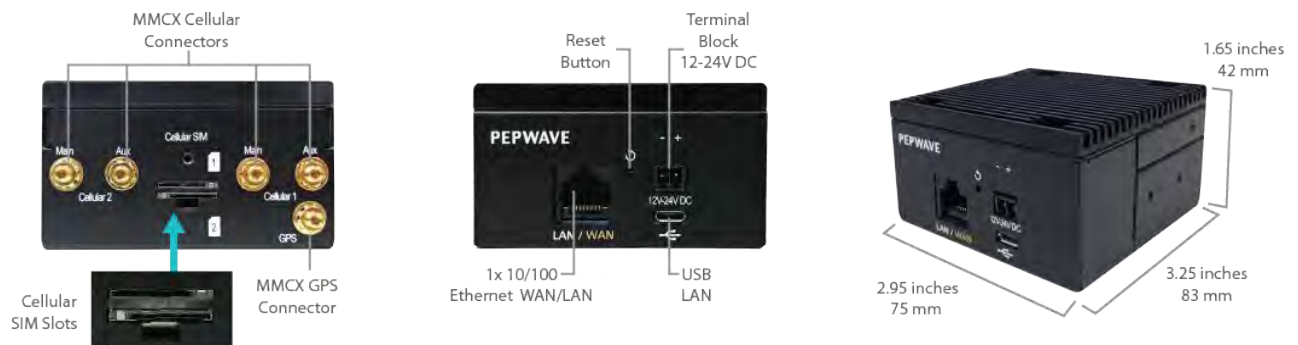
Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Green	Ready

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

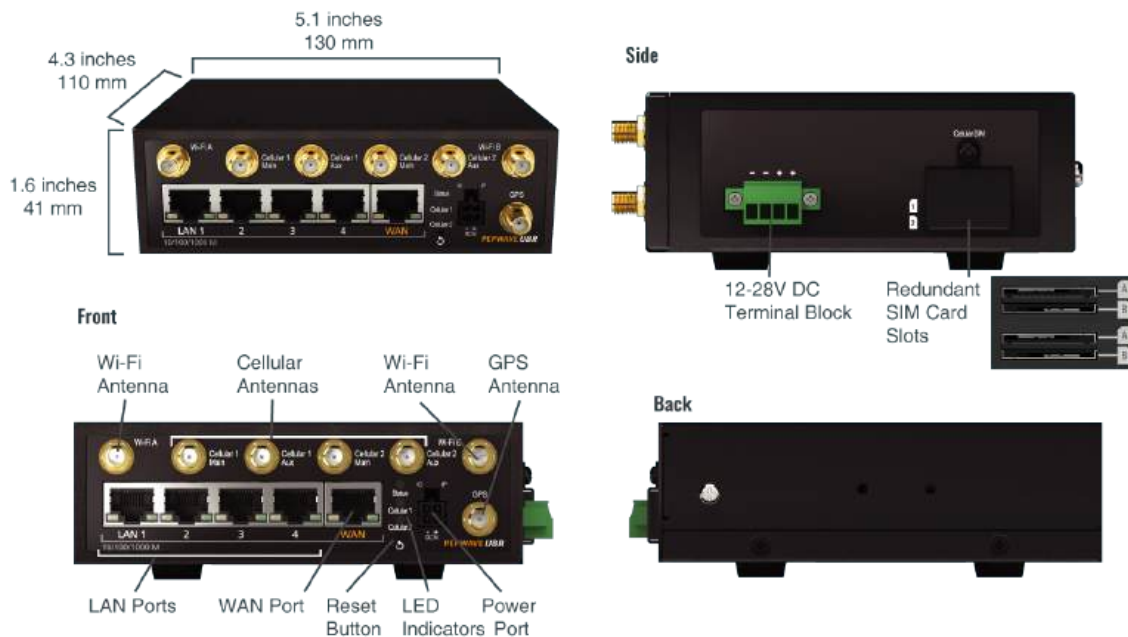
## 2.31 SpeedFusion Engine

### 2.31.1 Panel Appearance



## 2.32 UBR LTE

### 2.32.1 Panel Appearance



### 2.32.2 LED Indicators

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

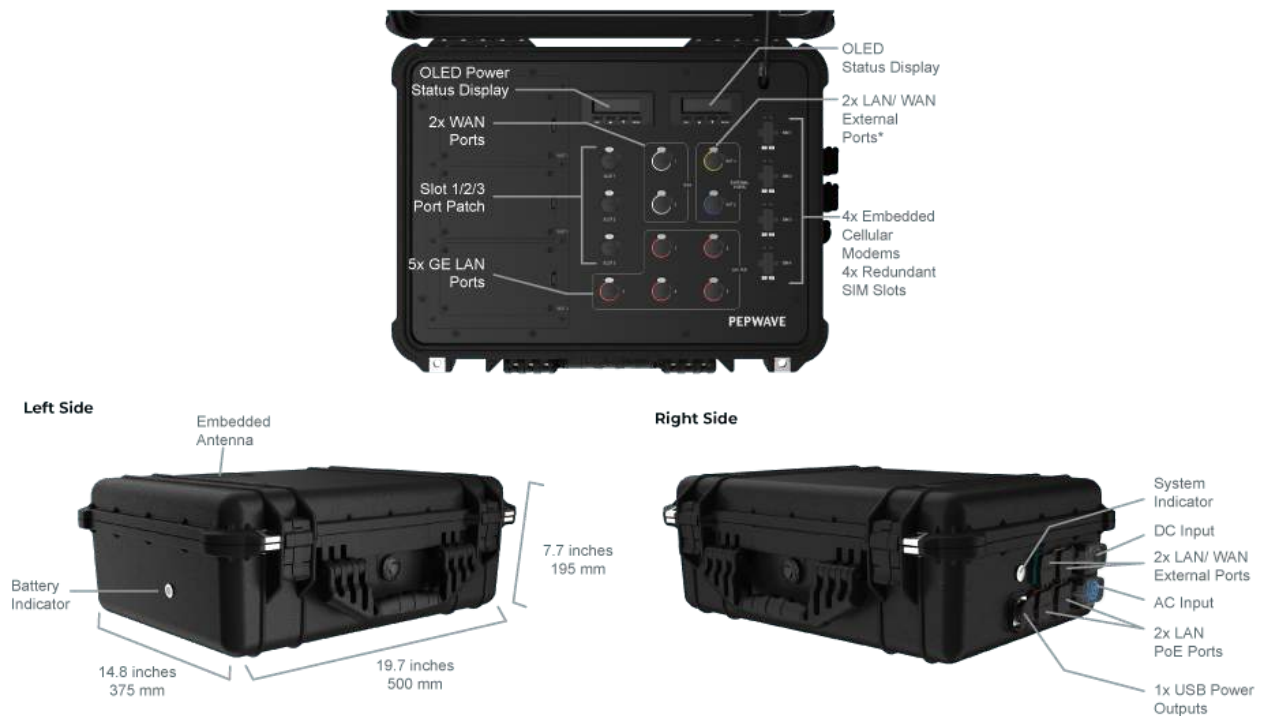
Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking Red	Boot up error
	Green	Ready

LAN and Ethernet WAN Ports		
Green LED	ON	1000 Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	Blinking Slowly	Connecting to network(s)
	Green	Connected to network(s)

## 2.33 PDX

### 2.33.1 Panel Appearance



### 2.33.2 LED Indicators



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

Status Indicators		
Status	OFF	No battery installed
	Red	Charging
	Blinking red	Low Battery
	Green	Full Charged

## 3 Advanced Feature Summary

### 3.1 Drop-in Mode and LAN Bypass: Transparent Deployment



As your organization grows, it may require more bandwidth, but modifying your network can be tedious. In **Drop-in Mode**, you can conveniently install your Peplink router without making any changes to your network. For any reason your Peplink router loses power, the **LAN Bypass** will safely and automatically bypass the Peplink router to resume your original network connection.

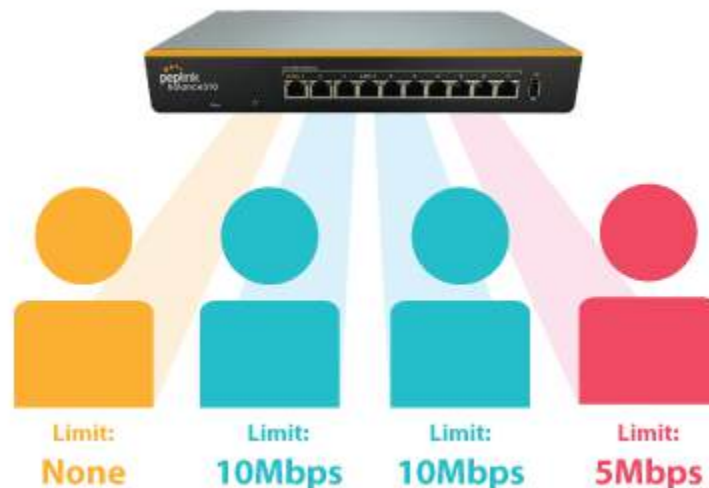
*Note: Drop-in mode is compatible for All MAX models except MAX BR1 IP67*

### 3.2 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.

### 3.3 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.

### 3.4 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)

### 3.5 USB Modem and Android Tethering



For increased WAN diversity, plug in a USB LTE modem as a 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)

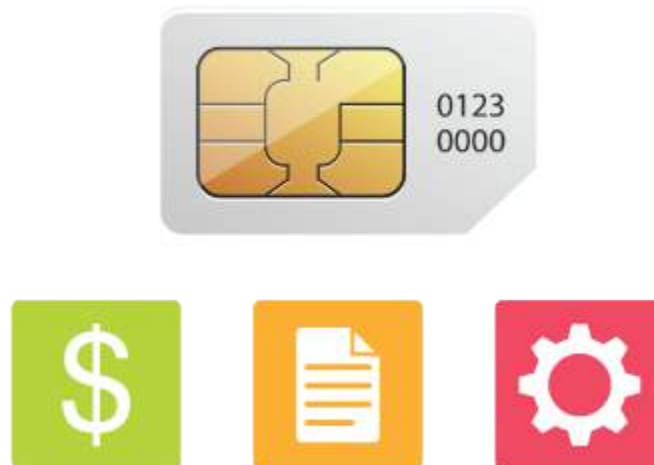
### 3.6 Built-In Remote User VPN Support



Use OpenVPN or 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 the full instructions on setting up L2TP with IPsec.](#)  
[Click here for the full instructions on setting up OpenVPN connections](#)

### 3.7 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.](#)

### 3.8 DPI Engine

The DPI report written in the updated KB article will show further information on InControl2 through breaking down application categories into subcategories.

<https://forum.peplink.com/t/updated-ic2-deep-packet-inspection-dpi-reports-and-everything-you-need-to-know-about-it/29658>

## 4 Installation

The following section details connecting Pepwave routers to your network.

### 4.1 Preparation

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

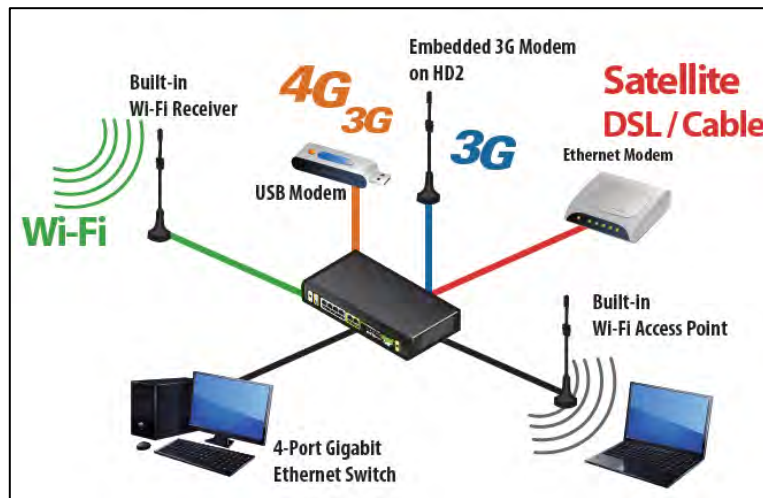
- At least one Internet/WAN access account and/or Wi-Fi access information
- Depending on network connection type(s), one or more of the following:
  - **Ethernet WAN:** A 10/100/1000BaseT UTP cable with RJ45 connector
  - **USB:** A USB modem
  - **Embedded modem:** A SIM card for GSM/HSPA service
  - **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 11 or above, Mozilla Firefox 24 or above, Apple Safari 7 or above, and Google Chrome 18 or above.

### 4.2 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:



## 4.3 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**.

# 5 Mounting the Unit

## 5.1 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. Recommended screw specification: M3.5 x 20mm, head diameter 6mm, head thickness 2.4mm.

The Pepwave MAX BR1 requires four screws for wall mounting.

## 5.2 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.

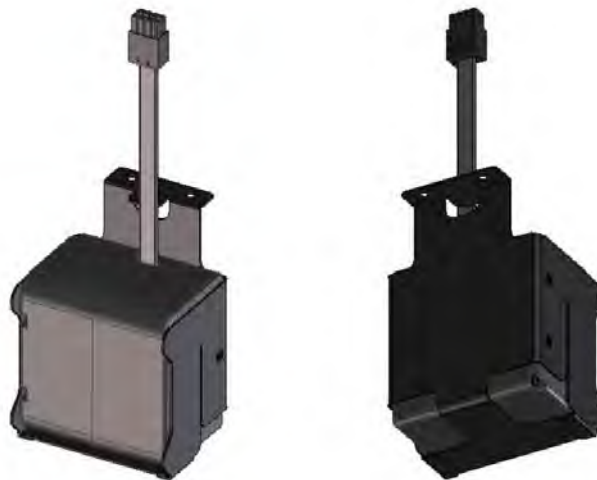


## 5.3 IP67 Installation Guide

Installation instructions for IP67 devices can be found here:  
[http://download.peplink.com/manual/IP67\\_Installation\\_Guide.pdf](http://download.peplink.com/manual/IP67_Installation_Guide.pdf)

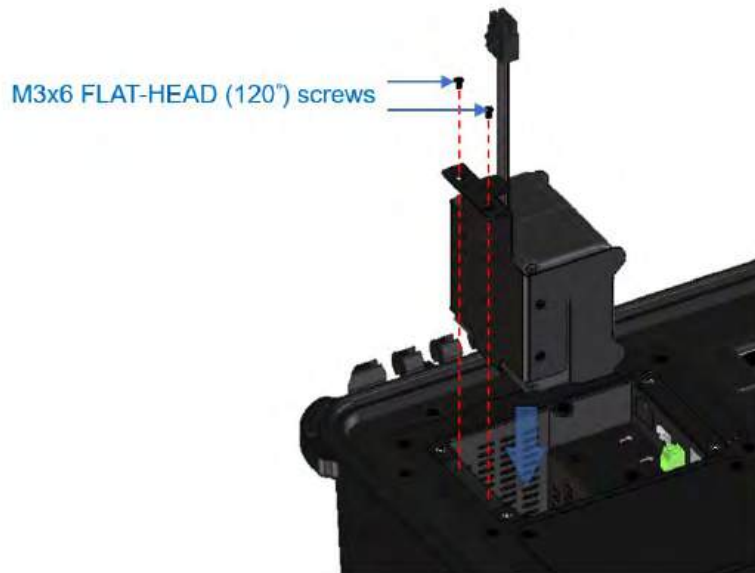
## 5.4 PDX Accessory Kit Installation Guide

### 5.4.1 Battery Set appearance



- Step 1: Lock the battery set in the slot with 2 pcs M3 screws.

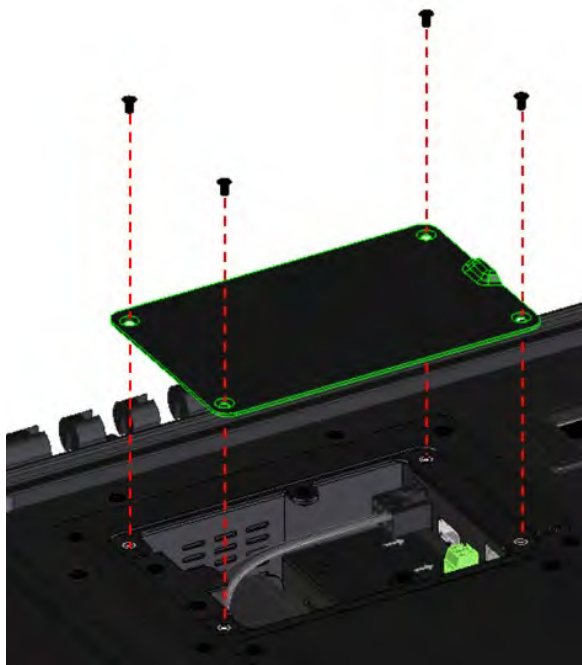




- Step 2: Plug power cable into the socket



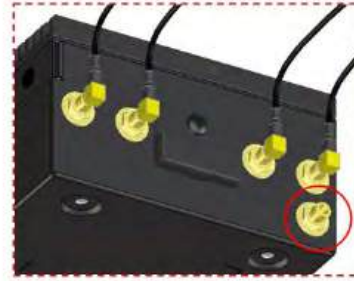
- STEP 3: Lock the slot cover with 4 pcs M3 screws.



#### 5.4.2 SFE-DUO Set appearance

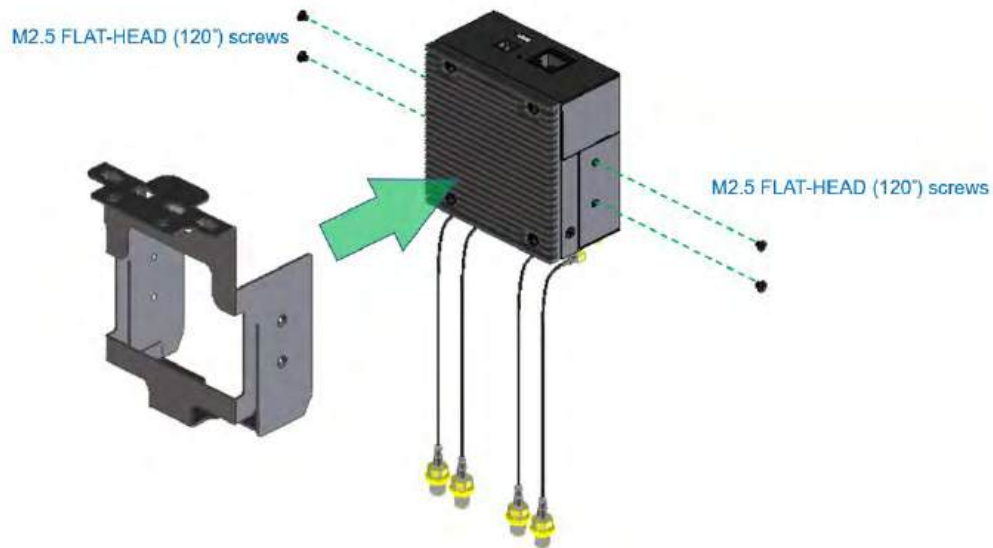


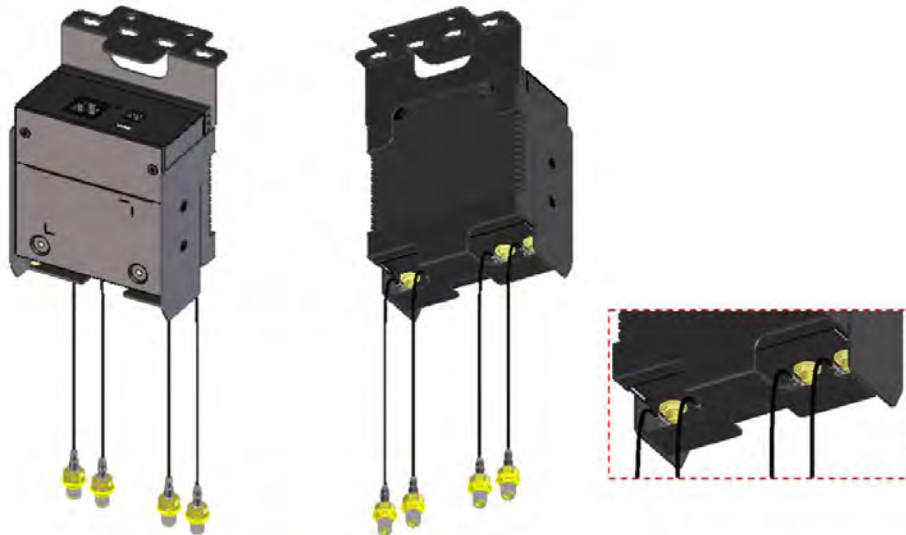
- STEP 1: Assemble SMA cables to the device



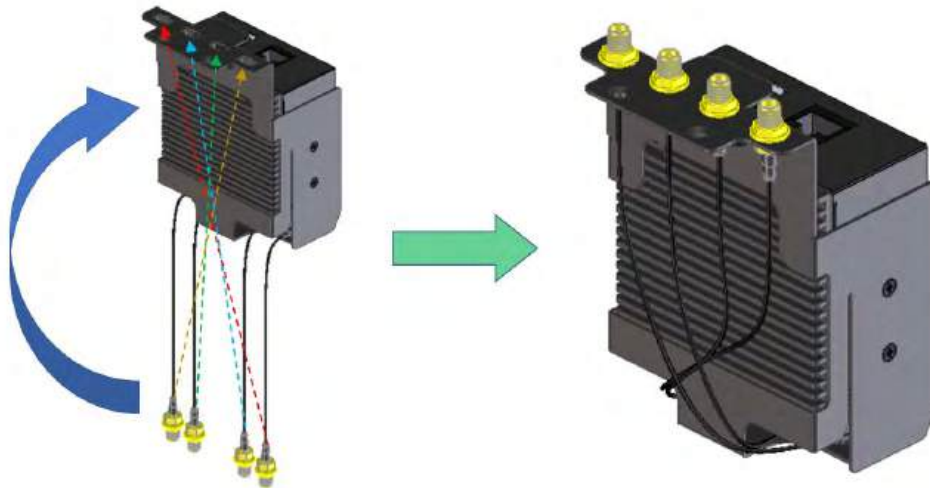
GPS port not in use

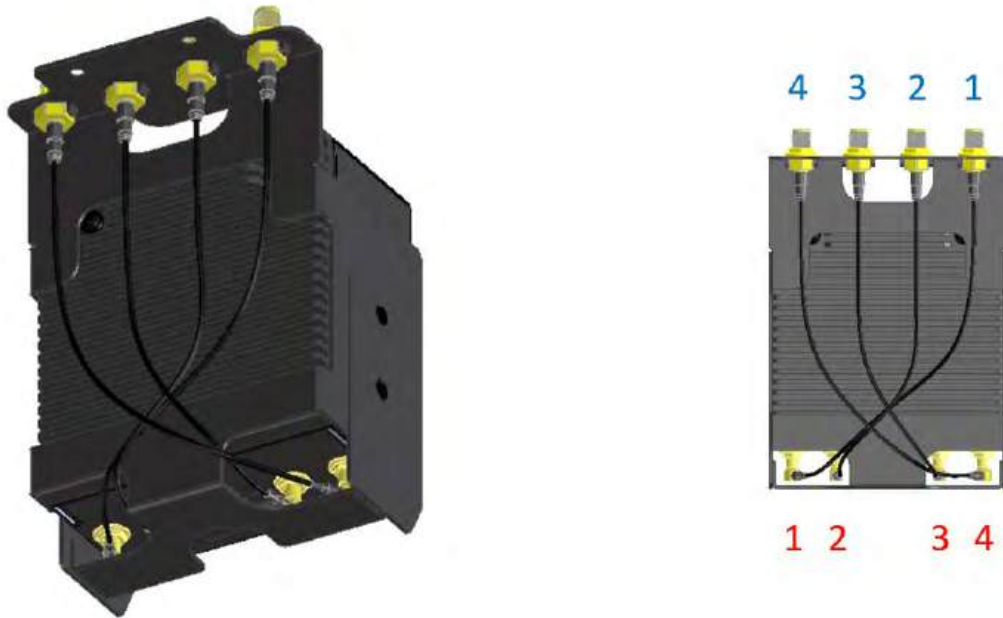
- STEP 2: Assemble bracket to the device



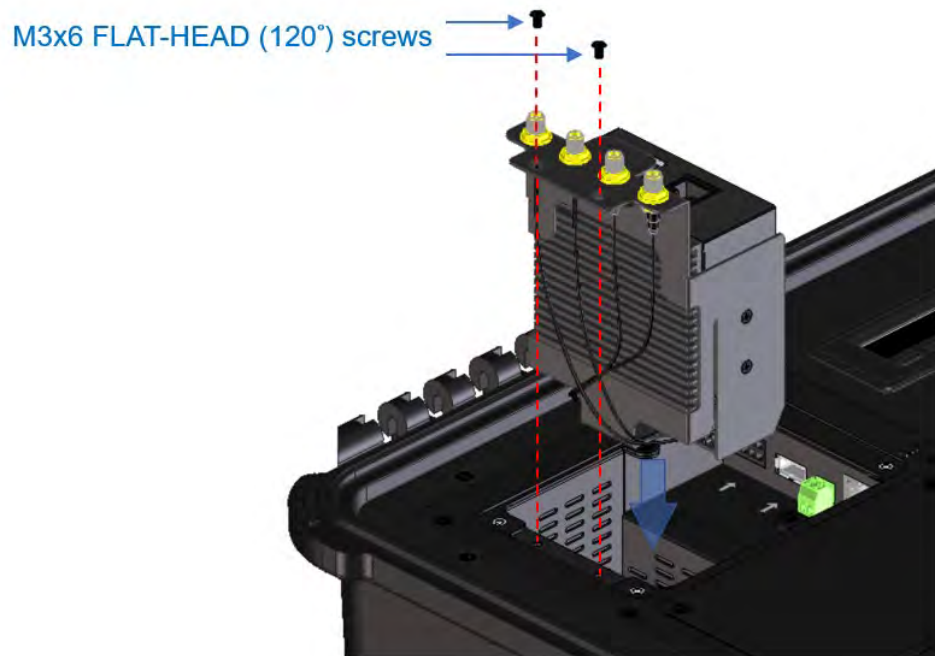


- STEP 3: Assemble SMA connectors to the bracket

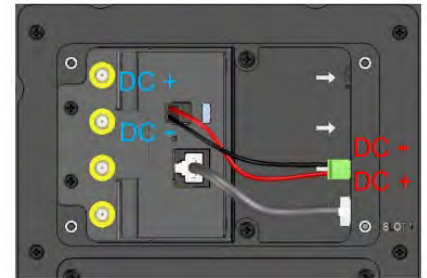
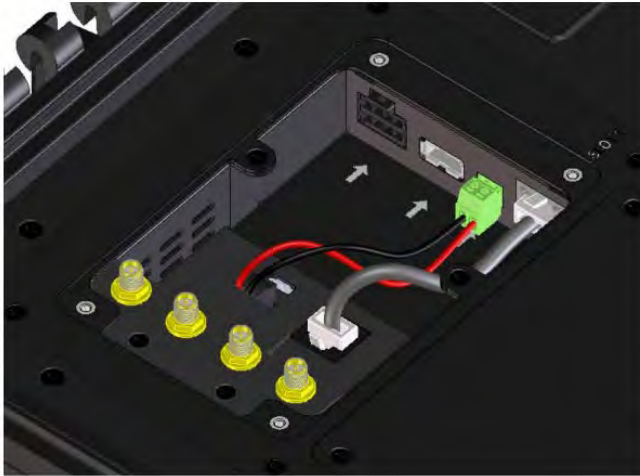




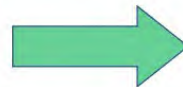
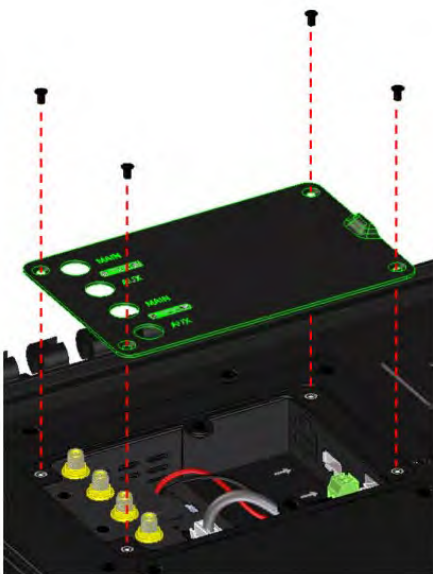
- STEP 4: Lock the SFE-Duo set in the slot with 2 pcs M3 screws.



- STEP 5: Connect DC power & ETH port



- STEP 6: Lock the slot cover with 4 pcs M3 screws.



## 6 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.)

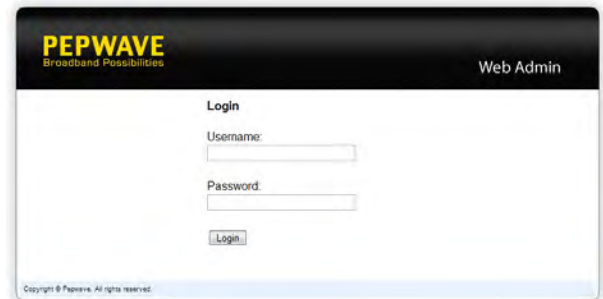


3. Enter the following to access the web admin interface.

**Username:** admin

**Password:** admin

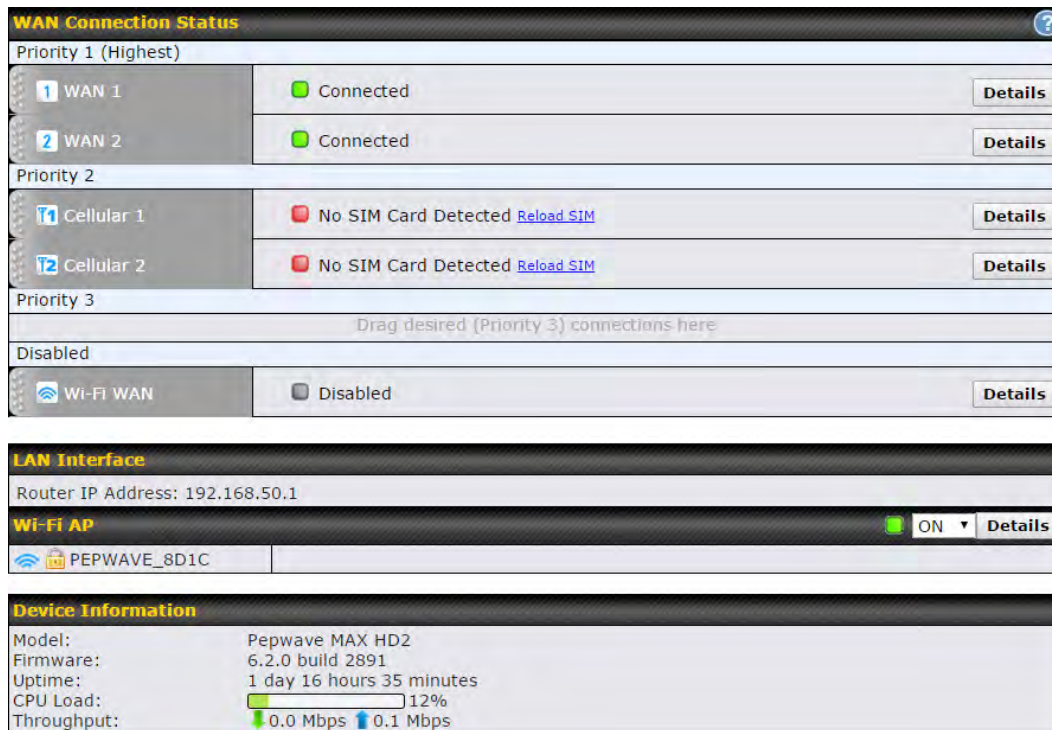
(This is the default username and password for Pepwave routers).



- You must change the default password on the first successful login.
- Password requirements are: A minimum of 10 lower AND upper case characters, including at least 1 number.
- When HTTP is selected, the URL will be redirected to HTTPS by default.



After successful login, the **Dashboard** of the web admin interface will be displayed.



**WAN Connection Status**

Priority 1 (Highest)

1 WAN 1	Connected	<a href="#">Details</a>
2 WAN 2	Connected	<a href="#">Details</a>

Priority 2

1 Cellular 1	No SIM Card Detected <a href="#">Reload SIM</a>	<a href="#">Details</a>
2 Cellular 2	No SIM Card Detected <a href="#">Reload SIM</a>	<a href="#">Details</a>

Priority 3

Drag desired (Priority 3) connections here

Disabled

Wi-Fi WAN	Disabled	<a href="#">Details</a>
-----------	----------	-------------------------

**LAN Interface**

Router IP Address: 192.168.50.1

**Wi-Fi AP** ON [Details](#)

PEPWAVE\_8D1C

**Device Information**

Model:	Pepwave MAX HD2
Firmware:	6.2.0 build 2891
Uptime:	1 day 16 hours 35 minutes
CPU Load:	12%
Throughput:	0.0 Mbps ↑ 0.1 Mbps

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.



## 7 SpeedFusion Cloud

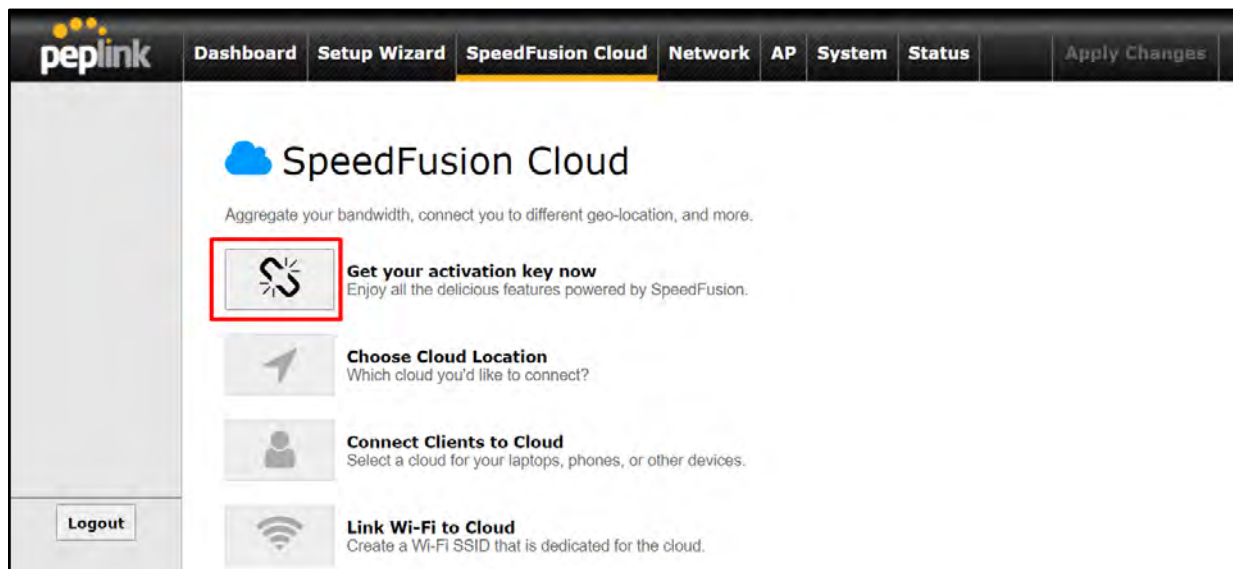
With Peplink products, your device is able to connect to SpeedFusion Cloud without the use of a second endpoint. This service has wide access to a number of SpeedFusion endpoints hosted from around the world, providing your device with unbreakable connectivity wherever you are.\*



\*SpeedFusion Cloud is supported in firmware version 8.1.0 and above. SpeedFusion Cloud is a subscription basis. SpeedFusion Cloud license can be purchased at <https://store.peplink.com/> > Cloud Solutions > SpeedFusion Cloud Service.

### 7.1 Activate SpeedFusion Cloud Service

You are entitled to a 90-day free period with 100GB of SpeedFusion traffic upon activation of the SpeedFusion Cloud service. This offer is limited to once per device. To get your activation key please visit SpeedFusion Cloud.



Enter an email address and device serial number, check **I'm not a robot** then click **Submit**. You should receive a SpeedFusion Cloud license key via email after clicking the **Submit** button.

SpeedFusion Cloud Device Entry

Please input the following details

Email \*

receiver@abc.com

Device Serial number(s) \*

1919-1D1D-0707

☐ I'm not a robot

Reset Submit

- **Step 1 - Update to Firmware 5.1.0 or above**
- **Step 2 - Enter Serial Numbers:** Enter the serial numbers of the devices you wish to enable the SpeedFusion Cloud service for. This page supports 200 devices maximum, so if you have more than that, please use multiple entries.
- **Step 3 - Receive Confirmation Email:** Once registration is complete, we will send you a confirmation email including license keys.
- **Step 4 - Apply SpeedFusion License:**
  - With InControl: InControl will then push the license automatically.
  - Without InControl: Apply the license keys from the WebUI by navigating to System > Feature Add-ons.
- **Step 5 - Assign Traffic:** Use Outbound Policy to define the traffic you want to protect using the SpeedFusion Cloud.

Please Note: The 90-day free period with 100GB of SpeedFusion traffic will begin once the SpeedFusion cloud service has been activated. Each device can only apply once.

From **System > Features Add-ons**, paste the license key into the window and click on **Activate** once you have received the license key.

PEPWAVE Dashboard SpeedFusion Cloud Network Advanced AP System Status Apply Changes

System

- Admin Security
- Firmware
- Time
- Schedule
- Email Notification
- Event Log
- SNMP
- SMS Control
- InControl
- Configuration
- Feature Add-ons
- Reboot

Tools

- Ping
- Traceroute
- Wake-on-LAN
- WAN Analysis

Feature Activation

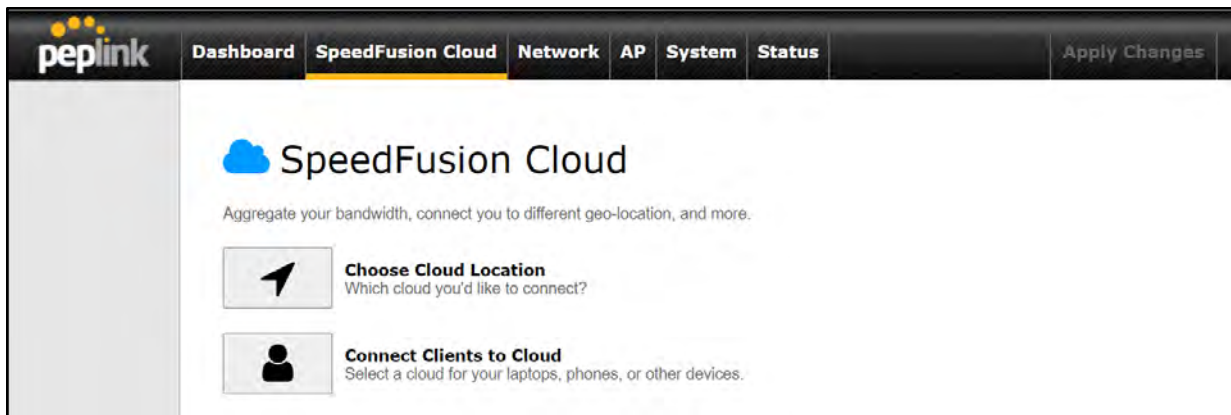
Activation Key

9629a523e54fe148f876e75cf95df776f248e248b618b618a6199b23e54fe148f876e75cf95df776f351e640e450b618b618a310ae10a711a219a6249c5af05ef747c958e346e248c95bf75df309a709a3199c7ae64cf34dd05ce540f947b66afa46e34db668f55dff5ff75dff46f809dd4cef09be18a619d16bbfa96c3083b48a7d337ade187a5ce2e4e1

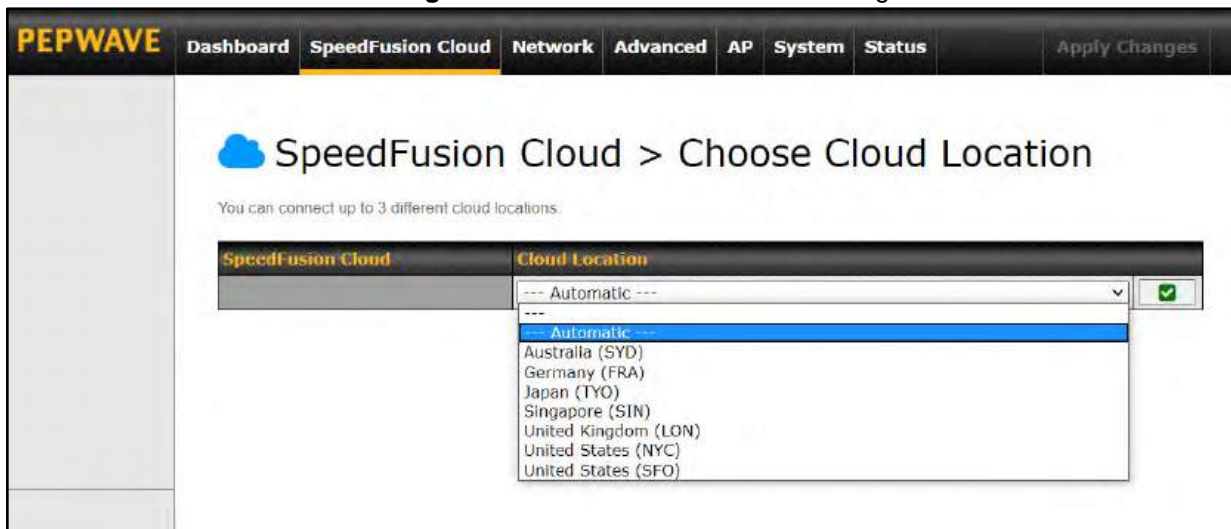
Activate

## 7.2 Enable SpeedFusion Cloud

Enable SpeedFusion Cloud from **SpeedFusion Cloud > Choose Cloud Location**.



Choose **Automatic** > Click on the **green tick button** to confirm the change.



Click on **Apply Changes** to save the change.

**PEPWAVE** Dashboard **SpeedFusion Cloud** Network Advanced AP System Status **Apply Changes**

Saved! Changes will be effective after clicking the 'Apply Changes' button.

## SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

SpeedFusion Cloud	Cloud Location
SFC	--- Automatic ---

**PEPWAVE** Dashboard **SpeedFusion Cloud** Network Advanced AP System Status **Apply Changes**

Changes applied successfully.

## SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

SpeedFusion Cloud	Cloud Location
SFC	--- Automatic ---

By default, the router will build a SpeedFusion tunnel to the SpeedFusion Cloud

**PEPWAVE** Dashboard SpeedFusion Cloud Network Advanced AP System Status Apply Changes

### WAN Connection Status

Priority 1 (Highest)  
Drag desired (Priority 1) connections here

Priority 2

1 Cellular 1	Connected to MY MAXIS LTE-A	Details
2 Cellular 2	Connected to MY MAXIS LTE-A	Details

Priority 3  
Drag desired (Priority 3) connections here

Disabled

1 WAN 1	Disabled	Details
2 WAN 2	Disabled	Details
3 Cellular 3	Disabled	Details
4 Cellular 4	Disabled	Details
Wi-Fi WAN	Disabled	Details
3 LAN 1 as WAN	Disabled	Details
4 LAN 2 as WAN	Disabled	Details
5 LAN 3 as WAN	Disabled	Details

### LAN Interface

Router IP Address: 192.168.50.1

### Wi-Fi AP

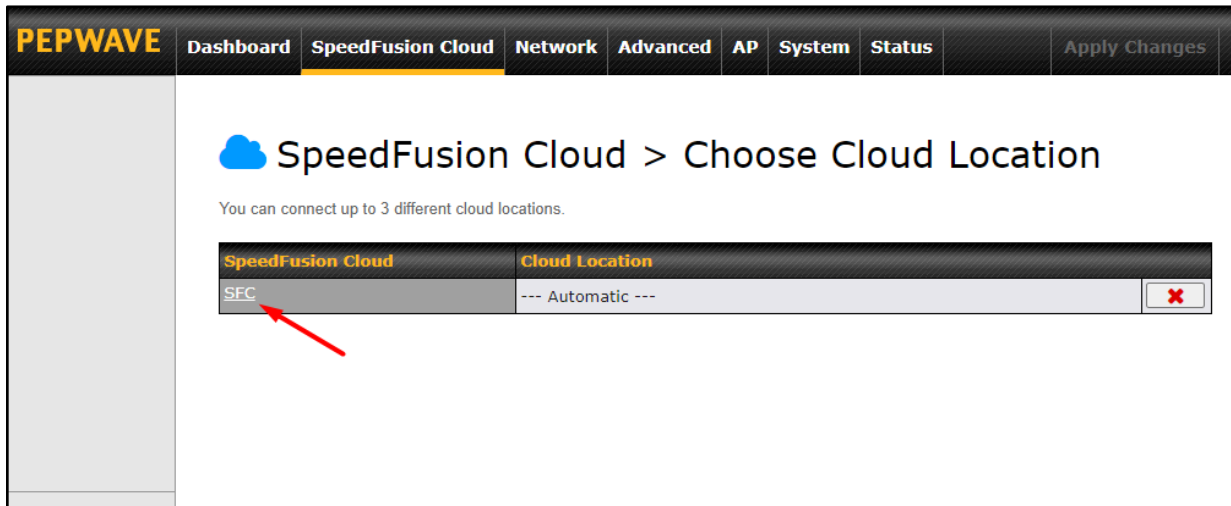
ON Details

PEPWAVE\_EBB4

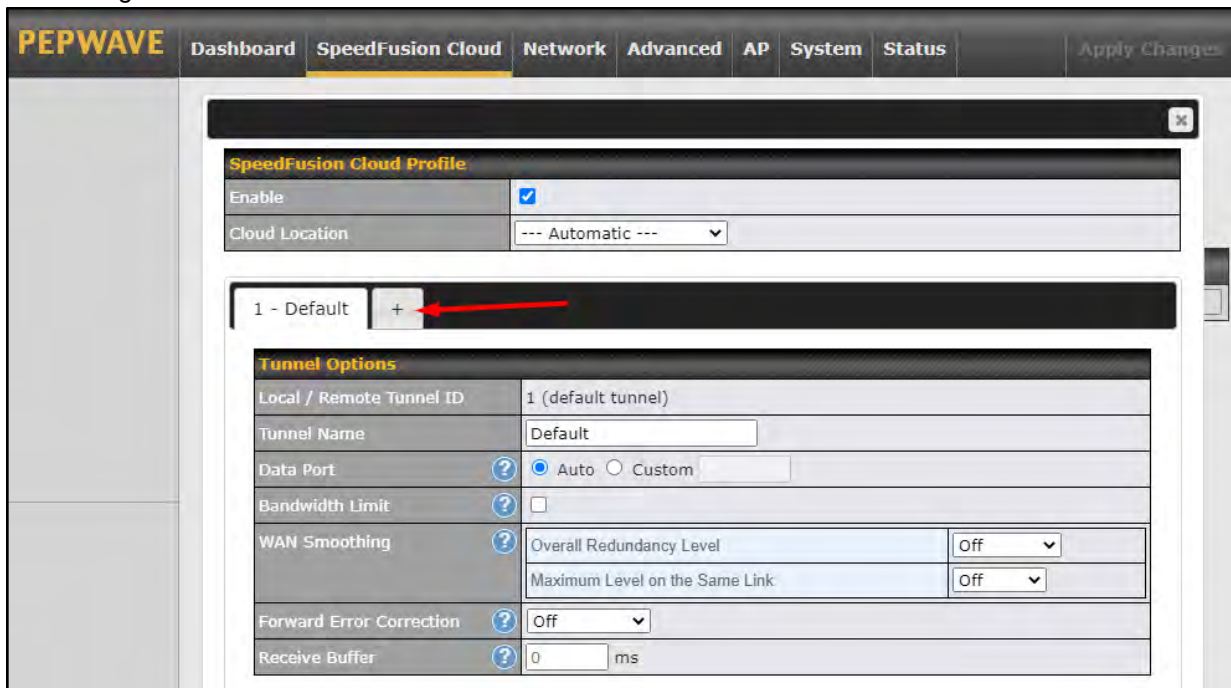
### SpeedFusion Cloud

SFC	Established
Data usage allowance: 98.40 GB (Expiry date: Sep 01, 2020)	

If you are running a latency sensitive service like video streaming or VOIP, a WAN Smoothing sub-tunnel can be created. Navigate to **Speedfusion Cloud > Choose a cloud location > SFC**.



A Speedfusion tunnel configuration window will pop out. Click on the + sign to create the WAN Smoothing sub-tunnel.





**PEPWAVE** Dashboard **SpeedFusion Cloud** Network Advanced AP System Status Apply Changes

**SpeedFusion Cloud Profile**

Enable	<input checked="" type="checkbox"/>
Cloud Location	--- Automatic ---

1 - Default 2 - WAN Smoo... +

**Tunnel Options**

Local / Remote Tunnel ID	2	
Tunnel Name	WAN Smoothing	
Data Port	<input checked="" type="radio"/> Auto <input type="radio"/> Custom	
Bandwidth Limit	<input type="checkbox"/>	
WAN Smoothing	Overall Redundancy Level	Normal
	Maximum Level on the Same Link	Normal
Forward Error Correction	Off	
Receive Buffer	0 ms	

Click on **Save** and **Apply Changes** to save the configuration. Now, the router has 2 Speedfusion tunnels to the Speedfusion Cloud.

**PEPWAVE**
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
Apply Changes

**WAN Connection Status**

Priority 1 (Highest)

Drag desired (Priority 1) connections here

Priority 2

1
Cellular 1

Connected to MY MAXIS **LTE-A**

Details

2
Cellular 2

Connected to MY MAXIS **LTE-A**

Details

Priority 3

Drag desired (Priority 3) connections here

Disabled

1
WAN 1

☐ Disabled

Details

2
WAN 2

☐ Disabled

Details

3
Cellular 3

☐ Disabled

Details

4
Cellular 4

☐ Disabled

Details

Wi-Fi WAN

☐ Disabled

Details

3
LAN 1 as WAN

☐ Disabled

Details

4
LAN 2 as WAN

☐ Disabled

Details

5
LAN 3 as WAN

☐ Disabled

Details

**LAN Interface**

Router IP Address: 192.168.50.1

**Wi-Fi AP**

☒ ON

Details

Wi-Fi
PEPWAVE\_EBB4

**SpeedFusion Cloud**

SFC (1 - Default)

☒ Established

SFC (2 - WAN Smoothing)

☒ Established

Data usage allowance: 98.40 GB (Expiry date: Sep 01, 2020)

Create an outbound policy to steer the internet traffic to go into Speedfusion Cloud. Please go to **Advanced > Outbound Policy**, click on **Add Rule** to create a new outbound policy.



PEPWAVE

DashboardSpeedFusion CloudNetworkAdvancedAPSystemStatus

Apply Changes

Advanced

SpeedFusion

IPsec VPN

GRE Tunnel

Outbound Policy

Port Forwarding

NAT Mappings

QoS

User Groups

Bandwidth Control

Application

Firewall

Access Rules

Content Blocking

Routing Protocols

OSPF & RIPv2

BGP

Remote User Access

Misc. Settings

High Availability

RADIUS Server

Certificate Manager

Service Forwarding

Service Passthrough

GPS Forwarding

NTP Server

Grouped Networks

Outbound Policy

Custom

Add a New Custom Rule

Service Name

to\_internet

Enable

☒

Source

IP Address

192.168.50.10

Destination

Any

Protocol

Any

:: Protocol Selection ::

Algorithm

Priority

Priority Order

Highest Priority

Cloud: SFC (1 - Defau...

Cloud: SFC (2 - WAN ...

WAN: WAN 1

WAN: WAN 2

WAN: Cellular 1

WAN: Cellular 2

WAN: Cellular 3

WAN: Cellular 4

WAN: USB

WAN: Wi-Fi WAN

WAN: LAN 1 as WAN

WAN: LAN 2 as WAN

WAN: LAN 3 as WAN

Lowest Priority

Not in Use

When No Connections are Available

Drop the Traffic

Terminate Sessions on Connection Recovery

☐ Enable

Save

Cancel

**Outbound Policy**

Custom

**Rules ( Drag and drop rows by the left to change rule order)**

Service	Algorithm	Source	Destination	Protocol / Port	
PepVPN / OSPF / BGP / RIPv2 Routes					
SpeedFusion Cloud Routes					
to internet	Priority VPN: SFC (1 - Def...	IP Address 192.168.50.10	Any	Any	✖
HTTPS Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	✖
Default	(Auto)				
Add Rule					

**Expert Mode**

Enabled

## 7.3 Connect Clients to Cloud

SpeedFusion Cloud provides a convenient way to route the LAN client to the cloud. From **SpeedFusion Cloud > Connect Clients to Cloud**.

peplink
Dashboard
SpeedFusion Cloud
Network
AP
System
Status
Apply Changes

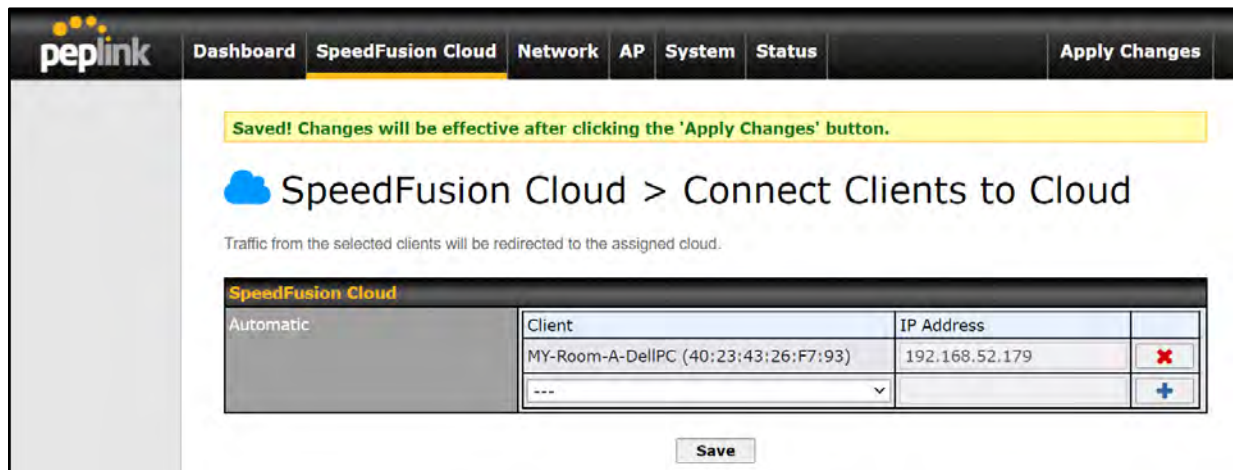
SpeedFusion Cloud

Aggregate your bandwidth, connect you to different geo-location, and more.

Choose Cloud Location  
Which cloud you'd like to connect?

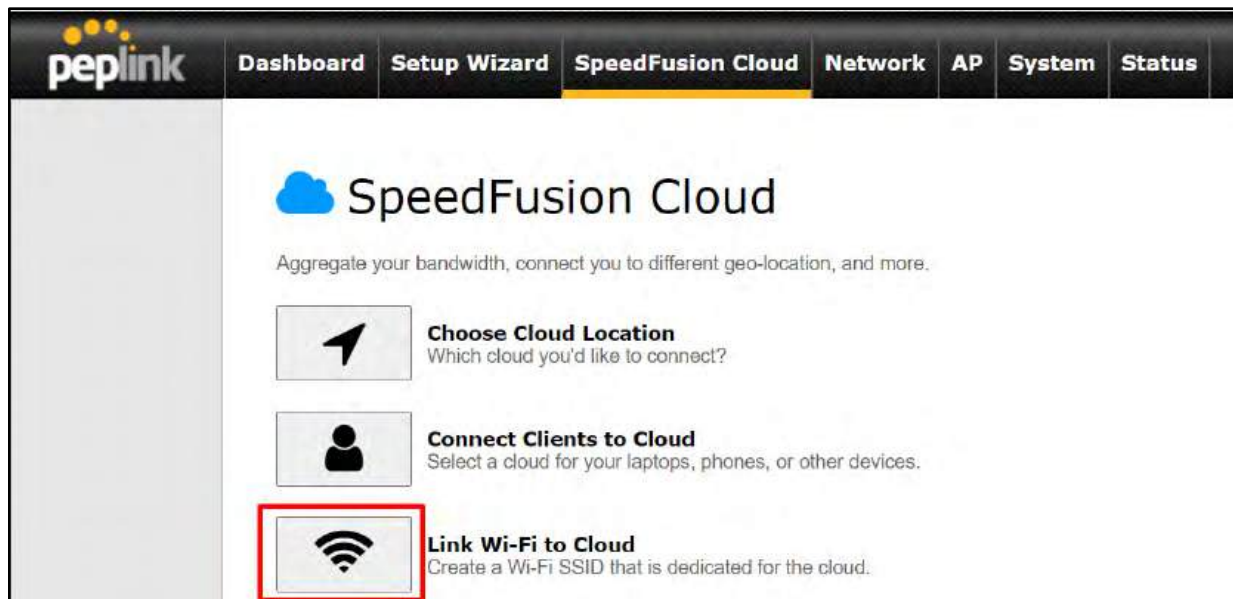
Connect Clients to Cloud  
Select a cloud for your laptops, phones, or other devices.

Choose a client from the drop down list > Click + > Save > Apply Changes.

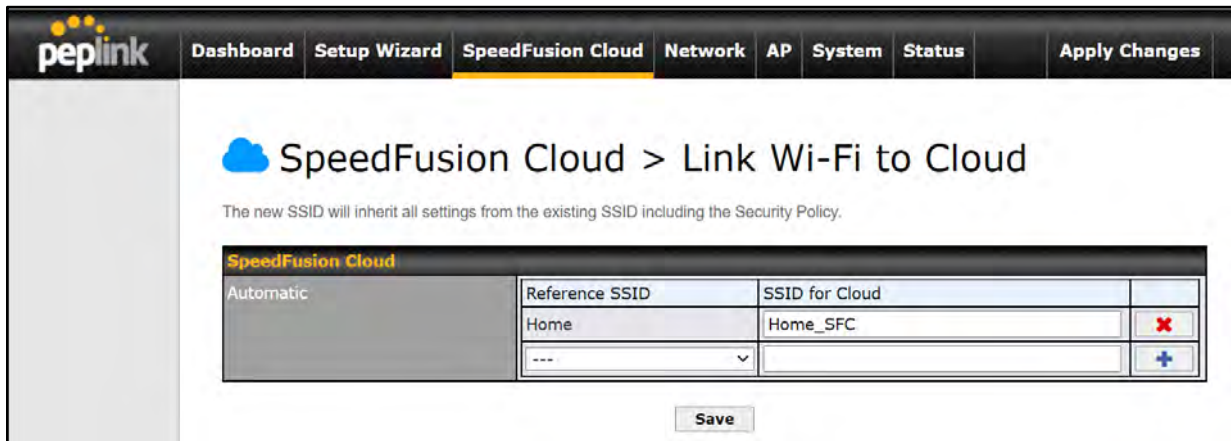


## 7.4 Link Wi-Fi to Cloud

SpeedFusion Cloud provides a convenient way to route the Wi-Fi client to the cloud from **SpeedFusion Cloud > Link Wi-Fi to Cloud**. This option is available for **Balance 20X**, **Balance 30 Pro**, and **Balance One**.



Create a new SSID for SpeedFusion Cloud. The new SSID will inherit all settings from one of the existing SSIDs including the Security Policy. Then click **Save** follow by **Apply Changes**.



**SpeedFusion Cloud > Link Wi-Fi to Cloud**

The new SSID will inherit all settings from the existing SSID including the Security Policy.

SpeedFusion Cloud	Reference SSID	SSID for Cloud	
Automatic	Home	Home_SFC	✖
	---		+

**Save**

SpeedFusion Cloud SSID will be shown on **Dashboard**.



**LAN Interface**

Router IP Address: 192.168.54.1


**Wi-Fi AP** ON **Details**

📶 HomeBunker	📶 Home	📶 Home_SFC
--------------	--------	------------

## 8 Configuring the LAN Interface(s)

### 8.1 Basic Settings

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

LAN	VLAN	Network	
<a href="#">LAN</a>	None	172.16.251.1/24	
<a href="#">VLAN1</a>	1	2.2.2.2/24	
<a href="#">VLAN2</a>	2	3.3.3.3/24	
<a href="#">New LAN</a>			

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 on any of the existing LAN interfaces (or creating a new one) will show the following :

IP Settings	
IP Address	<input type="text"/> 255.255.255.0 (/24) ▼

IP Settings	
<b>IP Address</b>	The IP address and subnet mask of the Pepwave router on the LAN.

Network Settings	
Name	<input type="text"/>
VLAN ID	<input type="text"/>
Inter-VLAN routing	<input checked="" type="checkbox"/>

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

Layer 2 PepVPN Bridging	
PepVPN Profiles to Bridge	<input type="checkbox"/> No profile is available
Remote Network Isolation	<input type="checkbox"/>
Spanning Tree Protocol	<input type="checkbox"/>
DHCP Option 82 Injection	<input checked="" type="checkbox"/>
Override IP Address when bridge connected	<input checked="" type="radio"/> Do not override <input type="radio"/> Static <input type="radio"/> By DHCP <input type="radio"/> As None



Layer 2 PepVPN Bridging	
<b>PepVPN Profiles to Bridge</b>	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.
<b>Remote Network Isolation</b>	Enable this option if you want to block network traffic between the remote networks, this will not affect the connectivity between them and this local LAN.
<b>Spanning Tree Protocol</b>	Click the box will enable STP for this layer 2 profile bridge.
<b>Override IP Address when bridge</b>	<p>Select "Do not override" if the LAN IP address and local DHCP server should remain unchanged after the Layer 2 PepVPN is up.</p> <p>If you choose to override IP address when the VPN is connected, the device will not</p>



<b>connected</b>	act as a router, and most Layer 3 routing functions will cease to work.
<b>DHCP Option 82</b>	<p>Click on the question Mark if you want to enable DHCP Option 82.</p> <p>This allows the device to inject Option 82 with Router Name information before forwarding the DHCP Request packet to a PepVPN peer, such that the DHCP Server can identify where the request originates from.</p>



DHCP Server											
DHCP Server		<input checked="" type="checkbox"/> Enable									
DHCP Server Logging		<input type="checkbox"/>									
IP Range		<input type="text"/> - <input type="text"/> 255.255.255.0 (/24) ▼									
Lease Time	1	Days 0	Hours 0 Mins								
DNS Servers	<input checked="" type="checkbox"/>	Assign DNS server automatically									
WINS Servers	<input type="checkbox"/>	Assign WINS server									
BOOTP	<input type="checkbox"/>										
Extended DHCP Option		<table border="1"> <thead> <tr> <th>Option</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td colspan="2">No Extended DHCP Option</td> </tr> <tr> <td colspan="2">Add</td> </tr> </tbody> </table>		Option	Value	No Extended DHCP Option		Add			
Option	Value										
No Extended DHCP Option											
Add											
DHCP Reservation		<table border="1"> <thead> <tr> <th>Name</th> <th>MAC Address</th> <th>Static IP</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td>00:00:00:00:00:00</td> <td></td> <td></td> </tr> </tbody> </table>		Name	MAC Address	Static IP			00:00:00:00:00:00		
Name	MAC Address	Static IP									
	00:00:00:00:00:00										

DHCP Server Settings	
<b>DHCP Server</b>	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.
<b>DHCP Server Logging</b>	Enable logging of DHCP events in the eventlog by selecting the checkbox.
<b>IP Range &amp; Subnet Mask</b>	These settings allocate a range of IP addresses that will be assigned to LAN computers by the Pepwave router's DHCP server.
<b>Lease Time</b>	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.
<b>DNS Servers</b>	This option allows you to input the DNS server addresses to be offered to DHCP clients. If <b>Assign DNS server automatically</b> is selected, the Pepwave router's built-in DNS server address (i.e., LAN IP address) will be offered.
<b>WINS Servers</b>	<p>This option allows you to optionally specify a Windows Internet Name Service (WINS) server. You may choose to use the <b>built-in WINS server</b> or <b>external WINS servers</b>.</p> <p>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</p>

	<b>WINS Server</b> 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 <b>Status&gt;WINS Clients</b> .
<b>BOOTP</b>	Check this box to enable BOOTP on older networks that still require it.
<b>Extended DHCP Option</b>	<p>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.</p> <p>To define an extended DHCP option, click the <b>Add</b> 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.</p>
<b>DHCP Reservation</b>	<p>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.</p> <p><b>Name</b> (an optional field) allows you to specify a name to represent the device. MAC addresses should be in the format of <b>00:AA:BB:CC:DD:EE</b>. Press  to create a new record. Press  to remove a record. Reserved client information can be imported from the <b>Client List</b>, located at <b>Status&gt;Client List</b>. For more details, please refer to <b>Section 22.3</b>.</p>

LAN Physical Settings	
Speed	Auto ▼

LAN Physical Settings	
<b>Speed</b>	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. <b>Auto</b> 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		Destination Network	Subnet Mask	Gateway
			255.255.255.0 (/24) ▼	
				



## 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

☐


## 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

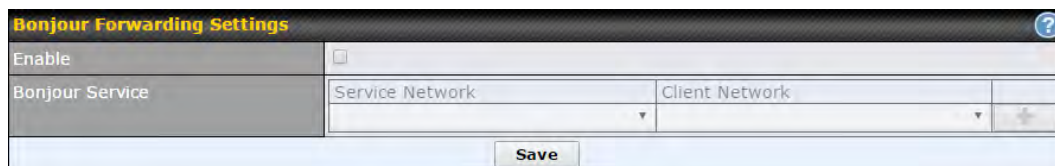
Enable	<input checked="" type="checkbox"/>																			
DNS Caching	<input type="checkbox"/>																			
Include Google Public DNS Servers	<input type="checkbox"/>																			
Local DNS Records	<table border="1"> <thead> <tr> <th>Host Name</th> <th>IP Address</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table>		Host Name	IP Address																
Host Name	IP Address																			
DNS Resolvers	<table border="1"> <thead> <tr> <th>Connection</th> <th>Current Status</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> WAN 1</td> <td>10.88.3.1</td> </tr> <tr> <td><input type="checkbox"/> WAN 2</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Wi-Fi WAN</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Cellular 1</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Cellular 2</td> <td></td> </tr> <tr> <td><input type="checkbox"/> USB</td> <td></td> </tr> <tr> <td>Connection</td> <td>DNS Servers</td> </tr> <tr> <td><input type="checkbox"/> LAN</td> <td></td> </tr> </tbody> </table>		Connection	Current Status	<input type="checkbox"/> WAN 1	10.88.3.1	<input type="checkbox"/> WAN 2		<input type="checkbox"/> Wi-Fi WAN		<input type="checkbox"/> Cellular 1		<input type="checkbox"/> Cellular 2		<input type="checkbox"/> USB		Connection	DNS Servers	<input type="checkbox"/> LAN	
Connection	Current Status																			
<input type="checkbox"/> WAN 1	10.88.3.1																			
<input type="checkbox"/> WAN 2																				
<input type="checkbox"/> Wi-Fi WAN																				
<input type="checkbox"/> Cellular 1																				
<input type="checkbox"/> Cellular 2																				
<input type="checkbox"/> USB																				
Connection	DNS Servers																			
<input type="checkbox"/> LAN																				

Preferred connections are shown with 



DNS Proxy Settings	
<b>Enable</b>	To enable the DNS proxy feature, check this box, and then set up the feature at <b>Network&gt;LAN&gt;DNS Proxy Settings</b> . A DNS proxy server can be enabled to serve DNS requests originating from LAN/PPTP/SpeedFusion™ peers. Requests are forwarded to the <b>DNS servers/resolvers</b> defined for each WAN connection.
<b>DNS Caching</b>	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, <b>DNS Caching</b> is disabled.
<b>Include Google Public DNS Servers</b>	When this option is <b>enabled</b> , 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.
<b>Local DNS Records</b>	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.
<b>DNS Resolvers <sup>A</sup></b>	Check the box to enable the WINS server. A list of WINS clients will be displayed at <b>Network&gt;LAN&gt;DNS Proxy Settings&gt;DNS Resolvers</b> . 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.

<sup>A</sup> - 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.



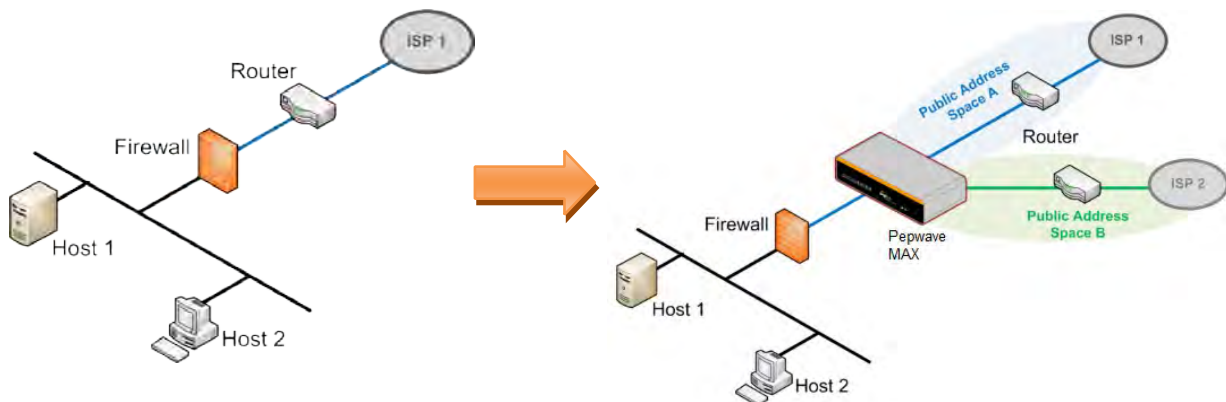
## Bonjour Forwarding Settings

<b>Enable</b>	Check this box to turn on Bonjour forwarding.
<b>Bonjour Service</b>	Choose <b>Service</b> and <b>Client</b> networks from the drop-down menus, and then click  to add the networks. To delete an existing Bonjour listing, click  .

## Drop-In Mode

Drop-in mode (or transparent bridging mode) eases the installation of the Pepwave MAX on a live network between the firewall and router, such that changes to the settings of existing equipment are not required.

The following diagram illustrates drop-in mode setup:



Check the box Enable to enable the Drop-in Mode. After enabling this feature and selecting the WAN for Drop-in mode, various settings including the WAN's connection method and IP address will be automatically updated.


When drop-in mode is enabled, the LAN and the WAN for drop-in mode ports will be bridged. Traffic between the LAN hosts and WAN router will be forwarded between the devices. In this case, the hosts on both sides will not notice any IP or MAC address changes.

After successfully setting up the Pepwave MAX as part of the network using drop-in mode, it will, depending on model, support one or more WAN connections. Some MAX units also support multiple WAN connections after activating drop-in mode, though a SpeedFusion license may be required to activate more than one WAN port.


**Please note the Drop-In Mode is mutually exclusive with VLAN.**

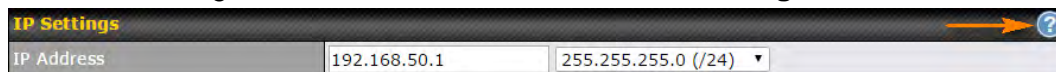
Drop-In Mode Settings							
Enable	<input checked="" type="checkbox"/>						
WAN for Drop-In Mode	<div> <span>?</span> <span>WAN ▼</span> </div> <div> <input checked="" type="checkbox"/> Apply NAT on VLAN networks outgoing Internet traffic            VLAN network(s) may route their outgoing Internet traffic to this unit. When this checkbox is checked their traffic will be NAT'd before forwarding out of this WAN. Leave this checkbox checked if you are not sure.         </div>						
Share Drop-In IP	<input checked="" type="checkbox"/>						
Shared IP Address	<div> <span>?</span> <div> <input type="text"/> 255.255.255.0 (/24) ▼         </div> </div>						
Static Route	<table border="1"> <thead> <tr> <th>Destination Network</th> <th>Subnet Mask</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td>255.255.255.0 (/24) ▼</td> <td><input type="button" value="+"/></td> </tr> </tbody> </table>	Destination Network	Subnet Mask		<input type="text"/>	255.255.255.0 (/24) ▼	<input type="button" value="+"/>
Destination Network	Subnet Mask						
<input type="text"/>	255.255.255.0 (/24) ▼	<input type="button" value="+"/>					
WAN Default Gateway	<div> <span>?</span> <div> <input type="text"/> </div> <div> <input checked="" type="checkbox"/> I have other host(s) on WAN segment           </div> <div>             IP Address <input type="text"/> - <input type="text"/> </div> <div> <input type="text"/> </div> </div>						
WAN DNS Servers	<div> <span>?</span> <div>             DNS server 1: <input type="text"/>              DNS server 2: <input type="text"/> </div> </div>						
<p>NOTE: The DHCP Server Settings will be overwritten.</p> <p>The following WAN settings will be overwritten: Connection Method, MTU, Health Check, Additional Public IP, and Dynamic DNS Settings.</p> <p>The PPTP Server will be disabled.</p> <p>Tip: please review the DNS Forwarding setting under the Service Forwarding section.</p>							

Drop-in Mode Settings	
<b>Enable</b>	Drop-in mode eases the installation of the Pepwave MAX 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.
<b>WAN for Drop-In Mode</b>	Select the WAN port to be used for drop-in mode. If <b>WAN</b> is selected, the high availability feature will be disabled automatically.
<b>Shared Drop-In IP<sup>A</sup></b>	<p>When this option is enabled, the passthrough IP address will be used to connect to WAN hosts (email notification, remote syslog, etc.). The MAX will listen for this IP address when WAN hosts access services provided by the MAX (web admin access from the WAN, DNS server requests, etc.).</p> <p>To connect to hosts on the LAN (email notification, remote syslog, etc.), the default gateway address will be used. The MAX will listen for this IP address when LAN hosts access services provided by the MAX (web admin access from the WAN, DNS</p>

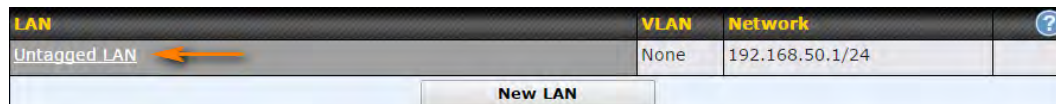
	proxy, etc.).
<b>Shared IP Address<sup>A</sup></b>	Access to this IP address will be passed through to the LAN port if this device is not serving the service being accessed. The shared IP address will be used in connecting to hosts on the WAN (e.g., email notification, remote syslog, etc.) The device will also listen on the IP address when hosts on the WAN access services served on this device (e.g., web admin accesses from WAN, DNS server, etc.)
<b>WAN Default Gateway</b>	Enter the WAN router's IP address in this field. If there are more hosts in addition to the router on the WAN segment, click the  button next to "WAN Default Gateway" and check the other <b>host(s) on the WAN segment</b> box and enter the IP address of the hosts that need to access LAN devices or be accessed by others.
<b>WAN DNS Servers</b>	Enter the selected WAN's corresponding DNS server IP addresses.

<sup>A</sup> - Advanced feature, please click the  button on the top right-hand corner to activate.

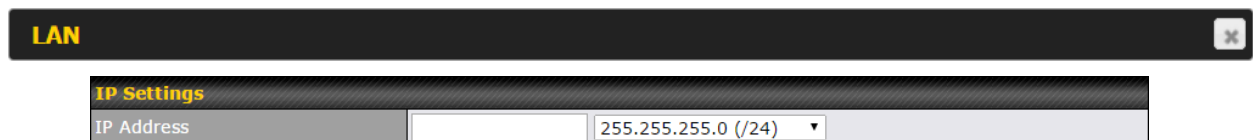
To enable VLAN configuration, click the  button in the **IP Settings** section.



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	
<b>IP Address &amp; Subnet Mask</b>	Enter the Pepwave router's IP address and subnet mask values to be used on the LAN.



Network Settings	
Name	<input type="text"/>
VLAN ID	<input type="text"/>
Inter-VLAN routing	<input checked="" type="checkbox"/>
Captive Portal	<input type="checkbox"/>


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




DHCP Server Settings							
DHCP Server	<input checked="" type="checkbox"/> Enable						
IP Range	<input type="text"/> - <input type="text"/> 255.255.255.0 (/24)						
Lease Time	1 Days 0 Hours 0 Mins						
DNS Servers	<input checked="" type="checkbox"/> Assign DNS server automatically						
WINS Servers	<input type="checkbox"/> Assign WINS server						
BOOTP	<input type="checkbox"/>						
Extended DHCP Option	<table border="1"> <thead> <tr> <th>Option</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td colspan="2">No Extended DHCP Option</td> </tr> <tr> <td colspan="2"><input type="button" value="Add"/></td> </tr> </tbody> </table>	Option	Value	No Extended DHCP Option		<input type="button" value="Add"/>	
Option	Value						
No Extended DHCP Option							
<input type="button" value="Add"/>							
DHCP Reservation	<table border="1"> <thead> <tr> <th>Name</th> <th>MAC Address</th> <th>Static IP</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>	Name	MAC Address	Static IP	<input type="text"/>	<input type="text"/>	<input type="text"/>
Name	MAC Address	Static IP					
<input type="text"/>	<input type="text"/>	<input type="text"/>					

DHCP Server Settings	
<b>DHCP Server</b>	<p>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.</p> <p>To enable DHCP bridge relay, please click the  icon on this menu item.</p>
<b>IP Range &amp; Subnet Mask</b>	These settings allocate a range of IP addresses that will be assigned to LAN computers by the Pepwave router's DHCP server.
<b>Lease Time</b>	This setting specifies the length of time throughout which an IP address of a DHCP




	client remains valid. Upon expiration of <b>Lease Time</b> , the assigned IP address will no longer be valid and the IP address assignment must be renewed.
<b>DNS Servers</b>	This option allows you to input the DNS server addresses to be offered to DHCP clients. If <b>Assign DNS server automatically</b> is selected, the Pepwave router's built-in DNS server address (i.e., LAN IP address) will be offered.
<b>WINS Servers</b>	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 <b>DHCP WINS Servers</b> 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 <b>Status&gt;WINS Clients</b> .
<b>BOOTP</b>	Check this box to enable BOOTP on older networks that still require it.
<b>Extended DHCP Option</b>	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 <b>Add</b> 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.
<b>DHCP Reservation</b>	<p>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.</p> <p><b>Name</b> (an optional field) allows you to specify a name to represent the device. MAC addresses should be in the format of <b>00:AA:BB:CC:DD:EE</b>. Press  to create a new record. Press  to remove a record. Reserved clients information can be imported from the <b>Client List</b>, located at <b>Status&gt;Client List</b>. For more details, please refer to <b>Section 22.3</b>.</p>

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

DHCP Relay Settings	
DHCP Relay	 <input checked="" type="checkbox"/> Enable
DHCP Server IP Address	 <div> DHCP Server 1: <input type="text"/>  DHCP Server 2: <input type="text"/> </div>
DHCP Option 82	 <input type="checkbox"/>

## DHCP Relay Settings

<b>Enable</b>	Check this box to turn on DHCP relay. Click the  icon to disable DHCP relay.
<b>DHCP Server IP Address</b>	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 <b>DHCP Server 1</b> and <b>DHCP Server 2</b> .
<b>DHCP Option 82</b>	DHCP 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.

## 8.2 Port Settings

To configure port settings, navigate to **Network > Port Settings**

Port Settings					
Port Name	Enable	Speed	Advertise Speed	Port Type	VLAN
LAN Port 1	<input checked="" type="checkbox"/>	Auto	<input checked="" type="checkbox"/>	Trunk ▾	Any ▾
LAN Port 2	<input checked="" type="checkbox"/>			Trunk ▾	Any ▾
LAN Port 3	<input checked="" type="checkbox"/>			Trunk ▾	Any ▾
LAN Port 4	<input checked="" type="checkbox"/>			Trunk ▾	Any ▾

On this screen, you can enable specific ports, as well as determine the speed of the LAN ports, whether each port is a trunk or access port, can well as which VLAN each link belongs to, if any.

## 8.3 Captive Portal

The captive portal serves as a 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	<input checked="" type="checkbox"/> Untagged LAN
Hostname	<input type="text" value="captive-portal.peplink.com"/> <b>Default</b>
Access Mode	<input checked="" type="radio"/> Open Access <input type="radio"/> User Authentication
Access Quota	30 mins (0: Unlimited) 0 MB (0: Unlimited)
Quota Reset Time	<input checked="" type="radio"/> Daily at 00 :00 <input type="radio"/> 1440 minutes after quota reached
Allowed Networks	Domain Name / IP Address <input type="text"/> <input data-bbox="1291 567 1323 598" type="button" value="+"/>
Allowed Clients	MAC / IP Address <input type="text"/> <input data-bbox="1291 630 1323 661" type="button" value="+"/>
Splash Page	<input checked="" type="radio"/> Built-in <input type="radio"/> External, URL: <input type="text" value="http://"/>

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:



Authentication	RADIUS Server		
Auth Server	<input type="text"/>	Port 1812	Default
Auth Server Secret	<input type="text"/>	<input checked="" type="checkbox"/> Hide Characters	
CoA-DM	<input type="checkbox"/>		
Accounting Server	<input type="text"/>	Port 1813	Default
Accounting Server Secret	<input type="text"/>	<input checked="" type="checkbox"/> Hide Characters	
Accounting Interim Interval	<input type="text"/>	seconds	





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:

Authentication	LDAP Server		
LDAP Server	<input type="text"/>	Port 389	Default
	<input type="checkbox"/> Use DN/Password to bind to LDAP Server		
Base DN	<input type="text"/>		
Base Filter	<input type="text"/>		

	Fill in the necessary information to complete your connection to the server and enable authentication.
<b>Access Quota</b>	Set a time and data cap to each user's Internet usage.
<b>Quota Reset Time</b>	This menu determines how your usage quota resets. Setting it to <b>Daily</b> will reset it at a specified time every day. Setting a number of <b>minutes after quota reached</b> establish a timer for each user that begins after the quota has been reached.
<b>Allowed Networks</b>	Add networks that can bypass the captive Portal in this field. 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.
<b>Allowed Clients</b>	Add MAC address and /or IP addresses for client devices that are allowed to bypass the Captive Portal. Clients accessing these domains and IP addresses will not be redirected to the splash page.
<b>Splash Page</b>	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:  and . Clicking  displays a pop-up previewing the captive portal that your clients will see. Clicking  displays the following menu:

Portal Customization	
Logo Image	<input checked="" type="radio"/> No image [Use default Logo Image] <input type="button" value="Choose File"/> No file chosen <small>NOTE: Size max 512KB. Supported images types: JPEG, PNG and GIF.</small>
Message	<div></div>
Terms & Conditions	<div>[Use default Terms &amp; Conditions]</div>
Custom Landing Page	<input checked="" type="checkbox"/> <input type="text" value="http://"/>

Portal Customization	
<b>Logo Image</b>	Click the <b>Choose File</b> button to select a logo to use for the built-in portal.
<b>Message</b>	If you have any additional messages for your users, enter them in this field.
<b>Terms &amp; Conditions</b>	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.
<b>Custom Landing Page</b>	Fill in this field to redirect clients to an external URL.

## 9 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.

WAN Connection Status		
Priority 1 (Highest)		
1 WAN 1	Connected	<a href="#">Details</a>
2 WAN 2	Connected	<a href="#">Details</a>
Priority 2		
1 Cellular 1	No SIM Card Detected <a href="#">Reload SIM</a>	<a href="#">Details</a>
2 Cellular 2	No SIM Card Detected <a href="#">Reload SIM</a>	<a href="#">Details</a>
Priority 3		
Drag desired (Priority 3) connections here		
Disabled		
Wi-Fi WAN	Disabled	<a href="#">Details</a>

IPv6
Disabled <a href="#">Edit</a>

To enable a particular WAN connection, drag on the appropriate WAN by holding the left mouse button, move it to 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.

## 9.1 Ethernet WAN

Health Check Settings	
Health Check Method	<a href="#">?</a> PING
PING Hosts	<a href="#">?</a> Host 1: 8.8.8.8 Host 2: <input type="text"/> <input type="checkbox"/> Use first two DNS servers as PING Hosts
Timeout	<a href="#">?</a> 5 second(s)
Health Check Interval	<a href="#">?</a> 5 second(s)
Health Check Retries	<a href="#">?</a> 3
Recovery Retries	<a href="#">?</a> 3

### Health Check Settings

#### Health Check Method

This field specifies the Health Check method to be used for this WAN connection.

- Disabled - The WAN connection is always considered to be up and will not

	<p>be treated as down for any IP routing errors.</p> <ul style="list-style-type: none"> <li>• PING - ICMP PING packets will be issued to test connectivity with configurable target IP addresses or host names.</li> <li>• DNS Lookup - DNS lookups will be issued to test the connectivity with configurable target DNS server IP addresses.</li> <li>• HTTP - HTTP connections will be issued to test the connectivity with configurable URLs and strings to match.</li> </ul> <p>Default: DNS Lookup</p>
<b>PING Hosts</b>	<p>These fields are for specifying the target IP addresses or host names where ICMP Ping packets will be sent to for health check.</p> <p>If the box Use first two DNS servers as PING Hosts is checked, the first two DNS servers will be the ping 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.</p> <p>The connection is considered to be up if ping responses are received from any one of the ping hosts.</p>
<b>Timeout</b>	If a health check test cannot be completed within the specified amount of time, the test will be treated as failed.
<b>Health Check Interval</b>	This is the time interval between each health check test.
<b>Health Check Retries</b>	This is the number of consecutive check failures before treating a connection as down.
<b>Recovery Retries</b>	This is the number of responses required after a health check failure before treating a connection as up again.

Bandwidth Allowance Monitor Settings	
Bandwidth Allowance Monitor	<input checked="" type="checkbox"/> Enable
Action	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling <a href="#">Email Notification</a> . <input checked="" type="checkbox"/> Disconnect when usage hits 100% of monthly allowance
Start Day	On 1st of each month at 00:00 midnight
Monthly Allowance	<input type="text"/> MB

## Bandwidth Allowance Monitor Settings

<b>Bandwidth Allowance Monitor</b>	Check the box <i>Enable</i> 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.
<b>Action</b>	<p>If Email Notification is enabled, you will receive an email notification when usage hits 75% and 95% of the monthly allowance.</p> <p>If the box 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 unless this option has been turned off or the usage has been reset when a new billing cycle starts.</p>
<b>Start Day</b>	This option allows you to select which day of the month a billing cycle starts.
<b>Monthly Allowance</b>	This field is to specify the bandwidth allowance for each billing cycle.

**Additional Public IP Settings**

Additional Public IP Address	IP Address	
	Subnet Mask	255.255.255.0 (/24) ▼
	<div>↓</div> <div></div>	
		Delete

### Additional Public IP Settings

If you have access to status public IP addresses, you can assign them on this field.

**Dynamic DNS Settings**

Dynamic DNS Service Provider	Disabled ▼
------------------------------	------------

### 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.

### 9.1.1 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.).

Connection Method	 DHCP
Routing Mode	  NAT
IP Address	10.88.3.158
Subnet Mask	255.255.255.0
Default Gateway	10.88.3.253
Hostname (Optional)	<div><input type="text"/></div> <div><input type="checkbox"/> Use custom hostname</div>
DNS Servers	<div><input checked="" type="checkbox"/> Obtain DNS server address automatically 10.88.3.1</div> <div><input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/></div>



## DHCP Connection Settings

<b>Routing Mode</b>	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 <b>IP Forwarding</b> option, if your network requires it.
<b>IP Address/ Subnet Mask/ Default Gateway</b>	This information is obtained from the ISP automatically.
<b>Hostname (Optional)</b>	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.
<b>DNS Servers</b>	<p>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.</p> <p>Selecting <b>Obtain DNS server address automatically</b> 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.)</p>

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.

## 9.1.2 Static IP Connection

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

Connection Method	 Static IP ▾
Routing Mode	 <input checked="" type="radio"/> NAT
IP Address	10.88.3.158
Subnet Mask	255.255.255.0
Default Gateway	10.88.3.253
IP Address	<input type="text"/>
Subnet Mask	255.255.255.0 (/24) ▾
Default Gateway	<input type="text"/>
DNS Servers	<input checked="" type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

### 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.



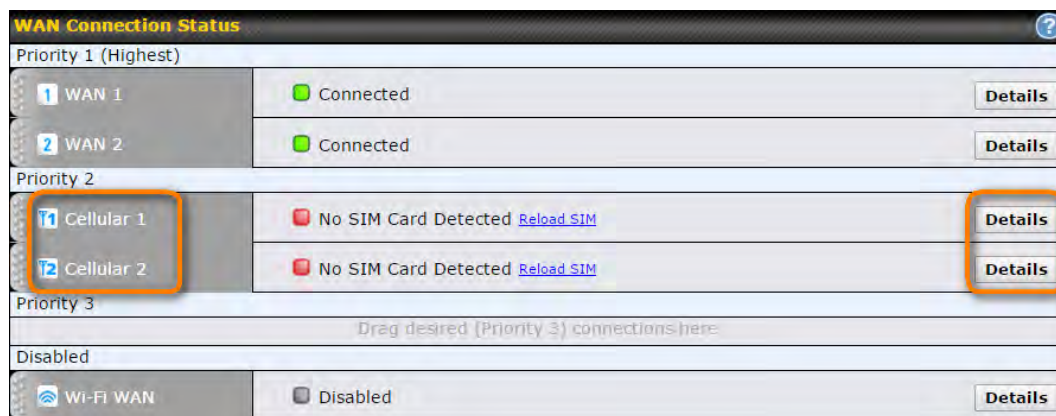


### 9.1.4 L2TP Connection

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	<input type="text"/>
L2TP Password	<input type="password"/>
Confirm L2TP Password	<input type="password"/>
Server IP Address / Host	<input type="text"/>
Address Type	● Dynamic IP ☐ Static IP
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically 10.88.3.1 <input checked="" type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>

L2TP Settings	
<b>L2TP Username / Password</b>	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.
<b>Confirm L2TP Password</b>	Verify your password by entering it again in this field.
<b>Server IP Address / Host</b>	L2TP server address is a parameter which is provided by your ISP. Note: Leave this field blank unless it is provided by your ISP.
<b>Address Type</b>	Your ISP will also indicate whether the server IP address is Dynamic or Static. Please click the appropriate value.
<b>DNS Servers</b>	<p>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.</p> <p>Selecting <b>Obtain DNS server address automatically</b> 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.)</p> <p>When <b>Use the following DNS server address(es)</b> is selected, you can enter custom DNS server addresses for this WAN connection into the <b>DNS server 1</b> and <b>DNS server 2</b> fields.</p>

## 9.2 Cellular WAN



To access cellular WAN settings, click **Network>WAN>Details**.

## Connection Details

Cellular 1 Status	
IMSI	(No SIM Card Detected)
MEID	A100001F7DC038 270113180708241208
ESN	8052FC8A
IMEI	356144040031862

### Cellular Status


<b>IMSI</b>	This is the International Mobile Subscriber Identity which uniquely identifies the SIM card. This is applicable to 3G modems only.
<b>MEID</b>	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.
<b>ESN</b>	This serves the same purpose as MEID HEX but uses an older format.
<b>IMEI</b>	This is the unique ID for identifying the modem in GSM/HSPA mode.

Connection Settings	
WAN Connection Name	Cellular
Enable	<input checked="" type="checkbox"/> Always on
Routing Mode	<input checked="" type="radio"/> NAT <input type="radio"/> IP Forwarding
Network Mode	<input type="radio"/> Auto <input type="radio"/> Generic <input type="radio"/> AT&T / T-Mobile <input checked="" type="radio"/> Sprint <input type="radio"/> Verizon Wireless
Subnet Selection	<input checked="" type="radio"/> Auto <input type="radio"/> Force /31 Subnet
Connection Priority	<input checked="" type="radio"/> Always-on (Priority 1) <input type="radio"/> Backup
Independent from Backup WANs	<input type="checkbox"/>
Idle Disconnect	<input checked="" type="checkbox"/> 1 minutes Time value is global. A change will affect all WAN profiles.
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>


### Connection Settings

#### WAN Connection

Indicate a name you wish to give this WAN connection

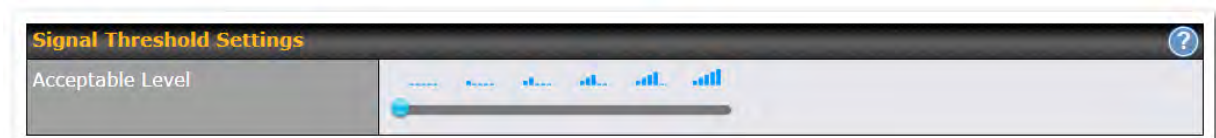
<b>Name</b>	
<b>Enable</b>	Click the checkbox to toggle the on and off state of this connection.
<b>Routing Mode</b>	<p>This option allows you to select the routing method to be used in routing IP frames via the WAN connection. The mode can be either NAT (Network Address Translation) or IP Forwarding.</p> <p>In the case if you need to choose IP Forwarding for your scenario. Click the  button to enable IP Forwarding.</p>
<b>Subnet Selection</b>	<p>Choose <span style="float: right;">between:</span></p> <p><b>Auto:</b> The subnet mask will be set automatically.</p> <p><b>Force /31 Subnet:</b> The subnet mask will be set as 255.255.255.254(/31), and the gateway IP address will be recalculated.</p>
<b>Connection Priority</b>	<p>This option allows you to configure the WAN connection whether for normal daily usage or as a backup connection only.</p> <p>If <b>Always-on</b> is chosen, the WAN connection will be kept on continuously, regardless of the priority of other WAN connections.</p> <p>If <b>Backup</b> is chosen, the WAN connection will depend on other WAN connections. It will not be used when one or more higher priority dependent WAN connections are connected.</p>
<b>Independent from Backup WANs</b>	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available.
<b>Idle Disconnect</b>	<p>If this is checked, the connection will disconnect when idle after the configured Time value.</p> <p>This option is disabled by default.</p>
<b>DNS Servers</b>	<p>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.</p> <p>Selecting Obtain DNS server address automatically results in the DNS servers assigned by the WAN DHCP server being used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned by 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.</p>

Cellular Settings		
SIM Card	<input checked="" type="radio"/> Both SIMs <input type="radio"/> SIM A Only <input type="radio"/> SIM B Only	
Preferred SIM Card	<input checked="" type="radio"/> No Preference <input type="radio"/> SIM A <input type="radio"/> SIM B	
	SIM Card A	SIM Card B
Network Selection	<input checked="" type="radio"/> Auto <input type="radio"/> Manual	<input checked="" type="radio"/> Auto <input type="radio"/> Manual
LTE/3G	LTE Only ▾	LTE Only ▾
Optimal Network Discovery	<input type="checkbox"/>	<input type="checkbox"/>
Band Selection	Auto ▾	Auto ▾
Data Roaming	<input type="checkbox"/>	<input type="checkbox"/>
Authentication	Auto ▾	Auto ▾
Operator Settings	<input checked="" type="radio"/> Auto <input type="radio"/> Custom	<input checked="" type="radio"/> Auto <input type="radio"/> Custom
APN	<input type="text"/>	<input type="text"/>
Username	<input type="text"/>	<input type="text"/>
Password	<input type="text"/>	<input type="text"/>
Confirm Password	<input type="text"/>	<input type="text"/>
SIM PIN (Optional)	<input type="text"/> (Confirm)	<input type="text"/> (Confirm)
Bandwidth Allowance Monitor	<input checked="" type="checkbox"/> Enable	<input checked="" type="checkbox"/> Enable
Action	<input checked="" type="checkbox"/> Receive email notification <input type="checkbox"/> Reserve for management traffic when usage hits 100% <input type="checkbox"/> Disconnect when usage hits 100%	<input checked="" type="checkbox"/> Receive email notification <input type="checkbox"/> Reserve for management traffic when usage hits 100% <input type="checkbox"/> Disconnect when usage hits 100%
Start Day	On 26th ▾ of each month	On 21st ▾ of each month
Monthly Allowance	4 GB ▾	22 GB ▾

Cellular Settings	
<b>SIM Card</b>	Indicate which SIM card this cellular WAN will use. Only applies to cellular WAN with redundant SIM cards.
<b>Preferred SIM Card</b>	If both cards were enabled on the above field, then you can designate the priority of the SIM card slots here.
<b>LTE/3G</b>	This drop-down menu allows restricting cellular to particular band. Click the  button to enable the selection of specific bands.
<b>Optimal Network Discovery</b>	Cellular WAsN by default will only handover from 3G to LTE network when there is no active data traffic, enable this option will make it run the handover procedures after fallback to 3G for a defined effective period, even this may interrupt the connectivity for a short while.
<b>Band Selection</b>	When set to <b>Auto</b> , band selection allows for automatically connecting to available, supported

	bands (frequencies) When set to Manual, you can manually select the bands (frequencies) the SIM will connect to.
<b>Data Roaming</b>	This checkbox enables data roaming on this particular SIM card. When data roaming is enabled this option allows you to select in which countries the SIM has a data connection. The option is configured by using MMC (country) codes. Please check your service provider's data roaming policy before proceeding.
<b>Authentication</b>	Choose from <b>PAP Only</b> or <b>CHAP Only</b> to use those authentication methods exclusively. Select <b>Auto</b> to automatically choose an authentication method.
<b>Operator Settings</b>	This setting allows you to configure the APN settings of your connection. If <b>Auto</b> 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 <b>Custom</b> to enter your carrier's <b>APN</b> , <b>Login</b> , <b>Password</b> , and <b>Dial Number</b> settings manually. The correct values can be obtained from your carrier. The default and recommended setting is <b>Auto</b> .
<b>APN / Login / Password / SIM PIN</b>	When <b>Auto</b> is selected, the information in these fields will be filled automatically. Select <b>Custom</b> to customize these parameters. The parameter values are determined by and can be obtained from the ISP.
<b>Bandwidth Allowance Monitor</b>	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.
<b>Action</b>	If email notification is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance. If <b>Disconnect when usage hits 100% of monthly allowance</b> 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.
<b>Start Day</b>	This option allows you to define which day of the month each billing cycle begins.
<b>Monthly Allowance</b>	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

## Signal Threshold Settings



If signal threshold is defined, this connection will be treated as down when a weaker than threshold signal is determined.

The following values are used by the threshold scale:



	0 bars	1 bar	2 bars	3 bars	4 bars	5 bars
<b>LTE / RSRP</b>	-140	-128	-121	-114	-108	-98
<b>3G / RSSI</b>	-120	-100	-95	-90	-85	-75

To define the threshold manually using specific signal strength values, please click on the question Mark and the following field will be visible.

Signal Threshold Settings ?			
LTE	RSRP:	<input type="text" value="n/a"/>	dBm (Recovery: <input type="text" value="n/a"/> dBm)
	SINR:	<input type="text" value="n/a"/>	dB (Recovery: <input type="text" value="n/a"/> dB)
3G	RSSI:	<input type="text" value="n/a"/>	dBm (Recovery: <input type="text" value="n/a"/> dBm)

General Settings	
<b>Independent from Backup WANs</b>	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available.
<b>Standby State</b>	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 <b>Remain connected</b> is chosen, bringing up this WAN connection to active makes it immediately available for use.
<b>Idle Disconnect</b>	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.

Health Check Settings	
Health Check Method	? <input type="text" value="SmartCheck"/>
Timeout	? <input type="text" value="5"/> second(s)
Health Check Interval	? <input type="text" value="10"/> second(s)
Health Check Retries	? <input type="text" value="3"/>
Recovery Retries	? <input type="text" value="3"/>



Health Check Settings	
<b>Health Check Method</b>	This setting allows you to specify the health check method for the cellular connection. Available options are <b>Disabled</b> , <b>Ping</b> , <b>DNS Lookup</b> , <b>HTTP</b> , and <b>SmartCheck</b> . The default method is <b>DNS Lookup</b> . See <b>Section 10.4</b> for configuration details.
<b>Timeout</b>	If a health check test cannot be completed within the specified amount of time, the test will be treated as failed.
<b>Health Check Interval</b>	This is the time interval between each health check test.
<b>Health Check Retries</b>	This is the number of consecutive check failures before treating a connection as down.
<b>Recovery Retries</b>	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	<input type="text" value="Disabled"/>
------------------------------	---------------------------------------

Dynamic DNS Settings	
<b>Dynamic DNS Service Provider</b>	<p>This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers:</p> <ul style="list-style-type: none"> <li>• changeip.com</li> <li>• dyndns.org</li> <li>• no-ip.org</li> <li>• tzo.com</li> <li>• DNS-O-Matic</li> </ul> <p>Select <b>Disabled</b> to disable this feature. See <b>Section 9.5</b> for configuration details.</p>

MTU

MTU	
<b>MTU</b>	This field is for specifying the Maximum Transmission Unit value of the WAN connection. An excessive MTU value can cause file downloads stall shortly after connected. You may consult your ISP for the connection's MTU value.

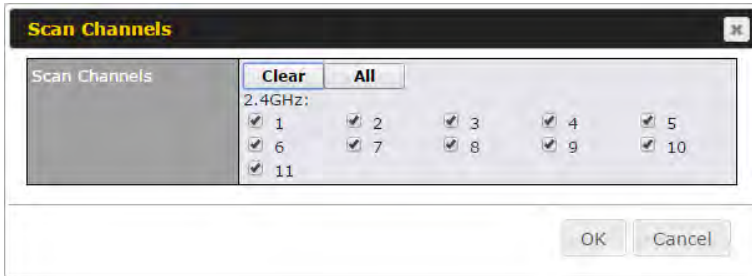

## 9.3 Wi-Fi WAN

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

WAN Connection Settings	
WAN Connection Name	<input type="text" value="Wi-Fi WAN"/> <input type="button" value="Default"/>
Operating Schedule	<input type="text" value="Always on"/> ▼
Independent from Backup WANs ?	<input type="checkbox"/>
Standby State	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnected
MTU ?	<input type="radio"/> Auto <input checked="" type="radio"/> Custom Value: <input type="text" value="1500"/> <input type="button" value="Default"/>
Reply to ICMP PING ?	<input checked="" type="radio"/> Yes <input type="radio"/> No

WAN Connection Settings	
<b>WAN Connection Name</b>	Enter a name to represent this WAN connection.
<b>Operating Schedule</b>	Click the drop-down menu to apply a time schedule to this interface.
<b>Independent from Backup WANs</b>	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available.
<b>Standby State</b>	This setting specifies the state of the WAN connection while in standby. The available options are <b>Remain Connected</b> (hot standby) and <b>Disconnect</b> (cold standby).
<b>MTU</b>	This setting specifies the maximum transmission unit. By default, MTU is set to <b>Custom 1440</b> . You may adjust the MTU value by editing the text field. Click <b>Default</b> to restore the default MTU value. Select <b>Auto</b> and the appropriate MTU value will be automatically detected. The auto-detection will run each time the WAN connection establishes
<b>Reply to ICMP PING</b>	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 Width	20 MHz
Channel Selection	<input checked="" type="radio"/> Auto <input type="radio"/> Custom
Data Rate	<input checked="" type="radio"/> Auto <input type="radio"/> Fixed
Output Power	Max <input type="checkbox"/> Boost
Roaming	<input type="checkbox"/>
Connect to Any Open Mode AP	<input type="radio"/> Yes <input checked="" type="radio"/> No
Beacon Miss Counter	5

Wi-Fi WAN Settings	
<b>Channel Width</b>	Select the channel width for this Wi-Fi WAN. 20MHz will have greater support for older devices using 2.4Ghz, while 40MHz is appropriate for networks with newer devices that connect using 5Ghz
<b>Channel Selection</b>	<p>Determine whether the channel will be automatically selected. If you select custom, the following table will appear:</p> 
<b>Data Rate</b>	Selecting Auto will enable the router to automatically determine the best data rate, while manually selecting a rate will force devices to connect using the fixed rate.
<b>Output Power</b>	If you are setting up a network with many Wi-Fi devices in close proximity, then you can configure the output power here. Click the "boost" button for additional power. However, with that option ticked, output power may exceed local regulatory limits.
<b>Roaming</b>	Checking this box will enable Wi-Fi roaming. Click the  icon for additional options.
<b>Connect to Any Open Mode AP</b>	This option is to specify whether the Wi-Fi WAN will connect to any open mode access points it finds.
<b>Beacon Miss Counter</b>	This sets the threshold for the number of missed beacons.


Bandwidth Allowance Monitor	
Bandwidth Allowance Monitor	<input checked="" type="checkbox"/> Enable
Action	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling <a href="#">Email Notification</a> . <input checked="" type="checkbox"/> Disconnect when usage hits 100% of monthly allowance
Start Day	On <input type="text" value="1st"/> of each month at 00:00 midnight
Monthly Allowance	<input type="text" value=""/> MB

Bandwidth Allowance Monitor	
<b>Action</b>	<p>If <b>Error! Reference source not found.</b> is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance.</p> <p>If <b>Disconnect when usage hits 100% of monthly allowance</b> 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.</p>
<b>Start Day</b>	This option allows you to define which day of the month each billing cycle begins.
<b>Monthly Allowance</b>	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

Health Check Settings	
Health Check Method	<input type="text" value="DNS Lookup"/>
Health Check DNS Servers	Host 1: <input type="text"/> Host 2: <input type="text"/> <input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers <input type="checkbox"/> Include public DNS servers
Timeout	<input type="text" value="5"/> second(s)
Health Check Interval	<input type="text" value="5"/> second(s)
Health Check Retries	<input type="text" value="3"/>
Recovery Retries	<input type="text" value="3"/>


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

### Health Check Settings

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: <input type="text"/> Host 2: <input type="text"/> <input checked="" type="checkbox"/> 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: <input type="text"/> Host 2: <input type="text"/> <input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers <input type="checkbox"/> 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:// <input type="text"/> Matching String: <input type="checkbox"/>
URL 2	 http:// <input type="text"/> Matching String: <input type="checkbox"/>

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

**URL 1** **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.

### 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	<input type="checkbox"/>
Hosts / IDs	

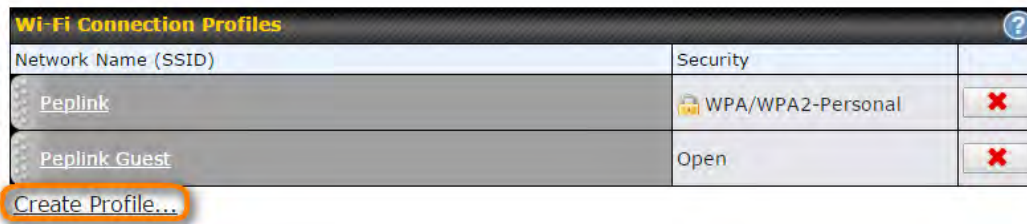
Dynamic DNS Settings	
<b>Service Provider</b>	<p>This setting specifies the dynamic DNS service provider to be used for the WAN. Supported providers are:</p> <ul style="list-style-type: none"> <li>• changeip.com</li> <li>• dyndns.org</li> <li>• no-ip.org</li> <li>• tzo.com</li> <li>• DNS-O-Matic</li> </ul> <p>Select <b>Disabled</b> to disable this feature.</p>
<b>User ID / User / Email</b>	This setting specifies the registered user name for the dynamic DNS service.
<b>Password / Pass / TZO Key</b>	This setting specifies the password for the dynamic DNS service.
<b>Update All Hosts</b>	Check this box to automatically update all hosts.
<b>Hosts / Domain</b>	This setting specifies a list of hostnames or domains to be associated with the public Internet IP address of the WAN connection.

Important Note	
<p>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.</p> <p>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.</p> <p>Due to dynamic DNS service providers' policies, a dynamic DNS host expires automatically when the host record has not been 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.</p>	

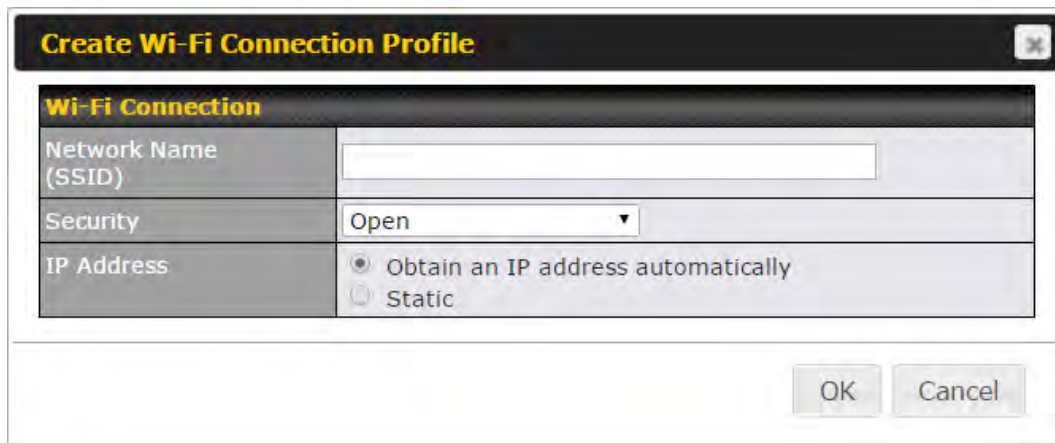


### 9.3.1 Creating Wi-Fi Connection Profiles

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	
<b>Type</b>	Select whether the network will connect automatically or manually.
<b>Network Name (SSID)</b>	Enter a name to represent this Wi-Fi connection.
<b>Security</b>	<p>This option allows you to select which security policy is used for this wireless network. Available options:</p> <ul style="list-style-type: none"> <li>• <b>Open</b></li> <li>• <b>WPA3 -Personal (AES:CCMP)</b></li> <li>• <b>WPA2/WPA3 -Personal (AES:CCMP)</b></li> <li>• <b>WPA2 – Personal: AES:CCMP</b></li> <li>• <b>WPA2 – Enterprise: AES: CCMP</b></li> <li>• <b>WPA/ WPA2 – Personal: TKIP/AES:CCMP</b></li> <li>• <b>WPA/ WPA2 – ENTERprise: TKIP/AES:CCMP</b></li> </ul>

## 9.4 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	
<b>Method</b>	This setting specifies the health check method for the WAN connection. This value can be configured as <b>Disabled</b> , <b>PING</b> , <b>DNS Lookup</b> , or <b>HTTP</b> . The default method is <b>DNS Lookup</b> . For mobile Internet connections, the value of <b>Method</b> can be configured as <b>Disabled</b> or <b>SmartCheck</b> .
<b>Health Check Disabled</b>	
Health Check Method	<div> <span>?</span> <div> Disabled </div> </div> <div>Health Check disabled. Network problem cannot be detected.</div>
When <b>Disabled</b> is chosen in the <b>Method</b> field, the WAN connection will always be considered as up. The connection will <b>NOT</b> be treated as down in the event of IP routing errors.	
<b>Health Check Method: PING</b>	
Health Check Method	<div> <span>?</span> <div> PING </div> </div>
PING Hosts	<div> <span>?</span> <div> Host 1: <input type="text"/>  Host 2: <input type="text"/>  <input checked="" type="checkbox"/> Use first two DNS servers as PING Hosts </div> </div>
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.	
<b>PING Hosts</b>	This setting specifies IP addresses or hostnames with which connectivity is to be tested via ICMP ping. If <b>Use first two DNS servers as Ping Hosts</b> 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.
<b>Health Check Method: DNS Lookup</b>	
Health Check Method	<div> <span>?</span> <div> DNS Lookup </div> </div>
Health Check DNS Servers	<div> <span>?</span> <div> Host 1: <input type="text"/>  Host 2: <input type="text"/>  <input checked="" type="checkbox"/> Use first two DNS servers as Health Check DNS Servers  <input type="checkbox"/> Include public DNS servers </div> </div>
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.	
<b>Health Check DNS Servers</b>	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.

Health Check Method		HTTP ▼
URL 1		http:// <input type="text"/> Matching String: <input type="checkbox"/>
URL 2		http:// <input type="text"/> Matching String: <input type="checkbox"/>

#### 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.

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

Other Health Check Settings	
<b>Timeout</b>	This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is <b>5 seconds</b> .
<b>Health Check Interval</b>	This setting specifies the time interval in seconds between ping or DNS lookup requests. The default health check interval is <b>5 seconds</b> .
<b>Health Check Retries</b>	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 <b>3</b> . Using the default <b>Health Retries</b> setting of <b>3</b> , the corresponding WAN connection will be treated as down after three consecutive timeouts.
<b>Recovery Retries</b>	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, <b>Recover Retries</b> is set to <b>3</b> . 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
<p>When the health check method is set to <b>DNS Lookup</b> 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:</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p> <b>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.</b></p> </div>

## 9.5 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	<input type="text" value="changeip.com"/>
User ID	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Hosts	<input type="text"/>

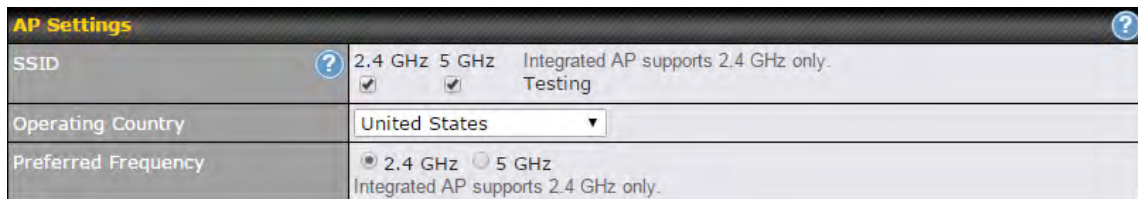
Dynamic DNS Settings	
<b>Dynamic DNS</b>	<p>This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers:</p> <ul style="list-style-type: none"> <li>• changeip.com</li> <li>• dyndns.org</li> <li>• no-ip.org</li> <li>• tzo.com</li> <li>• DNS-O-Matic</li> <li>• Others...</li> </ul>
<b>Account Name / Email Address</b>	<p>Support custom Dynamic DNS servers by entering its URL. Works with any service compatible with DynDNS API.</p> <p>Select <b>Disabled</b> to disable this feature.</p>
<b>Password / TZO Key</b>	<p>This setting specifies the registered user name for the dynamic DNS service.</p>
<b>Hosts / Domain</b>	<p>This setting specifies the password for the dynamic DNS service.</p>
	<p>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.</p>

Important Note
<p>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</p>

23 days, even if a WAN's IP address has not changed.

## 10 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.




AP Settings	
<b>SSID</b>	<p>You can select the wireless networks for 2.4 GHz or 5 GHz separately for each SSID.</p>
<b>Operating Country</b>	<p>This drop-down menu specifies the national/regional regulations which the Wi-Fi radio should follow.</p> <ul style="list-style-type: none"> <li>• If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW).</li> <li>• If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW).</li> </ul> <p>NOTE: Users are required to choose an option suitable to local laws and regulations.</p>
<b>Preferred Frequency</b>	<p>Indicate the preferred frequency to use for clients to connect.</p>

Important Note	
<p>Per FCC regulation, the country selection is not available on all models marketed in the US. All US models are fixed to US channels only.</p>	

	2.4 GHz	5 GHz
Protocol	802.11ng	802.11n/ac
Channel Width	20 MHz ▾	Auto ▾
Channel	Auto ▾ <input type="button" value="Edit"/> Channels: 1 2 3 4 5 6 7 8 9 10 11	Auto ▾ <input type="button" value="Edit"/> Channels: 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140 149 153 157 161 165
Auto Channel Update	Daily at 03 ▾ :00 <input checked="" type="checkbox"/> Wait until no active client associated	Daily at 03 ▾ :00 <input checked="" type="checkbox"/> Wait until no active client associated
Output Power	Fixed: Max ▾ <input type="checkbox"/> Boost	Fixed: Max ▾ <input type="checkbox"/> Boost
Client Signal Strength Threshold	0 -95 dBm (0: Unlimited)	0 -95 dBm (0: Unlimited)
Maximum number of clients	0 (0: Unlimited)	0 (0: Unlimited)

AP Settings (part 2)	
<b>Protocol</b>	This option allows you to specify whether 802.11b and/or 802.11g client association requests will be accepted. Available options are <b>802.11ng</b> and <b>802.11na</b> . By default, <b>802.11ng</b> is selected.
<b>Channel Width</b>	Available options are <b>20 MHz</b> , <b>40 MHz</b> , and <b>Auto (20/40 MHz)</b> . Default is <b>Auto (20/40 MHz)</b> , which allows both widths to be used simultaneously.
<b>Channel</b>	This option allows you to select which 802.11 RF channel will be utilized. <b>Channel 1 (2.412 GHz)</b> is selected by default.
<b>Auto Channel Update</b>	Indicate the time of day at which update automatic channel selection.
<b>Output Power</b>	This option is for specifying the transmission output power for the Wi-Fi AP. There are 4 relative power levels available – <b>Max</b> , <b>High</b> , <b>Mid</b> , and <b>Low</b> . The actual output power will be bound by the regulatory limits of the selected country.
<b>Client Signal Strength Threshold</b>	This setting determines the maximum strength at which the Wi-Fi AP can broadcast
<b>Maximum number of clients</b>	This setting determines the maximum number of clients that can connect to this Wi-Fi frequency.

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**.



Management VLAN ID	<input type="text" value="Untagged LAN (No VLAN)"/>
Operating Schedule	<input type="text" value="Always on"/>
Beacon Rate	<input type="text" value="1 Mbps"/> 6 Mbps will be used for 5 GHz radio
Beacon Interval	<input type="text" value="100 ms"/>
DTIM	<input type="text" value="1"/> <input type="button" value="Default"/>
RTS Threshold	<input type="text" value="0"/> <input type="button" value="Default"/>
Fragmentation Threshold	<input type="text" value="0"/> (0: Disable) <input type="button" value="Default"/>
Distance / Time Converter	<input type="text" value="4050"/> m <small>Note: Input distance for recommended values</small>
Slot Time	<input checked="" type="radio"/> Auto <input type="radio"/> Custom <input type="text" value="9"/> <input type="text" value="μs"/> <input type="button" value="Default"/>
ACK Timeout	<input type="text" value="48"/> <input type="text" value="μs"/> <input type="button" value="Default"/>
Frame Aggregation	<input type="checkbox"/>

Advanced AP Settings	
<b>Management VLAN ID</b>	<p>This field specifies the VLAN ID to tag to management traffic, such as communication traffic between the AP and the AP Controller. The value is zero by default, which means that no VLAN tagging will be applied.</p> <p>NOTE: Change this value with caution as alterations may result in loss of connection to the AP Controller.</p>
<b>Operating Schedule</b>	Choose from the schedules that you have defined in System>Schedule. Select the schedule for the integrated AP to follow from the drop-down menu.
<b>Beacon Rate</b> <sup>A</sup>	This option is for setting the transmit bit rate for sending a beacon. By default, <b>1Mbps</b> is selected.
<b>Beacon Interval</b> <sup>A</sup>	This option is for setting the time interval between each beacon. By default, <b>100ms</b> is selected.
<b>DTIM</b> <sup>A</sup>	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 <b>1 ms</b> .
<b>RTS Threshold</b> <sup>A</sup>	The RTS (Request to Clear) threshold determines the level of connection required before the AP starts sending data. The recommended standard of the RTS threshold is around 500.
<b>Fragmentation Threshold</b> <sup>A</sup>	This setting determines the maximum size of a packet before it gets fragmented into multiple pieces.
<b>Distance / Time Converter</b>	Select the range you wish to cover with your Wi-Fi, and the router will make recommendations for the Slot Time and ACK Timeout.

<b>Slot Time</b> <sup>A</sup>	This field is for specifying the unit wait time before transmitting a packet. By default, this field is set to <b>9 µs</b> .
<b>ACK Timeout</b> <sup>A</sup>	This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to <b>48 µs</b> .
<b>Frame Aggregation</b> <sup>A</sup>	This option allows you to enable frame aggregation to increase transmission throughput.

<sup>A</sup> - Advanced feature, please click the  button on the top right-hand corner to activate.

Web Administration Settings (on External AP)	
Enable	<input checked="" type="checkbox"/>
Web Access Protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Management Port	443
HTTP to HTTPS Redirection	<input checked="" type="checkbox"/>
Admin Username	admin
Admin Password	601202b1afc6 <input type="button" value="Generate"/>

Web Administration Settings	
<b>Enable</b>	Ticking this box enables web admin access for APs located on the WAN.
<b>Web Access Protocol</b>	Determines whether the web admin portal can be accessed through HTTP or HTTPS
<b>Management Port</b>	Determines the port at which the management UI can be accessed.
<b>Admin Username</b>	Determines the username to be used for logging into the web admin portal
<b>Admin Password</b>	Determines the password for the web admin portal on external AP.

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	20/40 MHz
Bit Rate	Auto
Output Power	Max <input type="checkbox"/> Boost

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

## 11 ContentHub Configuration

### 11.1 ContentHub

ContentHub allows you to deliver webpages and applications to users connected to the SSID using the local storage on your router like the Max HD2/HD4 with Mediafast, which can store up to 8GB of media.

Users will be able to access news, articles, videos, and access your web app, without the need for internet access.

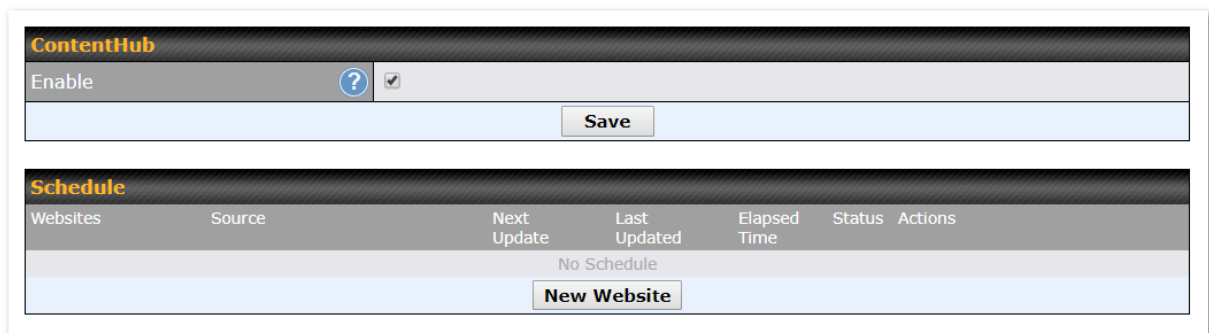
The ContentHub can be used to provide infotainment to connected users on transport.

### 11.2 Configuring the ContentHub

ContentHub Storage needs to be configured before content can be uploaded to the ContentHub. Follow the link on the information panel to configure storage.

ContentHub storage has not been configured. Click [here](#) to review storage configuration

To access the ContentHub, navigate to **Advanced > ContentHub** and check the **Enable** box



The screenshot shows the ContentHub configuration page. At the top, there's a section titled 'ContentHub' with an 'Enable' checkbox that is checked. Below this is a 'Save' button. The next section is titled 'Schedule' and contains a table with columns: Websites, Source, Next Update, Last Updated, Elapsed Time, Status, and Actions. The table is currently empty, showing 'No Schedule'. Below the table is a 'New Website' button.

On an external server configure content (a website or application) that will be synced to the ContentHub; for example a html5 website.

To configure a website or application as content follow these steps.

## 11.3 Configure a website to be published from the ContentHub

This option allows you to sync a website to the Peplink router, this website will then be published with the specified domain from the router itself and makes the content available to the client via the HTTP/HTTPS protocol. Only FTP sync is supported for this type of ContentHub content. The content should be uploaded to an FTP server before.

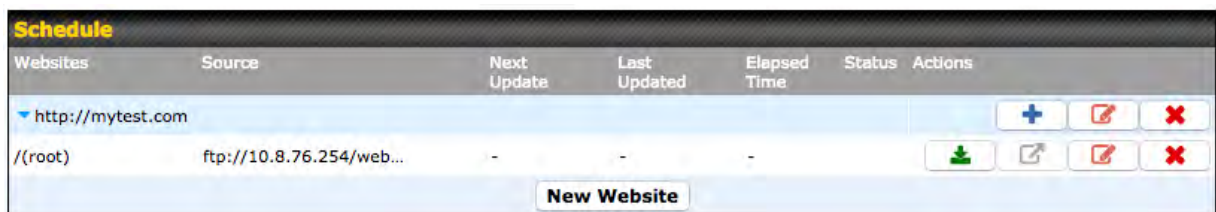
Click **New Website**, and the following configuration options will appear:

The Active checkbox toggles the activation of the content. For Website.


<b>Type</b>	HTTP,HTTPS or both
<b>Domain/Path</b>	The contenthub uses this as the domain name for client access (such as http://mytest.com).
<b>Source</b>	Enter the server details that the content will be downloaded from. Enter your credentials under <b>Username</b> and <b>Password</b> .
<b>Period</b>	This field determines how often the Router will search for updates to the

	source content.
<b>Method</b>	Only applicable for application: Choose between sync or file upload
<b>Bandwidth Limit</b>	Used to limit the bandwidth for each client to access the web server.

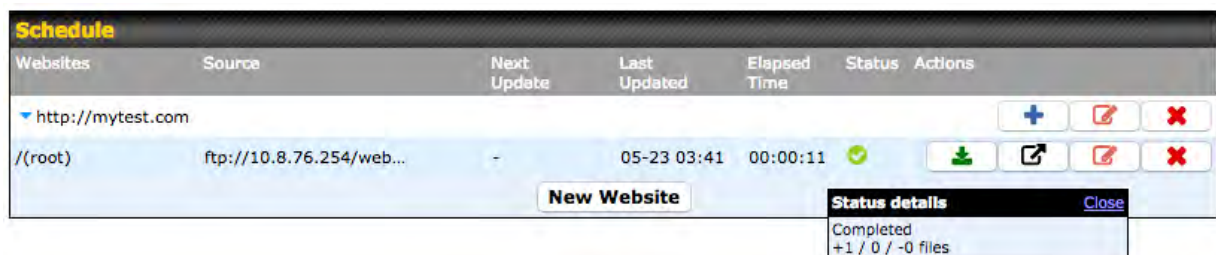
Click “Save & Apply Now” to activate the changes. Below is a screenshot after configuration:



The content will be sync based on the **Period** that is configured before.

If you want to trigger the sync manually, you can click “”. The “Status” column shows the sync progress.

When the sync complete, there is a summary as shown in the screenshot below:



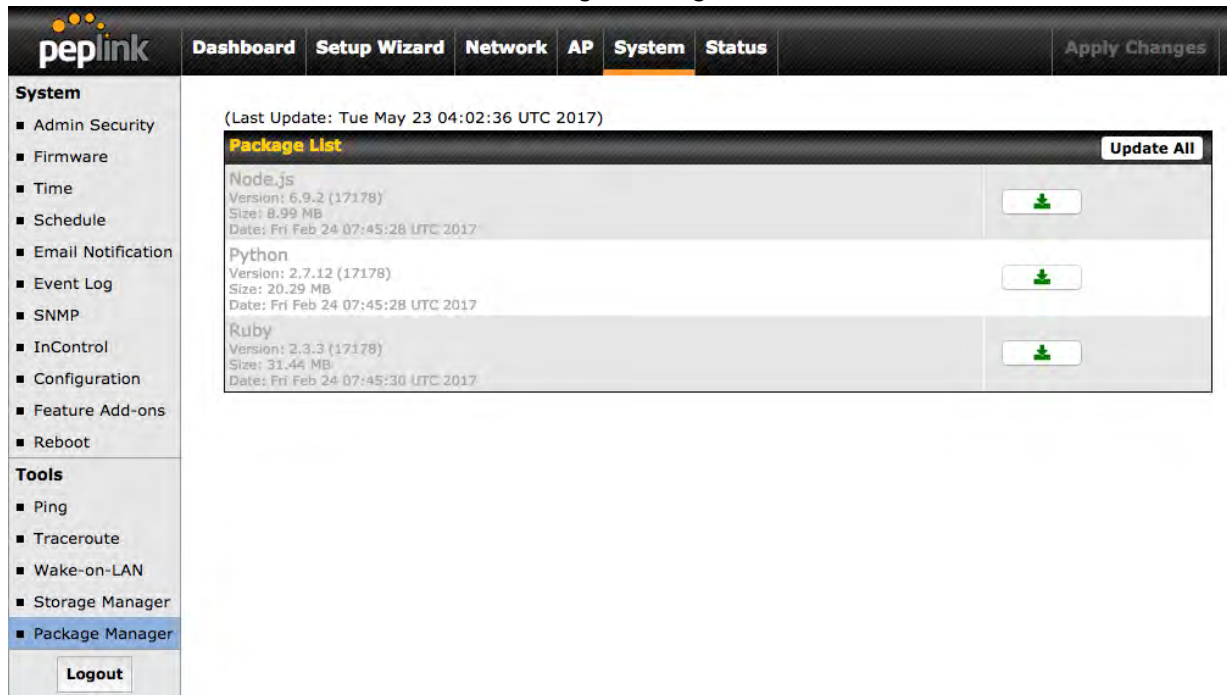
To access the content, open a browser in MFA’s client and enter the domain configured before (such as <http://mytest.com>).

## 11.4 Configure an application to be published from the ContentHub




Mediafast Routers allow you to configure and publish ant application from the router itself by using the supported framework

- Python (version 2.7.12)
- Ruby (version 2.3.3)
- Node.js (version 6.9.2)

First install the desired framework in “Package Manager” as below:



The screenshot shows the Peplink System configuration page. The left sidebar contains a menu with 'System' and 'Tools' sections. The 'System' section includes options like Admin Security, Firmware, Time, Schedule, Email Notification, Event Log, SNMP, InControl, Configuration, Feature Add-ons, and Reboot. The 'Tools' section includes Ping, Traceroute, Wake-on-LAN, Storage Manager, and Package Manager (which is highlighted). A 'Logout' button is at the bottom of the sidebar. The main content area shows the 'Package List' with a table of installed packages and their details.

Package List		Update All
(Last Update: Tue May 23 04:02:36 UTC 2017)		
Node.js	Version: 6.9.2 (17178) Size: 8.99 MB Date: Fri Feb 24 07:45:28 UTC 2017	
Python	Version: 2.7.12 (17178) Size: 20.29 MB Date: Fri Feb 24 07:45:28 UTC 2017	
Ruby	Version: 2.3.3 (17178) Size: 31.44 MB Date: Fri Feb 24 07:45:30 UTC 2017	

After installing the framework, you can select the type to “Application” and configure the website:



Schedule

Active	<input checked="" type="checkbox"/>
Type	<input type="radio"/> Website <input checked="" type="radio"/> Application
Protocol	HTTP
Domain	http://
Method	<input checked="" type="radio"/> Sync <input type="radio"/> File Upload
Source	<div>ftp ://</div> <div>Username:</div> <div>Password:</div>
Period	<div>Everyday</div> <div>From 00:00 to 01:00</div>
Bandwidth Limit	0 Gbps (0: Unlimited)

Save & Apply Now

Cancel

The setting is same as Website type and you can refer to the description in the above section

For the Application type, you need to pack your application as below:

1. Implement two bash script files, start.sh and stop.sh in root folder, to start and stop your application. the Mediafast router will only execute start.sh and stop.sh when the corresponding website is enabled and disabled respectively.
2. Compress your application files and the bash script to .tar.gz format.
3. Upload this tar file to the router.

## 12 MediaFast Configuration

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

## 12.1 Setting Up MediaFast Content Caching

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

**MediaFast**

Enable ☒

Domains / IP Addresses ☐ Cache all ☐ Whitelist ☒ Blacklist

Source IP Subnet ☒ Any ☐ Custom

MediaFast	
<b>Enable</b>	Click the checkbox to enable MediaFast content caching.
<b>Domains / IP Addresses</b>	Choose to <b>Cache on all domains</b> , or enter domain names and then choose either <b>Whitelist</b> (cache the specified domains only) or <b>Blacklist</b> (do not cache the specified domains).
<b>Source IP Subnet</b>	This setting allows caching to be enabled on custom subnets only. If "Any" is selected, then caching will apply to all subnets.

**Secure Content Caching**

Enable ☒ Note: Please enable MediaFast for Secure Content Caching

Domains / IP Addresses ☐ Cache all ☒ Whitelist ☐ Blacklist

googlevideo.com  
youtube.com

Source IP Subnet ☒ Any ☐ Custom

The **Secure Content Caching** menu operates identically to the **MediaFast** menu, except it is for secure content caching accessible through https://. In order for Mediafast devices to cache and deliver HTTPS content, every client needs to have the necessary certificates installed\*.





















\*See <https://forum.peplink.com/t/certificate-installation-for-mediafast-https-caching/>

Cache Control					
Content Type	<input checked="" type="checkbox"/> Video <input checked="" type="checkbox"/> Audio <input checked="" type="checkbox"/> Images <input checked="" type="checkbox"/> OS / Application Updates				
Cache Lifetime Settings	<table border="1"> <thead> <tr> <th>File Extension</th> <th>Lifetime (days)</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table> <div style="text-align: right;">+</div>	File Extension	Lifetime (days)		
File Extension	Lifetime (days)				







Cache Control	
<b>Content Type</b>	Check these boxes to cache the listed content types or leave boxes unchecked to disable caching for the listed types.
<b>Cache Lifetime Settings</b>	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.

## 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							
Name	Status	Next Run Time	Last Run Time	Last Duration	Result	Last Download	Actions
▶ Course Progress	Downloading	04-11 06:00	04-09 02:03	-		0 B	  
▶ National Geog	Ready	04-11 00:00	04-09 00:00	00:01		4.98 kB	  
▶ Syllabus	Downloading	04-11 06:00	04-09 06:00	-		0 B	  
▶ Vimeo	Ready	04-11 00:00	04-09 02:03	00:01		115.91 kB	  
▶ ted	Ready	04-11 00:00	04-09 00:00	00:01		62.26 kB	  
<a href="#">New Schedule</a>							

Tools	
<a href="#">Clear Web Cache</a>	<a href="#">Clear Statistics</a>

Prefetch Schedule Settings	
<b>Name</b>	This field displays the name given to the scheduled download.
<b>Status</b>	Check the status of your scheduled download here.
<b>Next Run Time/Last Run Time</b>	These fields display the date and time of the next and most recent occurrences of the scheduled download.
<b>Last Duration</b>	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.
<b>Result</b>	This field indicates whether downloads are in progress (  ) or complete (  ) .
<b>Last Download</b>	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.
<b>Actions</b>	<p>To begin a scheduled download immediately, click .</p> <p>To cancel a scheduled download, click .</p> <p>To edit a scheduled download, click .</p> <p>To delete a scheduled download, click .</p>
<b>New Schedule</b>	Click to begin creating a new scheduled download. Clicking the button will cause the following screen to appear:

**MediaFast Schedule**

Name (optional)		
Active	<input checked="" type="checkbox"/>	
URL	<div>URL</div> <div></div>	+
Depth	2 levels	Default
Time Period	From 00:00 to 01:00	
Repeat	Everyday	
Bandwidth Limit	0 Gbps (0: Unlimited)	

Save & Apply Now
Cancel

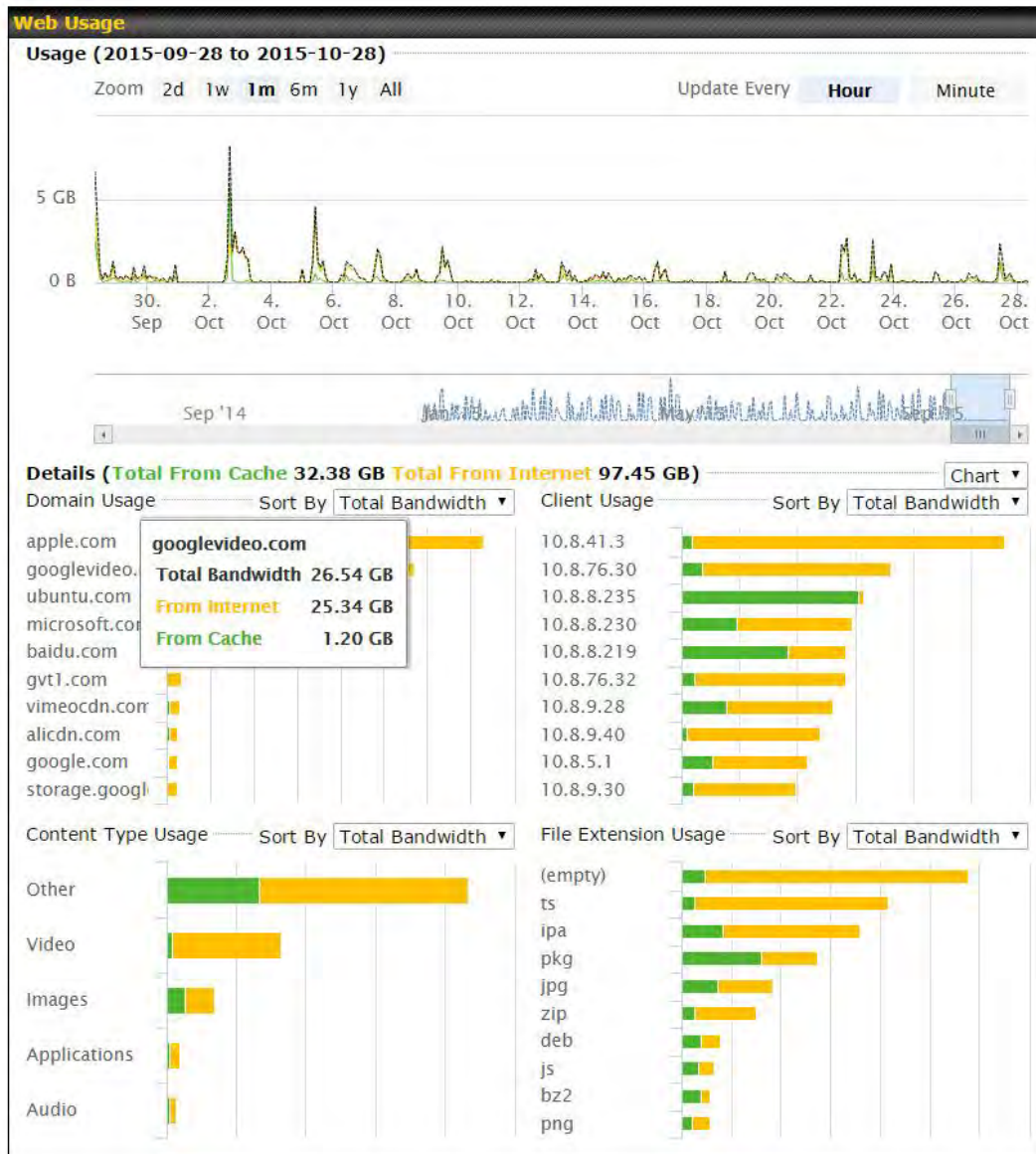
Simply provide the requested information to create your schedule.

**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.

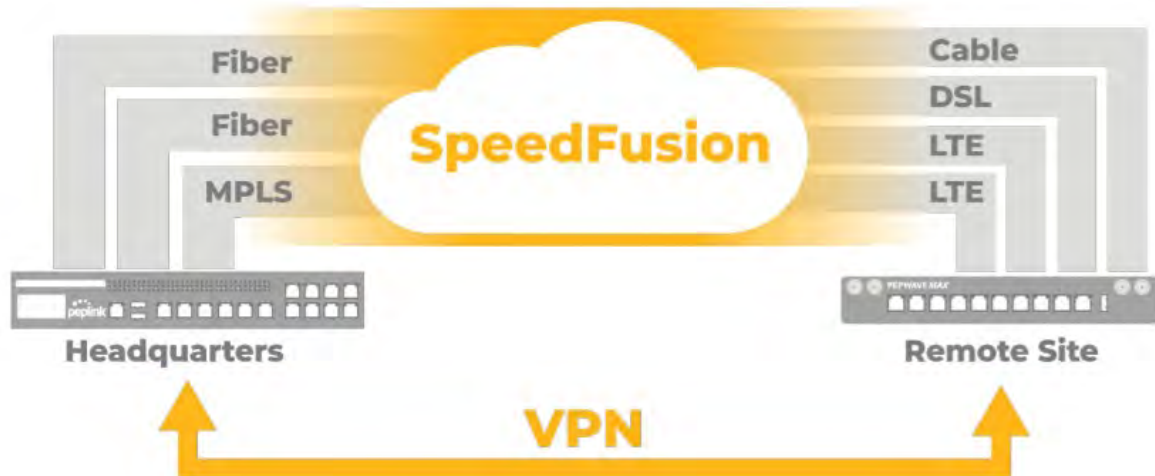
## 12.3 Viewing MediaFast Statistics

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





## 13 Bandwidth Bonding SpeedFusion™ / PepVPN



Pepwave bandwidth bonding SpeedFusion™ 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.


### 13.1 PepVPN


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




## PepVPN with SpeedFusion™




 InControl management enabled. Settings can now be configured on [InControl](#).

Profile	Remote ID	Remote Address(es)	
 FL Office	8345-5F7A-DE97		 
<a href="#">New Profile</a>			

Send All Traffic To
No PepVPN profile selected 

PepVPN
Local ID  MAX_HD2_DEF1 

Link Failure Detection
<div> <div>Link Failure Detection Time </div> <div> <input checked="" type="radio"/> Recommended (Approx. 15 secs)  <input type="radio"/> Fast (Approx. 6 secs)  <input type="radio"/> Faster (Approx. 2 secs)  <input type="radio"/> Extreme (Under 1 sec)  <small>Shorter detection time incurs more health checks and higher bandwidth overhead</small> </div> </div>
<a href="#">Save</a>


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 access 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					
Name	<input type="text"/>				
Active	<input checked="" type="checkbox"/>				
Encryption	<input checked="" type="radio"/> 256-bit AES <input type="radio"/> OFF				
Authentication	<input checked="" type="radio"/> Remote ID / Pre-shared Key <input type="radio"/> X.509				
Remote ID / Pre-shared Key	<table border="1"> <tr> <th>Remote ID</th> <th>Pre-shared Key</th> </tr> <tr> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </table>	Remote ID	Pre-shared Key	<input type="text"/>	<input type="text"/>
Remote ID	Pre-shared Key				
<input type="text"/>	<input type="text"/>				
NAT Mode	<input type="checkbox"/>				
Remote IP Address / Host Names (Optional)	<input type="text"/> <small>If this field is empty, this field on the remote unit must be filled</small>				
Cost	<input type="text" value="10"/>				
Data Port	<input checked="" type="radio"/> Auto <input type="radio"/> Custom <input type="text"/>				
Bandwidth Limit	<input type="checkbox"/>				
WAN Smoothing	<input type="text" value="Off"/>				
Use IP ToS	<input type="checkbox"/>				
Latency Difference Cutoff	<input type="text" value="500"/> ms				

PepVPN Profile Settings	
<b>Name</b>	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 ( ).
<b>Active</b>	When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled.
<b>Encryption</b>	By default, VPN traffic is encrypted with <b>256-bit AES</b> . If <b>Off</b> is selected on both sides of a VPN connection, no encryption will be applied.
<b>Authentication</b>	Select from <b>By Remote ID Only</b> , <b>Preshared Key</b> , or <b>X.509</b> to specify the method the Peplink Balance will use to authenticate peers. When selecting <b>By Remote ID Only</b> , be sure to enter a unique peer ID number in the <b>Remote ID</b> field.
<b>Remote ID / Pre-shared Key</b>	<p>This optional field becomes available when <b>Remote ID / Pre-shared Key</b> is selected as the Peplink Balance's VPN <b>Authentication</b> method, as explained above. <b>Pre-shared Key</b> 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.</p> <p>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.</p>
<b>Remote</b>	These optional fields become available when <b>X.509</b> is selected as the Peplink

<b>ID/Remote Certificate</b>	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 <b>Show Details</b> link below the field.
<b>Allow Shared Remote ID</b>	When this option is enabled, the router will allow multiple peers to run using the same remote ID.
<b>NAT Mode</b>	Check this box to allow the local DHCP server to assign an IP address to the remote peer. When <b>NAT Mode</b> is enabled, all remote traffic over the VPN will be tagged with the assigned IP address using network address translation.
<b>Remote IP Address / Host Names (Optional)</b>	<p>If <b>NAT Mode</b> 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.</p> <p>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.</p>
<b>Cost</b>	<p>Define path cost for this profile.</p> <p>OSPF will determine the best route through the network using the assigned cost.</p> <p>Default: 10</p>
<b>Data Port</b>	<p>This field is used to specify a UDP port number for transporting outgoing VPN data. If <b>Default</b> 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 <b>Custom</b> is selected, enter an outgoing port number from 1 to 65535.</p> <p>Click the  icon to configure data stream using TCP protocol [EXPERIMENTAL]. In the case TCP protocol is used, the exposed TCP session option can be authorised to work with TCP accelerated WAN link.</p>
<b>Bandwidth Limit</b>	Define maximum download and upload speed to each individual peer. This functionality requires the peer to use PepVPN version 4.0.0 or above.
<b>Cost</b>	<p>Define path cost for this profile.</p> <p>OSPF will determine the best route through the network using the assigned cost.</p> <p>Default: 10</p>
<b>WAN Smoothing<sup>A</sup></b>	Select the degree to which WAN Smoothing will be implemented across your WAN links.
<b>Use IP ToS</b>	Checking this button enables the use of IP ToS header field.
<b>Latency Difference Cutoff</b>	Traffic will be stopped for links that exceed the specified millisecond value with respect to the lowest latency link. (e.g. Lowest latency is 100ms, a value of 500ms means links with latency 600ms or more will not be used)

<sup>A</sup> - 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 					
	Priority	Direction	Connect to Remote	Cut-off latency (ms)	Suspension Time after Packet Loss (ms)
1. WAN 1	1 (Highest) ▼	Up/Down ▼	All ▼		
2. WAN 2	1 (Highest) ▼	Up/Down ▼	All ▼		
3. Wi-Fi WAN	1 (Highest) ▼	Up/Down ▼	All ▼		
4. Cellular 1	1 (Highest) ▼	Up/Down ▼	All ▼		
5. Cellular 2	1 (Highest) ▼	Up/Down ▼	All ▼		
6. USB	1 (Highest) ▼	Up/Down ▼	All ▼		


**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**

No PepVPN profile selected 

**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:

**Send All Traffic**

Send All Traffic To 
☒ Balance 2942-1257-1241 ▼

☐ DNS Server  
 8.8.8.8  
 8.8.4.4

☒ Backup Site Balance-4810-1825-068E-4810 ▼

☐ DNS Server  
 8.8.8.8  
 8.8.4.4

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.

The screenshot shows two configuration panels. The top panel, titled 'Outbound Policy', has a dropdown menu set to 'According to custom rules' and an edit icon. The bottom panel, titled 'PepVPN Outbound Custom Rules', is a table with columns: Service, Algorithm, Source, Destination, and Protocol. The 'Source' column is set to '(Auto)'. Below the table is an 'Add Rule' button.

The screenshot shows the 'PepVPN Local ID' configuration field. It contains the text 'MAX\_HD2\_8D1C' and an edit icon.

## 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**.

The screenshot shows the 'PepVPN Settings' panel with the following options:

- Handshake Port:** Radio buttons for 'Default' (selected) and 'Custom' (with an input field).
- Backward Compatibility:** Radio buttons for 'High (firmware 5.3+)' (selected) and 'Latest (firmware 6.2+)'.
- Link Failure Detection Time:** Radio buttons for 'Recommended (Approx. 15 secs)' (selected), 'Fast (Approx. 6 secs)', 'Faster (Approx. 2 secs)', and 'Extreme (Under 1 sec)'. A note below states: 'Shorter detection time incurs more health checks and higher bandwidth overhead'.

## PepVPN Settings

<b>Handshake Port<sup>A</sup></b>	To designate a custom handshake port (TCP), click the <b>custom</b> radio button and enter the port number you wish to designate.
<b>Backward Compatibility</b>	Determine the level of backward compatibility needed for PepVPN tunnels. The use of the <b>Latest</b> setting is recommended as it will improve the performance and resilience of SpeedFusion connections.
<b>Link Failure Detection Time</b>	<p>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.</p> <p>When <b>Recommended</b> (default) is selected, a health check packet is sent every five seconds, and the expected detection time is 15 seconds.</p> <p>When <b>Fast</b> is selected, a health check packet is sent every three seconds, and the</p>



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.

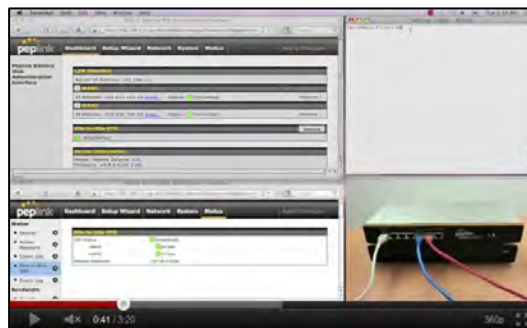
<sup>A</sup> - Advanced feature, please click the  button on the top right-hand corner to activate.

### 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>

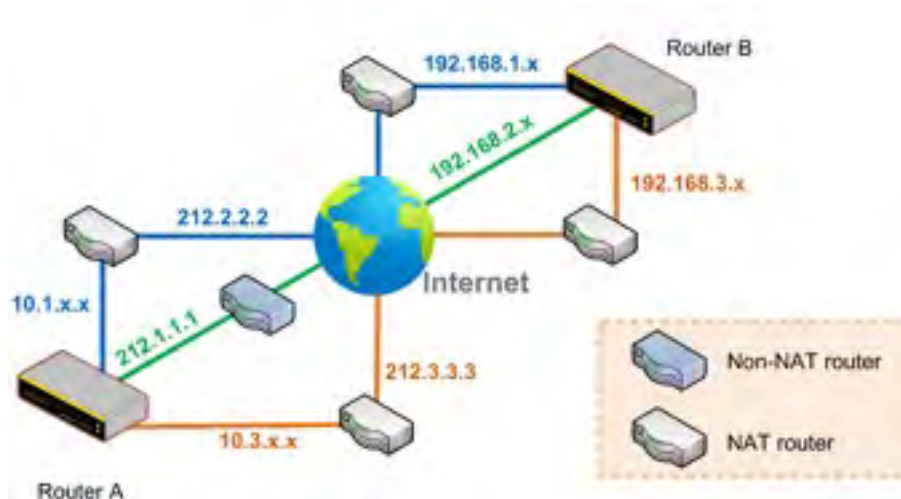
## 13.2 The Pepwave Router Behind a NAT Router

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.

### 13.3 SpeedFusion™ Status

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

SpeedFusion™ <span>Status</span>	
FL Office	Established
NY Office	Established

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.



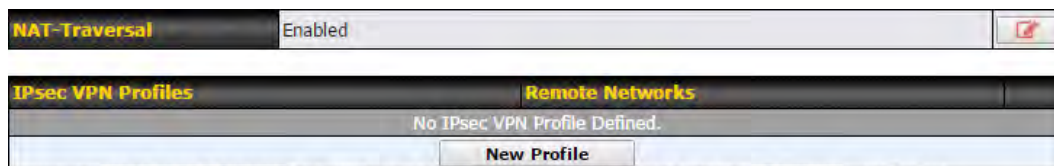
## 14 IPsec VPN

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**.



Pepwave MAX IPsec only supports network-to-network connection with Cisco, Juniper or Pepwave MAX devices.

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	<input checked="" type="checkbox"/>												
Connect Upon Disconnection of	<input checked="" type="checkbox"/> WAN 2												
Remote Gateway IP Address / Host Name	12.12.12.12												
Local Networks	<p>Propose the following networks to remote gateway:</p> <p> <input type="checkbox"/> 172.16.1.1/24  <input type="checkbox"/> 172.16.2.1/24  <input type="checkbox"/> 172.16.3.1/24  <input checked="" type="checkbox"/> 10.10.0.1/32  <input checked="" type="checkbox"/> 192.168.10.0/24  <input checked="" type="checkbox"/> 192.168.11.0/24  <input type="checkbox"/> <input type="text"/> </p> <p>Apply the following NAT policies:</p> <table border="0"> <tr> <td><input checked="" type="checkbox"/> 172.16.1.0/24</td> <td><input checked="" type="checkbox"/> 192.168.10.0/24</td> </tr> <tr> <td><input checked="" type="checkbox"/> 172.16.2.0/24</td> <td><input checked="" type="checkbox"/> 10.10.0.1/32</td> </tr> <tr> <td><input checked="" type="checkbox"/> 172.16.3.11/32</td> <td><input checked="" type="checkbox"/> 192.168.11.101/32</td> </tr> <tr> <td><input checked="" type="checkbox"/> 172.16.3.21/32</td> <td><input checked="" type="checkbox"/> 192.168.11.201/32</td> </tr> <tr> <td><input type="checkbox"/> Local Network</td> <td><input type="checkbox"/> NAT Network</td> </tr> </table>			<input checked="" type="checkbox"/> 172.16.1.0/24	<input checked="" type="checkbox"/> 192.168.10.0/24	<input checked="" type="checkbox"/> 172.16.2.0/24	<input checked="" type="checkbox"/> 10.10.0.1/32	<input checked="" type="checkbox"/> 172.16.3.11/32	<input checked="" type="checkbox"/> 192.168.11.101/32	<input checked="" type="checkbox"/> 172.16.3.21/32	<input checked="" type="checkbox"/> 192.168.11.201/32	<input type="checkbox"/> Local Network	<input type="checkbox"/> NAT Network
<input checked="" type="checkbox"/> 172.16.1.0/24	<input checked="" type="checkbox"/> 192.168.10.0/24												
<input checked="" type="checkbox"/> 172.16.2.0/24	<input checked="" type="checkbox"/> 10.10.0.1/32												
<input checked="" type="checkbox"/> 172.16.3.11/32	<input checked="" type="checkbox"/> 192.168.11.101/32												
<input checked="" type="checkbox"/> 172.16.3.21/32	<input checked="" type="checkbox"/> 192.168.11.201/32												
<input type="checkbox"/> Local Network	<input type="checkbox"/> NAT Network												
Remote Networks	<table border="1"> <thead> <tr> <th>Network</th> <th>Subnet Mask</th> <th></th> </tr> </thead> <tbody> <tr> <td>192.167.11.193</td> <td>255.255.255.0 (/24)</td> <td><input type="button" value="+"/></td> </tr> </tbody> </table>	Network	Subnet Mask		192.167.11.193	255.255.255.0 (/24)	<input type="button" value="+"/>						
Network	Subnet Mask												
192.167.11.193	255.255.255.0 (/24)	<input type="button" value="+"/>											
Authentication	<input checked="" type="radio"/> Preshared Key <input type="radio"/> X.509 Certificate												
Mode	<input checked="" type="radio"/> Main Mode (All WANs need to have Static IP) <input type="radio"/> Aggressive Mode												
Force UDP Encapsulation	<input type="checkbox"/>												
Preshared Key	<input type="text" value="....."/> <input checked="" type="checkbox"/> Hide Characters												
Local ID	<input type="text"/>												
Remote ID	<input type="text"/>												
Phase 1 (IKE) Proposal	1 AES-256 & SHA1 2 -----												
Phase 1 DH Group	<input checked="" type="checkbox"/> Group 2: MODP 1024 <input type="checkbox"/> Group 5: MODP 1536												
Phase 1 SA Lifetime	3600	seconds	Default										
Phase 2 (ESP) Proposal	1 AES-256 & SHA1 2 -----												
Phase 2 PFS Group	<input checked="" type="radio"/> None <input type="radio"/> Group 2: MODP 1024 <input type="radio"/> Group 5: MODP 1536												
Phase 2 SA Lifetime	28800	seconds	Default										

IPsec VPN Settings	
<b>Name</b>	This field is for specifying a local name to represent this connection profile.
<b>Active</b>	When this box is checked, this IPsec VPN connection profile will be enabled. Otherwise, it will be disabled.
<b>Connect Upon Disconnection of</b>	Check this box and select a WAN to connect to this VPN automatically when the specified WAN is disconnected.
<b>Remote Gateway IP Address / Host Name</b>	Enter the remote peer's public IP address. For <b>Aggressive Mode</b> , this is optional.
<b>Local Networks</b>	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.
<b>Remote Networks</b>	Enter the LAN and subnets that are located at the remote site here.
<b>Authentication</b>	To access your VPN, clients will need to authenticate by your choice of methods. Choose between the <b>Preshared Key</b> and <b>X.509 Certificate</b> methods of authentication.
<b>Mode</b>	Choose <b>Main Mode</b> if both IPsec peers use static IP addresses. Choose <b>Aggressive Mode</b> if one of the IPsec peers uses dynamic IP addresses.
<b>Force UDP</b>	For forced UDP encapsulation regardless of NAT-traversal, tick this checkbox.

Encapsulation	
<b>Pre-shared Key</b>	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.
<b>Remote Certificate (pem encoded)</b>	Available only when <b>X.509 Certificate</b> is chosen as the <b>Authentication</b> method, this field allows you to paste a valid X.509 certificate.
<b>Local ID</b>	In <b>Main Mode</b> , this field can be left blank. In <b>Aggressive Mode</b> , if <b>Remote Gateway IP Address</b> is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.
<b>Remote ID</b>	In <b>Main Mode</b> , this field can be left blank. In <b>Aggressive Mode</b> , if <b>Remote Gateway IP Address</b> is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.
<b>Phase 1 (IKE) Proposal</b>	In <b>Main Mode</b> , this allows setting up to six encryption standards, in descending order of priority, to be used in initial connection key negotiations. In <b>Aggressive Mode</b> , only one selection is permitted.
<b>Phase 1 DH Group</b>	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. <b>Group 2: 1024-bit</b> is the default value. <b>Group 5: 1536-bit</b> is the alternative option.
<b>Phase 1 SA Lifetime</b>	This setting specifies the lifetime limit of this Phase 1 Security Association. By default, it is set at <b>3600</b> seconds.
<b>Phase 2 (ESP) Proposal</b>	In <b>Main Mode</b> , 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 <b>Aggressive Mode</b> , only one selection is permitted.
<b>Phase 2 PFS Group</b>	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. <b>None</b> - 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. <b>Group 2: 1024-bit</b> Diffie-Hellman group. The larger the group number, the higher the security. <b>Group 5: 1536-bit</b> is the third option.
<b>Phase 2 SA Lifetime</b>	This setting specifies the lifetime limit of this Phase 2 Security Association. By default, it is set at <b>28800</b> seconds.

WAN Connection Priority	
Priority	WAN Selection
1	WAN 1
2	-----

### 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

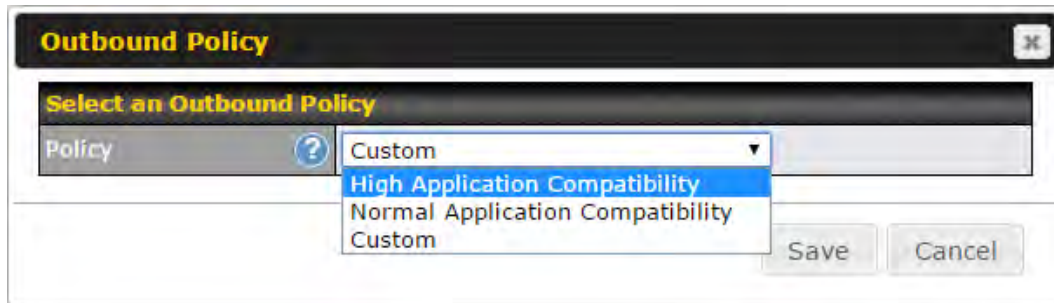
Outbound policy is applied only when more than one WAN connection is active.

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

Outbound Policy					
Custom					
Rules  Drag and drop rows to change rule order					
Service	Algorithm	Source	Destination	Protocol / Port	
HTTPS_Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	
Default	(Auto)				
<b>Add Rule</b>					

### 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.

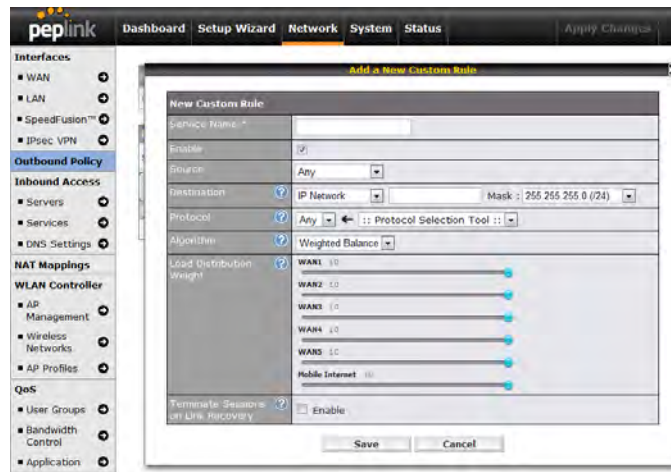
Outbound Policy Settings	
<b>High Application Compatibility</b>	Outbound traffic from a source LAN device is routed through the same WAN connection regardless of the destination Internet IP address and protocol. This option provides the highest application compatibility.
<b>Normal Application Compatibility</b>	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.
<b>Custom</b>	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](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.


**Outbound Policy**
?

Custom


**Rules** ⏏ Drag and drop rows to change rule order
?

Service	Algorithm	Source	Destination	Protocol / Port	
HTTPS Persistence	Persistence (Src) (Auto)	Any	IP Network 192.168.50.0/24	TCP 443	
PepVPN Routes					
Default	(Auto)				
Add Rule					

**Expert Mode**
?

Enabled


### 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**.



Algorithm ?	Weighted Balance ▼
Load Distribution Weight ?	<div>WAN 1 10</div> <div>WAN 2 10</div> <div>Wi-Fi WAN 10</div> <div>Cellular 1 10</div> <div>Cellular 2 10</div> <div>USB 10</div>

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  $16.7\% = (10 / 60 \times 100\%)$ .

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

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

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

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

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

### 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.

Algorithm	Persistence
Persistence Mode	<input checked="" type="radio"/> By Source <input type="radio"/> By Destination
Load Distribution	<input type="radio"/> Auto <input checked="" type="radio"/> Custom
Load Distribution Weight	<div> <div>WAN 1 10</div> <div>WAN 2 10</div> <div>Wi-Fi WAN 10</div> <div>Cellular 1 10</div> <div>Cellular 2 10</div> <div>USB 10</div> </div>

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

<b>By Source:</b>	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.
<b>By Destination:</b>	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**.

Algorithm	Enforced
Enforced Connection	<div> <div>WAN: WAN 1</div> <div> <div>WAN: WAN 1</div> <div>WAN: WAN 2</div> <div>WAN: Wi-Fi WAN</div> <div>WAN: Cellular 1</div> <div>WAN: Cellular 2</div> <div>WAN: USB</div> <div>VPN: Connection 1</div> </div> </div>
<div>Save</div> <div>Cancel</div>	

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.

Algorithm	Priority																
Priority Order	<table border="1"> <tr> <td>Highest Priority</td> <td>Not In Use</td> </tr> <tr> <td>WAN: WAN 1</td> <td>VPN: Connection 1</td> </tr> <tr> <td>WAN: WAN 2</td> <td></td> </tr> <tr> <td>WAN: Wi-Fi WAN</td> <td></td> </tr> <tr> <td>WAN: Cellular 1</td> <td></td> </tr> <tr> <td>WAN: Cellular 2</td> <td></td> </tr> <tr> <td>WAN: USB</td> <td></td> </tr> <tr> <td>Lowest Priority</td> <td></td> </tr> </table>	Highest Priority	Not In Use	WAN: WAN 1	VPN: Connection 1	WAN: WAN 2		WAN: Wi-Fi WAN		WAN: Cellular 1		WAN: Cellular 2		WAN: USB		Lowest Priority	
Highest Priority	Not In Use																
WAN: WAN 1	VPN: Connection 1																
WAN: WAN 2																	
WAN: Wi-Fi WAN																	
WAN: Cellular 1																	
WAN: Cellular 2																	
WAN: USB																	
Lowest Priority																	
Terminate Sessions on Link Recovery	<input type="checkbox"/> Enable																

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.

Algorithm	?	Overflow
Overflow Order	?	<div> <div>Highest Priority</div> <div> <div>WAN: WAN 1</div> <div>WAN: WAN 2</div> <div>WAN: Wi-Fi WAN</div> <div>WAN: Cellular 1</div> <div>WAN: Cellular 2</div> <div>WAN: USB</div> </div> <div>Lowest Priority</div> </div>

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

Algorithm	?	Least Used
Connection		<div> <div><input checked="" type="checkbox"/> WAN 1</div> <div><input checked="" type="checkbox"/> WAN 2</div> <div><input checked="" type="checkbox"/> Wi-Fi WAN</div> <div><input type="checkbox"/> Cellular 1</div> <div><input type="checkbox"/> Cellular 2</div> <div><input type="checkbox"/> USB</div> </div>

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

Algorithm	?	Lowest Latency <small>Note: Use of Lowest Latency will incur additional network usage.</small>
Connection		<div> <div><input checked="" type="checkbox"/> WAN 1</div> <div><input checked="" type="checkbox"/> WAN 2</div> <div><input checked="" type="checkbox"/> Wi-Fi WAN</div> <div><input type="checkbox"/> Cellular 1</div> <div><input type="checkbox"/> Cellular 2</div> <div><input type="checkbox"/> USB</div> </div>

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.

Help

Close

This table allows you to fine tune how the outbound traffic should be distributed to the WAN connections.

Click the *Add Rule* button to add a new rule. Click the *X* button to remove a rule. Drag a rule to promote or demote its precedence. A higher position of a rule signifies a higher precedence. You may change the default outbound policy behavior by clicking the *Default* link.

If you require advanced control of PepVPN traffic, [turn on Expert Mode](#).

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

Rules (Drag and drop rows to change rule order)				
Service	Algorithm	Source	Destination	Protocol / Port
HTTPS Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443
PepVPN Routes				
Default	(Auto)			
Add Rule				

## 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**.

Service	IP Address(es)	Server	Protocol
No Services Defined			
Add Service			

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

Enable	<input checked="" type="radio"/> Yes <input type="radio"/> No
Service Name	Service_1
IP Protocol	TCP <input type="button" value="←"/> :: Protocol Selection Tool :: <input type="button" value="→"/>
Port	Any Port
Inbound IP Address(es) (Require at least one IP address)	<div> <div>Connection / IP Address(es)</div> <div> <input checked="" type="checkbox"/> WAN 1  <input type="checkbox"/> WAN 2  <input type="checkbox"/> Wi-Fi WAN  <input type="checkbox"/> Cellular 1  <input type="checkbox"/> Cellular 2  <input type="checkbox"/> USB </div> <div> <input checked="" type="checkbox"/> 10.88.3.158 (Interface IP) </div> </div>
Server IP Address	120.78.95.7

Port Forwarding Settings	
<b>Enable</b>	This setting specifies whether the inbound service takes effect. When <b>Enable</b> 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.
<b>Service Name</b>	This setting identifies the service to the system administrator. Valid values for this setting consist of only alphanumeric and underscore “_” characters.
<b>IP Protocol</b>	The <b>IP Protocol</b> setting, along with the <b>Port</b> 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 <b>Servers</b> setting. Please see below for details on the <b>Port</b> and <b>Servers</b> settings. Alternatively, the <b>Protocol Selection Tool</b> 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 <b>Protocol Selection Tool</b> 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.

UPnP / NAT-PMP Settings	
UPnP	<input type="checkbox"/> Enable
NAT-PMP	<input type="checkbox"/> Enable
Save	

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'd traffic to and from an internal client IP address. Settings to configure NAT mappings are located at **Advanced>NAT Mappings**.

LAN Clients	Inbound Mappings	Outbound Mappings	
192.168.1.23	(WAN 1):10.88.3.158 (Interface IP)	Use Interface IP only	✖
Add NAT Rule			

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

LAN Client(s)	<input type="text" value="IP Address"/>												
Address	<input type="text"/>												
Inbound Mappings	<div>Connection / Inbound IP Address(es)</div> <div> <input type="checkbox"/> WAN 1  <input type="checkbox"/> WAN 2  <input type="checkbox"/> Wi-Fi WAN  <input type="checkbox"/> Cellular 1  <input type="checkbox"/> Cellular 2  <input type="checkbox"/> USB </div>												
Outbound Mappings	<div>Connection / Outbound IP Address</div> <table border="1"> <tr> <td>WAN 1</td> <td>10.88.3.158 (Interface IP)</td> </tr> <tr> <td>WAN 2</td> <td>Interface IP</td> </tr> <tr> <td>Wi-Fi WAN</td> <td>Interface IP</td> </tr> <tr> <td>Cellular 1</td> <td>Interface IP</td> </tr> <tr> <td>Cellular 2</td> <td>Interface IP</td> </tr> <tr> <td>USB</td> <td>Interface IP</td> </tr> </table>	WAN 1	10.88.3.158 (Interface IP)	WAN 2	Interface IP	Wi-Fi WAN	Interface IP	Cellular 1	Interface IP	Cellular 2	Interface IP	USB	Interface IP
WAN 1	10.88.3.158 (Interface IP)												
WAN 2	Interface IP												
Wi-Fi WAN	Interface IP												
Cellular 1	Interface IP												
Cellular 2	Interface IP												
USB	Interface IP												

NAT Mapping Settings	
LAN	NAT mapping rules can be defined for a single LAN IP Address, an IP Range, or

<b>Client(s)</b>	an <b>IP Network</b> .
<b>Address</b>	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 <b>IP Address</b> is selected.
<b>Range</b>	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 <b>IP Range</b> is selected.
<b>Network</b>	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 <b>IP Network</b> is selected.
<b>Inbound Mappings</b>	<p>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 <b>IP Address</b> is selected in the <b>LAN Client(s)</b> field.</p> <p>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.</p>
<b>Outbound Mappings</b>	<p>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).</p> <p>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 <b>Outbound Policy</b> section. Also note that WAN connections in drop-in mode or IP forwarding mode are not shown here.</p>

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

#### Important Note


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

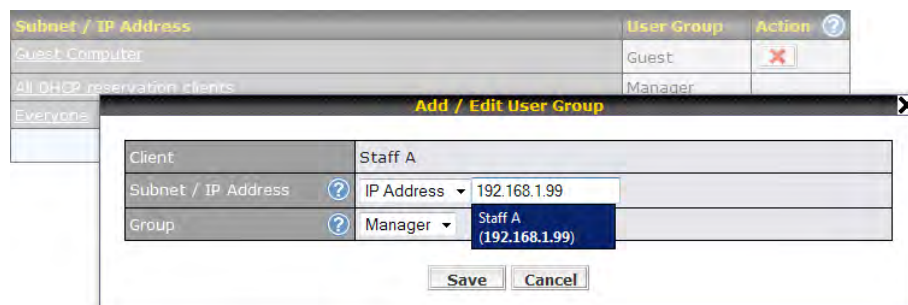
## 18

### 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.



Subnet / IP Address	User Group	Action
Guest Computer	Guest	
All DHCP reservation clients	Manager	
Everyone		

**Add / Edit User Group**

Client: Staff A

Subnet / IP Address: IP Address 192.168.1.99

Group: Manager Staff A (192.168.1.99)

Save Cancel

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

Group Bandwidth Reservation				
Enable		<input checked="" type="checkbox"/>		
	Manager	Staff	Guest	
Bandwidth %	50%	30%	20%	
WAN 1	500.0M/500.0M	300.0M/300.0M	200.0M/200.0M	
WAN 2	500.0M/500.0M	300.0M/300.0M	200.0M/200.0M	

## 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.

Application Prioritization	
<input checked="" type="radio"/> Apply same settings to all users	
<input type="radio"/> Customize	

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.

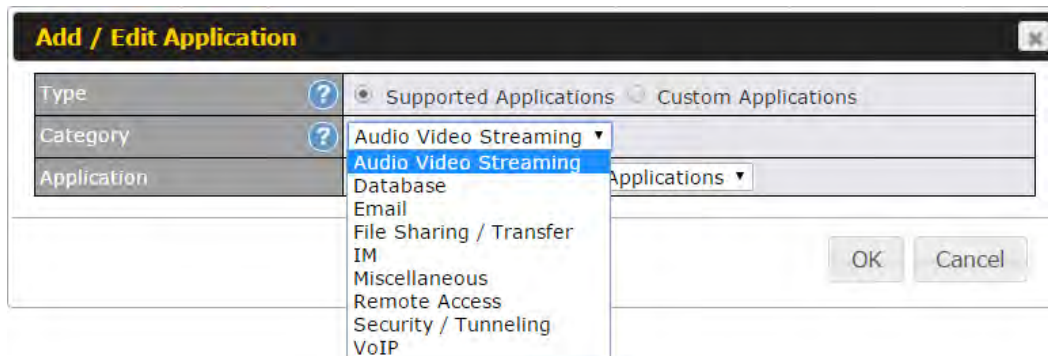
Application	Priority			
	Manager	Staff	Guest	
All Supported Streaming Applications	↑ High	— Normal	↑ High	✖
All Email Protocols	↑ High	↑ High	↑ High	✖
MySQL	↑ High	— Normal	↓ Low	✖
SIP	↑ High	↓ Low	↓ Low	✖
Add				

### 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.

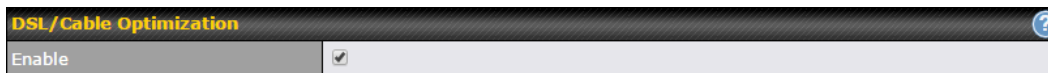
When **Supported Applications** is selected, the Pepwave router will inspect network traffic and

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.



**Outbound Firewall Rules** ( Drag and drop rows by the left to change rule order)

Rule	Protocol	Source	Destination	Action	
Default	Any	Any	Any	✓	
Add Rule					

**Inbound Firewall Rules** ( Drag and drop rows by the left to change rule order)

Rule	Protocol	WAN	Source	Destination	Action	
Default	Any	Any	Any	Any	✓	
Add Rule						

**Internal Network Firewall Rules** ( Drag and drop rows by the left to change rule order)

Rule	Protocol	Source	Destination	Action	
Default	Any	Any	Any	✓	
Add Rule					

**Intrusion Detection and DoS Prevention**

Disabled

**Local Service Firewall Rules** ( Drag and drop rows by the left to change rule order)

Rule	Service	WAN	Source	Action	
Default	Any	Any	Any	✓	
Add Rule					

## 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**.

**Outbound Firewall Rules** ( Drag and drop rows by the left to change rule order)

Rule	Protocol	Source	Destination	Action	
test	Any	Any	Any	✓	✗
Default	Any	Any	Any	✓	
Add Rule					

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

Add a New Outbound Firewall Rule

### New Firewall Rule

Rule Name	
Enable	<input checked="" type="checkbox"/> Always on
Protocol	Any :: Protocol Selection Tool ::
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Event Logging	<input type="checkbox"/> Enable

Save
Cancel

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

Inbound Firewall Rules ( Drag and drop rows by the left to change rule order)

Rule	Protocol	WAN	Source	Destination	Action	
test	Any	Any	Any	Any		
Default	Any	Any	Any	Any		

Add Rule

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

Add a New Inbound Firewall Rule

### New Firewall Rule


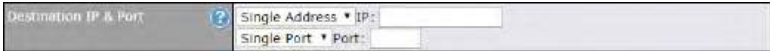
Rule Name	
Enable	<input checked="" type="checkbox"/>
WAN Connection	Any
Protocol	Any :: Protocol Selection Tool ::
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Event Logging	<input type="checkbox"/> Enable

Save
Cancel

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.

## Inbound / Outbound Firewall Settings



<b>Rule Name</b>	This setting specifies a name for the firewall rule.
<b>Enable</b>	<p>This setting specifies whether the firewall rule should take effect. If the box is checked, the firewall rule takes effect. If the traffic matches the specified protocol/IP/port, actions will be taken by the Pepwave router based on the other parameters of the rule. If the box is not checked, the firewall rule does not take effect. The Pepwave router will disregard the other parameters of the rule.</p> <p>Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule.</p>
<b>WAN Connection (Inbound)</b>	Select the WAN connection that this firewall rule should apply to.
<b>Protocol</b>	<p>This setting specifies the protocol to be matched. Via a drop-down menu, the following protocols can be specified:</p> <ul style="list-style-type: none"> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> <li>• IP</li> </ul> <p>Alternatively, the <b>Protocol Selection Tool</b> drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.)</p> <p>After selecting an item from the <b>Protocol Selection Tool</b> drop-down menu, the protocol and port number remains manually modifiable.</p>
<b>Source IP &amp; Port</b>	<p>This specifies the source IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the <b>Source IP &amp; Port</b> setting, as indicated by the following screenshot:</p>  <p>In addition, a single port, or a range of ports, can be specified for the <b>Source IP &amp; Port</b> settings.</p>
<b>Destination IP &amp; Port</b>	<p>This specifies the destination IP address(es) and port number(s) to be matched for the firewall rule. A single address, or a network, can be specified as the <b>Destination IP &amp; Port</b> setting, as indicated by the following screenshot:</p>  <p>In addition, a single port, or a range of ports, can be specified for the <b>Destination IP &amp; Port</b> settings.</p>
<b>Action</b>	<p>This setting specifies the action to be taken by the router upon encountering traffic that matches the both of the following:</p> <ul style="list-style-type: none"> <li>• Source IP &amp; port</li> <li>• Destination IP &amp; port</li> </ul> <p>With the value of <b>Allow</b> for the <b>Action</b> setting, the matching traffic passes through the router (to be routed to the destination). If the value of the <b>Action</b> setting is set</p>

to **Deny**, the matching traffic does not pass through the router (and is discarded).

This setting specifies whether or not to log matched firewall events. The logged messages are shown on the page **Status>Event Log**. A sample message is as follows:

Aug 13 23:47:44 Denied CONN=Ethernet WAN SRC=20.3.2.1  
DST=192.168.1.20 LEN=48 PROTO=TCP SPT=2260 DPT=80

#### Event Logging

- **CONN:** The connection where the log entry refers to
- **SRC:** Source IP address
- **DST:** Destination IP address
- **LEN:** Packet length
- **PROTO:** Protocol
- **SPT:** Source port
- **DPT:** Destination port

Click **Save** to store your changes. To create an additional firewall rule, click **Add Rule** and repeat the above steps.

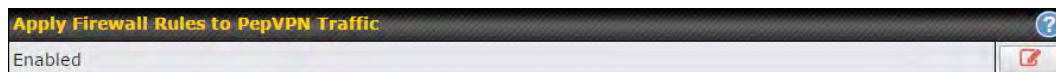
To change a rule's priority, simply drag and drop the rule:


- Hold the left mouse button on the rule.
- Move it to the desired position.
- Drop it by releasing the mouse button.

#### Tip

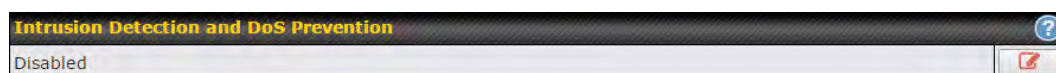
If the default inbound rule is set to **Allow** for NAT-enabled WANs, no inbound Allow firewall rules will be required for inbound port forwarding and inbound NAT mapping rules. However, if the default inbound rule is set as **Deny**, a corresponding Allow firewall rule will be required.

### 19.1.2 Apply Firewall Rules to PepVpn Traffic



When this option is enabled, Outbound Firewall Rules will be applied to PepVPN traffic. To turn on this feature, click , check the **Enable** check box, and press the **Save** button.

### 19.1.3 Intrusion Detection and DoS Prevention



Pepwave routers can detect and prevent intrusions and denial-of-service (DoS) attacks from the Internet. To turn on this feature, click , check the **Enable** check box, and press the

**Save** button.

When this feature is enabled, the Pepwave router will detect and prevent the following kinds of intrusions and denial-of-service attacks.

- Port scan
  - NMAP FIN/URG/PSH
  - Xmas tree
  - Another Xmas tree
  - Null scan
  - SYN/RST
  - SYN/FIN
- SYN flood prevention
- Ping flood attack prevention

## 19.2 Content Blocking

**Application Blocking**

Please Select Application...

**Web Blocking**

Preset Category

☐ High
☐ Moderate
☐ Low
☒ Custom

☐ Abortion
☐ Alcohol
☐ Dating
☐ Entertainment
☐ Gambling
☐ Instant Messaging
☐ Lingerie
☐ Nudity
☐ Phishing
☐ Radio
☐ Search Engines
☐ Sports
☐ Update Sites
☐ Viruses
☐ Webmail

☐ Adware
☐ Anti-Spyware
☐ Drugs
☐ File Hosting
☐ Games
☐ Job Search/Employment
☐ Malware
☐ News/Media
☐ Pornography
☐ Remote Access
☐ Sexuality Education
☐ Spyware
☐ Vacation
☐ Weapons
☐ WebTV

☐ Aggressive
☐ Chatroom
☐ Ecommerce/Shopping
☐ P2P/File sharing
☐ Hacking
☐ Kids Time Wasting
☐ Manga/Anime/Webcomic
☐ Auctions
☐ Proxy/Anonymizer
☐ Ringtones
☐ Social Networking
☐ Tobacco
☐ Violence
☐ Weather

Customized Domains

cbs.com

✖

+

Exempted Domains from Web Blocking

+

**Exempted User Groups**

Manager	<input type="checkbox"/> Exempt
Staff	<input type="checkbox"/> Exempt
Guest	<input type="checkbox"/> Exempt

**Exempted Subnets**

Network	Subnet Mask
<div></div>	<div>255.255.255.0 (/24)</div> <div>+</div>

**URL Logging**

Enable	<input type="checkbox"/>
Log Server Host	<div></div> <div>Port: <div></div></div>

### 19.2.1 Application Blocking

Choose applications to be blocked from LAN/PPTP/PepVPN peer clients' access, except for those on the Exempted User Groups or Exempted Subnets defined below.

### 19.2.2 Web Blocking

Defines website domain names to be blocked from LAN/PPTP/PepVPN peer clients' access

except for those on the Exempted User Groups or Exempted Subnets defined below.

If "foobar.com" is entered, any web site with a host name ending in foobar.com will be blocked, e.g. www.foobar.com, foobar.com, etc. However, "myfoobar.com" will not be blocked.

You may enter the wild card "." at the end of a domain name to block any web site with a host name having the domain name in the middle. If you enter "foobar.", then "www.foobar.com", "www.foobar.co.jp", or "foobar.co.uk" will be blocked. Placing the wild card in any other position is not supported.

The device will inspect and look for blocked domain names on all HTTP and HTTPS traffic.

### 19.2.3 Customized Domains

Enter an appropriate website address, and the Peplink Balance will block and disallow LAN/PPTP/SpeedFusion™ peer clients to access these websites. Exceptions can be added using the instructions in Sections 20.1.3.2 and 20.1.3.3.

You may enter the wild card "." at the end of a domain name to block any web site with a host name having the domain name in the middle. For example, If you enter "foobar.," then "www.foobar.com," "www.foobar.co.jp," or "foobar.co.uk" will be blocked. Placing the wild card in any other position is not supported.

The Peplink Balance will inspect and look for blocked domain names on all HTTP traffic. Secure web (HTTPS) traffic is not supported.

### 19.2.4 Exempted User Groups

Check and select pre-defined user group(s) who can be exempted from the access blocking rules. User groups can be defined at **QoS>User Groups** section. Please refer to **Section 17.1** for details.

### 19.2.5 Exempted Subnets

With the subnet defined in the field, clients on the particular subnet(s) can be exempted from the access blocking rules.



### 19.2.6 URL Logging


Click **enable**, and then enter the ip address and port (if applicable) where your remote syslog server is located.


## 20 OSPF & RIPv2


The Pepwave supports OSPF and RIPv2 dynamic routing protocols. Click the **Advanced** tab from the top bar, and then click the **Routing Protocols >OSPF &**

RIPv2 item on the sidebar to reach the following menu:

OSPF		
Router ID	LAN IP Address	
Area	Interfaces	
0.0.0.0	PepVPN	
<b>Add</b>		

PepVPN OSPF Area	
0.0.0.0	

RIPv2	
No RIPv2 Defined.	
	

OSPF	
<b>Router ID</b>	This field determines the ID of the router. By default, this is specified as the LAN IP address. If you want to specify your own ID, enter it in the <b>Custom</b> field.
<b>Area</b>	This is an overview of the OSPFv2 areas you have defined. Click on the area name to configure it. To set a new area, click <b>Add</b> . To delete an existing area, click  .

OSPF settings

Area ID

0.0.0.0

Link Type

☒ Broadcast
 ☐ Point-to-Point

Authentication

None ▾


Interfaces

☐ Untagged LAN  
☐ V167 (192.168.167.1/24)  
☐ WAN 1  
☐ WAN 2  
☐ WAN 3  
☐ WAN 4  
☐ WAN 5  
☒ PepVPN

Save

Cancel

OSPF Settings	
<b>Area ID</b>	Determine the name of your <b>Area ID</b> to apply to this group. Machines linked to this group will send and receive related OSPF packets, while unlinked machines will ignore it.
<b>Link Type</b>	Choose the network type that this area will use.
<b>Authentication</b>	Choose an authentication method, if one is used, from this drop-down menu. Available options are <b>MD5</b> and <b>Text</b> . Enter the authentication key next to the drop-down menu.
<b>Interfaces</b>	Determine which interfaces this area will use to listen to and deliver OSPF packets

To access RIPv2 settings, click .



**RIPv2 settings** ✕

Authentication	None ▾
Interfaces	<input type="checkbox"/> Untagged LAN <input type="checkbox"/> V167 (192.168.167.1/24) <input type="checkbox"/> WAN 1 <input type="checkbox"/> WAN 2 <input type="checkbox"/> WAN 3 <input type="checkbox"/> WAN 4 <input type="checkbox"/> WAN 5

RIPv2 Settings	
<b>Authentication</b>	Choose an authentication method, if one is used, from this drop-down menu. Available options are <b>MD5</b> and <b>Text</b> . Enter the authentication key next to the drop-down menu.
<b>Interfaces</b>	Determine which interfaces this group will use to listen to and deliver RIPv2 packets.


**OSPF & RIPv2 Route Advertisement**

PepVPN Route Isolation	?	<input type="checkbox"/> Enable						
Network Advertising	?	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> <span style="flex-grow: 1;">---</span> <span style="font-size: 0.8em;">▾</span> </div> <div style="font-size: 0.8em; margin-top: 2px;">All LAN/VLAN networks will be advertised when no network advertising is chosen.</div> <div style="text-align: right; margin-top: 2px;">+ <input type="button" value="Add"/></div>						
Static Route Advertising	?	<input checked="" type="checkbox"/> Enable <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 5px;"> <thead> <tr> <th style="width: 50%;">Excluded Networks</th> <th style="width: 30%;">Subnet Mask</th> <th style="width: 20%;"></th> </tr> </thead> <tbody> <tr> <td style="height: 20px;"></td> <td>255.255.255.0 (/24) ▾</td> <td style="text-align: right;">+ <input type="button" value="Add"/></td> </tr> </tbody> </table>	Excluded Networks	Subnet Mask			255.255.255.0 (/24) ▾	+ <input type="button" value="Add"/>
Excluded Networks	Subnet Mask							
	255.255.255.0 (/24) ▾	+ <input type="button" value="Add"/>						

OSPF & RIPv2 Route Advertisement	
<b>PepVPN Route Isolation</b>	Isolate PepVPN peers from each other. Received PepVPN routes will not be forwarded to other PepVPN peers to reduce bandwidth consumption..
<b>Network Advertising</b>	Networks to be advertised over OSPF & RIPv2. If no network is selected, all LAN / VLAN networks will be advertised by default.
<b>Static Route Advertising</b>	Enable this option to advertise LAN static routes over OSPF & RIPv2. Static routes that match the Excluded Networks table will not be advertised.


## 21 BGP

Click the **Advanced** tab from the top bar, and then click the **Routing Protocols>BGP** item on the sidebar to configure BGP.

BGP	AS	Neighbors	
<a href="#">Uplink</a>	64520	172.16.51.1	
<a href="#">Add</a>			

Click "x" to delete a BGP profile

Click "Add" to add a new BGP profile

BGP Profile						
Profile Name	<input type="text"/>					
Enable	<input checked="" type="checkbox"/>					
Interface	WAN 1 ▼					
Router ID	<input checked="" type="radio"/> LAN IP Address <input type="radio"/> Custom: <input type="text"/>					
Autonomous System	<input type="text"/>					
Neighbor	IP Address	Autonomous System	Multihop / TTL	Password	AS-Path Prepending	
	<input type="text"/>	<input type="text"/>	disable	<input type="text"/>	<input type="text"/>	<a href="#">+</a>
Hold Time 	240 <input type="text"/>					

BGP	
<b>Name</b>	This field is for specifying a name to represent this profile.
<b>Enable</b>	When this box is checked, this BGP profile will be enabled. Otherwise, it will be disabled.
<b>Interface</b>	The interface where BGP neighbor is located
<b>Autonomous System</b>	The Autonomous System Number (ASN) of this profile
<b>Neighbor</b>	BGP Neighbor's details
<b>IP address</b>	Neighbor's IP address
<b>Autonomous System</b>	Neighbor's ASN
<b>Multihop/TTL</b>	Time-to-live (TTL) of BGP packet. Leave it blank if BGP neighbor is directly connected, otherwise you must specify a TTL value. Accurately, this option should be used if the configured neighbor IP

	address does not match the selected Interface's network subnets. TTL value must be between 2 to 255.
<b>Password</b>	Optional password for MD5 authentication of BGP sessions.
<b>AS-Path Prepending:</b>	AS path to be prepended to the routes received from this neighbor. The value must be a comma separated ASN. For example "64530,64531" will prepend "64530, 64531" to received routes.
<b>Hold Time</b>	Time in seconds to wait for a keepalive message from the neighbor before considering the BGP connection is staled. This value must be either 0 (infinite hold time) or between 3 and 65535 inclusively.

Route Advertisement			
Network Advertising	?	---	+
Static Route Advertising	?	<input checked="" type="checkbox"/> Enable	
		Excluded Networks	Subnet Mask
			255.255.255.0 (/24) +
Advertise OSPF Route	?	<input type="checkbox"/>	

<b>Network Advertising</b>	Networks to be advertised to BGP neighbor.
<b>Static Route Advertising</b>	Enable this option to advertise LAN static routes. Static routes that match the Excluded Networks table will not be advertised.
<b>Advertise OSPF Route</b>	When this box is checked, all learnt OSPF routes will be advertised.

Route Import			
Filter Mode	?	Accept ▼	
Restricted Networks		Network	Subnet Mask
			255.255.255.0 (/24) ▼
		Exact Match	<input type="checkbox"/> +

<b>Filter Mode</b>	<p>This option selects the route import filter mode.</p> <p><b>None:</b> all BGP routes will be accepted.</p> <p><b>Accept:</b> Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected.</p> <p><b>Reject:</b> Routes in "Restricted Networks" will be rejected, routes not in the list will be accepted.</p>
<b>Restricted</b>	This specifies the network in the "route import" entry

### Networks

**Exact Match:** When this box is checked, only routes with the same Networks and Subnet Mask will be filtered. Otherwise, routes within the Networks and Subnet will be filtered.

### Route Export

Export to other BGP Profile


☐

Export to OSPF


☐

### Export to other BGP Profile

When this box is checked, routes learnt from this BGP profile will export to other BGP profiles.

### Export to OSPF


When this box is checked, routes learnt from this BGP profile will export to the OSPF routing protocol.

## 22 Remote User Access

A remote-access VPN connection allows an individual user to connect to a private business network from a remote location using a laptop or desktop computer connected to the Internet. Networks routed by a Peplink router can be remotely accessed via OpenVPN, L2TP with IPsec or PPTP. To configure this feature, navigate to **Network > Remote User Access** and choose the required VPN type.

## 22.1 L2TP with IPsec

Remote User Access Settings	
Enable	<input checked="" type="checkbox"/>
VPN Type	<input checked="" type="radio"/> L2TP with IPsec <input type="radio"/> PPTP <input type="radio"/> OpenVPN
Preshared Key	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters

L2TP with IPsec Remote User Access Settings	
<b>Pre-shared Key</b>	Enter your pre shared key in the text field. Please note that remote devices will need this preshared key to access the Balance.
<b>Listen On</b>	This setting is for specifying the WAN IP addresses that allow remote user access.
<b>Disable Weak Ciphers</b>	Click the  button to show and enable this option. When checked, weak ciphers such as 3DES will be disabled.

Continue to configure the authentication method.

## 22.2 OpenVPN

Remote User Access Settings	
Enable	<input checked="" type="checkbox"/>
VPN Type	<input type="radio"/> L2TP with IPsec <input type="radio"/> PPTP <input checked="" type="radio"/> OpenVPN You can obtain the OpenVPN client profile from the <a href="#">status page</a> .

Select OpenVPN and continue to configure the authentication method.

The OpenVPN Client profile can be downloaded from the **Status > device** page after the configuration has been saved.

OpenVPN Client Profile	<input checked="" type="radio"/> Route all traffic <input type="radio"/> Split tunnel
------------------------	---

You have a choice between 2 different OpenVPN Client profiles.

- "route all traffic" profile**  
 Using this profile, VPN clients will send all the traffic through the OpenVPN tunnel
- "split tunnel" profile**  
 Using this profile, VPN clients will ONLY send those traffic designated to the untagged LAN and VLAN segment through the OpenVPN tunnel.

## 22.3 PPTP

Remote User Access Settings	
Enable	<input checked="" type="checkbox"/>
VPN Type	<input type="radio"/> L2TP with IPsec <input checked="" type="radio"/> PPTP <input type="radio"/> OpenVPN

No additional configuration required.

The Point-to-Point Tunneling Protocol (PPTP) is an obsolete method for implementing virtual private networks. PPTP has many well known security issues

Continue to configure authentication method.

## 22.4 Authentication Methods

Connect to Network	<input type="button" value="?"/> Untagged LAN ▼		
Authentication	Local User Accounts ▼		
User Accounts	<input type="button" value="?"/> Username <input type="button" value="1"/>	Password <input type="button" value="1"/>	<input type="button" value="+"/>

Authentication Method	
<b>Connect to Network</b>	Select the VLAN network for remote users to enable remote user access on.
<b>Authentication</b>	Determine the method of authenticating remote users

### User accounts:


This setting allows you to define the Remote User Accounts. Click Add to input username and password to create an account. After adding the user accounts, you can click on a username to edit the account password.

### Note:

The username must contain lowercase letters, numerics, underscore(\_), dash(-), at sign(@), and period(.) only.

The password must be between 8 and 12 characters long.

### LDAP Server:

Connect to Network	 Untagged LAN ▼
Authentication	LDAP Server ▼
LDAP Server	<input type="text"/> Port 389 <input type="button" value="Default"/>
	<input type="checkbox"/> Use DN/Password to bind to LDAP Server
Base DN	<input type="text"/>
Base Filter	<input type="text"/>


Enter the matching LDAP server details to allow for LDAP server authentication.

### Radius Server:

Authentication	RADIUS Server ▼
Auth Protocol	MS-CHAP v2 ▼
Auth Server	<input type="text"/> Port 1812 <input type="button" value="Default"/>
Auth Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters
Accounting Server	<input type="text"/> Port 1813 <input type="button" value="Default"/>
Accounting Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters

Enter the matching Radius server details to allow for Radius server authentication.

### Active Directory:

Connect to Network	 Untagged LAN ▼
Authentication	Active Directory ▼
Server Hostname	<input type="text"/>
Domain	<input type="text"/>
Admin Username	<input type="text"/>
Admin Password	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters

Enter the matching Active Directory details to allow for Active Directory server authentication.

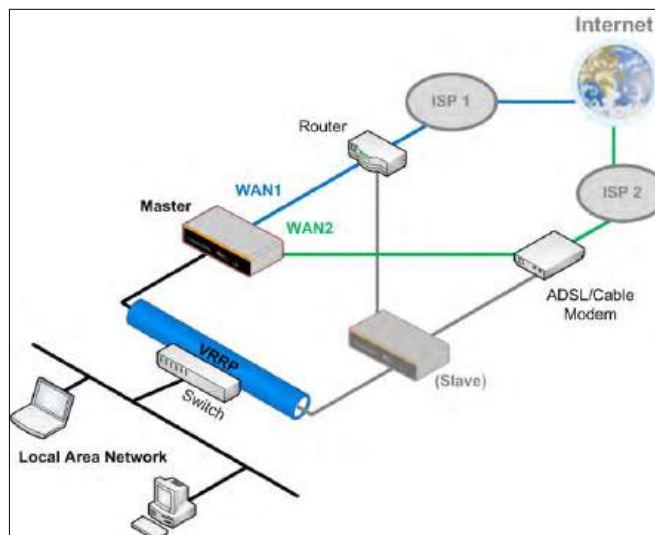


## 23 Miscellaneous Settings

The miscellaneous settings include configuration for High Availability, Certificate Manager, service forwarding, service passthrough, GPS forwarding, GPIO, Groupe Networks and SIM Toolkit (depending the feature is supported on the model of Peplin router that is being used).

### 23.1 High Availability

Many Pepwave routers support high availability (HA) configurations via an open standard virtual router redundancy protocol (VRRP, RFC 3768). In an HA configuration, two Pepwave routers provide redundancy and failover in a master-slave arrangement. In the event that the master unit is down, the slave unit becomes active. High availability will be disabled automatically where there is a drop-in connection configured on a LAN bypass port.



In the diagram, the WAN ports of each Pepwave router connect to the router and to the modem. Both Pepwave routers connect to the same LAN switch via a LAN port.

An elaboration on the technical details of the implementation of the virtual router redundancy protocol (VRRP, RFC 3768) by Pepwave routers follows:

- In an HA configuration, the two Pepwave routers communicate with each other using VRRP over the LAN.
- The two Pepwave routers broadcast heartbeat signals to the LAN at a frequency of one heartbeat signal per second.
- In the event that no heartbeat signal from the master Pepwave router is received in 3 seconds (or longer) since the last heartbeat signal, the slave Pepwave router becomes active.
- The slave Pepwave router initiates the WAN connections and binds to a previously configured LAN IP address.
- At a subsequent point when the master Pepwave router recovers, it will once again become active.

You can configure high availability at **Advanced>Misc. Settings>High Availability**.

Interface for Master Router

High Availability	
Enable	<input checked="" type="checkbox"/>
Group Number	<input type="text"/>
Preferred Role	<input checked="" type="radio"/> Master <input type="radio"/> Slave
Resume Master Role Upon Recovery	<input checked="" type="checkbox"/>
Virtual IP Address	<input type="text"/>
LAN Administration IP Address	192.168.86.1
Subnet Mask	255.255.255.0

Interface for Slave Router

High Availability	
Enable	<input checked="" type="checkbox"/>
Group Number	<input type="text"/>
Preferred Role	<input type="radio"/> Master <input checked="" type="radio"/> Slave
Configuration Sync	<input type="checkbox"/> Master Serial Number: <input type="text"/>
Establish Connections in Slave Role	<input type="checkbox"/>
Virtual IP Address	<input type="text"/>
LAN Administration IP Address	192.168.86.1
Subnet Mask	255.255.255.0

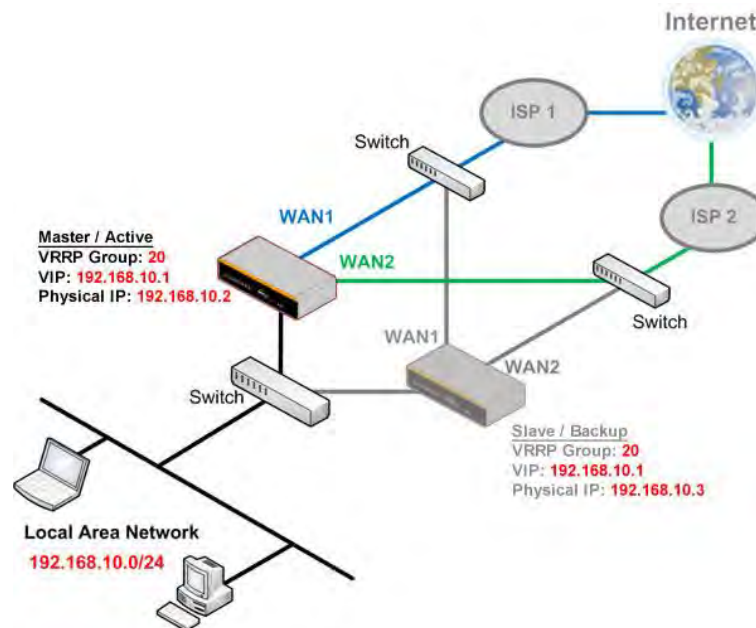
High Availability	
<b>Enable</b>	Checking this box specifies that the Pepwave router is part of a high availability configuration.
<b>Group Number</b>	This number identifies a pair of Pepwave routers operating in a high availability configuration. The two Pepwave routers in the pair must have the same <b>Group Number</b> value.
<b>Preferred Role</b>	This setting specifies whether the Pepwave router operates in master or slave mode. Click the corresponding radio button to set the role of the unit. One of the units in the pair must be configured as the master, and the other unit must be configured as the slave.
<b>Resume Master Role Upon Recovery</b>	This option is displayed when <b>Master</b> mode is selected in <b>Preferred Role</b> . If this option is enabled, once the device has recovered from an outage, it will take over and resume its <b>Master</b> role from the slave unit.
<b>Configuration Sync.</b>	This option is displayed when <b>Slave</b> mode is selected in <b>Preferred Role</b> . If this option is enabled and the <b>Master Serial Number</b> entered matches with the actual master unit's, the master unit will automatically transfer the configuration to this unit. Please make sure the <b>LAN IP Address</b> and the <b>Subnet Mask</b> fields are set correctly in the LAN settings page. You can refer to the <b>Event Log</b> for the configuration synchronization status.
<b>Master Serial Number</b>	If <b>Configuration Sync.</b> is checked, the serial number of the master unit is required here for the feature to work properly.
<b>Virtual IP</b>	The HA pair must share the same <b>Virtual IP</b> . The <b>Virtual IP</b> and the <b>LAN Administration IP</b> must be under the same network.
<b>LAN Administration</b>	This setting specifies a LAN IP address to be used for accessing administration functionality. This address should be unique within the LAN.

## IP

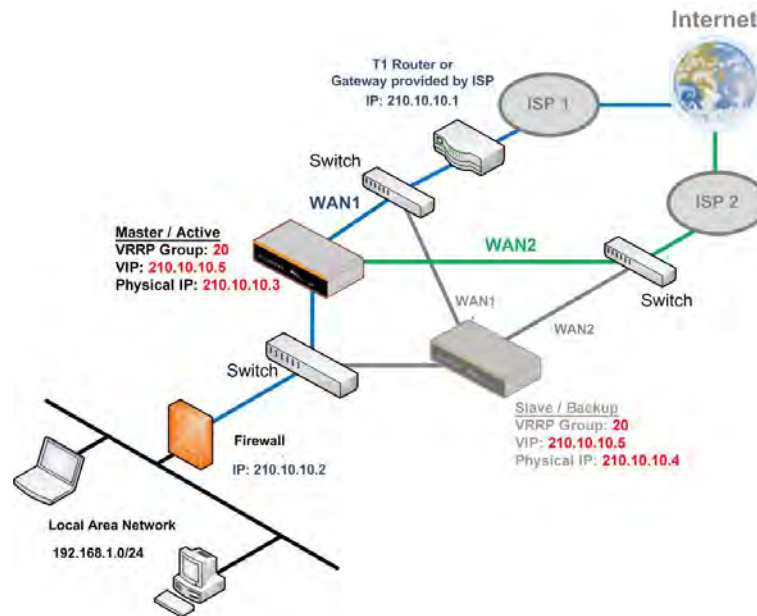
**Subnet Mask** This setting specifies the subnet mask of the LAN.

### Important Note

For Pepwave routers in NAT mode, the virtual IP (VIP) should be set as the default gateway for all hosts on the LAN segment. For example, a firewall sitting behind the Pepwave router should set its default gateway as the virtual IP instead of the IP of the master router.



In drop-in mode, no other configuration needs to be set.



Please note that the drop-in WAN cannot be configured as a LAN bypass port while it is configured for high availability.

## 23.2 Certificate Manager

Certificate		
SpeedFusion/IPsec VPN	No Certificate	
Web Admin SSL	Default Certificate is in use	
Captive Portal SSL	Default Certificate is in use	
OpenVPN CA	Default Certificate is in use	
Wi-Fi WAN Client Certificate		
No Certificates defined		
<a href="#">Add Certificate</a>		
Wi-Fi WAN CA Certificate		
No Certificates defined		
<a href="#">Add Certificate</a>		

This section allows for certificates to be assigned to the local VPN, Web Admin SSL, Captive Portal SSL, OpenVPN CA, Wi-Fi WAN Client certificate and Wi-Fi WAN CA Certificate.

The following knowledge base article describes how to create self-signed certificates and import it to a Peplink Product.

<https://forum.peplink.com/t/how-to-create-a-self-signed-certificate-and-import-it-to-a-peplink-product/>

## 23.3 Service Forwarding

Service forwarding settings are located at **Advanced>Misc. Settings>Service Forwarding**.

The screenshot shows the 'Service Forwarding' configuration page. It contains four distinct sections, each with a title bar and a checkbox:

- SMTP Forwarding Setup:** Includes a checkbox for 'SMTP Forwarding' with an 'Enable' label.
- Web Proxy Forwarding Setup:** Includes a checkbox for 'Web Proxy Forwarding' with an 'Enable' label.
- DNS Forwarding Setup:** Includes a checkbox for 'Forward Outgoing DNS Requests to Local DNS Proxy' with an 'Enable' label.
- Custom Service Forwarding Setup:** Includes a checkbox for 'Custom Service Forwarding' with an 'Enable' label.

Service Forwarding	
<b>SMTP Forwarding</b>	When this option is enabled, all outgoing SMTP connections destined for any host at TCP port 25 will be intercepted. These connections will be redirected to a specified SMTP server and port number. SMTP server settings for each WAN can be specified after selecting <b>Enable</b> .
<b>Web Proxy Forwarding</b>	When this option is enabled, all outgoing connections destined for the proxy server specified in <b>Web Proxy Interception Settings</b> will be intercepted. These connections will be redirected to a specified web proxy server and port number. Web proxy interception settings and proxy server settings for each WAN can be specified after selecting <b>Enable</b> .
<b>DNS Forwarding</b>	When this option is enabled, all outgoing DNS lookups will be intercepted and redirected to the built-in DNS name server. If any LAN device is using the DNS name servers of a WAN connection, you may want to enable this option to enhance the DNS availability without modifying the DNS server setting of the clients. The built-in DNS name server will distribute DNS lookups to corresponding DNS servers of all available WAN connections. In this case, DNS service will not be interrupted, even if any WAN connection is down.
<b>Custom Service Forwarding</b>	When custom service forwarding is enabled, outgoing traffic with the specified TCP port will be forwarded to a local or remote server by defining its IP address and port number.

### 23.3.1 SMTP Forwarding

Some ISPs require their users to send e-mails via the ISP's SMTP server. All outgoing SMTP connections are blocked except those connecting to the ISP's. Pepwave routers support intercepting and redirecting all outgoing SMTP connections (destined for TCP port 25) via a

WAN connection to the WAN's corresponding SMTP server.



**SMTP Forwarding Setup**

SMTP Forwarding ☒ Enable

Connection	Enable Forwarding?	SMTP Server	SMTP Port
WAN 1	<input type="checkbox"/>		
WAN 2	<input type="checkbox"/>		
Wi-Fi WAN	<input type="checkbox"/>		
Cellular 1	<input type="checkbox"/>		
Cellular 2	<input type="checkbox"/>		
USB	<input type="checkbox"/>		

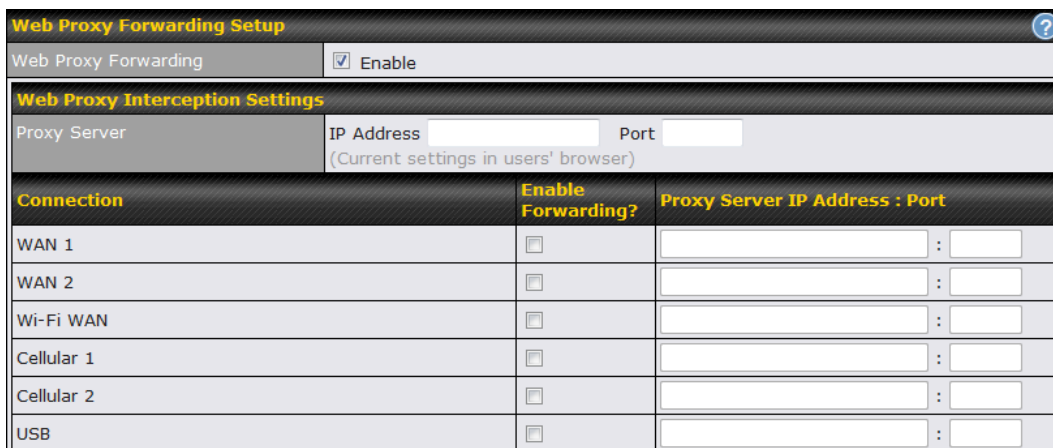
To enable the feature, select **Enable** under **SMTP Forwarding Setup**. Check **Enable Forwarding** for the WAN connection(s) that needs forwarding. Under **SMTP Server**, enter the ISP's e-mail server host name or IP address. Under **SMTP Port**, enter the TCP port number for each WAN.

The Pepwave router will intercept SMTP connections. Choose a WAN port according to the outbound policy, and then forward the connection to the SMTP server if the chosen WAN has enabled forwarding. If the forwarding is disabled for a WAN connection, SMTP connections for the WAN will be simply be forwarded to the connection's original destination.

#### Note

If you want to route all SMTP connections only to particular WAN connection(s), you should create a custom rule in outbound policy (see **Section 14.2**).

### 23.3.2 Web Proxy Forwarding



**Web Proxy Forwarding Setup**

Web Proxy Forwarding ☒ Enable

**Web Proxy Interception Settings**

Proxy Server IP Address  Port   
(Current settings in users' browser)

Connection	Enable Forwarding?	Proxy Server IP Address : Port
WAN 1	<input type="checkbox"/>	<input type="text"/> : <input type="text"/>
WAN 2	<input type="checkbox"/>	<input type="text"/> : <input type="text"/>
Wi-Fi WAN	<input type="checkbox"/>	<input type="text"/> : <input type="text"/>
Cellular 1	<input type="checkbox"/>	<input type="text"/> : <input type="text"/>
Cellular 2	<input type="checkbox"/>	<input type="text"/> : <input type="text"/>
USB	<input type="checkbox"/>	<input type="text"/> : <input type="text"/>

When this feature is enabled, the Pepwave router will intercept all outgoing connections destined for the proxy server specified in **Web Proxy Interception Settings**, choose a WAN connection with reference to the outbound policy, and then forward them to the specified web proxy server and port number. Redirected server settings for each WAN can be set here. If forwarding is disabled for a WAN, web proxy connections for the WAN will be simply forwarded



to the connection's original destination.

### 23.3.3 DNS Forwarding

DNS Forwarding Setup	
Forward Outgoing DNS Requests to Local DNS Proxy	<input type="checkbox"/> Enable

When DNS forwarding is enabled, all clients' outgoing DNS requests will also be intercepted and forwarded to the built-in DNS proxy server.

### 23.3.4 Custom Service Forwarding

Custom Service Forwarding Setup			
Custom Service Forwarding	<input checked="" type="checkbox"/> Enable		
Settings	TCP Port	Server IP Address	Server Port
	<input type="text"/>	<input type="text"/>	<input type="text"/> +

After clicking the **enable** checkbox, enter your TCP port for traffic heading to the router, and then specify the IP Address and Port of the server you wish to forward to the service to.

## 23.4 Service Passthrough

Service passthrough settings can be found at **Advanced>Misc. Settings>Service Passthrough**.

Service Passthrough Support	
SIP	<input checked="" type="radio"/> Standard Mode <input type="radio"/> Compatibility Mode <input checked="" type="checkbox"/> Define custom signal ports 1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/>
H.323	<input checked="" type="checkbox"/> Enable
FTP	<input checked="" type="checkbox"/> Enable <input type="checkbox"/> Define custom control ports
TFTP	<input checked="" type="checkbox"/> Enable
IPsec NAT-T	<input checked="" type="checkbox"/> Enable <input checked="" type="checkbox"/> Define custom ports 1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> <input checked="" type="checkbox"/> Route IPsec Site-to-Site VPN via <input type="text" value="WAN 1"/>

Some Internet services need to be specially handled in a multi-WAN environment. Pepwave routers can handle these services such that Internet applications do not notice being behind a multi-WAN router. Settings for service passthrough support are available here.

### Service Passthrough Support



<b>SIP</b>	Session initiation protocol, aka SIP, is a voice-over-IP protocol. The Pepwave router can act as a SIP application layer gateway (ALG) which binds connections for the same SIP session to the same WAN connection and translate IP address in the SIP packets correctly in NAT mode. Such passthrough support is always enabled, and there are two modes for selection: <b>Standard Mode</b> and <b>Compatibility Mode</b> . If your SIP server's signal port number is non-standard, you can check the box <b>Define custom signal ports</b> and input the port numbers to the text boxes.
<b>H.323</b>	With this option enabled, protocols that provide audio-visual communication sessions will be defined on any packet network and pass through the Pepwave router.
<b>FTP</b>	FTP sessions consist of two TCP connections; one for control and one for data. In a multi-WAN situation, they must be routed to the same WAN connection. Otherwise, problems will arise in transferring files. By default, the Pepwave router monitors TCP control connections on port 21 for any FTP connections and binds TCP connections of the same FTP session to the same WAN. If you have an FTP server listening on a port number other than 21, you can check <b>Define custom control ports</b> and enter the port numbers in the text boxes.
<b>TFTP</b>	The Pepwave router monitors outgoing TFTP connections and routes any incoming TFTP data packets back to the client. Select <b>Enable</b> if you want to enable TFTP passthrough support.
<b>IPsec NAT-T</b>	This field is for enabling the support of IPsec NAT-T passthrough. UDP ports 500, 4500, and 10000 are monitored by default. You may add more custom data ports that your IPsec system uses by checking <b>Define custom ports</b> . If the VPN contains IPsec site-to-site VPN traffic, check <b>Route IPsec Site-to-Site VPN</b> and choose the WAN connection to route the traffic to.

## 23.5 UART

Selected Pepwave MAX routers feature a RS-232 serial interface on the built-in terminal block. The RS-232 serial interface can be used to connect to a serial device and make it accessible over an TCP/IP network.

The serial interface can be enabled and parameters can be set on the web admin page under **Advanced > UART**. Make sure they match the serial device you are connecting to.

Serial to Network	
Enable	<input checked="" type="checkbox"/>
Allowed Source IP Subnets	<input checked="" type="radio"/> Any <input type="radio"/> Allows access from the following IP subnets only
Web Console	<input type="checkbox"/>

Serial Parameters	
Baud Rate	9600 ▼
Data Bits	8 ▼
Stop Bits	1 ▼
Parity	None ▼
Flow Control	None ▼
Interface	RS232 ▼

Operating Settings	
Operation Mode	TCP Server Mode ▼
Local TCP Port	4001
Max Connection	1
TCP Alive Check Time	7 min(s)
Inactivity Time	0 ms

Data Packing	
Packing Length	0 byte(s)
Delimiter	<input type="checkbox"/>
Delimiter process	Do Nothing ▼
Force Transmit	0 ms

There are 4 pins i.e. TX, RX, RTS, CTS on the terminal block for serial connection and they correspond to the pins in a DB-9 connector as follows:

**DB-9 Pepwave MAX Terminal Block**

Pin 1	–
Pin 2	Rx (rated +-25V)
Pin 3	Tx (rated +-12V)
Pin 4	–
Pin 5	–
Pin 6	–
Pin 7	RTS
Pin 8	CTS
Pin 9	–

The RS232 serial interface is not an isolated RS232. External galvanic isolation may be added if required.


Be sure to check whether your serial cable is a null modem cable, commonly known as crossover cable, or a straight through cable. If in doubt, swap Rx and Tx, and RTS and CTS, at the other end and give it another go.

Once connected, your serial device should be accessible on your Pepwave MAX router LAN IP address at the specified TCP port.

## 23.6 GPS Forwarding

Using the GPS forwarding feature, some Pepwave routers can automatically send GPS reports to a specified server. To set up GPS forwarding, navigate to **Advanced>GPS Forwarding**.

GPS Forwarding				
Enable	<input checked="" type="checkbox"/>			
Server	Server IP Address / Host Name	Port	Protocol	Report Interval (s)
			UDP	1
GPS Report Format	<input checked="" type="radio"/> NMEA <input type="radio"/> TAIP			
NMEA Sentence Type	<input checked="" type="checkbox"/> GPRMC <input type="checkbox"/> GPGGA <input type="checkbox"/> GPVTG <input type="checkbox"/> GPGSA <input type="checkbox"/> GPGSV			
Vehicle ID	<input type="checkbox"/>			

GPS Forwarding	
<b>Enable</b>	Check this box to turn on GPS forwarding.
<b>Server</b>	Enter the name/IP address of the server that will receive GPS data. Also specify a port number, protocol ( <b>UDP</b> or <b>TCP</b> ), and a report interval of between 1 and 10 seconds. Click  to save these settings.
<b>GPS Report Format</b>	Choose from NMEA or TAIP format for sending GPS reports.
<b>NMEA Sentence Type</b>	If you've chosen to send GPS reports in NMEA format, select one or more sentence types for sending the data ( <b>GPRMC</b> , <b>GPGGA</b> , <b>GPVTG</b> , <b>GPGSA</b> , and <b>GPGSV</b> ).
<b>Vehicle ID</b>	The vehicle ID will be appended in the last field of the NMEA sentence. Note that the NMEA sentence will become customized and non-standard.
<b>TAIP Sentence Type/TAIP ID (optional)</b>	If you've chosen to send GPS reports in TAIP format, select one or more sentence types for sending the data ( <b>PV—Position / Velocity Solution</b> and <b>CP—Compact Velocity Solution</b> ). You can also optionally include an ID number in the <b>TAIP ID</b> field.


## 23.7 Ignition Sensing

Ignition Sensing detects the ignition signal status of a vehicle it is installed in.

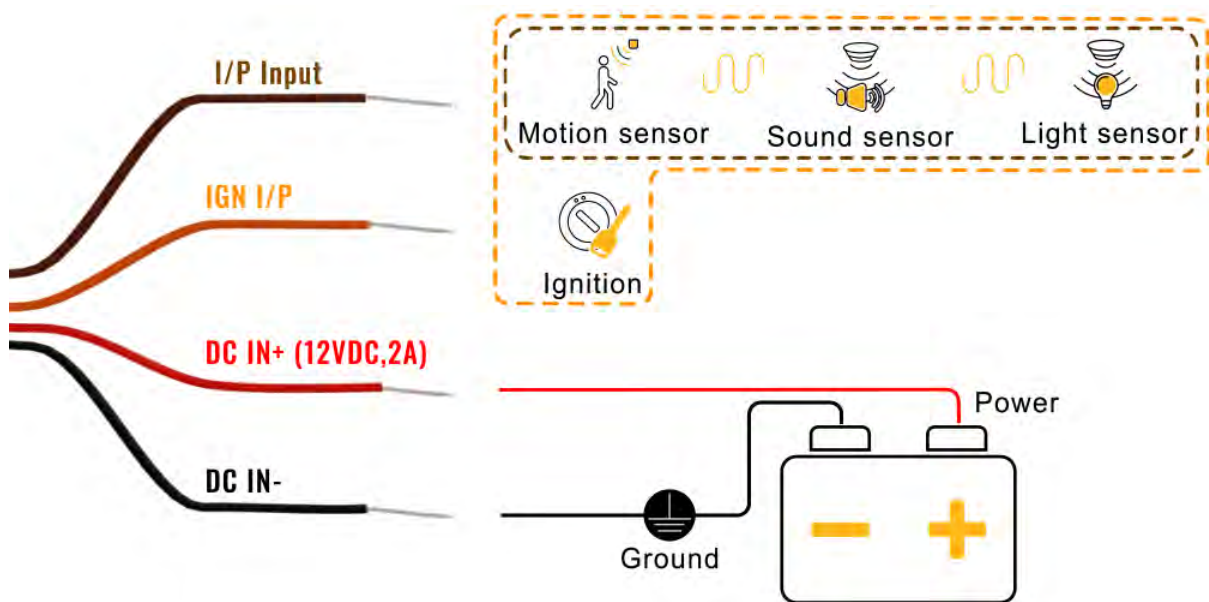
This feature allows the cellular router to start up or shut down when the engine of that vehicle is started or turned off.

The time delay setting between ignition off and power down of the router is a configurable setting, which allows the router to stay on for a period of time after the engine of a vehicle is turned off.

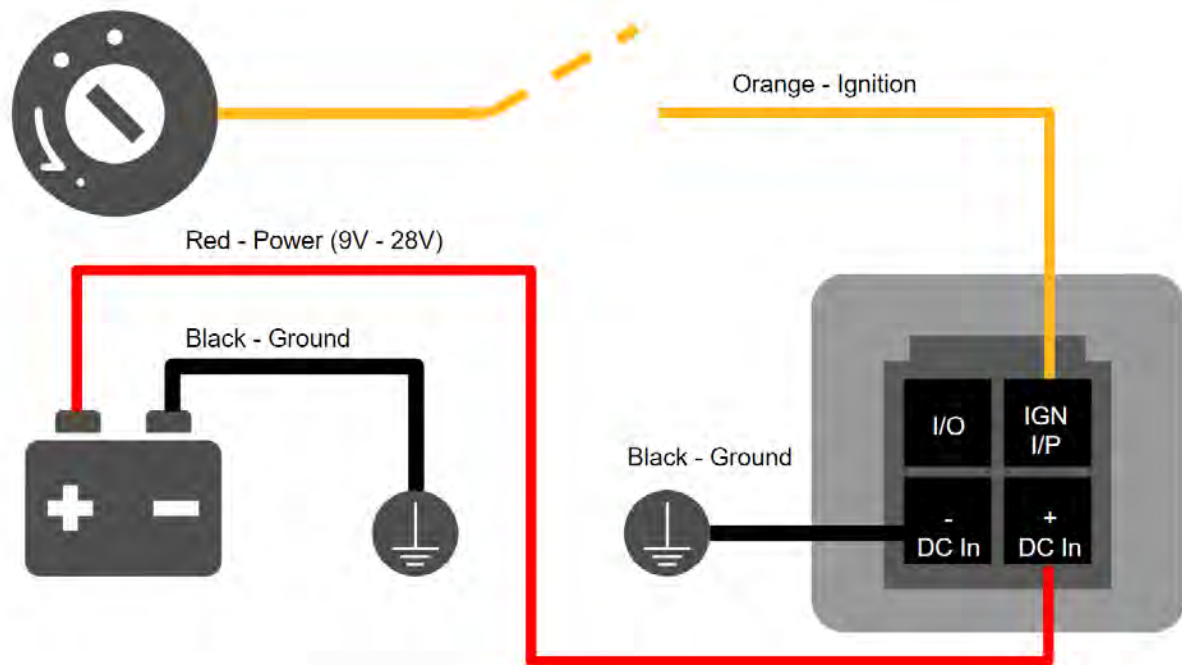
## Ignition Sensing installation

Function		Colour Wire
	I/O optional*	Brown
	IGN I/P connected to positive feed on the ignition .	Orange
	DC IN - connected to permanent negative feed (ground)	Black
	DC IN + connected to permanent positive feed (power 12VDC, 2A)).	Red

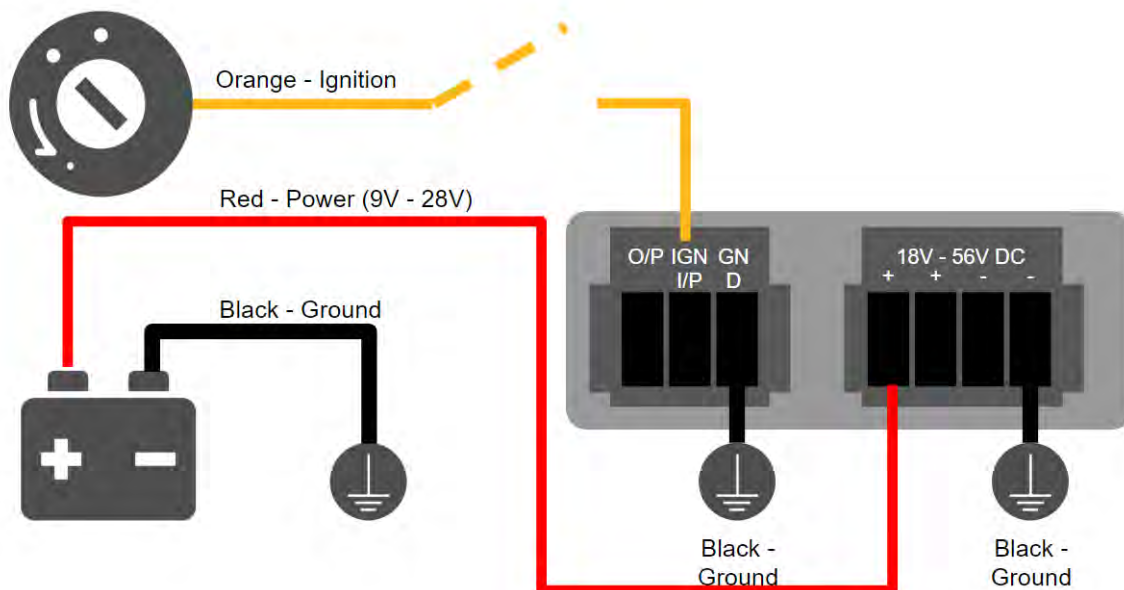
\* Currently not functional; will be used for additional features in future firmware



### Connectivity diagram for devices with 4-pin connector



### Connectivity diagram for devices with terminal block connection



## GPIO Menu

The Ignition Sensing options are available in **Advanced > GPIO**

The configurable option for Ignition Input is **Delay**; the time in seconds the router stays powered on after the ignition is turned off.

IGN I/P	
Enable	<input checked="" type="checkbox"/>
Type	Digital Input ▼
Mode	Ignition Sensing ▼
Delay	<input type="text"/> seconds

Still under development:

O/P (connected to I/O pin on 4 pin connector) can be configured as a digital input, digital output or analog input.

Digital Input - the connection supports input sensing; it reads the external input and determine if the settings should be 'High' (on) or 'Low' (off).

Digital Output - when there is a healthy WAN connection, the output pin is marked as 'High' (on). Otherwise, it will be marked as 'Low' (off).

Analog Input - to be confirmed. In most cases should read the external input and determine the voltage level.

O/P	
Enable	<input checked="" type="checkbox"/>
Type	Digital Output ▼
Mode	WAN Status ▼



## 23.8 NTP Server

Pepwave routers can now serve as a local NTP server. Upon start up, it is now able to provide connected devices with the accurate time, precise UTC from either an external NTP server or via GPS and ensuring that connected devices always receive the correct time.

Compatible with: BR1 ENT, 700 HW3, HD2/4, Transit

NTP Server setting can be found via: **Advanced>Misc. Settings>NTP Server**

NTP Server	
Enable	<input type="checkbox"/>

Time Settings can be found at **System>Time>Time Settings**

Time Settings	
Time Zone	(GMT) Casablanca <input type="checkbox"/> Show all
Time Sync	Time Server
Time Server	0.peplink.pool.ntp.org

## 23.9 Grouped Networks

**Advanced > Grouped Networks** allows to configure destination networks in grouped format.

Grouped Networks		
Name	Networks	
Example	192.168.1.71/28	<input type="button" value="X"/>
<input type="button" value="Add Group"/>		

Select Add group to create a new group with single IPAddresses or subnets from different VLANs.

Grouped Networks										
Name	Example									
Networks	<table border="1"> <thead> <tr> <th>Network</th> <th>Subnet Mask</th> <th></th> </tr> </thead> <tbody> <tr> <td>192.168.1.71</td> <td>255.255.255.240 (/28)</td> <td>✖</td> </tr> <tr> <td></td> <td>255.255.255.255 (/32)</td> <td>+</td> </tr> </tbody> </table>	Network	Subnet Mask		192.168.1.71	255.255.255.240 (/28)	✖		255.255.255.255 (/32)	+
	Network	Subnet Mask								
192.168.1.71	255.255.255.240 (/28)	✖								
	255.255.255.255 (/32)	+								
<div>Save Cancel</div>										

The created network groups can be used in outbound policies, firewall rules.

## 23.10 SIM Toolkit

The SIM Toolkit, accessible via **Advanced > Misc Settings > SIM Toolkit**, supports two functionalities, USSD and SMS.

### USSD

Unstructured Supplementary Service Data (USSD) is a protocol used by mobile phones to communicate with their service provider's computers. One of the most common uses is to query the available balance.

SIM Status	
WAN Connection	Cellular
SIM Card	1
IMSI	856195002108538
Tool	USSD

USSD	
USSD Code	<input type="text"/> <input type="button" value="Submit"/>

Enter your USSD code under the **USSD Code** text field and click **Submit**.

SIM Status	
WAN Connection	Cellular
SIM Card	1
IMSI	856195002108538
USSD Code	*138# <input type="button" value="Submit"/>
Receive SMS	<input type="button" value="Get"/>

You will receive a confirmation. To check the SMS response, click **Get**.

SIM Status	
WAN Connection	Cellular ▼
SIM Card	1
IMSI	856195002108538
USSD Code	*138# <input type="button" value="Submit"/>
USSD Status	Request is sent successfully
Receive SMS	<input type="button" value="Get"/>

After a few minutes you will receive a response to your USSD code

Received SMS	
May 27 20:02	<b>PCX</b> As of May 27th Account Balance: \$ 0.00 Amount Unbilled Voice Calls: 0 minutes Video Calls: 0 minutes SMS (Roaming): 0 SMS (Within Network): 0 MMS (Roaming):0 MMS (Within Network): 0 Data Usage: 7384KB (For reference only, please refer to bill)
Aug 8 , 2013 14:51	<b>PCX</b> iPhone & Android users need to make sure "PCX" is entered as the APN under "Settings" > "Mobile network setting" for web browsing and mobile data service. Other handset models will receive handset settings via SMS shortly (PIN: 1234) (Consumer Service Hotline: 1000 / Business Customer Hotline 10088)

## SMS

The SMS option allows you to read SMS (text) messages that have been sent to the SIM in your Peplink router.

SIM Status	
WAN Connection	Cellular ▼
SIM Card	1
IMSI	856195002108538
Tool	SMS ▼

SMS		Refresh
Jun 21, 2017 18:00	Hi, Hello! you, your web portal is available - you can change it when you first login at <a href="#">http://www.peplink.com</a>	✖
May 06, 2017 12:23	Hi, Hi! you still is ready to use. Go to your M2 account on your desktop or on a mobile phone click <a href="#">http://m2.peplink.com/m2/m2.html</a>	✖
Mar 15, 2017 10:03	Hi, Hi! There is planned maintenance in the database that M2 accounts will be. If your service is affected, you can get updates from <a href="#">http://www.peplink.com</a>	✖
Mar 06, 2017 14:50	Hi, Hi! you still is ready to use. Go to your M2 account on your desktop or on a mobile phone click <a href="#">http://m2.peplink.com/m2/m2.html</a>	✖
Dec 28, 2016 09:53	Hi, Hi, we hope you're enjoying our 1 month full-price offer. As we remind you, this offer applied to your first 100k. Your 100kth order will be the last of the offer. Thank you for your order.	✖
Dec 06, 2016 13:09	Hi, Hi! you still is ready to use. Go to your M2 account on your desktop or on a mobile phone click <a href="#">http://m2.peplink.com/m2/m2.html</a>	✖
Nov 08, 2016 11:29	Hi, Hi! There is planned maintenance in the database that M2 accounts will be. If your service is affected, you can get updates from <a href="#">http://www.peplink.com</a>	✖
Sep 07, 2016 17:05	Hi, Hi! you still is ready to use. Go to your M2 account on your desktop or on a mobile phone click <a href="#">http://m2.peplink.com/m2/m2.html</a>	✖

## 24 AP - access point

### 25 AP Controller

The AP controller acts as a centralized controller of Pepwave Access Points. With this feature, users can customize and manage up to 1500 Access Points from a single Pepwave router interface. To configure, navigate to the **AP** tab. and the following screen appears.

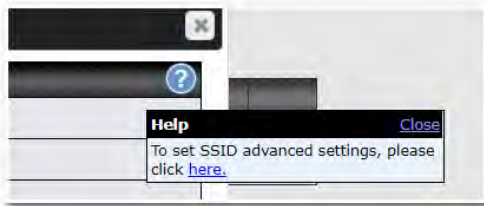
AP Controller	
AP Management	<input checked="" type="checkbox"/> Integrated AP <input checked="" type="checkbox"/> External AP
Sync. Method	As soon as possible ▼
Permitted AP	<input checked="" type="radio"/> Any <input type="radio"/> Approved List

AP Controller	
<b>AP Management</b>	The AP controller for managing Pepwave APs can be enabled by checking this box. When this option is enabled, the AP controller will wait for management connections originating from APs over the LAN on TCP and UDP port 11753. It will also wait for captive portal connections on TCP port 443. An extended DHCP option, <b>CAPWAP Access Controller addresses</b> (field 138), will be added to the DHCP server. A local DNS record, <b>AP Controller</b> , will be added to the local DNS proxy.
<b>Sync Method</b>	<ul style="list-style-type: none"> <li>As soon as possible</li> <li>Progressively</li> <li>One at a time</li> </ul>
<b>Permitted AP</b>	Access points to manage can be specified here. If <b>Any</b> is selected, the AP controller will manage any AP that reports to it. If <b>Approved List</b> is selected, only APs with serial numbers listed in the provided text box will be managed.

#### 25.1 Wireless SSID

SSID	Security Policy
No SSID Defined	
<input type="button" value="Add"/>	

Current SSID information appears in the **SSID** section. To edit an existing SSID, click its name in the list. To add a new SSID, click **Add**. Note that the following settings vary by model. The below settings shows a new SSID window with Advanced Settings enabled (these are available by selecting the question mark in the top right corner).



**SSID**

**SSID Settings**

SSID	<input type="text"/>
Enable	<input checked="" type="checkbox"/>
VLAN	Untagged LAN ▾
Broadcast SSID	<input checked="" type="checkbox"/>
Data Rate	<input checked="" type="radio"/> Auto <input type="radio"/> Fixed
Multicast Filter	<input type="checkbox"/>
Multicast Rate	MCS0/6M ▾
IGMP Snooping	<input type="checkbox"/>
Layer 2 Isolation	<input type="checkbox"/>
Maximum number of clients	2.4 GHz: <input type="text" value="0"/> 5 GHz: <input type="text" value="0"/> (0: Unlimited)

**Security Settings**

Security Policy	Open (No Encryption) ▾
-----------------	------------------------


**Access Control Settings**


Restricted Mode	None ▾
-----------------	--------

Save Cancel

SSID Settings	
<b>SSID</b>	This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients.
<b>Enable</b>	Click the drop-down menu to apply a time schedule to this interface
<b>VLAN</b>	This setting specifies the VLAN ID to be tagged on all outgoing packets generated from this wireless network (i.e., packets that travel from the Wi-Fi segment through the Pepwave AP One unit to the Ethernet segment via the LAN port). The default value of this setting is <b>0</b> , which means VLAN tagging is disabled (instead of tagged with zero).

<b>Broadcast SSID</b>	This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. <b>Broadcast SSID</b> is enabled by default.
<b>Data Rate</b> <sup>A</sup>	Select <b>Auto</b> to allow the Pepwave router to set the data rate automatically, or select <b>Fixed</b> and choose a rate from the displayed drop-down menu.
<b>Multicast Filter</b> <sup>A</sup>	This setting enables the filtering of multicast network traffic to the wireless SSID.
<b>Multicast Rate</b> <sup>A</sup>	This setting specifies the transmit rate to be used for sending multicast network traffic. The selected <b>Protocol</b> and <b>Channel Bonding</b> settings will affect the rate options and values available here.
<b>IGMP Snooping</b> <sup>A</sup>	To allow the Pepwave router to listen to internet group management protocol (IGMP) network traffic, select this option.
<b>DHCP Option 82</b> <sup>A</sup>	If you use a distributed DHCP server/relay environment, you can enable this option to provide additional information on the manner in which clients are physically connected to the network.
<b>Layer 2 Isolation</b> <sup>A</sup>	<b>Layer 2</b> refers to the second layer in the ISO Open System Interconnect model. When this option is enabled, clients on the same VLAN, SSID, or subnet are isolated to that VLAN, SSID, or subnet, which can enhance security. Traffic is passed to the upper communication layer(s). By default, the setting is disabled.
<b>Maximum Number of Clients</b>	Indicate the maximum number of clients that should be able to connect to each frequency.

<sup>A</sup> - Advanced feature. Click the  button on the top right-hand corner to activate.

Security Settings	
Security Policy	WPA2 - Personal ▼
Encryption	AES:CCMP
Shared Key	<div>  <input type="password" value="....."/> </div> <input checked="" type="checkbox"/> Hide Characters

Security Settings	
<b>Security Policy</b>	This setting configures the wireless authentication and encryption methods. Available options : <ul style="list-style-type: none"> <li>• <b>Open</b> (No Encryption)</li> </ul>



- **WPA3 -Personal** (AES:CCMP)
- **WPA2/WPA3 -Personal** (AES:CCMP)
- **WPA2 -Personal** (AES:CCMP)
- **WPA2 – Enterprise**
- **WPA/WPA2 - Personal** (TKIP/AES: CCMP)
- **WPA/WPA2 – Enterprise**

When **WPA/WPA2 - Enterprise** is configured, RADIUS-based 802.1 x authentication is enabled. Under this configuration, the **Shared Key** option should be disabled. When using this method, select the appropriate version using the **V1/V2** controls. The security level of this method is known to be very high.

When **WPA/WPA2- Personal** is configured, a shared key is used for data encryption and authentication. When using this configuration, the **Shared Key** option should be enabled. Key length must be between eight and 63 characters (inclusive). The security level of this method is known to be high.

**NOTE:**

When **WPA2/WPA3- Personal** is configured, if a managed AP which is NOT WPA3 PSK capable, the AP Controller will not push those WPA3 and WPA2/WPA3 SSID to that AP.

Access Control Settings	
Restricted Mode	Deny all except listed ▼
MAC Address List	<div>?</div> <div></div>

Access Control	
<b>Restricted Mode</b>	The settings allow administrator to control access using MAC address filtering. Available options are <b>None</b> , <b>Deny all except listed</b> , and <b>Accept all except listed</b>
<b>MAC Address List</b>	Connection coming from the MAC addresses in this list will be either denied or accepted based on the option selected in the previous field. If more than one MAC address needs to be entered, you can use a carriage return to separate them.

RADIUS Server Settings	Primary Server	Secondary Server
Host	<input type="text"/>	<input type="text"/>
Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters
Authentication Port	<input type="text" value="1812"/> <input type="button" value="Default"/>	<input type="text" value="1812"/> <input type="button" value="Default"/>
Accounting Port	<input type="text" value="1813"/> <input type="button" value="Default"/>	<input type="text" value="1813"/> <input type="button" value="Default"/>
NAS-Identifier	<input type="text" value="Device Name"/>	

RADIUS Server Settings	
<b>Host</b>	Enter the IP address of the primary RADIUS server and, if applicable, the secondary RADIUS server.
<b>Secret</b>	Enter the RADIUS shared secret for the primary server and, if applicable, the secondary RADIUS server.
<b>Authentication Port</b>	In field, enter the UDP authentication port(s) used by your RADIUS server(s) or click the <b>Default</b> button to enter <b>1812</b> .
<b>Accounting Port</b>	In field, enter the UDP accounting port(s) used by your RADIUS server(s) or click the <b>Default</b> button to enter <b>1813</b> .
<b>NAS-Identifier</b>	Choose between <b>Device Name</b> , <b>LAN MAC address</b> , <b>Device Serial Number</b> and <b>Custom Value</b>

## 25.2 Settings


On many Pepwave models, the AP settings screen (**AP>Settings**) looks similar to the example below:

AP Settings	
SSID	<input checked="" type="checkbox"/> 2.4 GHz <input checked="" type="checkbox"/> 5 GHz Integrated AP supports 2.4 GHz only. <input checked="" type="checkbox"/> Testing
Operating Country	United States
Preferred Frequency	<input checked="" type="radio"/> 2.4 GHz <input type="radio"/> 5 GHz Integrated AP supports 2.4 GHz only.
	<div>2.4 GHz</div> <div>5 GHz</div>
Protocol	<div>802.11ng</div> <div>802.11n/ac</div>
Channel Width	<div>20 MHz</div> <div>Auto</div>
Channel	<div>Auto</div> <div>Edit</div> <div>Channels: 1 2 3 4 5 6 7 8 9 10 11</div> <div>Auto</div> <div>Edit</div> <div>Channels: 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140 149 153 157 161 165</div>
Auto Channel Update	<div>Daily at 03:00</div> <div><input checked="" type="checkbox"/> Wait until no active client associated</div> <div>Daily at 03:00</div> <div><input checked="" type="checkbox"/> Wait until no active client associated</div>
Output Power	<div>Fixed: Max</div> <div><input type="checkbox"/> Boost</div> <div>Fixed: Max</div> <div><input type="checkbox"/> Boost</div>
Client Signal Strength Threshold	<div>0 -95 dBm (0: Unlimited)</div> <div>0 -95 dBm (0: Unlimited)</div>
Maximum number of clients	<div>0 (0: Unlimited)</div> <div>0 (0: Unlimited)</div>
Management VLAN ID	Untagged LAN (No VLAN)
Operating Schedule	Always on
Beacon Rate	<div>1 Mbps</div> <div>6 Mbps will be used for 5 GHz radio</div>
Beacon Interval	100 ms
DTIM	<div>1</div> <div>Default</div>
RTS Threshold	<div>0</div> <div>Default</div>
Fragmentation Threshold	<div>0 (0: Disable)</div> <div>Default</div>
Distance / Time Converter	<div>4050 m</div> <div>Note: Input distance for recommended values</div>
Slot Time	<div><input type="checkbox"/> Auto <input checked="" type="checkbox"/> Custom 9 μs</div> <div>Default</div>
ACK Timeout	<div>48 μs</div> <div>Default</div>
Frame Aggregation	<input type="checkbox"/>

AP Settings	
SSID	These buttons specify which wireless networks will use this AP profile. You can also select the frequencies at which each network will transmit. Please note that the Peplink Balance does not detect whether the AP is capable of transmitting at both frequencies. Instructions to transmit at unsupported frequencies will be ignored by the AP.
Operating Country	This drop-down menu specifies the national / regional regulations which the AP

	<p>should follow.</p> <ul style="list-style-type: none"> <li>• If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW).</li> <li>• If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW).</li> </ul> <p>NOTE: Users are required to choose an option suitable to local laws and regulations.</p> <p>Per FCC regulation, the country selection is not available on all models marketed in the US. All US models are fixed to US channels only.</p>
<b>Preferred Frequency</b>	These buttons determine the frequency at which access points will attempt to broadcast. This feature will only work for APs that can transmit at both 5.4GHz and 5GHz frequencies.
<b>Protocol</b>	This section displays the 2.4 GHz protocols your APs are using.
<b>Channel Width</b>	There are three options: 20 MHz, 20/40 MHz, and 40 MHz. With this feature enabled, the Wi-Fi system can use two channels at once. Using two channels improves the performance of the Wi-Fi connection.
<b>Channel</b>	This drop-down menu selects the 802.11 channel to be utilized. Available options are from 1 to 11 and from 1 to 13 for the North America region and Europe region, respectively. (Channel 14 is only available when the country is selected as Japan with protocol 802.11b.) If <b>Auto</b> is set, the system will perform channel scanning based on the scheduled time set and choose the most suitable channel automatically.
<b>Auto Channel Update</b>	Indicate the time of day at which update automatic channel selection.
<b>Output Power<sup>A</sup></b>	<p>This drop-down menu determines the power at which the AP under this profile will broadcast. When fixed settings are selected, the AP will broadcast at the specified power level, regardless of context. When <b>Dynamic</b> settings are selected, the AP will adjust its power level based on its surrounding APs in order to maximize performance.</p> <p>The <b>Dynamic: Auto</b> setting will set the AP to do this automatically. Otherwise, the <b>Dynamic: Manual</b> setting will set the AP to dynamically adjust only if instructed to do so. If you have set <b>Dynamic:Manual</b>, you can go to <b>AP&gt;Toolbox&gt;Auto Power Adj.</b> to give your AP further instructions.</p> <p>If you click the <b>Boost</b> checkbox, the AP under this profile will transmit using additional power. Please note that using this option with several APs in close proximity will lead to increased interference.</p>
<b>Client Signal Strength Threshold<sup>A</sup></b>	This field determines that maximum signal strength each individual client will receive. The measurement unit is megawatts.
<b>Max number of Clients<sup>A</sup></b>	This field determines the maximum clients that can be connected to APs under this profile.

<b>Management VLAN ID</b>	This field specifies the VLAN ID to tag to management traffic, such as AP to AP controller communication traffic. The value is <b>0</b> by default, meaning that no VLAN tagging will be applied. NOTE: change this value with caution as alterations may result in loss of connection to the AP controller.
<b>Operating Schedule</b>	Choose from the schedules that you have defined in <b>System&gt;Schedule</b> . Select the schedule for the integrated AP to follow from the drop-down menu.
<b>Beacon Rate<sup>A</sup></b>	This drop-down menu provides the option to send beacons in different transmit bit rates. The bit rates are <b>1Mbps</b> , <b>2Mbps</b> , <b>5.5Mbps</b> , <b>6Mbps</b> , and <b>11Mbps</b> .
<b>Beacon Interval<sup>A</sup></b>	This drop-down menu provides the option to set the time between each beacon send. Available options are <b>100ms</b> , <b>250ms</b> , and <b>500ms</b> .
<b>DTIM<sup>A</sup></b>	This field provides the option to set the frequency for beacon to include delivery traffic indication message (DTIM). The interval unit is measured in milliseconds.
<b>RTS Threshold<sup>A</sup></b>	This field provides the option to set the minimum packet size for the unit to send an RTS using the RTS/CTS handshake. Setting <b>0</b> disables this feature.
<b>Fragmentation Threshold<sup>A</sup></b>	Determines the maximum size (in bytes) that each packet fragment will be broken down into. Set 0 to disable fragmentation.
<b>Distance/Time Converter<sup>A</sup></b>	Select the distance you want your Wi-Fi to cover in order to adjust the below parameters. Default values are recommended.
<b>Slot Time<sup>A</sup></b>	This field provides the option to modify the unit wait time before it transmits. The default value is <b>9μs</b> .
<b>ACK Timeout<sup>A</sup></b>	This field provides the option to set the wait time to receive acknowledgement packet before doing retransmission. The default value is <b>48μs</b> .
<b>Frame Aggregation<sup>A</sup></b>	With this feature enabled, throughput will be increased by sending two or more data frames in a single transmission.
<b>Frame Length</b>	This field is only available when <b>Frame Aggregation</b> is enabled. It specifies the frame length for frame aggregation. By default, it is set to <b>50000</b> .

<sup>A</sup> - Advanced feature. Click the  button on the top right-hand corner to activate.

Web Administration Settings (on External AP)	
Enable	<input checked="" type="checkbox"/>
Web Access Protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Management Port	<input type="text" value="443"/>
HTTP to HTTPS Redirection	<input checked="" type="checkbox"/>
Admin Username	<input type="text" value="admin"/>
Admin Password	<input type="text" value="25db591396e0"/> <input type="button" value="Generate"/>

### Web Administration Settings

<b>Enable</b>	Check the box to allow the Pepwave router to manage the web admin access information of the AP.
<b>Web Access Protocol</b>	These buttons specify the web access protocol used for accessing the web admin of the AP. The two available options are <b>HTTP</b> and <b>HTTPS</b> .
<b>Management Port</b>	This field specifies the management port used for accessing the device.
<b>HTTP to HTTPS Redirection</b>	This option will be available if you have chosen <b>HTTPS</b> as the <b>Web Access Protocol</b> . With this enabled, any HTTP access to the web admin will redirect to HTTPS automatically.
<b>Admin User Name</b>	This field specifies the administrator username of the web admin. It is set as <i>admin</i> by default.
<b>Admin Password</b>	This field allows you to specify a new administrator password. You may also click the <b>Generate</b> button and let the system generate a random password automatically.







Navigating to **AP>Settings** on some Pepwave models displays a screen similar to the one shown below:



 InControl management enabled. Settings can now be configured on [InControl](#).

Wi-Fi Radio Settings	
Operating Country	United States ▼
Wi-Fi Antenna	<input type="radio"/> Internal <input checked="" type="radio"/> External

Wi-Fi AP Settings 	
Protocol	802.11ng ▼
Channel	1 (2.412 GHz) ▼
Channel Width	Auto ▼
Output Power	Max ▼ <input type="checkbox"/> Boost
Beacon Rate 	1Mbps ▼
Beacon Interval 	100ms ▼
DTIM 	1
Slot Time 	9 μs
ACK Timeout 	48 μs
Frame Aggregation	<input checked="" type="checkbox"/> Enable
Guard Interval	<input checked="" type="radio"/> Short <input type="radio"/> Long

### Wi-Fi Radio Settings

#### Operating Country

This option sets the country whose regulations the Pepwave router follows.

#### Wi-Fi Antenna

Choose from the router's internal or optional external antennas, if so equipped.

### Important Note

Per FCC regulations, the country selection is not available on all models marketed in the US. All US models are fixed to US channels only.

### 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 used. **Channel 1 (2.412 GHz)** is selected by default.

#### Channel Width

**Auto (20/40 MHz)** and **20 MHz** are available. The default setting 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.

#### Beacon Rate<sup>A</sup>

This option is for setting the transmit bit rate for sending a beacon. By default, **1Mbps** is selected.



<b>Beacon Interval<sup>A</sup></b>	This option is for setting the time interval between each beacon. By default, <b>100ms</b> is selected.
<b>DTIM<sup>A</sup></b>	This field allows you to set the frequency for the beacon to include a delivery traffic indication message. The interval is measured in milliseconds. The default value is set to <b>1 ms</b> .
<b>Slot Time<sup>A</sup></b>	This field is for specifying the wait time before the Router transmits a packet. By default, this field is set to <b>9 µs</b> .
<b>ACK Timeout<sup>A</sup></b>	This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to <b>48 µs</b> .
<b>Frame Aggregation<sup>A</sup></b>	This option allows you to enable frame aggregation to increase transmission throughput.
<b>Guard Interval<sup>A</sup></b>	This setting allows choosing a short or long guard period interval for your transmissions.

<sup>A</sup> - Advanced feature, please click the  button on the top right-hand corner to activate.

## 26 AP Controller Status

### 26.1 Info

A comprehensive overview of your AP can be accessed by navigating to **AP > Controller Status > Info**.



AP Controller	
<b>License Limit</b>	This field displays the maximum number of AP your Balance router can control. You can purchase licenses to increase the number of AP you can manage.
<b>Frequency</b>	Underneath, there are two check boxes labeled <b>2.4 Ghz</b> and <b>5 Ghz</b> . Clicking either box will toggle the display of information for that frequency. By default, the graphs display the number of clients and data usage for both 2.4GHz and 5 GHz frequencies.
<b>SSID</b>	The colored boxes indicate the SSID to display information for. Clicking any colored box will toggle the display of information for that SSID. By default, all the graphs show information for all SSIDs.
<b>No. of APs</b>	This pie chart and table indicates how many APs are online and how many are offline.

<b>No.of Clients</b>	This graph displays the number of clients connected to each network at any given time. Mouse over any line on the graph to see how many clients connected to a specific SSID for that point in time.
<b>Data Usage</b>	This graph enables you to see the data usage of any SSID for any given time period. Mouse over any line on the graph to see the data usage by each SSID for that point in time. Use the buttons next to <b>Zoom</b> to select the time scale you wish to view. In addition, you could use the sliders at the bottom to further refine your timescale.

Events		View Alerts
Jan 2 11:01:11	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 11:00:42	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 11:00:38	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 11:00:36	AP One 300M: Client 00:21:6A:35:59:A4 associated with Balance_11a	
Jan 2 11:00:20	AP One 300M: Client 60:67:20:24:B6:4C disassociated from Marketing_11a	
Jan 2 11:00:09	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:59:09	AP One 300M: Client 00:21:6A:35:59:A4 disassociated from Balance_11a	
Jan 2 10:59:08	Office Fiber AP: Client 18:00:2D:3D:4E:7F associated with Balance	
Jan 2 10:58:53	Michael's Desk: Client 18:00:2D:3D:4E:7F disassociated from Wireless	
Jan 2 10:58:18	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:58:03	Office InWall: Client 10:BF:48:E9:76:C7 associated with Wireless	
Jan 2 10:57:47	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:57:19	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:57:09	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:56:48	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:56:39	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:56:19	AP One 300M: Client 00:26:BB:05:84:A4 associated with Marketing_11a	
Jan 2 10:56:09	AP One 300M: Client 9C:04:EB:10:39:4C associated with Marketing_11a	
Jan 2 10:55:42	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:55:29	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
		More...

## Events






This event log displays all activity on your AP network, down to the client level. Click **View Alerts** to see only alerts, and click the **More...** link for additional records.

## 26.2 Access Point (Usage)

A detailed breakdown of data usage for each AP is available at **AP > Controller Status > Access Point**.

Search Filter	
AP Name / Serial Number / SSID	All <input type="text"/>
	<input type="checkbox"/> Include Offline APs
Search Result	


Managed APs							Expand	Collapse
Name	IP Address	MAC	Location	Firmware	Pack ID	Configuration		
▼ Default (8/9 online)								
10.8.82.11	00:1A:DD:BD:73:E0	-	3.5.2	None	✓	-		

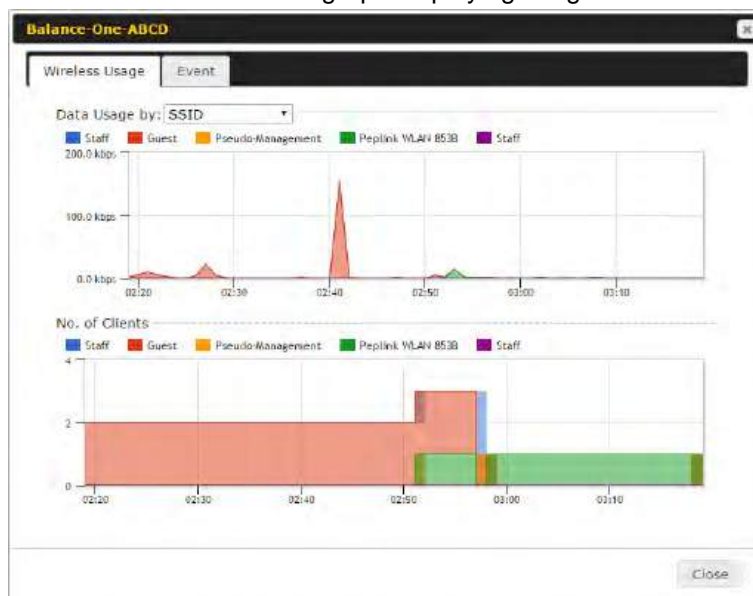
Usage																																																																																																									
<b>AP Name/Serial Number</b>	This field enables you to quickly find your device if you know its name or serial number. Fill in the field to begin searching. Partial names and serial numbers are supported.																																																																																																								
<b>Online Status</b>	This button toggles whether your search will include offline devices.																																																																																																								
<b>Managed Wireless Devices</b>	<p>This table shows the detailed information on each AP, including channel, number of clients, upload traffic, and download traffic. Click the blue arrows at the left of the table to expand and collapse information on each device group. You could also expand and collapse all groups by using the <b>Expand</b> <b>Collapse</b> buttons.</p> <p>On the right of the table, you will see the following icons:   .</p> <p>Click the  icon to see a usage table for each client:</p> <table border="1"> <thead> <tr> <th colspan="8">Client List</th> </tr> <tr> <th>MAC Address</th> <th>IP Address</th> <th>Type</th> <th>Signal</th> <th>SSID</th> <th>Upload</th> <th>Download</th> <th></th> </tr> </thead> <tbody> <tr> <td>80:56:f2:98:75:ff</td> <td>10.9.2.7</td> <td>802.11ng</td> <td>Excellent (37)</td> <td>Balance</td> <td>66.26 MB</td> <td>36.26 MB</td> <td></td> </tr> <tr> <td>c4:6a:b7:bf:d7:15</td> <td>10.9.2.123</td> <td>802.11ng</td> <td>Excellent (42)</td> <td>Balance</td> <td>6.65 MB</td> <td>2.26 MB</td> <td></td> </tr> <tr> <td>70:56:81:1d:87:f3</td> <td>10.9.2.102</td> <td>802.11ng</td> <td>Good (23)</td> <td>Balance</td> <td>1.86 MB</td> <td>606.63 KB</td> <td></td> </tr> <tr> <td>e0:63:e5:83:45:c8</td> <td>10.9.2.101</td> <td>802.11ng</td> <td>Excellent (39)</td> <td>Balance</td> <td>3.42 MB</td> <td>474.52 KB</td> <td></td> </tr> <tr> <td>18:00:2d:3d:4e:7f</td> <td>10.9.2.66</td> <td>802.11ng</td> <td>Excellent (25)</td> <td>Balance</td> <td>640.29 KB</td> <td>443.57 KB</td> <td></td> </tr> <tr> <td>14:5a:05:80:4f:40</td> <td>10.9.2.76</td> <td>802.11ng</td> <td>Excellent (29)</td> <td>Balance</td> <td>2.24 KB</td> <td>3.67 KB</td> <td></td> </tr> <tr> <td>00:1a:dd:c5:4e:24</td> <td>10.8.9.84</td> <td>802.11ng</td> <td>Excellent (29)</td> <td>Wireless</td> <td>9.86 MB</td> <td>9.76 MB</td> <td></td> </tr> <tr> <td>00:1a:dd:bb:29:ec</td> <td>10.8.9.73</td> <td>802.11ng</td> <td>Excellent (25)</td> <td>Wireless</td> <td>9.36 MB</td> <td>11.14 MB</td> <td></td> </tr> <tr> <td>40:b0:fa:c3:26:2c</td> <td>10.8.9.18</td> <td>802.11ng</td> <td>Good (23)</td> <td>Wireless</td> <td>118.05 MB</td> <td>7.92 MB</td> <td></td> </tr> <tr> <td>e4:25:e7:8a:d3:12</td> <td>10.10.11.23</td> <td>802.11ng</td> <td>Excellent (35)</td> <td>Marketing</td> <td>74.78 MB</td> <td>4.58 MB</td> <td></td> </tr> <tr> <td>04:f7:e4:ef:68:05</td> <td>10.10.11.71</td> <td>802.11ng</td> <td>Poor (12)</td> <td>Marketing</td> <td>84.84 KB</td> <td>119.32 KB</td> <td></td> </tr> </tbody> </table> <p>Click the  icon to configure each client</p>	Client List								MAC Address	IP Address	Type	Signal	SSID	Upload	Download		80:56:f2:98:75:ff	10.9.2.7	802.11ng	Excellent (37)	Balance	66.26 MB	36.26 MB		c4:6a:b7:bf:d7:15	10.9.2.123	802.11ng	Excellent (42)	Balance	6.65 MB	2.26 MB		70:56:81:1d:87:f3	10.9.2.102	802.11ng	Good (23)	Balance	1.86 MB	606.63 KB		e0:63:e5:83:45:c8	10.9.2.101	802.11ng	Excellent (39)	Balance	3.42 MB	474.52 KB		18:00:2d:3d:4e:7f	10.9.2.66	802.11ng	Excellent (25)	Balance	640.29 KB	443.57 KB		14:5a:05:80:4f:40	10.9.2.76	802.11ng	Excellent (29)	Balance	2.24 KB	3.67 KB		00:1a:dd:c5:4e:24	10.8.9.84	802.11ng	Excellent (29)	Wireless	9.86 MB	9.76 MB		00:1a:dd:bb:29:ec	10.8.9.73	802.11ng	Excellent (25)	Wireless	9.36 MB	11.14 MB		40:b0:fa:c3:26:2c	10.8.9.18	802.11ng	Good (23)	Wireless	118.05 MB	7.92 MB		e4:25:e7:8a:d3:12	10.10.11.23	802.11ng	Excellent (35)	Marketing	74.78 MB	4.58 MB		04:f7:e4:ef:68:05	10.10.11.71	802.11ng	Poor (12)	Marketing	84.84 KB	119.32 KB	
Client List																																																																																																									
MAC Address	IP Address	Type	Signal	SSID	Upload	Download																																																																																																			
80:56:f2:98:75:ff	10.9.2.7	802.11ng	Excellent (37)	Balance	66.26 MB	36.26 MB																																																																																																			
c4:6a:b7:bf:d7:15	10.9.2.123	802.11ng	Excellent (42)	Balance	6.65 MB	2.26 MB																																																																																																			
70:56:81:1d:87:f3	10.9.2.102	802.11ng	Good (23)	Balance	1.86 MB	606.63 KB																																																																																																			
e0:63:e5:83:45:c8	10.9.2.101	802.11ng	Excellent (39)	Balance	3.42 MB	474.52 KB																																																																																																			
18:00:2d:3d:4e:7f	10.9.2.66	802.11ng	Excellent (25)	Balance	640.29 KB	443.57 KB																																																																																																			
14:5a:05:80:4f:40	10.9.2.76	802.11ng	Excellent (29)	Balance	2.24 KB	3.67 KB																																																																																																			
00:1a:dd:c5:4e:24	10.8.9.84	802.11ng	Excellent (29)	Wireless	9.86 MB	9.76 MB																																																																																																			
00:1a:dd:bb:29:ec	10.8.9.73	802.11ng	Excellent (25)	Wireless	9.36 MB	11.14 MB																																																																																																			
40:b0:fa:c3:26:2c	10.8.9.18	802.11ng	Good (23)	Wireless	118.05 MB	7.92 MB																																																																																																			
e4:25:e7:8a:d3:12	10.10.11.23	802.11ng	Excellent (35)	Marketing	74.78 MB	4.58 MB																																																																																																			
04:f7:e4:ef:68:05	10.10.11.71	802.11ng	Poor (12)	Marketing	84.84 KB	119.32 KB																																																																																																			

AP Details	
Serial Number	1111-2222-3333
MAC Address	00:1A:DD:BD:73:E0
Product Name	Pepwave AP Pro Duo
Name	<input type="text"/>
Location	<input type="text"/>
Firmware Version	3.5.2
Firmware Pack	Default (None) ▼
AP Client Limit	<input checked="" type="radio"/> Follow AP Profile <input type="radio"/> Custom
2.4 GHz SSID List	T4Open
5 GHz SSID List	T4Open
Last config applied by controller	Mon Nov 23 11:25:03 HKT 2015
Uptime	Wed Nov 11 15:00:27 HKT 2015
Current Channel	1 (2.4 GHz) 153 (5 GHz)
Channel	2.4 GHz: Follow AP Profile ▼ 5 GHz: Follow AP Profile ▼
Output Power	2.4 GHz: Follow AP Profile ▼ 5 GHz: Follow AP Profile ▼

Close

For easier network management, you can give each client a name and designate its location. You can also designate which firmware pack (if any) this client will follow, as well as the channels on which the client will broadcast.

Click the  icon to see a graph displaying usage:

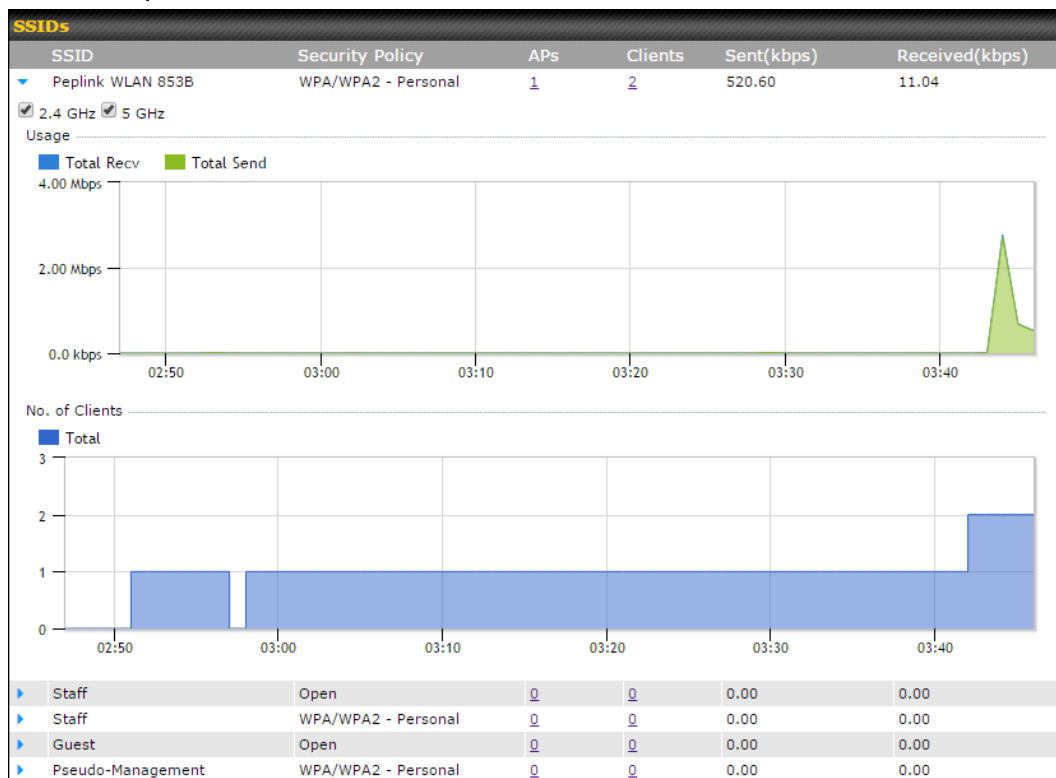


Click any point in the graphs to display detailed usage and client information for that device, using that SSID, at that point in time. On the **Data Usage by** menu, you can display the information by SSID or by AP send/receive rate. Click the **Event** tab next to **Wireless Usage** to view a detailed event log for that particular device:

Event Information	
Events	
Jan 2 11:53:39	Client 00:26:BB:08:AC:FD associated with Wireless_11a
Jan 2 11:39:31	Client 60:67:20:24:B6:4C disassociated from Marketing_11a
Jan 2 11:16:55	Client A8:BB:CF:E1:0F:1E disassociated from Balance_11a
Jan 2 11:11:54	Client A8:BB:CF:E1:0F:1E associated with Balance_11a
Jan 2 11:10:45	Client 60:67:20:24:B6:4C associated with Marketing_11a
Jan 2 11:00:36	Client 00:21:6A:35:59:A4 associated with Balance_11a
Jan 2 11:00:20	Client 60:67:20:24:B6:4C disassociated from Marketing_11a
Jan 2 10:59:09	Client 00:21:6A:35:59:A4 disassociated from Balance_11a
Jan 2 10:42:28	Client F4:B7:E2:16:35:E9 associated with Balance_11a
Jan 2 10:29:12	Client 84:7A:88:78:1E:4B associated with Balance_11a
Jan 2 10:24:27	Client 90:B9:31:0D:11:EC disassociated from Marketing_11a
Jan 2 10:24:27	Client 90:B9:31:0D:11:EC roamed to Marketing_11a at 2830-BFC8-D230
Jan 2 10:13:22	Client E8:8D:28:A8:43:93 associated with Balance_11a
Jan 2 10:13:22	Client E8:8D:28:A8:43:93 roamed to Balance_11a from 2830-BF7F-694C
Jan 2 10:07:52	Client CC:3A:61:89:07:F3 associated with Wireless_11a
Jan 2 10:04:35	Client 60:67:20:24:B6:4C associated with Marketing_11a
Jan 2 10:03:38	Client 60:67:20:24:B6:4C disassociated from Marketing_11a
Jan 2 09:58:27	Client 00:26:BB:08:AC:FD disassociated from Wireless_11a
Jan 2 09:52:46	Client 00:26:BB:08:AC:FD associated with Wireless_11a
Jan 2 09:20:26	Client 8C:3A:E3:3F:17:62 associated with Balance_11a
More...	
Close	

## 26.3 Wireless SSID

In-depth SSID reports are available under **AP > Controller Status > Wireless SSID**.




Click the blue arrow on any SSID to obtain more detailed usage information on each SSID.


## 26.4 Wireless Client

You can search for specific Wi-Fi users by navigating to **AP > Controller Status > Wireless Client**.

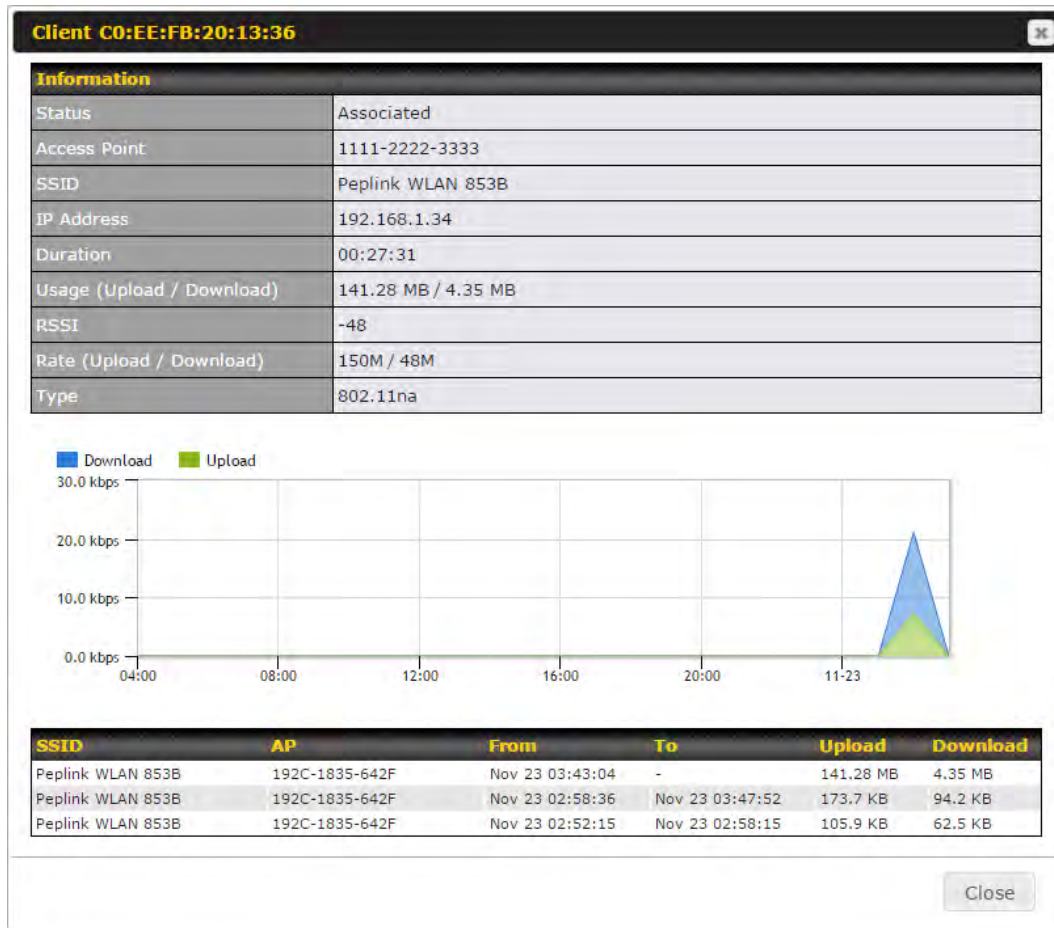
Search Filter		
Client MAC / SSID / AP Serial Number	<input type="text"/>	
Maximum Result (1-256)	<input type="text" value="50"/>	
Search Result		
<input type="button" value="Search"/>		

Top 10 Clients of last hour (Updated at 03:00)			
Client MAC Address	Upload	Download	
C0:EE:FB:20:13:36	53.5 KB	101.4 KB	☆ 

Here, you will be able to see your network's heaviest users as well as search for specific users. Click the ☆ icon to bookmark specific users, and click the  icon for additional details about each user:





## 26.5 Nearby Device

A listing of near devices can be accessed by navigating to **AP > Controller Status > Nearby**

## Device.

Suspected Rogue APs					
BSSID	SSID	Channel	Encryption	Last Seen	Mark as
00:1A:DD:EC:25:22	Wireless	11	WPA2	10 hours ago	
00:1A:DD:EC:25:23	Accounting	11	WPA2	10 hours ago	
00:1A:DD:EC:25:24	Marketing	11	WPA2	11 hours ago	
00:03:7F:00:00:00	MYB1PUSH	1	WPA & WPA2	11 minutes ago	
00:03:7F:00:00:01	MYB1	1	WPA2	15 minutes ago	
00:1A:DD:B9:60:88	PEPWAVE_CB7E	1	WPA & WPA2	5 minutes ago	
00:1A:DD:BB:09:C1	Micro_S1_1	6	WPA & WPA2	1 hour ago	
00:1A:DD:BB:52:A8	MAX HD2 Gobi	11	WPA & WPA2	2 minutes ago	
00:1A:DD:BF:75:81	PEPLINK_05B5	4	WPA & WPA2	1 minute ago	
00:1A:DD:BF:75:82	LK_05B5	4	WPA2	1 minute ago	
00:1A:DD:BF:75:83	LK_05B5_VLAN22	4	WPA2	1 minute ago	
00:1A:DD:C1:ED:E4	dev_captive_portal_test	1	WPA & WPA2	3 minutes ago	
00:1A:DD:C2:E4:C5	PEPWAVE_7052	11	WPA & WPA2	2 hours ago	
00:1A:DD:C3:F1:64	dev_captive_portal_test	6	WPA & WPA2	6 minutes ago	
00:1A:DD:C4:DC:24	ssid_test	8	WPA & WPA2	2 minutes ago	
00:1A:DD:C4:DC:25	SSID New	8	WPA & WPA2	2 minutes ago	
00:1A:DD:C5:46:04	Guest SSID	9	WPA2	2 minutes ago	
00:1A:DD:C5:47:04	PEPWAVE_67B8	1	WPA & WPA2	5 minutes ago	
00:1A:DD:C5:4E:24	G BR1 Portal	2	WPA2	2 minutes ago	
00:1A:DD:C6:9A:48	ssid_test	8	WPA & WPA2	2 hours ago	

### Suspected Rogue Devices

Hovering over the device MAC address will result in a popup with information on how this device was detected. Click the icons and the device will be moved to the bottom table of identified devices.

## 26.6 Event Log

You can access the AP Controller Event log by navigating to **AP > Controller Status > Event Log**.

Filter	
Search key	<input type="text" value="Client MAC Address / Wireless SSID / AP Serial Number / AP Profile Name"/>
Time	From <input type="text" value=""/> <input type="text" value="hh:mm"/> to <input type="text" value=""/> <input type="text" value="hh:mm"/>
Alerts only	<input type="checkbox"/>
<input type="button" value="Search"/>	

Events		<a href="#">View Alerts</a>
Jan 2 11:01:11	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 11:00:42	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 11:00:38	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 11:00:36	AP One 300M: Client 00:21:6A:35:59:A4 associated with Balance_11a	
Jan 2 11:00:20	AP One 300M: Client 60:67:20:24:B6:4C disassociated from Marketing_11a	
Jan 2 11:00:09	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:59:09	AP One 300M: Client 00:21:6A:35:59:A4 disassociated from Balance_11a	
Jan 2 10:59:08	Office Fiber AP: Client 18:00:2D:3D:4E:7F associated with Balance	
Jan 2 10:58:53	Michael's Desk: Client 18:00:2D:3D:4E:7F disassociated from Wireless	
Jan 2 10:58:18	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:58:03	Office InWall: Client 10:BF:48:E9:76:C7 associated with Wireless	
Jan 2 10:57:47	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:57:19	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:57:09	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:56:48	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:56:39	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
Jan 2 10:56:19	AP One 300M: Client 00:26:BB:05:84:A4 associated with Marketing_11a	
Jan 2 10:56:09	AP One 300M: Client 9C:04:EB:10:39:4C associated with Marketing_11a	
Jan 2 10:55:42	AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a	
Jan 2 10:55:29	AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a	
		<a href="#">More...</a>

## Events


This event log displays all activity on your AP network, down to the client level. Use to filter box to search by MAC address, SSID, AP Serial Number, or AP Profile name. Click **View Alerts** to see only alerts, and click the **More...** link for additional records.

## 27 Toolbox

Tools for managing firmware packs can be found at **AP>Toolbox**.

Firmware Packs			
Pack ID	Release Date	Details	Action
1126	2013-08-26		
<input type="button" value="Check for Updates"/> <input type="button" value="Manual Upload"/> <input type="button" value="Default..."/> No default defined.			

## Firmware Packs

Here, you can manage the firmware of your AP. Clicking on  will result in information regarding each firmware pack. To receive new firmware packs, you can click **Check for Updates** to download new packs, or you can click **Manual Upload** to manually upload a firmware pack. Click **Default** to define which firmware pack is default.

## 28 System Settings

### 28.1 Admin Security

There are two types of user accounts available for accessing the web admin: *admin* and *user*. They represent two user levels: the admin level has full administrative access, while the user level is read-only. The user level can access only the device's status information; users cannot make any changes on the device.

A web login session will be logged out automatically when it has been idle longer than the **Web Session Timeout**. Before the session expires, you may click the **Logout** button in the web admin to exit the session.

**0 hours 0 minutes** signifies an unlimited session time. This setting should be used only in special situations, as it will lower the system security level if users do not log out before closing the browser. The **default** is 4 hours, 0 minutes.

For security reasons, after logging in to the web admin Interface for the first time, it is recommended to change the administrator password. Configuring the administration interface to be accessible only from the LAN can further improve system security. Administrative settings configuration is located at **System>Admin Security**.

Admin Settings	
Router Name	MBX-345A hostname: mbx-345a ⚙️ This configuration is being managed by InControl.
Admin User Name	admin
Admin Password	••••••••
Confirm Admin Password	••••••••
Read-only User Name	DemoPep
User Password	••••••••
Confirm User Password	••••••••
Web Session Timeout	? 4 Hours 0 Minutes
Authentication by RADIUS	? <input type="checkbox"/> Enable
CLI SSH & Console	? <input type="checkbox"/> Enable
Security	HTTP / HTTPS ▾ <input type="checkbox"/> Redirect HTTP to HTTPS
Web Admin Access	HTTP: LAN Only ▾ HTTPS: LAN Only ▾
Web Admin Port	HTTP: 80 HTTPS: 443 Default

LAN Connection Access Settings	
Allowed LAN Networks	<input checked="" type="radio"/> Any <input type="radio"/> Allow this network only

Save

Admin Settings	
<b>Router Name</b>	This field allows you to define a name for this Pepwave router. By default, <b>Router Name</b> is set as <b>MAX_XXXX</b> , where <b>XXXX</b> refers to the last 4 digits of the unit's serial number.
<b>Admin User Name</b>	<b>Admin User Name</b> is set as <i>admin</i> by default, but can be changed, if desired.
<b>Admin Password</b>	This field allows you to specify a new administrator password.
<b>Confirm Admin Password</b>	This field allows you to verify and confirm the new administrator password.
<b>Read-only User Name</b>	<b>Read-only User Name</b> is set as <i>user</i> by default, but can be changed, if desired.
<b>User Password</b>	This field allows you to specify a new user password. Once the user password is set, the read-only user feature will be enabled.
<b>Confirm User Password</b>	This field allows you to verify and confirm the new user password.
<b>Web Session Timeout</b>	This field specifies the number of hours and minutes that a web session can remain idle before the Pepwave router terminates its access to the web admin interface. By default, it is set to <b>4 hours</b> .
<b>Authentication by RADIUS</b>	With this box is checked, the web admin will authenticate using an external RADIUS server. Authenticated users are treated as either "admin" with full read-write permission or "user" with read-only access. Local admin and user accounts will be disabled. When the device is not able to communicate with the external RADIUS server, local accounts will be enabled again for emergency access. Additional authentication options will be available once this box is checked.
<b>Auth Protocol</b>	This specifies the authentication protocol used. Available options are <b>MS-CHAP v2</b> and <b>PAP</b> .
<b>Auth Server</b>	This specifies the access address and port of the external RADIUS server.
<b>Auth Server Secret</b>	This field is for entering the secret key for accessing the RADIUS server.
<b>Auth Timeout</b>	This option specifies the time value for authentication timeout.
<b>Accounting Server</b>	This specifies the access address and port of the external accounting server.
<b>Accounting Server Secret</b>	This field is for entering the secret key for accessing the accounting server.

<b>Network Connection</b>	This option is for specifying the network connection to be used for authentication. Users can choose from LAN, WAN, and VPN connections.
<b>CLI SSH</b>	The CLI (command line interface) can be accessed via SSH. This field enables CLI support. For additional information regarding CLI, please refer to <b>Section 30.5</b> .
<b>CLI SSH Port</b>	This field determines the port on which clients can access CLI SSH.
<b>CLI SSH Access</b>	This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only.
<b>Security</b>	<p>This option is for specifying the protocol(s) through which the web admin interface can be accessed:</p> <ul style="list-style-type: none"> <li>• HTTP</li> <li>• HTTPS</li> <li>• HTTP/HTTPS</li> </ul>
<b>Web Admin Port</b>	This field is for specifying the port number on which the web admin interface can be accessed.
<b>Web Admin Access</b>	<p>This option is for specifying the network interfaces through which the web admin interface can be accessed:</p> <ul style="list-style-type: none"> <li>• LAN only</li> <li>• LAN/WAN</li> </ul> <p>If LAN/WAN is chosen, the <b>WAN Connection Access Settings</b> form will be displayed.</p>

**LAN Connection Access Settings**

Allowed LAN Networks

☐ Any
☒ Allow this network only
Public (10) ▼

LAN Connection Access Settings	
<b>Allowed LAN Networks</b>	This field allows you to permit only specific networks or VLANs to access the Web UI.



**WAN Connection Access Settings**

Allowed Source IP Subnets ? ☐ Any ☒ Allow access from the following IP subnets only

Allowed WAN IP Address(es)

Connection / IP Address(es)	All	Clear
<input checked="" type="checkbox"/> WAN 1	<input checked="" type="checkbox"/> 10.88.3.158 (Interface IP)	
<input type="checkbox"/> WAN 2		
<input type="checkbox"/> Wi-Fi WAN		
<input type="checkbox"/> Cellular 1		
<input type="checkbox"/> Cellular 2		
<input type="checkbox"/> USB		

WAN Connection Access Settings	
Allowed Source IP Subnets	<p>This field allows you to restrict web admin access only from defined IP subnets.</p> <ul style="list-style-type: none"> <li><b>Any</b> - Allow web admin accesses to be from anywhere, without IP address restriction.</li> <li><b>Allow access from the following IP subnets only</b> - Restrict web admin access only from the defined IP subnets. When this is chosen, a text input area will be displayed beneath:</li> </ul> <p>The allowed IP subnet addresses should be entered into this text area. Each IP subnet must be in form of <i>w.x.y.z/m</i>, where <i>w.x.y.z</i> is an IP address (e.g., 192.168.0.0), and <i>m</i> is the subnet mask in CIDR format, which is between 0 and 32 inclusively (For example, 192.168.0.0/24).</p> <p>To define multiple subnets, separate each IP subnet one in a line. For example:</p> <ul style="list-style-type: none"> <li>192.168.0.0/24</li> <li>10.8.0.0/16</li> </ul>
	<p>Allowed WAN IP Address(es)</p> <p>This is to choose which WAN IP address(es) the web server should listen on.</p>

## 28.2 Firmware

### 28.2.1 Web admin interface : automatically check for updates

Upgrading firmware can be done in one of three ways. Using the router's interface to automatically check for an update, using the router's interface to manually upgrade the firmware, or using InControl2 to push an upgrade to a router.

The automatic upgrade can be done from **System > Firmware**.





If an update is found the buttons will change to allow you to **Download and Update** the firmware.



Click on the **Download and Upgrade** button. A prompt will be displayed advising to download the Current Active Configuration. Please click on the underlined download text. After downloading the current config click the **Ok** button to start the upgrade process.

The router will download and then apply the firmware. The time that this process takes will depend on your internet connection's speed.



The firmware will now be applied to the router\*. The amount of time it takes for the firmware to upgrade will also depend on the router that's being upgraded.

#### Firmware Upgrade

It may take up to 8 minutes.



**\*Upgrading the firmware will cause the router to reboot.**

### 28.2.2 Web admin interface : install updates manually

In some cases, a special build may be provided via a ticket or it may be found in the forum. Upgrading to the special build can be done using this method, or using IC2 if you are using that to manage your firmware upgrades. A manual upgrade using the GA firmware posted on the site may also be recommended or required for a couple of reasons.

All of the Peplink/Peplink GA firmware can be found [here](#). Navigate to the relevant product line (ie. Balance, Max, FusionHub, SOHO, etc). Some product lines may have a dropdown that lists all of the products in that product line. Here is a screenshot from the Balance line.

Balance

Product ▼

Search:

Product	Hardware Revision	Firmware Version	Download Link	Release Notes	User Manual
Balance 1350	HW2	7.1.2	<a href="#">Download</a>	<a href="#">PDF</a>	<a href="#">PDF</a>
Balance 1350	HW1	6.3.4	<a href="#">Download</a>	<a href="#">PDF</a>	<a href="#">PDF</a>
Balance 20	HW1-6	7.1.2	<a href="#">Download</a>	<a href="#">PDF</a>	<a href="#">PDF</a>
Balance 210	HW4	7.1.2	<a href="#">Download</a>	<a href="#">PDF</a>	<a href="#">PDF</a>

If the device has more than one firmware version the current hardware revision will be required to know what firmware to download.

Navigate to System > Firmware and click the Choose File button under the Manual Firmware Upgrade section. Navigate to the location that the firmware was downloaded to select the “.img” file and click the Open button.

Click on the Manual Upgrade button to start the upgrade process.

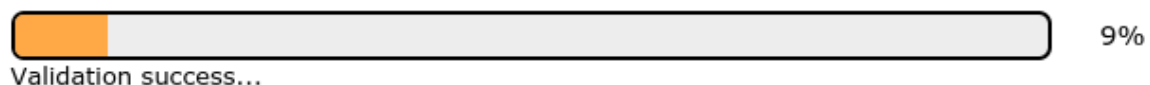
**Manual Firmware Upgrade** ?

Firmware Image  No file chosen

A prompt will be displayed advising to download the Current Active Configuration. Please click on the underlined download text. After downloading the current config click the Ok button to start the upgrade process. The firmware will now be applied to the router\*. The amount of time it takes for the firmware to upgrade will depend on the router that's being upgraded.

### Firmware Upgrade

It may take up to 8 minutes.



**\*Upgrading the firmware will cause the router to reboot.**

### 28.2.3 The InControl method

[Described in this knowledgebase article on our forum.](#)

## 28.3 Time



**Time Settings** enables the system clock of the Pepwave router to be synchronized with a specified time server. Time settings are located at **System>Time**.

Time Settings	
Time Zone	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, Lon ▼ <input type="checkbox"/> Show all
Time Server	0.pepwave.pool.ntp.org <span>Default</span>
<span>Save</span>	

Time Settings	
<b>Time Zone</b>	This specifies the time zone (along with the corresponding Daylight Savings Time scheme). The <b>Time Zone</b> value affects the time stamps in the Pepwave router's event log and e-mail notifications. Check <b>Show all</b> to show all time zone options.
<b>Time Server</b>	This setting specifies the NTP network time server to be utilized by the Pepwave router.

## 28.4 Schedule

Enable and disable different functions (such as WAN connections, outbound policy, and firewalls at different times, based on a user-scheduled configuration profile. The settings for this are located at **System > Schedule**

Schedule			
Enabled			
Name	Time	Used by	
Weekdays Only	Weekdays only	-	
<span>New Schedule</span>			

Enable scheduling, and then click on your schedule name or on the **New Schedule** button to begin.

[illegible]

Edit Schedule Profile	
Enabling	Click this checkbox to enable this schedule profile. Note that if this is disabled, then any associated features will also have their scheduling disabled.
Name	Enter your desired name for this particular schedule profile.
Schedule	Click the drop-down menu to choose pre-defined schedules as your starting point. Please note that upon selection, previous changes on the schedule map will be deleted.
Schedule Map	Click on the desired times to enable features at that time period. You can hold your mouse for faster entry.

## 28.5 Email Notification

Email notification functionality provides a system administrator with up-to-date information on network status. The settings for configuring email notifications are found at **System>Email Notification**.

Email Notification Setup	
Email Notification	<input checked="" type="checkbox"/> Enable
SMTP Server	smtp.mycompany.com <input checked="" type="checkbox"/> Require authentication
SSL Encryption	<input checked="" type="checkbox"/> (Note: any server certificate will be accepted)
SMTP Port	465 <span>Default</span>
SMTP User Name	smtpuser
SMTP Password	•••••
Confirm SMTP Password	•••••
Sender's Email Address	idmin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

[Test Email Notification](#)
[Save](#)

Email Notification Settings	
<b>Email Notification</b>	This setting specifies whether or not to enable email notification. If <b>Enable</b> is checked, the Pepwave router will send email messages to system administrators when the WAN status changes or when new firmware is available. If <b>Enable</b> is not checked, email notification is disabled and the Pepwave router will not send email messages.
<b>SMTP Server</b>	This setting specifies the SMTP server to be used for sending email. If the server requires authentication, check <b>Require authentication</b> .
<b>SSL Encryption</b>	Check the box to enable SMTPS. When the box is checked, <b>SMTP Port</b> will be changed to <b>465</b> automatically.
<b>SMTP Port</b>	This field is for specifying the SMTP port number. By default, this is set to <b>25</b> ; when <b>SSL Encryption</b> is checked, the default port number will be set to <b>465</b> . You may customize the port number by editing this field. Click <b>Default</b> to restore the number to its default setting.
<b>SMTP User Name / Password</b>	This setting specifies the SMTP username and password while sending email. These options are shown only if <b>Require authentication</b> is checked in the <b>SMTP Server</b> setting.
<b>Confirm SMTP Password</b>	This field allows you to verify and confirm the new administrator password.
<b>Sender's Email Address</b>	This setting specifies the email address the Pepwave router will use to send reports.
<b>Recipient's Email Address</b>	This setting specifies the email address(es) to which the Pepwave router will send email notifications. For multiple recipients, separate each email addresses using the

enter key.

After you have finished setting up email notifications, you can click the **Test Email Notification** button to test the settings before saving. After **Test Email Notification** is clicked, you will see this screen to confirm the settings:

Test Email Notification	
SMTP Server	smtp.mycompany.com
SMTP Port	465
SMTP UserName	smtpuser
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

Click **Send Test Notification** to confirm. In a few seconds, you will see a message with detailed test results.

Test email sent. Email notification settings are not saved, it will be saved after clicked the 'Save' button.

### Test Result

```
[INFO] Try email through connection #3
[<-] 220 ESMTP
[->] EHLO balance
[<-] 250-smtp Hello balance [210.210.210.210]
250-SIZE 1000000000
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250-UTF8
```


## 28.6 Event Log

Event log functionality enables event logging at a specified remote syslog server. The settings for configuring the remote system log can be found at **System>Event Log**.

Send Events to Remote Syslog Server	
Remote Syslog	<input checked="" type="checkbox"/>
Remote Syslog Host	<input type="text"/>

Push Events to Mobile Devices	
Push Events	<input checked="" type="checkbox"/>

Event Log Settings	
<b>Remote Syslog</b>	This setting specifies whether or not to log events at the specified remote syslog server.
<b>Remote Syslog Host</b>	This setting specifies the IP address or hostname of the remote syslog server.
<b>Push Events</b>	The Pepwave router can also send push notifications to mobile devices that have our Mobile Router Utility installed. Check the box to activate this feature.
	For more information on the Router Utility, go to: <a href="http://www.peplink.com/products/router-utility">www.peplink.com/products/router-utility</a>

## 28.7 SNMP

SNMP or simple network management protocol is an open standard that can be used to collect information about the Pepwave router. SNMP configuration is located at **System>SNMP**.

SNMP Settings	
SNMP Device Name	MAX_HD2_8D1C
SNMP Port	161 <input type="button" value="Default"/>
SNMPv1	<input type="checkbox"/> Enable
SNMPv2c	<input type="checkbox"/> Enable
SNMPv3	<input type="checkbox"/> Enable
<input type="button" value="Save"/>	

Community Name	Allowed Source Network	Access Mode
No SNMPv1 / SNMPv2c Communities Defined		
<input type="button" value="Add SNMP Community"/>		

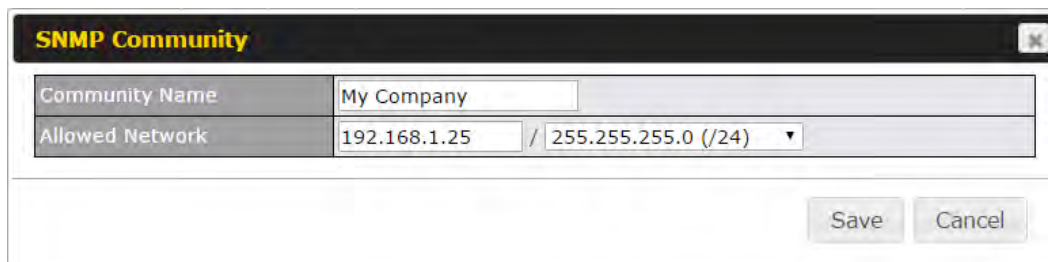
SNMPv3 User Name	Authentication / Privacy	Access Mode
No SNMPv3 Users Defined		
<input type="button" value="Add SNMP User"/>		

SNMP Settings	
<b>SNMP Device Name</b>	This field shows the router name defined at <b>System&gt;Admin Security</b> .
<b>SNMP Port</b>	This option specifies the port which SNMP will use. The default port is <b>161</b> .

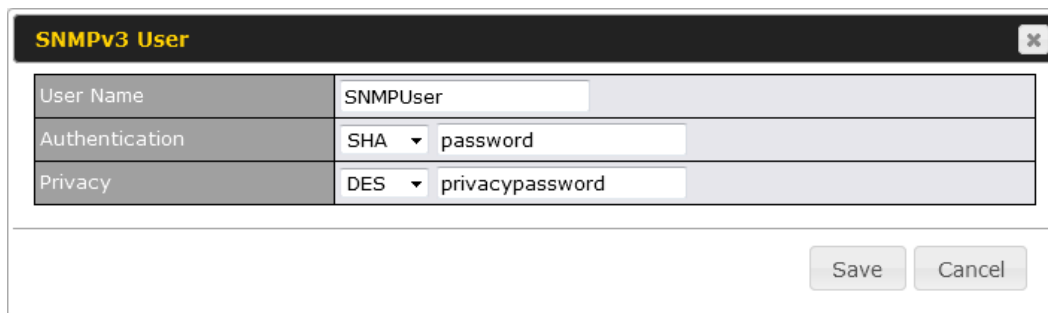


<b>SNMPv1</b>	This option allows you to enable SNMP version 1.
<b>SNMPv2</b>	This option allows you to enable SNMP version 2.
<b>SNMPv3</b>	This option allows you to enable SNMP version 3.

To add a community for either SNMPv1 or SNMPv2, click the **Add SNMP Community** button in the **Community Name** table, upon which the following screen is displayed:



The dialog box is titled "SNMP Community". It contains two input fields: "Community Name" with the value "My Company" and "Allowed Network" with the value "192.168.1.25 / 255.255.255.0 (/24)". At the bottom right, there are "Save" and "Cancel" buttons.



The dialog box is titled "SNMPv3 User". It contains three input fields: "User Name" with the value "SNMPUser", "Authentication" with a dropdown menu set to "SHA" and a text field with "password", and "Privacy" with a dropdown menu set to "DES" and a text field with "privacypassword". At the bottom right, there are "Save" and "Cancel" buttons.

SNMP Community Settings	
<b>Community Name</b>	This setting specifies the SNMP community name.
<b>Allowed Source Subnet Address</b>	This setting specifies a subnet from which access to the SNMP server is allowed. Enter subnet address here (e.g., 192.168.1.0) and select the appropriate subnet mask.

To define a user name for SNMPv3, click **Add SNMP User** in the **SNMPv3 User Name** table, upon which the following screen is displayed:

SNMPv3 User Settings	
<b>User Name</b>	This setting specifies a user name to be used in SNMPv3.
<b>Authentication Protocol</b>	This setting specifies via a drop-down menu one of the following valid authentication protocols:

	<ul style="list-style-type: none"> <li>• NONE</li> <li>• MD5</li> <li>• SHA</li> </ul> <p>When MD5 or SHA is selected, an entry field will appear for the password.</p>
<b>Privacy Protocol</b>	<p>This setting specifies via a drop-down menu one of the following valid privacy protocols:</p> <ul style="list-style-type: none"> <li>• NONE</li> <li>• DES</li> </ul> <p>When DES is selected, an entry field will appear for the password.</p>

## 28.8 InControl

InControl Management	
InControl Management	<input checked="" type="checkbox"/> Allow InControl Management
Privately Host InControl	<input checked="" type="checkbox"/>
InControl Host	<input type="text"/>

InControl is a cloud-based service which allows you to manage all of your Peplink and Pepwave devices with one unified system. With it, you can generate reports, gather statistics, and configure your devices automatically. All of this is now possible with InControl.

When this check box is checked, the device's status information will be sent to the Peplink InControl system. This device's usage data and configuration will be sent to the system if you enable the features in the system.

Alternately, you could also privately host InControl. Simply check the box beside the "Privately Host InControl" open, and enter the IP Address of your InControl Host.

You can sign up for an InControl account at <https://incontrol2.peplink.com/>. You can register your devices under the account, monitor their status, see their usage reports, and receive offline notifications.

## 28.9 Configuration

Backing up Pepwave router settings immediately after successful completion of initial setup is strongly recommended. The functionality to download and upload Pepwave router settings is found at **System>Configuration**. Note that available options vary by model.

Restore Configuration to Factory Settings ?

Restore Factory Settings

Download Active Configurations ?

Download

Upload Configurations ?

Configuration File  No file selected.

Upload

Upload Configurations from High Availability Pair ?

Configuration File  No file selected.

Upload

Configuration	
<b>Restore Configuration to Factory Settings</b>	The <b>Restore Factory Settings</b> button is to reset the configuration to factory default settings. After clicking the button, you will need to click the <b>Apply Changes</b> button on the top right corner to make the settings effective.
<b>Download Active Configurations</b>	Click <b>Download</b> to backup the current active settings.
<b>Upload Configurations</b>	To restore or change settings based on a configuration file, click <b>Choose File</b> to locate the configuration file on the local computer, and then click <b>Upload</b> . The new settings can then be applied by clicking the <b>Apply Changes</b> button on the page header, or you can cancel the procedure by pressing <b>discard</b> on the main page of the web admin interface.
<b>Upload Configurations from High Availability Pair</b>	In a high availability (HA) configuration, a Pepwave router can quickly load the configuration of its HA counterpart. To do so, click the <b>Upload</b> button. After loading the settings, configure the LAN IP address of the Pepwave router so that it is different from the HA counterpart.

## 28.10 Feature Add-ons

Some Pepwave routers have features that can be activated upon purchase. Once the purchase is complete, you will receive an activation key. Enter the key in the **Activation Key** field, click **Activate**, and then click **Apply Changes**.

Feature Activation

Activation Key

## 28.11 Reboot

This page provides a reboot button for restarting the system. For maximum reliability, the Pepwave router can equip with two copies of firmware. Each copy can be a different version. You can select the firmware version you would like to reboot the device with. The firmware marked with **(Running)** is the current system boot up firmware.

**Please note that a firmware upgrade will always replace the inactive firmware partition.**

Reboot System

Select the firmware you want to use to start up this device:


☒ Firmware 1: 6.2.1 build 2977 (Running)
 ☐ Firmware 2: 6.2.1b01 build 2949

Reboot

## 29 Tools

### 29.1 Ping

The ping test tool sends pings through a specific Ethernet interface or a SpeedFusion™ VPN connection. You can specify the number of pings in the field **Number of times**, to a maximum number of 10 times. **Packet Size** can be set to a maximum of 1472 bytes. The ping utility is located at **System>Tools>Ping**, illustrated below:

Ping	
Connection	WAN 1 ▼
Destination	10.10.10.1
Packet Size	56
Number of times	Times 5 
<div>Start Stop</div>	

Results	Clear Log
PING 10.10.10.1 (10.10.10.1) from 10.88.3.158 56(84) bytes of data.	
64 bytes from 10.10.10.1: icmp_req=1 ttl=62 time=27.6 ms	
64 bytes from 10.10.10.1: icmp_req=2 ttl=62 time=26.5 ms	
64 bytes from 10.10.10.1: icmp_req=3 ttl=62 time=28.9 ms	
64 bytes from 10.10.10.1: icmp_req=4 ttl=62 time=28.3 ms	
64 bytes from 10.10.10.1: icmp_req=5 ttl=62 time=27.7 ms	
---	
--- 10.10.10.1 ping statistics ---	
5 packets transmitted, 5 received, 0% packet loss, time 4005ms	
rtt min/avg/max/mdev = 26.516/27.855/28.933/0.814 ms	

### Tip

A system administrator can use the ping utility to manually check the connectivity of a particular LAN/WAN connection.

## 29.2 Traceroute Test

The traceroute test tool traces the routing path to the destination through a particular Ethernet interface or a SpeedFusion™ connection. The traceroute test utility is located at **System>Tools>Traceroute**.

**Tip**

A system administrator can use the traceroute utility to analyze the connection path of a LAN/WAN connection.

### 29.3 PepVPN Test

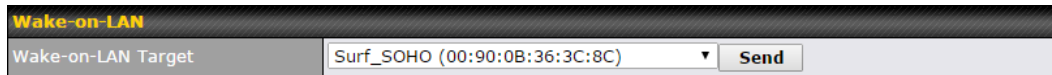
The **PepVPN Test** tool can help to test the throughput between different VPN peers.

You can define the **Test Type**, **Direction**, and **Duration** of the test, and press **Go!** to perform the throughput test. The VPN test utility is located at **System>Tools>PepVPN Test**, illustrated as follows:

PepVPN Throughput Test	
Profile	NY Office ▾
Type	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
Direction	<input checked="" type="radio"/> Upload <input type="radio"/> Download
Duration	10 seconds (5 - 600)
<input type="button" value="Go!"/>	
Results	
(Empty)	

## 29.4 Wake-on-LAN

Peplink routers can send special “magic packets” to any client specified from the Web UI. To access this feature, navigate to **System > Tools > Wake-on-LAN**



Select a client from the drop-down list and click **Send** to send a “magic packet”

## 29.5 CLI (Command Line Interface Support)

The CLI (command line interface) can be accessed via SSH. This field enables CLI support. The below settings specify which TCP port and which interface(s) should accept remote SSH CLI access. The user name and password used for remote SSH CLI access are the same as those used for web admin access.





## 30 Status

### 30.1 Device

System information is located at **Status>Device**.

System Information	
Router Name	MBX-345A
Model	Pepwave MAX HD4 MBX
Product Code	MAX-HD4-MBX-LTEA-R
Hardware Revision	2
Serial Number	[REDACTED]
Firmware	8.0.0 build 1218
PepVPN Version	8.0.0
Modem Support Version	1023 ( <a href="#">Modem Support List</a> )
InControl Managed Configurations	Firmware, LAN
Host Name	mbx-345a
Uptime	3 days 3 minutes
System Time	Fri Mar 22 13:57:08 GMT 2019
OpenVPN Client Profile	<a href="#">Route all traffic</a>   <a href="#">Split tunnel</a>
Diagnostic Report	<a href="#">Download</a>
Remote Assistance	<a href="#">Turn On</a>


  

MAC Address	
LAN	00:1A: [REDACTED]
WAN 1	00:1A: [REDACTED]
WAN 2	00:1A: [REDACTED]
WAN 3	00:1A: [REDACTED]


[Legal](#)

System Information	
<b>Router Name</b>	This is the name specified in the <b>Router Name</b> field located at <b>System&gt;Admin Security</b> .
<b>Model</b>	This shows the model name and number of this device.
<b>Product Code</b>	If your model uses a product code, it will appear here.
<b>Hardware</b>	This shows the hardware version of this device.

<b>Revision</b>	
<b>Serial Number</b>	This shows the serial number of this device.
<b>Firmware</b>	This shows the firmware version this device is currently running.
<b>PepVPN Version</b>	This shows the current PepVPN version.
<b>Modem Support Version</b>	This shows the modem support version. For a list of supported modems, click <b>Modem Support List</b> .
<b>InControl Managed Configuration</b>	InControl Managed Configurations (firmware, VLAN, Captive Portal, etcetera)
<b>Host Name</b>	The host name assigned to the Pepwave router appears here.
<b>Uptime</b>	This shows the length of time since the device has been rebooted.
<b>System Time</b>	This shows the current system time.
<b>OpenVPN Client Profile</b>	Link to download OpenVpn Client profile when this is enabled in Remote User Access
<b>Diagnostic Report</b>	The <b>Download</b> link is for exporting a diagnostic report file required for system investigation.
<b>Remote Assistance</b>	Click <b>Turn on</b> to enable remote assistance.

The second table shows the MAC address of each LAN/WAN interface connected. To view your device's End User License Agreement (EULA), click  [Legal](#).

## 30.2 GPS Data

GPX File		2019-03-22 (Today) ▾	<b>Download</b>
Diagnostic Report		2019-03-22 (Today)	
Remote Assistance		2019-03-21	
		2019-03-20	
		2019-03-19	
<b>MAC Address</b>		2019-03-18	
		2019-03-17	
LAN		2019-03-16	

GPS enabled models automatically store up to seven days of GPS location data in GPS eXchange format (GPX). To review this data using third-party applications, click **Status>Device** and then download your GPX file.

The Pepwave GPS enabled devices export real-time location data in NMEA format through the LAN IP address at TCP port 60660. It is accessible from the LAN or over a SpeedFusion connection. To access the data via a virtual serial port, install a virtual serial port driver. Visit <http://www.peplink.com/index.php?view=faq&id=294> to download the driver.

### 30.3 Active Sessions

Information on active sessions can be found at **Status>Active Sessions>Overview**.

Overview	Search
----------	--------

Session data captured within one minute. [Refresh](#)

Service	Inbound Sessions	Outbound Sessions
<a href="#">AIM/ICQ</a>	0	1
<a href="#">Bittorrent</a>	0	32
<a href="#">DNS</a>	0	51
<a href="#">Flash</a>	0	1
<a href="#">HTTPS</a>	0	76
<a href="#">Jabber</a>	0	5
<a href="#">MSN</a>	0	11
<a href="#">NTP</a>	0	4
<a href="#">QQ</a>	0	1
<a href="#">Remote Desktop</a>	0	3
<a href="#">SSH</a>	0	12
<a href="#">SSL</a>	0	64
<a href="#">XMPP</a>	0	4
<a href="#">Yahoo</a>	0	1

Interface	Inbound Sessions	Outbound Sessions
<a href="#">WAN 1</a>	0	176
<a href="#">WAN 2</a>	0	32
<a href="#">Wi-Fi WAN</a>	0	51
<a href="#">Cellular 1</a>	0	64
<a href="#">Cellular 2</a>	0	0
<a href="#">USB</a>	0	0

**Top Clients**

Client IP Address	Total Sessions
10.9.66.66	1069
10.9.98.144	147
10.9.2.18	63
10.9.66.14	56
10.9.2.26	33

This screen displays the number of sessions initiated by each application. Click on each service listing for additional information. This screen also indicates the number of sessions initiated by each WAN port. In addition, you can see which clients are initiating the most sessions.

You can also perform a filtered search for specific sessions. You can filter by subnet, port, protocol, and interface. To perform a search, navigate to **Status>Active Sessions>Search**.

Overview
Search

Session data captured within one minute. [Refresh](#)

IP / Subnet
Source or Destination
255.255.255.255 (/32)

Port
Source or Destination

Protocol / Service
TCP

Interface

☐ WAN 1
☐ WAN 2
☐ Wi-Fi WAN

☐ Cellular 1
☐ Cellular 2
☐ USB

☐ VPN

Search

Outbound

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

Total searched results: 0

Inbound

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

Total searched results: 0

Transit


Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

Total searched results: 0

This **Active Sessions** section displays the active inbound/outbound sessions of each WAN connection on the Pepwave router. A filter is available to sort active session information. Enter a keyword in the field or check one of the WAN connection boxes for filtering.

## 30.4 Client List

The client list table is located at **Status>Client List**. It lists DHCP and online client IP addresses, names (retrieved from the DHCP reservation table or defined by users), current download and upload rate, and MAC address.

Clients can be imported into the DHCP reservation table by clicking the  button on the right. You can update the record after import by going to **Network>LAN**.

Filter

☐ Online Clients Only

☐ DHCP Clients Only

Client List

IP Address

Name

Download (kbps)

Upload (kbps)

MAC Address

Import

192.168.1.100

0

0

00:50:56:99:E1:76

Scale: 

kbps

Mbps

If the PPTP server (see **Section 19.2**), SpeedFusion™ (see **Section 12.1**), or AP controller (see **Section 20**) is enabled, you may see the corresponding connection name listed in the **Name** field.

## 30.5 WINS Client

The WINS client list table is located at **Status>WINS Client**.








WINS Client List	
Name ▲	IP Address
UserA	10.9.2.1
UserB	10.9.30.1
UserC	10.9.2.4


The WINS client table lists the IP addresses and names of WINS clients. This option will only be available when you have enabled the WINS server (navigation: **Network>Interfaces>LAN**). The names of clients retrieved will be automatically matched into the Client List (see previous section). Click **Flush All** to flush all WINS client records.

WINS Client List	
Name ▲	IP Address
UserA	10.9.2.1
UserB	10.9.30.1
UserC	10.9.2.4


## 30.6 UPnP / NAT-PMP

The table that shows the forwarded ports under UPnP and NAT-PMP protocols is located at **Status>UPnP/NAT-PMP**. This section appears only if you have enabled UPnP / NAT-PMP as mentioned in **Section 16.1.1**.

Forwarded Ports						
External	Internal	Internal Address	Type	Protocol	Description	
47453	3392	192.168.1.100	UPnP	UDP	Application 031	
35892	11265	192.168.1.50	NAT-PMP	TCP	NAT-PMP 58	
4500	3560	192.168.1.20	UPnP	TCP	Application 013	
5921	236	192.168.1.30	UPnP	TCP	Application 047	
22409	8943	192.168.1.70	NAT-PMP	UDP	NAT-PMP 97	
2388	27549	192.168.1.40	UPnP	TCP	Application 004	
						

Click  to delete a single UPnP / NAT-PMP record in its corresponding row. To delete all records, click **Delete All** on the right-hand side below the table.

### Important Note

UPnP / NAT-PMP records will be deleted immediately after clicking the button  or **Delete All**, without the need to click **Save** or **Confirm**.

## 30.7 OSPF & RIPv2

Shows status of OSPF and RIPv2

peplink

Dashboard

Setup Wizard

Network

AP

System

Status

Apply Changes

Status

■ Device

■ Active Sessions

■ Client List

■ OSPF & RIPv2

■ BGP

OSPF & RIPv2

Area

Remote Networks

0.0.0.0

PepVPN

10.0.2.0/24 10.0.3.0/24 192.168.63.0/24 10.0.100.0/24 192.168.100.0/24 192.168.162.0/24

## 30.8 BGP

Shows status of BGP



## 30.9 SpeedFusion Status

Current SpeedFusion™ status information is located at **Status>SpeedFusion™**.

Details about SpeedFusion™ connection peers appears as below:

PepVPN with SpeedFusion - Remote Peer Details			<input type="checkbox"/> Show disconnected profiles
Search	<input type="text"/>		
Remote Peer ▲	Profile	Information	
▶ ADA0-FFFC-11F8	FH	192.168.77.0/24	
▶ 3ED2-8F63-1824	380-5 - NO NAT	192.168.3.0/24	

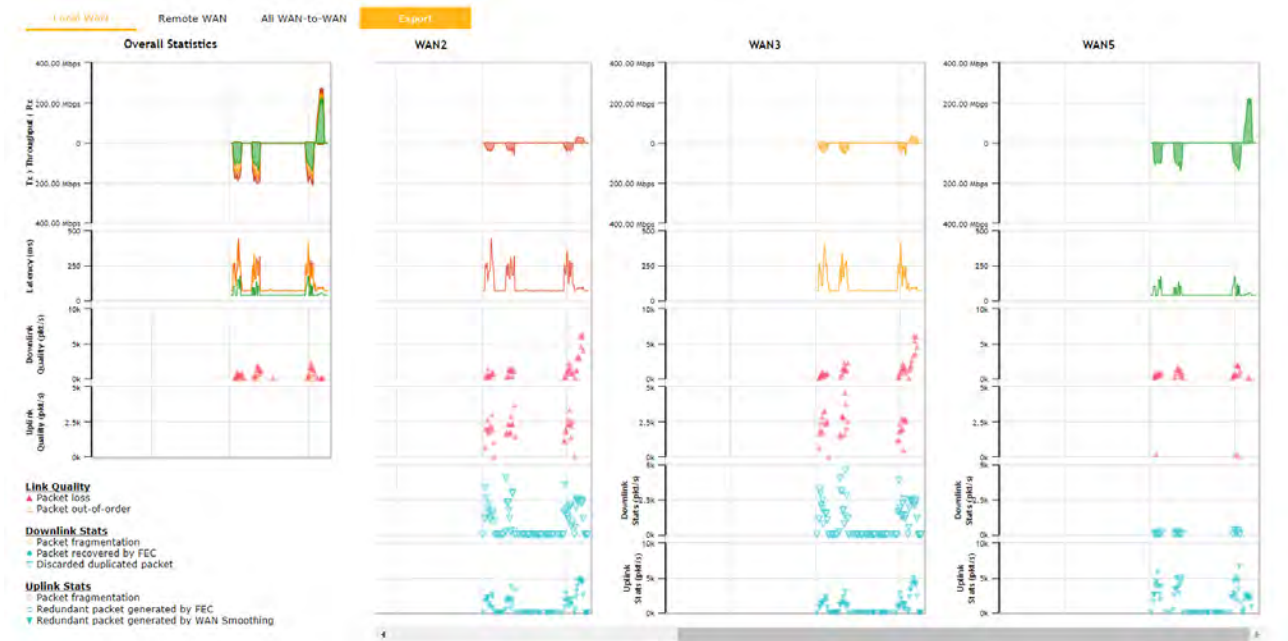
Click on the corresponding peer name to explore the WAN connection(s) status and subnet information of each VPN peer.

PepVPN with SpeedFusion - Remote Peer			<input type="checkbox"/> Show all profiles
Search	<input type="text" value="SFC"/>		
Remote Peer ▲	Profile	Information	
▼ SFC-SIN-001 (SFC-SIN-001)	SFC	SpeedFusion Cloud	
WAN1		Not available - WAN disabled	
WAN2	Rx: < 1 kbps Tx: < 1 kbps	Loss rate: 0.0 pkt/s Latency: 42 ms	
WAN3	Rx: < 1 kbps Tx: < 1 kbps	Loss rate: 0.0 pkt/s Latency: 42 ms	
WAN4		Not available - WAN disabled	
WAN5	Rx: < 1 kbps Tx: < 1 kbps	Loss rate: 0.0 pkt/s Latency: 10 ms	
Mobile Internet	Rx: < 1 kbps Tx: < 1 kbps	Loss rate: 0.0 pkt/s Latency: 32 ms	
Total	Rx: < 1 kbps Tx: 1.1 kbps	Loss rate: 0.0 pkt/s	

Click the button for a SpeedFusion chart displaying real-time throughput, latency, and



drop-rate information for each WAN connection.



When pressing the  button, the following menu will appear:

PepVPN Details

Connection Information
More information

Profile	SFC
Remote ID	SFC-SIN-001
Device Name	SFC-SIN-001
Serial Number	1197-A047-2E3D

WAN Statistics

Remote Connections
Show remote connections

WAN Label
WAN Name IP Address and Port

WAN1	Not available - WAN disabled				
WAN2	Rx: < 1 kbps	Tx: < 1 kbps	Loss rate: 0.0 pkt/s	Latency: 43 ms	
WAN3	Rx: < 1 kbps	Tx: < 1 kbps	Loss rate: 0.0 pkt/s	Latency: 44 ms	
WAN4	Not available - WAN disabled				
WAN5	Rx: < 1 kbps	Tx: < 1 kbps	Loss rate: 0.0 pkt/s	Latency: 10 ms	
Mobile Internet	Rx: < 1 kbps	Tx: < 1 kbps	Loss rate: 0.0 pkt/s	Latency: 42 ms	
Total	Rx: < 1 kbps	Tx: < 1 kbps	Loss rate: 0.0 pkt/s		

PepVPN Test Configuration

Type
TCP UDP

Streams
4

Direction
Upload Download

Duration
20 seconds (5 - 600)

Start

The Speedfusion status page shows all related information about the PepVPN connection. This screen also allows you to run PepVPN Tests allowing throughput tests.

Peplink also published a whitepaper about Speedfusion which can be downloaded from the following url:  
<http://download.peplink.com/resources/whitepaper-speedfusion-and-best-practices-2019.pdf>

## 30.10 Event Log

Event log information is located at **Status>Event Log**.

<https://www.peplink.com>

246

Copyright @ 2020 Pepwave

Device Event Log	
Device Event Log <input checked="" type="checkbox"/> Auto Refresh	
Mar 22 14:29:44	System: Changes applied
Mar 22 14:28:29	System: Changes applied
Mar 22 14:00:26	WAN: Wi-Fi WAN connected to PEPLINK_1 (10.22.1.152)
Mar 22 11:47:45	Admin: DemoPep (10.22.1.160) login successful
Mar 22 11:47:28	Admin: admin (10.22.1.160) login failed
Mar 22 11:46:59	System: Changes applied
Mar 22 11:45:42	System: Changes applied
Mar 20 15:43:27	System: Changes applied
Mar 20 11:20:15	System: Changes applied
Mar 19 15:23:26	System: Changes applied
Mar 19 15:21:35	System: Changes applied
Mar 19 15:21:31	System: InControl has updated the configuration as InControl configuration updated
Mar 19 15:21:31	System: LAN Configuration has been updated by InControl
Mar 19 15:07:38	System: Changes applied
Mar 19 14:09:27	System: WAN Analysis server stopped
Mar 19 14:09:22	System: WAN Analysis server started (control port: 6000, max. streams: 8)
Mar 19 14:05:30	WAN: WAN 2 connected (10.22.1.165)
Mar 19 14:05:30	WAN: WAN 1 connected (10.22.1.151)
Mar 19 14:05:18	WAN: WAN 2 disconnected
Mar 19 14:05:18	WAN: WAN 1 disconnected
Mar 19 14:05:18	System: Changes applied
Mar 19 13:56:31	WAN: WAN 2 connected (10.22.1.165)
Clear Log	

The log section displays a list of events that has taken place on the Pepwave router. Check **Auto Refresh** to refresh log entries automatically. Click the **Clear Log** button to clear the log.

## 31 WAN Quality



The **Status > WAN Quality** allow to show detailed information about each connected WAN connection.

For cellular connections it shows signal strength, quality, throughput and latency for the past hour.

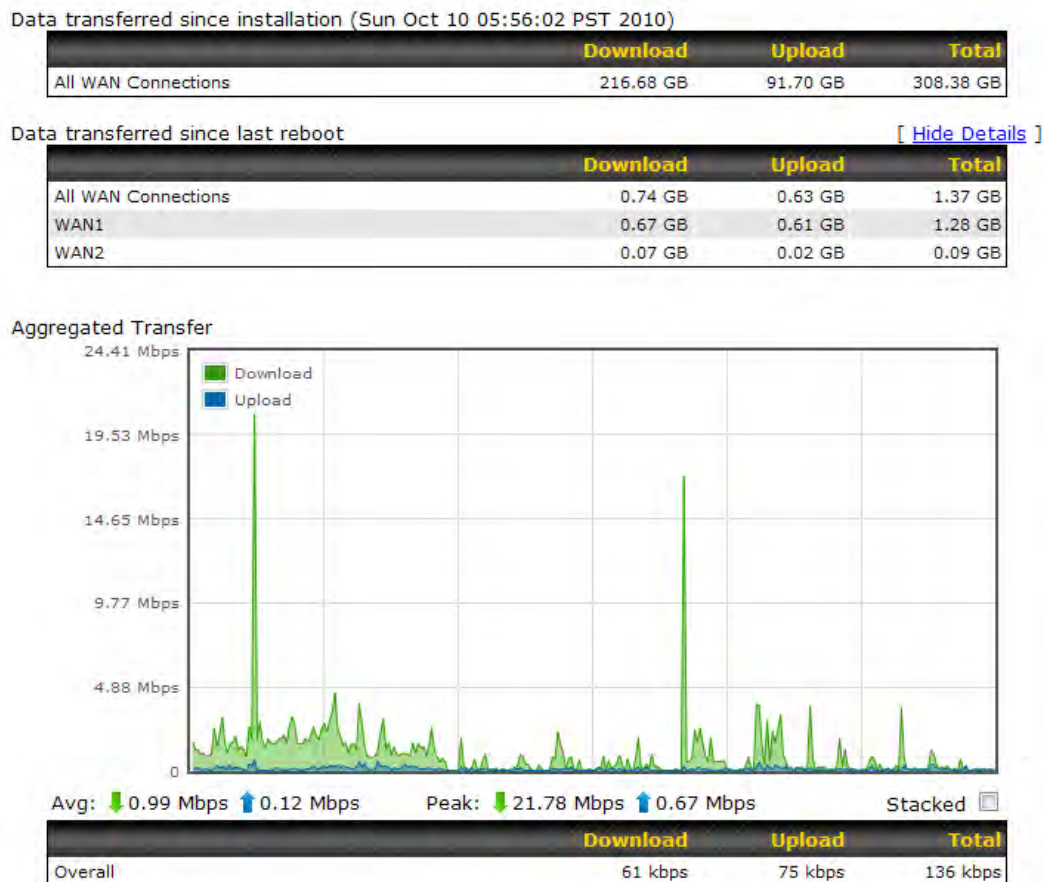
## 32 Usage Reports

This section shows bandwidth usage statistics and is located at **Status > Usage Reports**

Bandwidth usage at the LAN while the device is switched off (e.g., LAN bypass) is neither recorded nor shown.

## 32.1 Real-Time

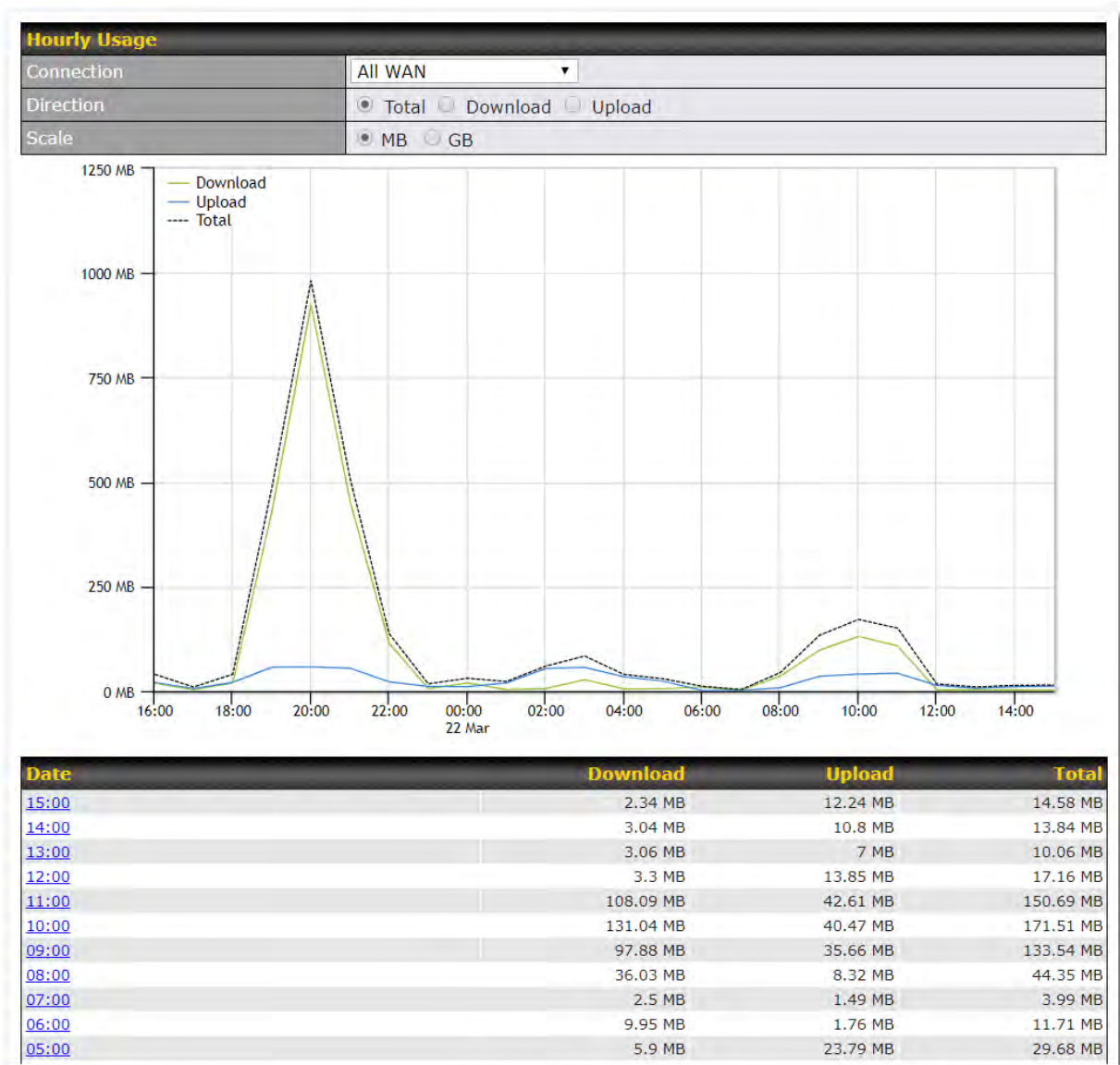
The **Data transferred since installation** table indicates how much network traffic has been processed by the device since the first bootup. The **Data transferred since last reboot** table indicates how much network traffic has been processed by the device since the last bootup.



## 32.2 Hourly

This page shows the hourly bandwidth usage for all WAN connections, with the option of viewing each individual connection. Select the desired connection to check from the drop-down menu.



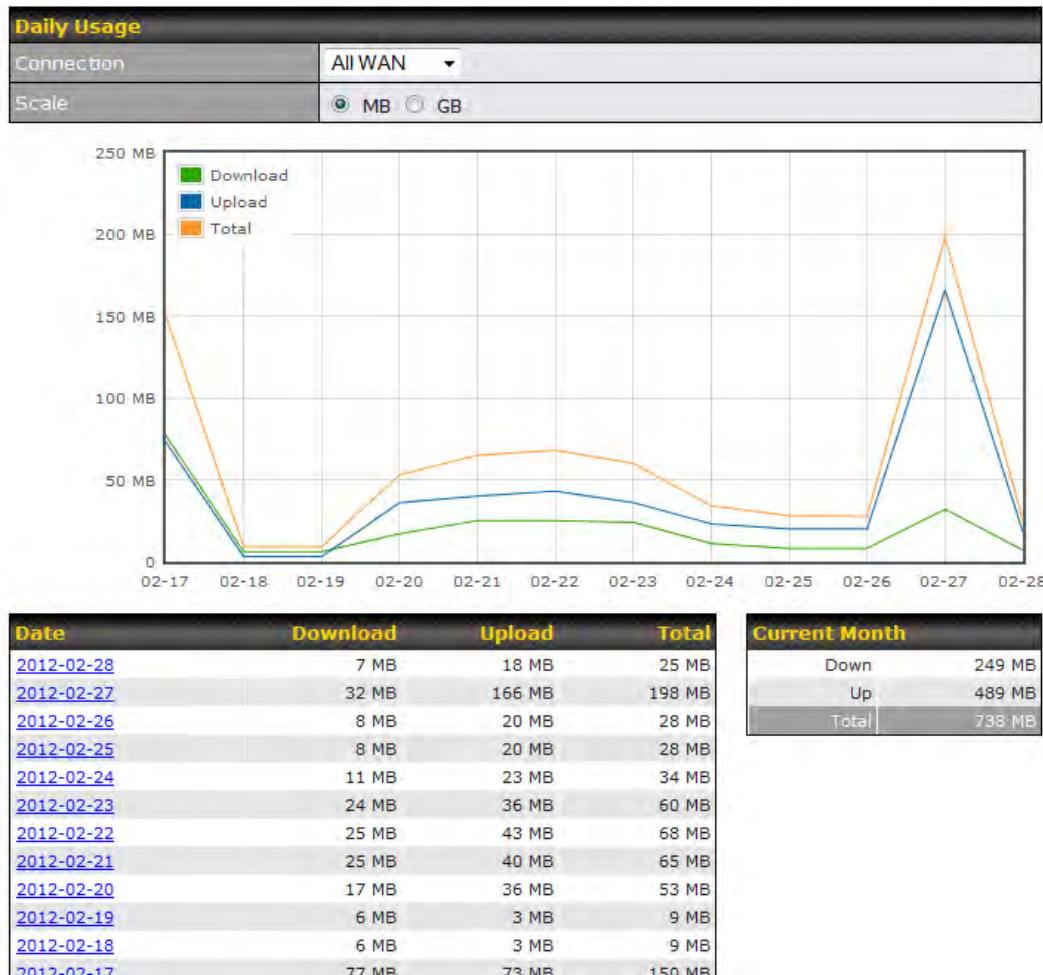


### 32.3 Daily

This page shows the daily bandwidth usage for all WAN connections, with the option of viewing each individual connection.

Select the connection to check from the drop-down menu. If you have enabled the **Bandwidth Monitoring** feature, the **Current Billing Cycle** table for that WAN connection will be displayed.

Click on a date to view the client bandwidth usage of that specific date. This feature is not available if you have selected to view the bandwidth usage of only a particular WAN connection. The scale of the graph can be set to display megabytes (**MB**) or gigabytes (**GB**).



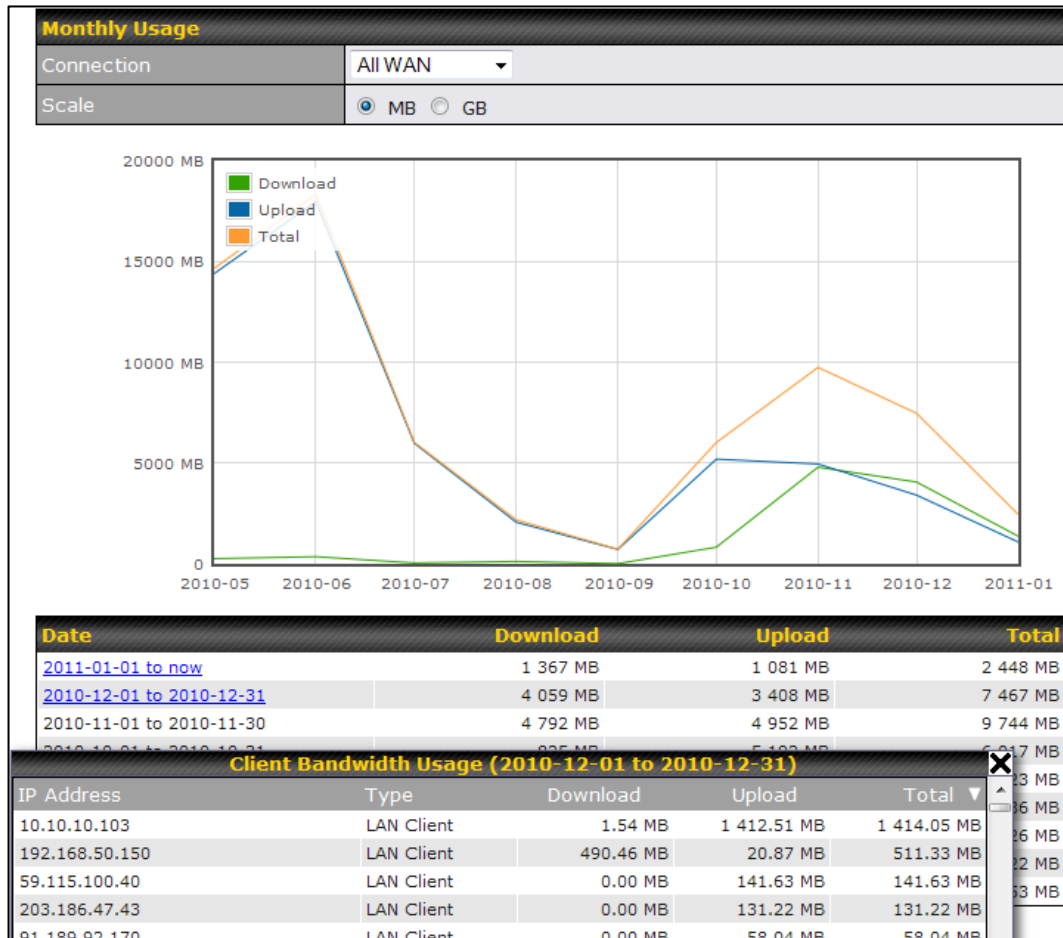
All WAN Daily Bandwidth Usage

## 32.4 Monthly

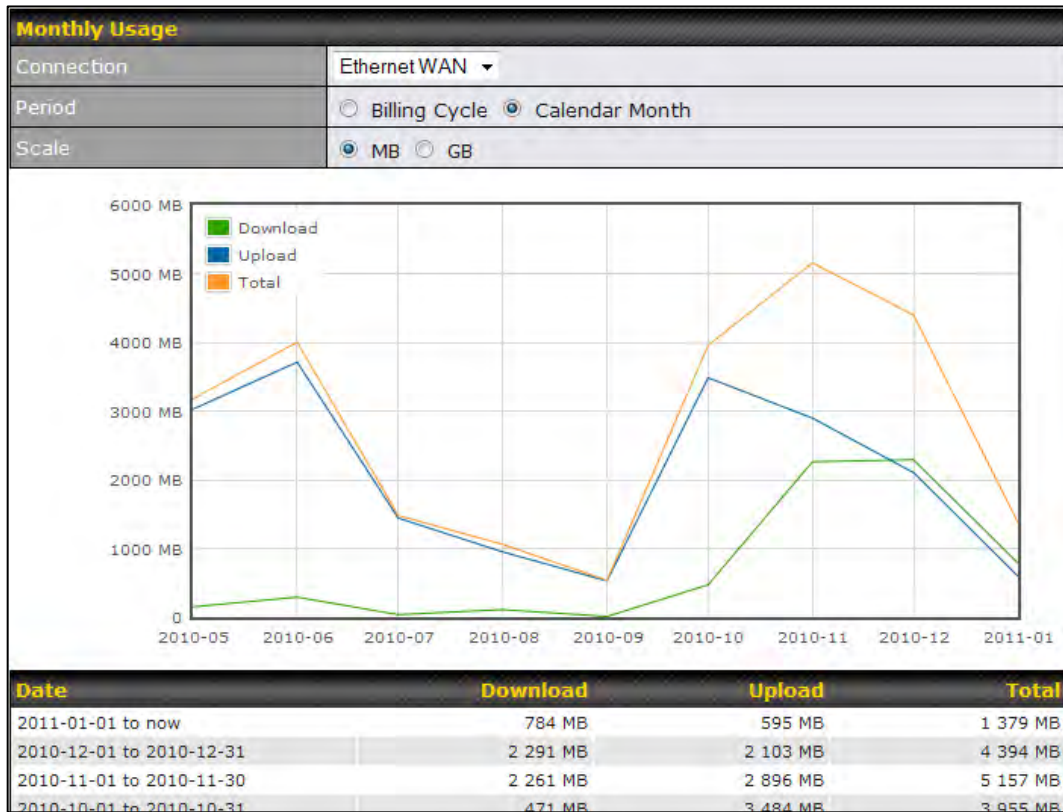
This page shows the monthly bandwidth usage for each WAN connection. If you have enabled the **Bandwidth Monitoring** feature, you can check the usage of each particular connection and view the information by **Billing Cycle** or by **Calendar Month**.

Click the first two rows to view the client bandwidth usage in the last two months. This feature is not available if you have chosen to view the bandwidth of an individual WAN connection. The scale of the graph can be set to display megabytes (**MB**) or gigabytes (**GB**).





All WAN Monthly Bandwidth Usage



Ethernet WAN Monthly Bandwidth Usage

**Tip**

By default, the scale of data size is in **MB**. 1GB equals 1024MB.

## Appendix A: Restoration of Factory Defaults

To restore the factory default settings on a Pepwave router, follow the steps below:

1. Locate the reset button on the front or back panel of the Pepwave router.
2. With a paperclip, press and keep the reset button pressed.

Note: There is a dual function to the reset button.

Hold for 5-10 seconds for admin password reset (Note: The LED status light blinks in RED 2 times and release the button, green status light starts blinking)

Hold for approximately 20 seconds for factory reset (Note: The LED status light blinks in RED 3 times and release the button, all WAN/LAN port lights start blinking)

After the Pepwave router finishes rebooting, the factory default settings will be restored.

### Important Note

All previous configurations and bandwidth usage data will be lost after restoring factory default settings. Regular backup of configuration settings is strongly recommended.



## Appendix B: Declaration

### FCC Requirements for Operation in the United States

## **Federal Communications Commission (FCC) Compliance Notice:**

### **For MAX BR1 Mini**

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

### **FCC Radiation Exposure Statement (for MAX BR1 mini)**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

**The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination.**

#### **1. CE Statement for Pepwave Routers ( MAX BR1 Mini )**

## DECLARATION OF CONFORMITY

We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU.

Name of manufacturer	PISMO LABS TECHNOLOGY LIMITED
Contact information of the manufacturer	A8, 5/F, HK Spinners Industrial. Building., Phase 6, 481 Castle Peak Road, Cheung Sha Wan, Kowloon, Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	PEPWAVE / PEPLINK Wireless Product
Model name of the appliance	MAX BR1 Mini MAX BR1 Mini LTE Pismo930 Lite
Trade name of the appliance	PEPWAVE / PEPLINK

The construction of the appliance is in accordance with the following standards:


EN 301 908-1 V11.1.1  
 EN 300 328 V2.2.2  
 EN 303 413 V1.1.1  
 EN 50385 : 2017  
 EN 301 489-1 V2.2.3  
 EN 301 489-17 V3.1.1  
 Draft EN 301 489-19 V2.1.0  
 EN 55032: 2015  
 EN 55035: 2017  
 EN 61000-3-2: 2014  
 EN 61000-3-3: 2013  
 EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013

Yours sincerely,



Antony Chong  
 Director of Hardware Engineering  
 Peplink International Limited



	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV
	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	

**2.4GHz ( 2412 – 2472 MHz ) : 17.31dBm**

This equipment complies with CE radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator & your body.

**contact as:** <https://www.peplink.com/>



### **Industry Canada Statement (for MAX BR1 Mini)**

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This equipment complies with Innovation, Science and Economic Development Canada RF exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated to ensure a minimum of 20 cm spacing to any person at all times.

Déclaration d'exposition aux radiations: Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

**FCC Requirements for Operation in the United States**  
**Federal Communications Commission (FCC) Compliance Notice:**

**For MAX BR1 MK2**

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

**IMPORTANT NOTE**

**FCC Radiation Exposure Statement (for MAX BR1 MK2)**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 24cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination.

## Industry Canada Statement (for MAX BR1 MK2)

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

To maintain compliance with the RF exposure guidelines, place the unit at least 30cm from nearby persons.

Mise en garde\_: Pour assurer la conformité aux directives relatives à l'exposition aux fréquences radio, le jouet doit être placé à au moins 30\_cm des personnes à proximité.

The device could automatically discontinue transmission in case of absence of information to transmit, or operational failure. Note that this is not intended to prohibit transmission of control or signaling information or the use of repetitive codes where required by the technology. The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems; The maximum antenna gain permitted for devices in the bands

L'appareil peut interrompre automatiquement la transmission en cas d'absence d'informations à transmettre ou de panne opérationnelle. Notez que ceci n'est pas destiné à interdire la transmission d'informations de contrôle ou de signalisation ou l'utilisation de codes répétitifs lorsque cela est requis par la technologie. Le dispositif utilisé dans la bande 5150-5250 MHz est réservé à une utilisation en intérieur afin de réduire le risque de brouillage préjudiciable aux systèmes mobiles par satellite dans le même canal; Le gain d'antenne maximal autorisé pour les dispositifs dans les bandes

This radio transmitter 20682-P1AC4 has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

WIFI Antenna type: Omni-directional

WIFI Antenna gain: 2.4GHz / 2.44 dBi , 5GH / 4.73 dBi

LTE Antenna type: Omni-directional

LTE Antenna gain: 4.38 dBi

**Caution : ( for MAX BR1 MK2 )**

- (i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
- (ii) the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and
- (iii) Users should also be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

**Avertissement: ( for MAX BR1 MK2 )**

- (i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- (ii) le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;
- (iii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

**CE Statement for Pepwave Routers ( MAX BR1 MK2 )**



Peplink International Limited  
A8, 5/F, HK Spinners Industrial Building  
Phase 6, 481 Castle Peak Road  
Cheung Sha Wan  
Hong Kong

September 6, 2017

## DECLARATION OF CONFORMITY

We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU.

Name of manufacturer	Pismo Labs Technology Limited
Contact information of the manufacturer	A8, 5/F, HK Spinners Ind. Bldg., Phase 6, 481 Castle Peak Road, Cheung Sha Wan, Kowloon, Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	Pepwave / Peplink / Pismo Wireless Product
Model name of the appliance	MAX BR1 MK2
Trade name of the appliance	Pepwave / Peplink / Pismo



The construction of the appliance is in accordance with the following standards:

EN 300 328 V2.1.1  
 EN 301 893 V2.1.1  
 EN 303 413 V1.1.1  
 EN 301 908-1 V11.1.1  
 EN 301 489-1 V2.1.1  
 Draft EN 301 489-17 V3.2.0  
 Draft EN 301 489-19 V2.1.0  
 Draft EN 301 489-52 V1.1.0  
 EN 55032:2015 +AC: 2016, Class A  
 EN 61000-3-2: 2014, Class A  
 EN 61000-3-3: 2013  
 EN 62311:2008  
 EN 60950-1:2006+A11: 2009+A1:2010+A12:2011+A2:2013  
 EN 55024:2010+A1:2015

Yours sincerely,

Keith Chau  
 General Manager  
 Peplink International Limited

	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV
	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	

**2.4GHz ( 2412 – 2472 MHz ) : 19.95 dBm**

**5GHz ( 5150 - 5250 MHz ) : 22.73 dBm**

This equipment complies with CE radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator & your body.

**contact as: <https://www.peplink.com/>**



**FCC Requirements for Operation in the United States**  
**Federal Communications Commission (FCC) Compliance Notice:**

**For MAX BR1 Classic**

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

**FCC Radiation Exposure Statement (for MAX BR1 Classic )**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## Industry Canada Statement ( for MAX BR1 Classic )

This device complies with Industry Canada's licence-exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause interference; and (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

This equipment complies with Innovation, Science and Economic Development Canada RF exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated to ensure a minimum of 20 cm spacing to any person at all times.

Déclaration d'exposition aux radiations: Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

This radio transmitter has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Antenna types: Replacement Antenna  
gain (in dBi): 5.33 dBi

Innovation, Sciences et Développement économique Canada a approuvé l'utilisation de ce transmetteur radio avec les types d'antenne énumérés ci-dessous, le gain maximal admissible étant indiqué. Les types d'antennes non inclus dans cette liste qui ont un gain supérieur au gain maximal indiqué pour tout type listé sont strictement interdits pour une utilisation avec cet appareil.

Types d'antennes: Replacement Antenna  
Gain d'antenne (en dBi): 5.33 dBi

**CE Statement for Pepwave Routers ( MAX BR1 Classic )**

## DECLARATION OF CONFORMITY

We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU.

Name of manufacturer	PISMO LABS TECHNOLOGY LIMITED
Contact information of the manufacturer	A8, 5/F, HK Spinners Industrial. Building., Phase 6, 481 Castle Peak Road, Cheung Sha Wan, Kowloon, Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	PEPWAVE / PEPLINK Wireless Product
Model name of the appliance	MAX BR1 ESN MAX BR1 ESN LTEA Pepwave MAX BR1 ESN Pepwave MAX BR1 ESN LTEA Peplink MAX BR1 ESN Peplink MAX BR1 ESN LTEA Pismo930 Lite MAX-BR1-ESN-LTEA-W-T MAX BR1 Classic MAX BR1 Classic LTEA Pepwave MAX BR1 Classic Pepwave MAX BR1 Classic LTEA Peplink MAX BR1 Classic Peplink MAX BR1 Classic LTEA MAX-BR1-LTEA-W-T MAX BR1 MAX BR1 LTEA Pepwave MAX BR1 Pepwave MAX BR1 LTEA
Trade name of the appliance	PEPWAVE / PEPLINK


The construction of the appliance is in accordance with the following standards:

EN 301 908-1 V13.1.1  
 EN 300 328 V2.2.2  
 EN 303 413 V1.1.1  
 EN 62311 : 2008  
 EN 301 489-1 V2.2.3  
 Draft EN 301 489-17 V3.2.0  
 EN 301 489-19 V2.1.1  
 Draft EN 301 489-52 V1.1.0  
 EN 55032: 2015 + AC:2016-07  
 EN 55035: 2017  
 EN 61000-3-2: 2014  
 EN 61000-3-3: 2013  
 EN 62368-1:2014 + A11:2017

Yours sincerely,




Antony Chong  
 Director of Hardware Engineering  
 Peplink International Limited

	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV
	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	

**2.4GHz ( 2412 – 2472 MHz ) : 19.78 dBm**

This equipment complies with CE radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator & your body.

**contact as: <https://www.peplink.com/>**

## **FCC Requirements for Operation in the United States**

### **Federal Communications Commission (FCC) Compliance Notice:**

#### **For MAX HD4 MBX**

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

### **IMPORTANT NOTE**

#### **FCC Radiation Exposure Statement**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

### **ISED Warning Statement**

#### **Industry Canada Statement**

This device complies with Industry Canada's licence-exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause interference; and (2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

The device could automatically discontinue transmission in case of absence of information to transmit, or operational failure. Note that this is not intended to prohibit transmission of control or signaling

information or the use of repetitive codes where required by the technology. The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems; The maximum antenna gain permitted for devices in the bands 5250–5350 MHz and 5470–5725 MHz shall comply with the e.i.r.p. limit; and The maximum antenna gain permitted for devices in the band 5725–5825 MHz shall comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate.

L'appareil peut interrompre automatiquement la transmission en cas d'absence d'informations à transmettre ou de panne opérationnelle. Notez que ceci n'est pas destiné à interdire la transmission d'informations de contrôle ou de signalisation ou l'utilisation de codes répétitifs lorsque cela est requis par la technologie. Le dispositif utilisé dans la bande 5150-5250 MHz est réservé à une utilisation en intérieur afin de réduire le risque de brouillage préjudiciable aux systèmes mobiles par satellite dans le même canal; Le gain d'antenne maximal autorisé pour les dispositifs dans les bandes 5250-5350 MHz et 5470-5725 MHz doit être conforme à la norme e.r.p. limite; et Le gain d'antenne maximal autorisé pour les appareils de la bande 5725-5825 MHz doit être conforme à la norme e.i.r.p. les limites spécifiées pour un fonctionnement point à point et non point à point, selon le cas.

## IC Radiation Exposure Statement

This equipment complies with Innovation, Science and Economic Development Canada RF exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated to ensure a minimum of 20 cm spacing to any person at all times.

Déclaration d'exposition aux radiations: Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

This radio transmitter 20682-P1MBX has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

WIFI Antenna type: Replacement Antenna

WIFI Antenna gain: 2.4GHz / 2.44 dBi , 5GH / 4.73 dBi

LTE Antenna type: Replacement Antenna

LTE Antenna gain: 4.38 dBi



## CE Statement for Pepwave Routers ( MAX HD4 MBX )

### DECLARATION OF CONFORMITY

We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU.

Name of manufacturer	PISMO LABS TECHNOLOGY LIMITED
Contact information of the manufacturer	A8, 5/F, HK Spinners Industrial Building Phase 6, 481 Castle Peak Road Cheung Sha Wan Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	PEPWAVE / PEPLINK Wireless Product
Model name of the appliance	MAX HD4 MBX MAX-HD4-MBX-LTEA-K-T HD4 MBX MBX MAX HD4 MBX LTEA EXM-T4-LTEA-R Peplink Balance 310X Balance 310X BPL-310X-LTE-E-T
Trade name of the appliance	PEPWAVE / PEPLINK

The construction of the appliance is in accordance with the following standards:

EN 300 328 V2.1.1  
 EN 303 413 V1.1.1  
 EN 301908-1 V11.1.1  
 Draft EN 301 489-1 V2.2.1  
 Draft EN 301 489-17 V3.2.0  
 Draft EN 301 489-52 V1.1.0  
 EN 55032: 2015 + AC:2016-07  
 EN 61000-3-2: 2014  
 EN 61000-3-3: 2013  
 EN 55035 : 2017  
 EN 50385 : 2017  
 EN 62368-1:2014/A11:2017  
 EN 301 489-19 V2.1.1  
 EN 301 893 V2.1.1

Yours sincerely,

*Anthony Chong*



Anthony Chong  
 Director of Hardware Engineering  
 Peplink International Limited

	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV
	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	

**2.4GHz ( 2412 – 2472 MHz ) : 19.6 dBm**

**5GHz ( 5150 - 5250 MHz ) : 19.4 dBm**

This equipment complies with CE radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator & your body.

**contact as: <https://www.peplink.com/>**

## **FCC Requirements for Operation in the United States**

### **Federal Communications Commission (FCC) Compliance Notice:**

#### **For MAX HD2**

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

## IMPORTANT NOTE

1. 20cm minimum when the product is operated alone without co-transmitting with a plug-in 3G USB dongle device.
2. 65cm minimum when the product is operated with a plug-in 3G USB device which has maximum of 7W ERP output power.
3. For co-transmission scenario which is not covered above, please consult the RF technician or device supplier.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination.

FCC Radiation Exposure Statement (for MAX HD2 LTE/ MAX HD2 LTEA)

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 27cm between the radiator & your body.

50cm minimum when the product is operated with a plug-in 3G USB device which has maximum of 7W ERP output power.

For WLAN							
Antenna No.	Brand	Model	Antenna Net Gain(dBi)	Frequency range	Antenna Type	Connector Type	Cable Length (mm)
WAN(2.4G)-1	SmartAnt	SAA06-220690	3	2400 ~ 2500 MHz	Dipole	R-SMA	150
WAN(2.4G)-2	SmartAnt	SAA06-220690	3	2400 ~ 2500 MHz	Dipole	R-SMA	150
AP(5G)-1	SmartAnt	SAA06-220690	5.5	5150 ~ 5350 MHz	Dipole	R-SMA	260
			6	5350 ~ 5875 MHz			260
AP(5G)-2	SmartAnt	SAA06-220690	5.5	5150 ~ 5350 MHz	Dipole	R-SMA	260
			6	5350 ~ 5875 MHz			260
For GPS							
Antenna No.	Brand	Model	Antenna Net Gain(dBi)	Frequency range	Antenna Type	Connector Type	
1	MASTER WAVE TECHNOLOGY CO., LTD.	98335KSAF000	4.5 ±0.5	1575.42 MHz	Magnetic	SMA	
For WWAN(LTE)							
Antenna No.	Brand	Model	Antenna Net Gain(dBi)	Frequency range	Antenna Type	Connector Type	
Cellular 1 Main	MASTER WAVE TECHNOLOGY CO., LTD.	98619ZSAX025	1.99	699~960 MHz	Dipole	SMA	
Cellular 1 Diversity/Aux			4	1575~2170 MHz			
Cellular 2 Main			1	2300~2320 MHz			
Cellular 1 Diversity/Aux			2.8	2325~2690 MHz			



## **Industry Canada Statement (for MAX HD2 LTE/LTEA)**

This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

### **Caution : (for MAX HD2 LTE/LTEA)**

- (i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
- (ii) the maximum antenna gain permitted for devices in the band 5725-5850 MHz shall be such that the equipment still complies with the e.i.r.p. limits specified for point-to-point and non-point-to-point operation as appropriate; and
- (iii) Users should also be advised that high-power radars are allocated as primary users (i.e. priority users) of the bands 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

### **Avertissement: (for MAX HD2 LTE/LTEA)**

- (i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- (ii) le gain maximal d'antenne permis (pour les dispositifs utilisant la bande de 5725 à 5 850 MHz) doit être conforme à la limite de la p.i.r.e. spécifiée pour l'exploitation point à point et l'exploitation non point à point, selon le cas;
- (iii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.



**Radiation Exposure Statement: (for MAX HD2 LTE/LTEA)**

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 37cm between the radiator & your body.

70cm minimum when the product is operated with a plug-in 3G USB device which has maximum of 7W ERP output power.

**Déclaration d'exposition aux radiations: (for MAX HD2 LTE/LTEA)**

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 37 cm de distance entre la source de rayonnement et votre corps.

70cm minimum lorsque le produit est utilisé avec un plug-in 3G périphérique USB qui a un maximum de 7W ERP puissance de sortie.

**CE Statement for Pepwave Routers ( MAX HD2 )**

## DECLARATION OF CONFORMITY

We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU.

Name of manufacturer	PISMO LABS TECHNOLOGY LIMITED
Contact information of the manufacturer	A8, 5/F, HK Spinners Industrial Building, Phase 6, 481 Castle Peak Road, Cheung Sha Wan, Kowloon, Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	PEPWAVE / PEPLINK Wireless Product
Model name of the appliance	MAX HD2, MAX HD2 LTE, MAX HD2 LTEA Pismo 811AC
Trade name of the appliance	PEPWAVE / PEPLINK


The construction of the appliance is in accordance with the following standards:

EN 300 328 V2.2.2  
 EN 301 893 V2.1.1  
 EN 301 908-1 V11.1.1  
 Draft EN 301 489-1 V2.2.0  
 Draft EN 301 489-19 V2.1.0  
 Draft EN 301 489-52 V1.1.0  
 Draft EN 301 489-17 V3.2.0  
 EN 55032:2015 +AC: 2016  
 EN 61000-3-2: 2014,  
 EN 61000-3-3: 2013,  
 EN 55024:2010+A1:2015  
 EN 62311:2008  
 EN 60950-1:2006+A11: 2009+A1:2010+A12:2011+A2:2013  
 EN 303 413 V1.1.1

Yours sincerely,




Antony Chong  
 Director of Hardware Engineering  
 Peplink International Limited

	BE	BG	CZ	DK	DE	EE	IE	EL	ES	FR	HR	IT	CY	LV
	LT	LU	HU	MT	NL	AT	PL	PT	RO	SI	SK	FI	SE	

**2.4GHz ( 2412 – 2472 MHz ) : 19.90 dBm**

**5GHz ( 5150 - 5250 MHz ) : 22.88 dBm**

This equipment complies with CE radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20cm between the radiator & your body.

**contact as: <https://www.peplink.com/>**