MAX Series

User Manual

Pepwave Products:

MAX 700 / HD2 / HD2 IP67 / HD2 Mini / HD2 MBX / HD Dome / HD4 / HD4 MBX / MBX Mini / HD4 IP67 / Transit / Transit Duo / Transit 5G / Transit Core / Transit Mini / Transit Pro E / BR1 Classic / BR1 MK2 / BR1 Slim / BR1 ENT / BR1 M2M / BR1 Mini / BR1 Mini Core / BR1 ESN / BR1 Pro LTE / BR1 Pro (CAT-20) / BR1 Pro 5G / BR1 IP55 / BR1 IP67/ BR2 IP55 / On-The-Go / HD2 with MediaFast / HD4 with MediaFast / SpeedFusion Engine / UBR LTE / PDX

Pepwave Firmware 8.1.3
January 2022

COPYRIGHT & TRADEMARKS
Specifications are subject to change without notice.
Copyright © 2021 Peplink Pepwave Ltd. All Rights Reserved. Pepwave and the Pepwave logo are trademarks of Peplink International Ltd. Other brands or products mentioned may be trademarks or registered trademarks of their respective owners.

Table of Contents

Introduction and Scope **8**

Glossary **9**

Product Features **10**

Supported Network Features 10

Other Supported Features 13

Pepwave MAX Mobile Router Overview **14**

MAX 700 14

MAX HD2 16

MAX HD2 IP67 18

MAX HD2 mini 19

MAX HD Dome 20

MAX Transit / MAX Transit Duo (CAT-12) 22

MAX Transit (CAT-18) 24

MAX Transit 5G 26

MAX Transit Mini 27

MAX Transit Pro E 28

MAX Transit Core 29

MAX BR1 ESN 31

MAX HD2 and HD4 with MediaFast 32

MAX HD4 34

MAX HD4 MBX (CAT-12) 36

MAX HD2/4 MBX (CAT-18) 38

MAX HD2/4 MBX (5G) 39

MAX MBX Mini 41

MAX HD4 IP67 42

MAX BR1 Classic 43

MAX BR1 MK2 45

MAX BR1 Slim 47

MAX BR1 Mini 48

MAX BR1 Mini Core 50

MAX BR1 M2M 51

MAX BR1 ENT 53

MAX BR1 Pro 54

MAX BR1 Pro (CAT-20) 55
MAX BR1 Pro 5G 57
MAX Hotspot 59
MAX BR1 IP55 60
MAX BR2 IP55 62
MAX BR1 IP67 63
MAX On-The-Go 64
SpeedFusion Engine 65
UBR LTE 65
PDX 67

Advanced Feature Summary 68
Drop-in Mode and LAN Bypass: Transparent Deployment 68
QoS: Clearer VoIP 68
Per-User Bandwidth Control 69
High Availability via VRRP 69
USB Modem and Android Tethering 70
Built-In Remote User VPN Support 70
SIM-card USSD support 71
KVM Virtualization 71
DPI Engine 72
NetFlow 72
Wi-Fi Air Monitoring 72
SP Default Configuration 72

Installation 73
Preparation 73
Constructing the Network 73
Configuring the Network Environment 74

Mounting the Unit 75
Wall Mount 75
Car Mount 75
IP67 Installation Guide 75
PDX Accessory Kit Installation Guide 76

Connecting to the Web Admin Interface 83

SpeedFusion Cloud 85
Activate SpeedFusion Cloud Service 85

Enable SpeedFusion Cloud 88
Connect Clients to Cloud 95
Link Wi-Fi to Cloud 96
Optimize Cloud Application 98

Configuring the LAN Interface(s) 99
Basic Settings 99
Port Settings 111
Captive Portal 112

Configuring the WAN Interface(s) 115
Ethernet WAN 116
Cellular WAN 127
Wi-Fi WAN 133
WAN Health Check 140
Dynamic DNS Settings 142

Advanced Wi-Fi Settings 144

MediaFast Configuration 148
Setting Up MediaFast Content Caching 148
Scheduling Content Prefetching 150
Viewing MediaFast Statistics 152

ContentHub 153
Configuring the ContentHub 153
Configure a website for ContentHub 153
Configure an application for ContentHub 156

Docker 158

KVM 158

Bandwidth Bonding SpeedFusionTM / PepVPN 160
PepVPN 160
The Pepwave Router Behind a NAT Router 167

IPsec VPN 169
IPsec VPN Settings 169
GRE Tunnel 173

Outbound Policy 175
Outbound Policy 176

Adding Rules for Outbound Policy 177

Port Forwarding 187
UPnP / NAT-PMP Settings 189

NAT Mappings 190

QoS 192
User Groups 192
Bandwidth Control 193
Application 193

Firewall 195
Outbound and Inbound Firewall Rules 196
Content Blocking 201

Routing Protocols 203
OSPF & RIPv2 203
BGP 205

Remote User Access 210
L2TP with IPsec 210
OpenVPN 210
PPTP 211
Authentication Methods 211

Miscellaneous Settings 213
High Availability 213
Certificate Manager 216
Service Forwarding 217
Service Passthrough 219
UART 221
GPS Forwarding 223
Ignition Sensing 223
Ignition Sensing installation 224
GPIO Menu 226
NTP Server 227
Grouped Networks 227
Remote SIM Management 229
SIM Toolkit 231

AP **233**
AP Controller 233
Wireless SSID 233
Wireless Mesh 237
Settings 238

AP Controller Status **244**
Info 244
Access Point (Usage) 246
Wireless SSID 248
Mesh / WDS 249
Wireless Client 250
Nearby Device 252
Event Log 252

Toolbox **253**

System Settings **254**
Admin Security 254
Firmware 258
Time 260
Schedule 260
Email Notification 262
Event Log 265
SNMP 266
SMS Control 268
InControl 269
Configuration 270
Feature Add-ons 271
Reboot 271

Tools **272**
Ping 272
Traceroute Test 273
PepVPN Test 273
Wake-on-LAN 274
CLI (Command Line Interface Support) 274

Status **275**

- Device 275
  - GPS Data 277
- Active Sessions 278
- Client List 280
- WINS Client 280
- UPnP / NAT-PMP 281
- OSPF & RIPv2 281
- BGP 282
- SpeedFusion Status 282
- Event Log 285

WAN Quality 286

Usage Reports 287

- Real-Time 287
- Hourly 288
- Daily 289
- Monthly 290

Appendix A: Restoration of Factory Defaults 292

Appendix B: FusionSIM Manual 293

Appendix C: Overview of ports used by Peplink SD-WAN routers and other Peplink services 305

Appendix D: Declaration 307

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!

SMART CITIES
CITY OF THE FUTURE
DATA-TRANSFER 500086780
INCOMING CALL

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 compared 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.

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, dyndns.org, no-ip.org, tzo.com and 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)
- 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

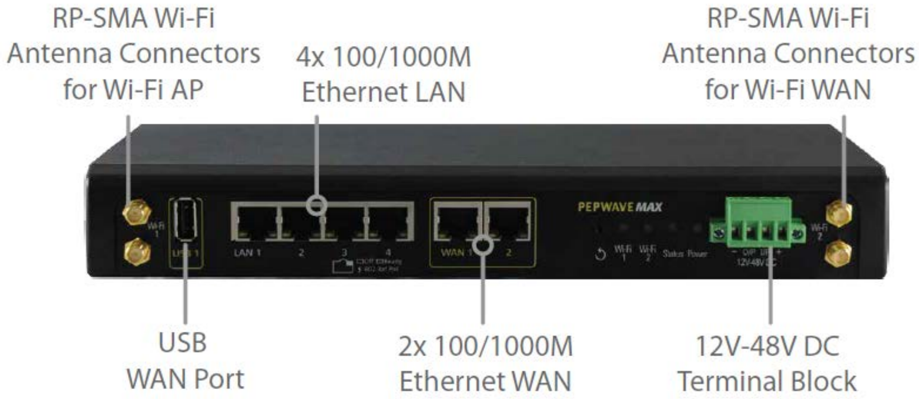
- User-friendly web-based administration interface
- HTTP and HTTPS support for web admin interface (default redirection to HTTPS)
- Configurable web administration port and administrator password
- Firmware upgrades, configuration backups, ping, and traceroute via web admin interface
- Remote web-based configuration (via WAN and LAN interfaces)
- Time server synchronization
- SNMP
- Email notification
- Read-only user access 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

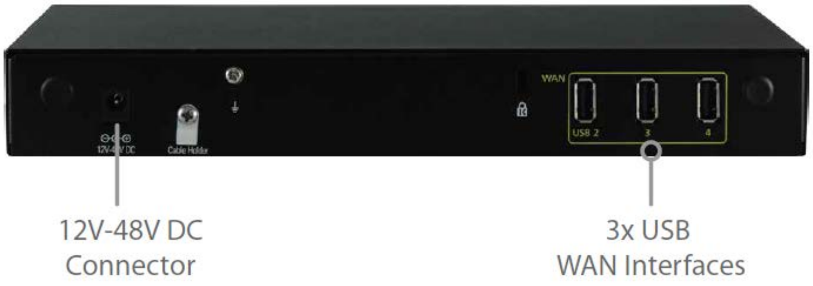
* Not supported on MAX Surf-On-The-Go, and BR1 variants

2 Pepwave MAX Mobile Router Overview

2.1 MAX 700

2.1.1 Panel Appearance


RP-SMA Wi-Fi Antenna Connectors for Wi-Fi AP
4x 100/1000M Ethernet LAN
RP-SMA Wi-Fi Antenna Connectors for Wi-Fi WAN
USB WAN Port
2x 100/1000M Ethernet WAN
12V-48V DC Terminal Block


12V-48V DC Connector
3x USB WAN Interfaces

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

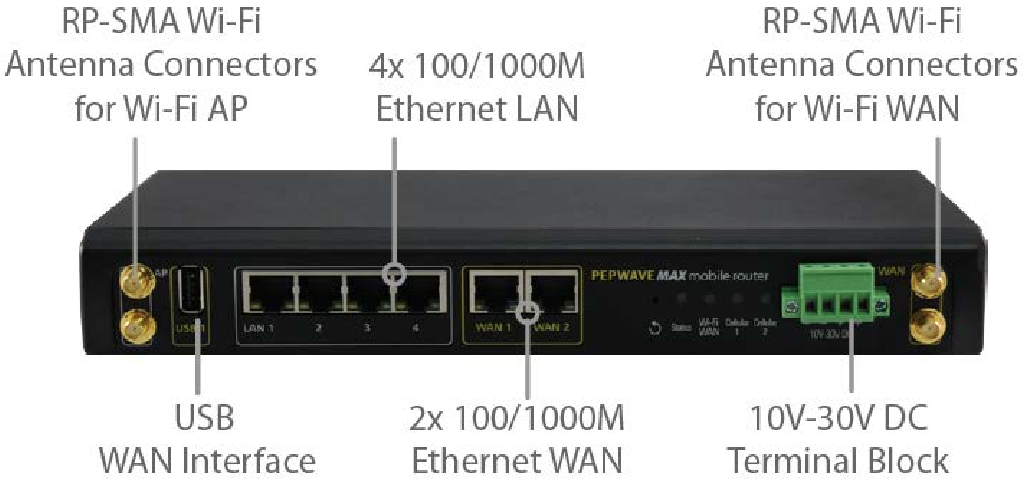
Wi-Fi AP and Wi-Fi WAN Indicators		
Wi-Fi WAN	OFF	Disconnected
	Blinking slowly	Connecting to network
	Blinking	Connected to network with traffic
	ON	Connected to network without traffic
Wi-Fi AP	OFF	Disabled
	Blinking slowly	Enabled but no client connected
	Blinking	Connected to network with traffic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

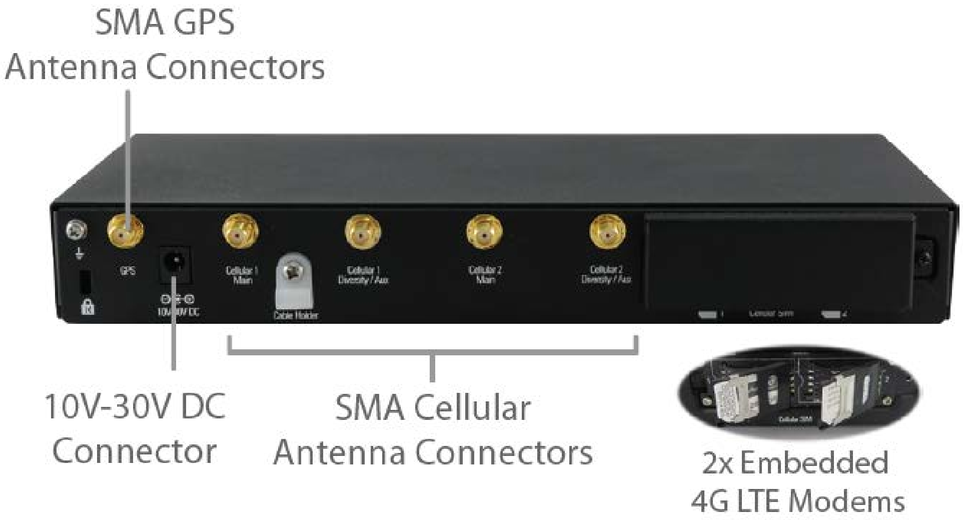
LAN and Ethernet WAN Ports		
Green LED	ON	10 / 100/ 1000 Mbps
Orange LED	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

2.2 MAX HD2

For certification information, please refer to Appendix B: Declaration

2.2.1 Panel Appearance


RP-SMA Wi-Fi Antenna Connectors for Wi-Fi AP
4x 100/1000M Ethernet LAN
RP-SMA Wi-Fi Antenna Connectors for Wi-Fi WAN
USB WAN Interface
2x 100/1000M Ethernet WAN
10V-30V DC Terminal Block


SMA GPS Antenna Connectors
10V-30V DC Connector
SMA Cellular Antenna Connectors
2x Embedded 4G LTE Modems

2.2.2 LED Indicators

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

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

Wi-Fi AP and Wi-Fi WAN Indicators		
Wi-Fi WAN / Wi-Fi AP	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

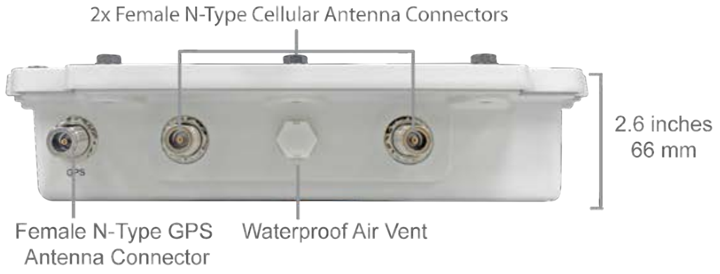
Cellular Indicators		
Cellular 1 / Cellular 2	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

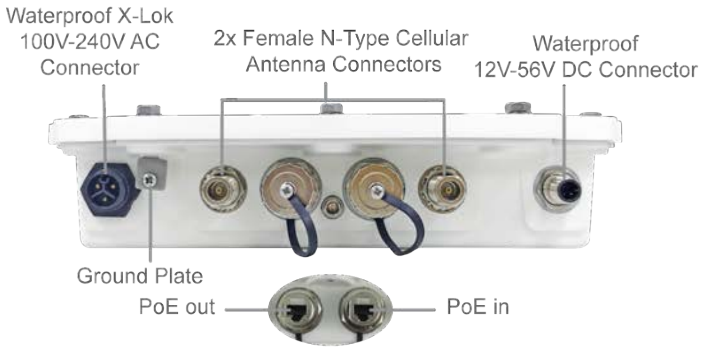
LAN and Ethernet WAN Ports		
Green LED	ON	1000 Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

2.3 MAX HD2 IP67

2.3.1 Panel Appearance

PEPWAVE
Broadband Possibilities


2x Female N-Type Cellular Antenna Connectors
2.6 inches
66 mm
GPS
Female N-Type GPS Antenna Connector
Waterproof Air Vent


Waterproof X-Lok 100V-240V AC Connector
2x Female N-Type Cellular Antenna Connectors
Waterproof 12V-56V DC Connector
Ground Plate
PoE out
PoE in

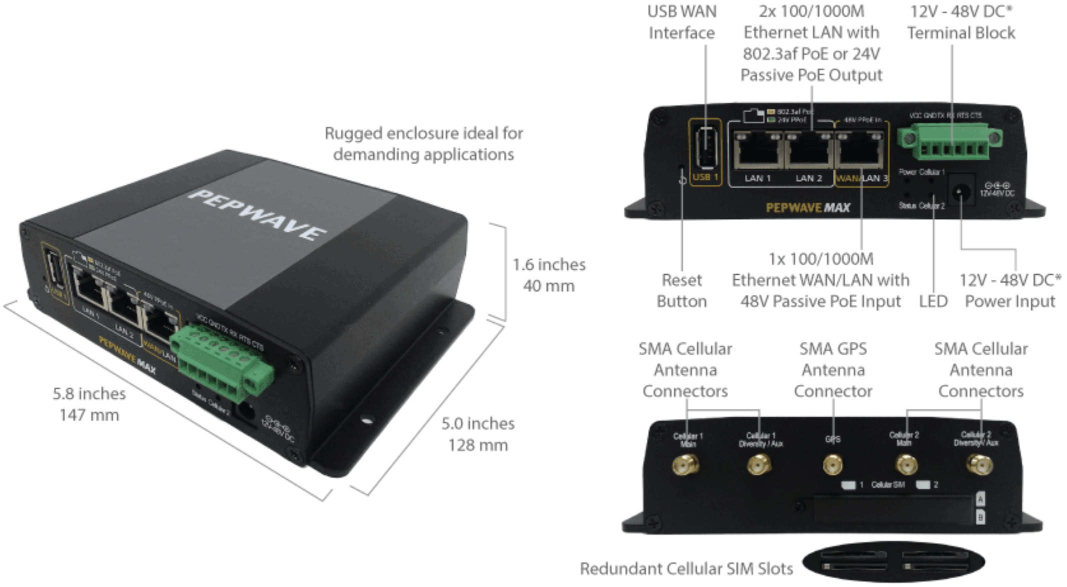
2.3.2 LED Indicators

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

2.4 MAX HD2 mini

2.4.1 Panel Appearance


Rugged enclosure ideal for demanding applications
1.6 inches
40 mm
5.8 inches
147 mm
5.0 inches
128 mm
USB WAN Interface
2x 100/1000M Ethernet LAN with 802.3af PoE or 24V Passive PoE Output
12V - 48V DC* Terminal Block
Reset Button
1x 100/1000M Ethernet WAN/LAN with 48V Passive PoE Input
LED
12V - 48V DC* Power Input
SMA Cellular Antenna Connectors
SMA GPS Antenna Connector
SMA Cellular Antenna Connectors
Redundant Cellular SIM Slots
PEPWAVE
PEPWAVE MAX
LAN 1
LAN 2
WAN/LAN 3
USB 1

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

2.4.2 LED Indicators

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

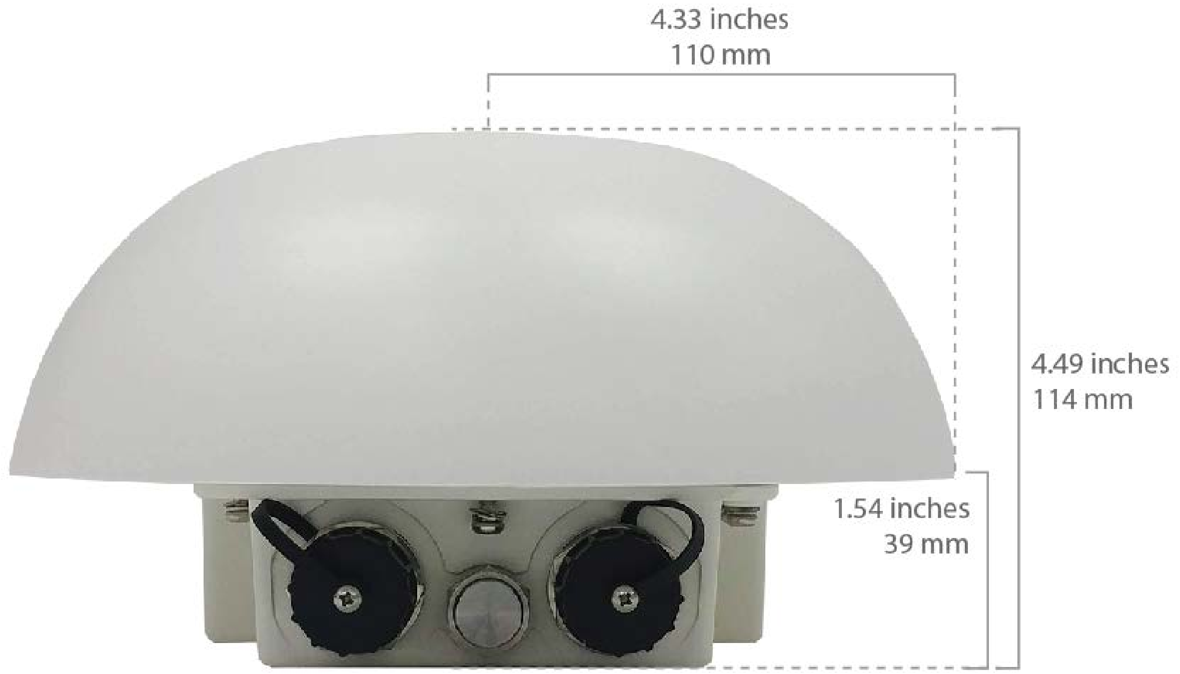
Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

Cellular Indicators		
Cellular 1 / Cellular 2	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

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

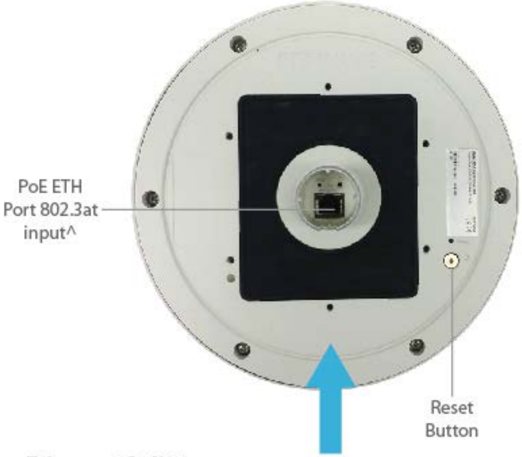
2.5 MAX HD Dome

2.5.1 Panel Appearance

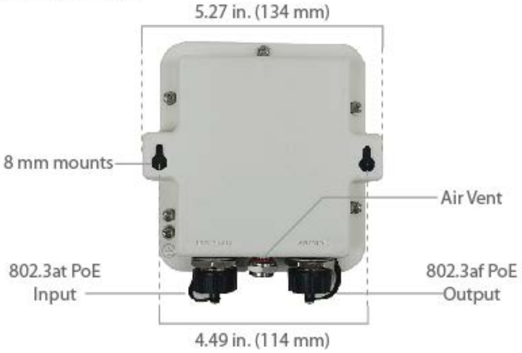


#SIM Injector is available separately
^Ethernet LAN port can be split into two LAN ports
using the included splitter (1x LAN 802.3af PoE out, 1x LAN PoE in)

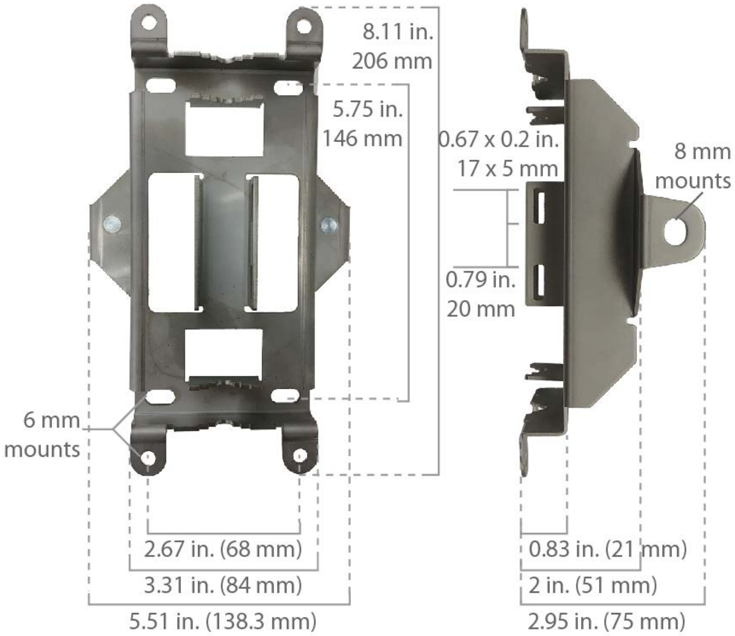
HD2 Dome


PoE ETH
Port 802.3at
input^
Reset
Button

Ethernet Splitter


5.27 in. (134 mm)
8 mm mounts
Air Vent
802.3at PoE
Input
802.3af PoE
Output
4.49 in. (114 mm)

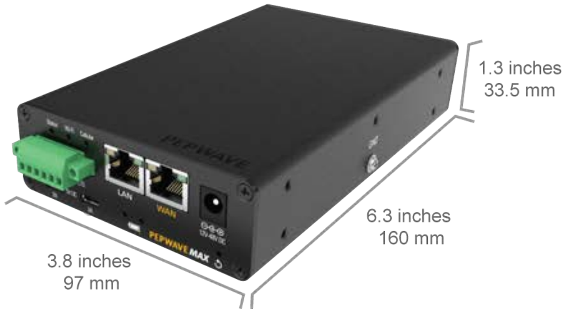
Mounting Bracket


8.11 in.
206 mm
5.75 in.
146 mm
0.67 x 0.2 in.
17 x 5 mm
8 mm
mounts
0.79 in.
20 mm
6 mm
mounts
2.67 in. (68 mm)
3.31 in. (84 mm)
5.51 in. (138.3 mm)
0.83 in. (21 mm)
2 in. (51 mm)
2.95 in. (75 mm)

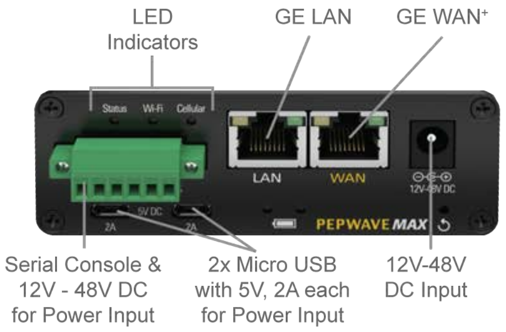
2.6 MAX Transit / MAX Transit Duo (CAT-12)

2.6.1 Panel Appearance

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

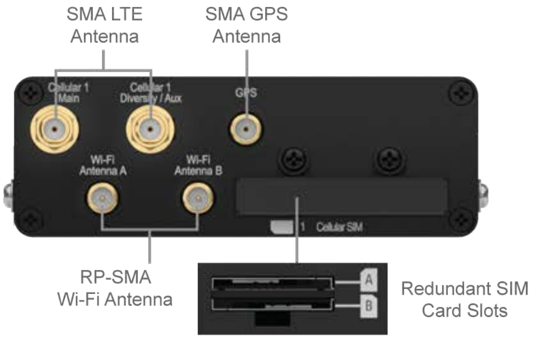

1.3 inches
33.5 mm
6.3 inches
160 mm
3.8 inches
97 mm
LAN
WAN
PEPWAVE MAX

Front

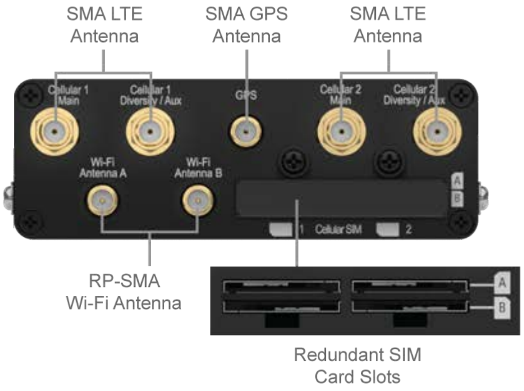

LED Indicators
GE LAN
GE WAN+
Status
Wi-Fi
Cellular
LAN
WAN
12V-48V DC
5V DC
2A
2A
PEPWAVE MAX
Serial Console & 12V - 48V DC for Power Input
2x Micro USB with 5V, 2A each for Power Input
12V-48V DC Input

Back

MAX-TST (CAT-12)


SMA LTE Antenna
SMA GPS Antenna
Cellular 1 Main
Cellular 1 Diversity / Aux
GPS
Wi-Fi Antenna A
Wi-Fi Antenna B
1
Cellular SIM
A
B
RP-SMA Wi-Fi Antenna
Redundant SIM Card Slots

MAX-TST-DUO (CAT-12)


SMA LTE Antenna
SMA GPS Antenna
SMA LTE Antenna
Cellular 1 Main
Cellular 1 Diversity / Aux
GPS
Cellular 2 Main
Cellular 2 Diversity / Aux
Wi-Fi Antenna A
Wi-Fi Antenna B
A
B
1
Cellular SIM
2
RP-SMA Wi-Fi Antenna
Redundant SIM Card Slots

2.6.2 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 1 / Cellular 2*	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

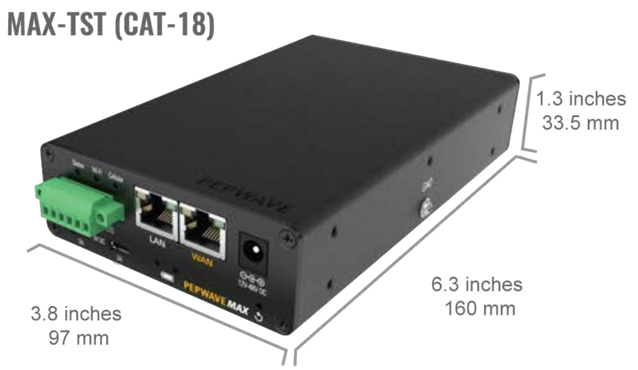
* For MAX-TST_DUO

Wi-Fi Indicators		
Wi-Fi	OFF	Wi-Fi AP is turn off
	Blinking	Wi-Fi AP is turn on

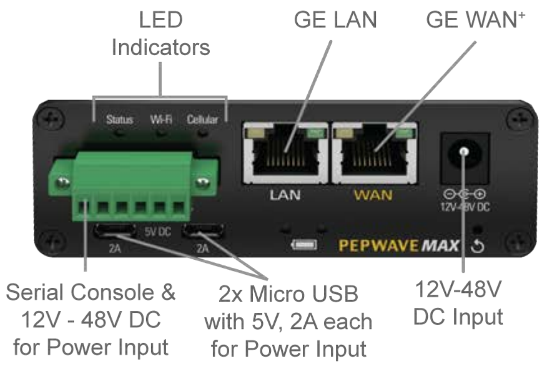
LAN and Ethernet WAN Ports		
Green LED	ON	1000 Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

2.7 MAX Transit (CAT-18)

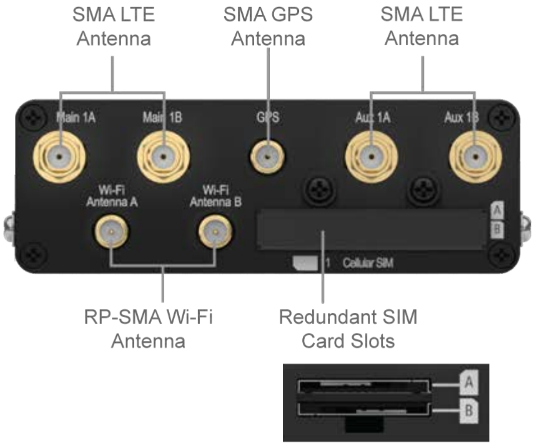
2.7.1 Panel Appearance


MAX-TST (CAT-18)
1.3 inches
33.5 mm
6.3 inches
160 mm
3.8 inches
97 mm
PEPWAVE MAX
LAN
WAN

Front


LED
Indicators
GE LAN
GE WAN+
Status
Wi-Fi
Cellular
LAN
WAN
12V-48V DC
5V DC
2A
2A
PEPWAVE MAX
Serial Console &
12V - 48V DC
for Power Input
2x Micro USB
with 5V, 2A each
for Power Input
12V-48V
DC Input

Back


SMA LTE
Antenna
SMA GPS
Antenna
SMA LTE
Antenna
Main 1A
Main 1B
GPS
Aux 1A
Aux 1B
Wi-Fi
Antenna A
Wi-Fi
Antenna B
A
B
1 Cellular SIM
RP-SMA Wi-Fi
Antenna
Redundant SIM
Card Slots
A
B

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 Indicators		
Cellular 1 / Cellular 2*	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

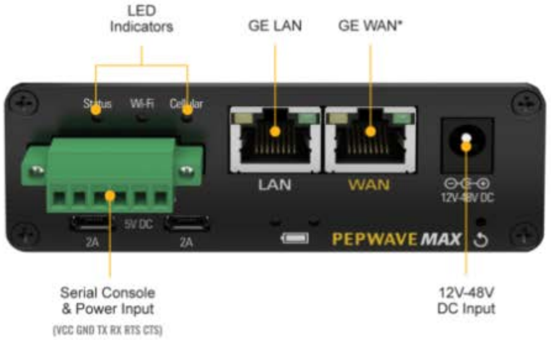
* For MAX-TST_DUO

Wi-Fi Indicators		
Wi-Fi	OFF	Wi-Fi AP is turn off
	Blinking	Wi-Fi AP is turn on

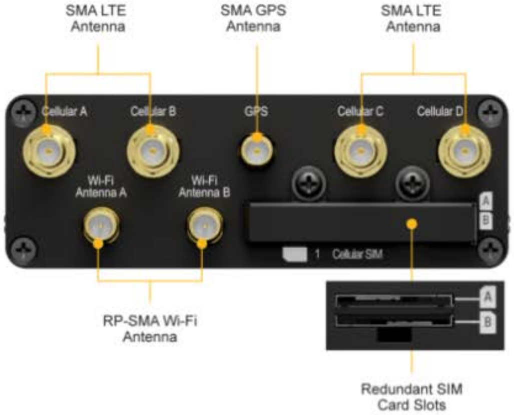
LAN and Ethernet WAN Ports		
Green LED	ON	1000 Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

2.8 MAX Transit 5G

2.8.1 Panel Appearance


LED Indicators
GE LAN
GE WAN*
Status
Wi-Fi
Cellular
LAN
WAN
12V-48V DC
5V DC
2A
2A
PEPWAVE MAX
Serial Console & Power Input
(VCC GND TX RX RTS CTS)
12V-48V DC Input

* The WAN port can act as a LAN port if needed.


SMA LTE Antenna
SMA GPS Antenna
SMA LTE Antenna
Cellular A
Cellular B
GPS
Cellular C
Cellular D
Wi-Fi Antenna A
Wi-Fi Antenna B
A
B
1 Cellular SIM
RP-SMA Wi-Fi Antenna
A
B
Redundant SIM Card Slots

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

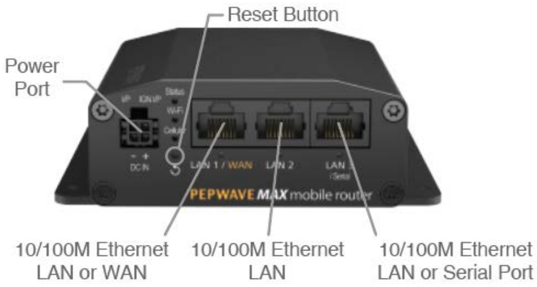
Cellular Indicators		
Cellular 1 / Status	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

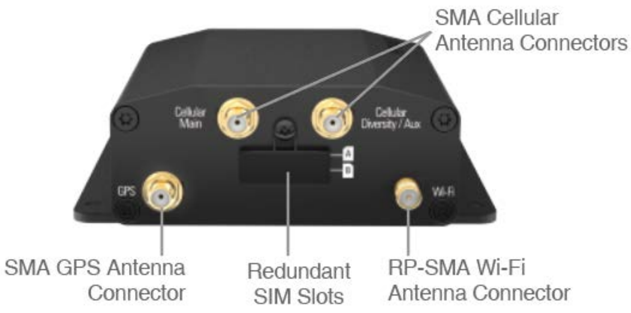
Wi-Fi Indicators		
Wi-Fi	OFF	Wi-Fi AP is turn off
	Blinking	Wi-Fi AP is turn on

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	Port is not connected
Port Type	Auto MDI/MDI-X ports	

2.9 MAX Transit Mini

2.9.1 Panel Appearance


Reset Button
Power Port
PEPWAVE MAX mobile router
LAN 1 / WAN
LAN 2
LAN (Serial)
10/100M Ethernet LAN or WAN
10/100M Ethernet LAN
10/100M Ethernet LAN or Serial Port


SMA Cellular Antenna Connectors
Cellular Main
Cellular Diversity / Aux
GPS
A
B
Wi-Fi
SMA GPS Antenna Connector
Redundant SIM Slots
RP-SMA Wi-Fi Antenna Connector

2.9.2 LED indicators

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

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

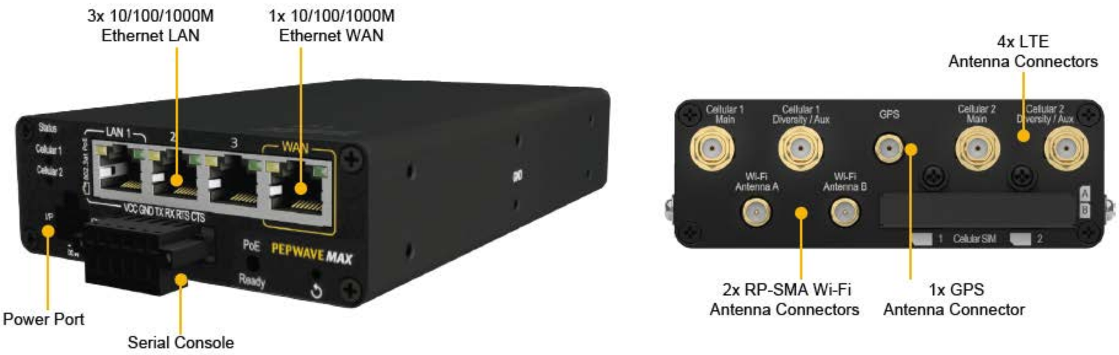
Wi-Fi Indicators		
Wi-Fi	OFF	Disabled intermittent
	Blinking slowly	Connecting to wireless network(s)

	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

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

2.10 MAX Transit Pro E

2.10.1 Panel Appearance


3x 10/100/1000M Ethernet LAN
1x 10/100/1000M Ethernet WAN
Status
Cellular 1
Cellular 2
LAN 1
2
3
WAN
VCC GND TX RX RTS CTS
PoE
PEPWAVE MAX
Ready
Power Port
Serial Console
4x LTE Antenna Connectors
Cellular 1 Main
Cellular 1 Diversity / Aux
GPS
Cellular 2 Main
Cellular 2 Diversity / Aux
Wi-Fi Antenna A
Wi-Fi Antenna B
A
B
1
Cellular SIM
2
2x RP-SMA Wi-Fi Antenna Connectors
1x GPS Antenna Connector

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

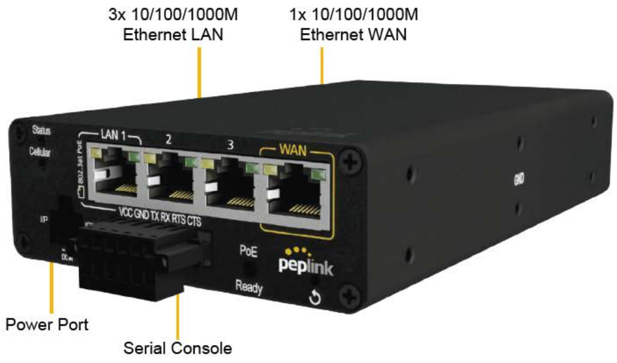
LAN 1 Port		
Green LED	ON	POE Enabled
	OFF	POE Disabled
Orange LED	Blinking	10 / 100 / 1000 Mbps and Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

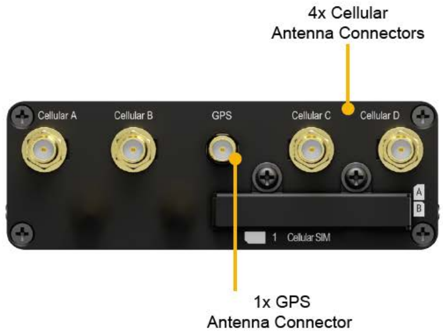
LAN 2-3 Port and Ethernet WAN Port		
Green LED	ON	1000 Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

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

2.11 MAX Transit Core

2.11.1 Panel Appearance


3x 10/100/1000M Ethernet LAN
1x 10/100/1000M Ethernet WAN
Status
Cellular
LAN 1
2
3
WAN
PoE
Ready
peplink
Power Port
Serial Console


4x Cellular Antenna Connectors
Cellular A
Cellular B
GPS
Cellular C
Cellular D
Cellular SIM
1x GPS Antenna Connector

2.11.2 LED indicators

Status indicated in the front panel is as follows:

LED Indicator	
Power LED	OFF – Power off
	GREEN – Power on

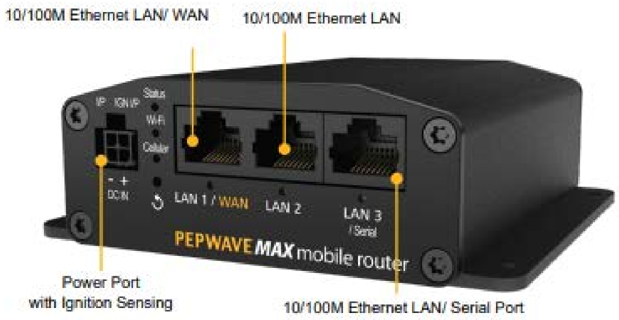
LAN 1 Port	
Green LED	ON – POE Enabled OFF - POE Disabled
Orange LED	Blinking – 10 / 100 / 1000 Mbps with activity
	OFF – No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports

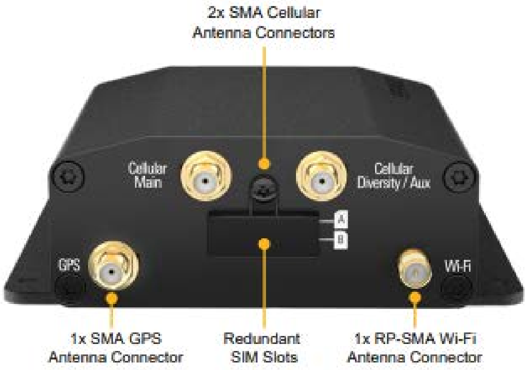
LAN 2-3 Ports, WAN Port	
Right LED	GREEN – 1000 Mbps
	OFF – 10 / 100 Mbps or ports are not connected
Left LED	ORANGE – Port is connected without traffic
	Blinking – Data is transferring
	OFF – Port is not connected
Port Type	Auto MDI/MDI-X ports

Console & USB Ports	
Console Port	Reserved for engineering use
USB Ports	For connecting 4G/3G USB modems

2.12 MAX BR1 ESN

2.12.1 Panel Appearance


10/100M Ethernet LAN/ WAN
10/100M Ethernet LAN
I/P
IGN I/P
Status
Wi-Fi
Cellular
- +
DC IN
LAN 1 / WAN
LAN 2
LAN 3 / Serial
PEPWAVE MAX mobile router
Power Port with Ignition Sensing
10/100M Ethernet LAN/ Serial Port


2x SMA Cellular Antenna Connectors
Cellular Main
Cellular Diversity / Aux
A
B
GPS
Wi-Fi
1x SMA GPS Antenna Connector
Redundant SIM Slots
1x RP-SMA Wi-Fi Antenna Connector

2.12.2 LED indicators

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

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

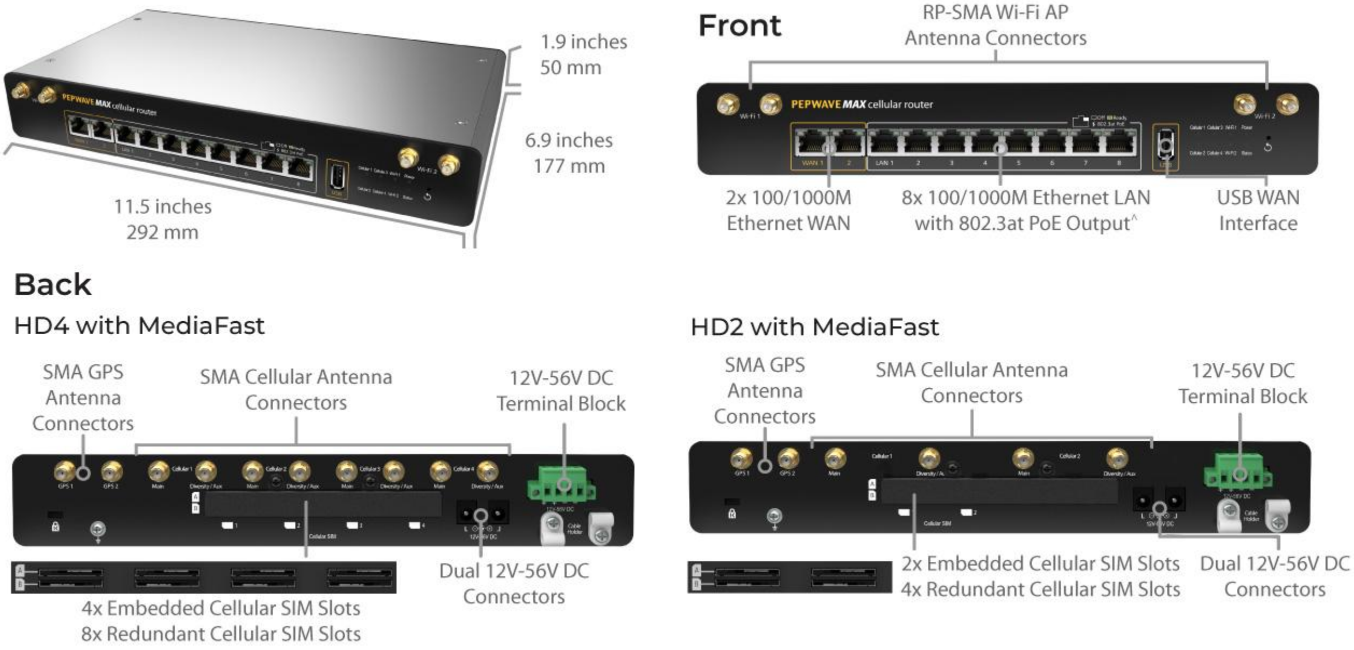
Wi-Fi Indicators

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
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

2.13 MAX HD2 and HD4 with MediaFast

2.13.1 Panel Appearance


1.9 inches
50 mm
6.9 inches
177 mm
11.5 inches
292 mm
Front
RP-SMA Wi-Fi AP
Antenna Connectors
2x 100/1000M
Ethernet WAN
8x 100/1000M Ethernet LAN
with 802.3at PoE Output^
USB WAN
Interface
Back
HD4 with MediaFast
SMA GPS
Antenna
Connectors
SMA Cellular Antenna
Connectors
12V-56V DC
Terminal Block
Dual 12V-56V DC
Connectors
4x Embedded Cellular SIM Slots
8x Redundant Cellular SIM Slots
HD2 with MediaFast
SMA GPS
Antenna
Connectors
SMA Cellular Antenna
Connectors
12V-56V DC
Terminal Block
2x Embedded Cellular SIM Slots
4x Redundant Cellular SIM Slots
Dual 12V-56V DC
Connectors

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		
Wi-Fi WAN / Wi-Fi AP	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

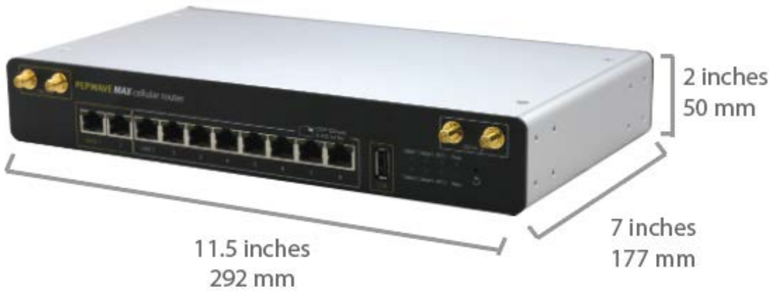
Cellular Indicators		
Cellular 1 / Cellular 2	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

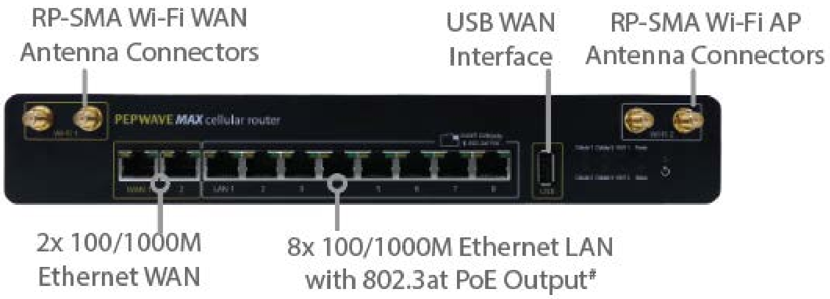
LAN Ports		
Green LED	ON	POE Enabled
	OFF	POE Disabled
Orange LED	Blinking	10 / 100 / 1000 Mbps and Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

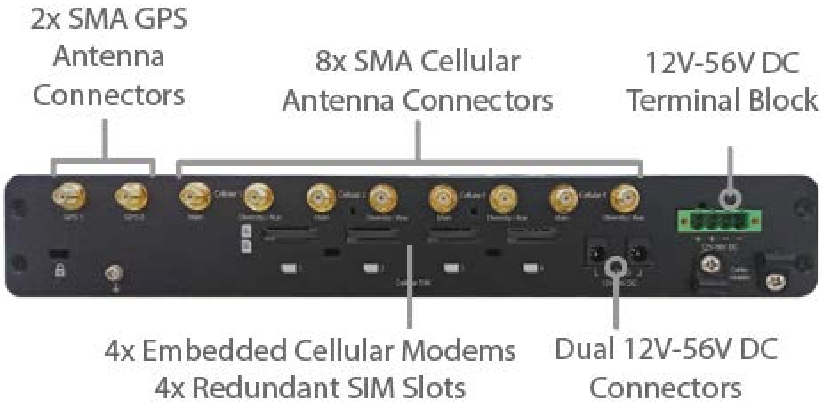
Ethernet WAN Ports		
Green LED	ON	1000 Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

2.14 MAX HD4

2.14.1 Panel Appearance


2 inches
50 mm
7 inches
177 mm
11.5 inches
292 mm


RP-SMA Wi-Fi WAN Antenna Connectors
USB WAN Interface
RP-SMA Wi-Fi AP Antenna Connectors
PEPWAVE MAX cellular router
2x 100/1000M Ethernet WAN
8x 100/1000M Ethernet LAN with 802.3at PoE Output*


2x SMA GPS Antenna Connectors
8x SMA Cellular Antenna Connectors
12V-56V DC Terminal Block
4x Embedded Cellular Modems 4x Redundant SIM Slots
Dual 12V-56V DC Connectors

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 / Wi-Fi AP	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 1 / Cellular 2	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

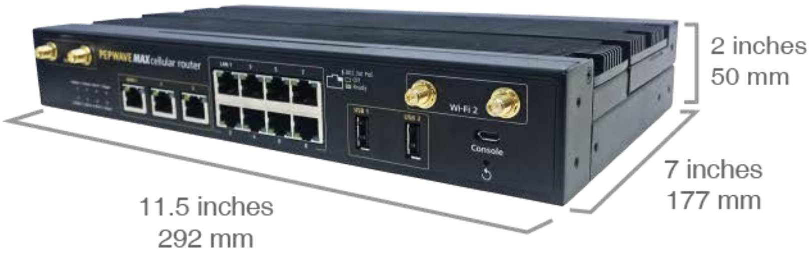
LAN Ports		
Green LED	ON	POE Enabled
	OFF	POE Disabled
Orange LED	Blinking	10 / 100 / 1000 Mbps and Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

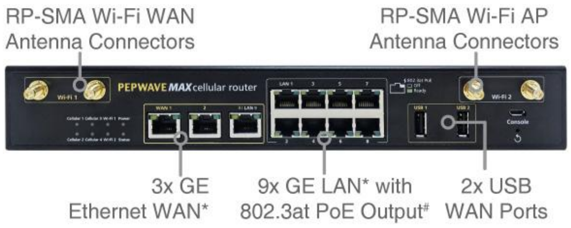
Ethernet WAN Ports		
Green LED	ON	1000 Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

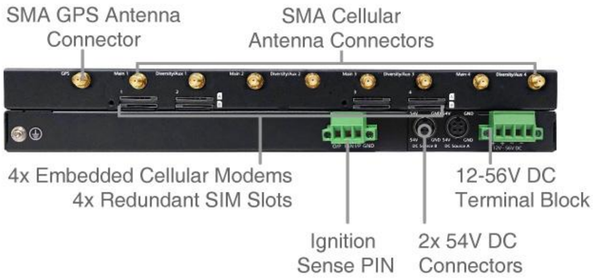
2.15 MAX HD4 MBX (CAT-12)

For certification information, please refer to Appendix B: Declaration

2.15.1 Panel Appearance


2 inches
50 mm
7 inches
177 mm
11.5 inches
292 mm


RP-SMA Wi-Fi WAN
Antenna Connectors
RP-SMA Wi-Fi AP
Antenna Connectors
3x GE
Ethernet WAN*
9x GE LAN* with
802.3at PoE Output#
2x USB
WAN Ports


SMA GPS Antenna
Connector
SMA Cellular
Antenna Connectors
4x Embedded Cellular Modems
4x Redundant SIM Slots
12-56V DC
Terminal Block
Ignition
Sense PIN
2x 54V DC
Connectors

*WAN 3 is configured as a LAN port by default, configuration is changeable on the Web Admin.

#2x 54V DC input is needed for all 8x LAN ports to have 802.3at PoE. Plugging in 1x 54V DC input will result in 4x LAN ports having 802.3at PoE

2.15.2 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

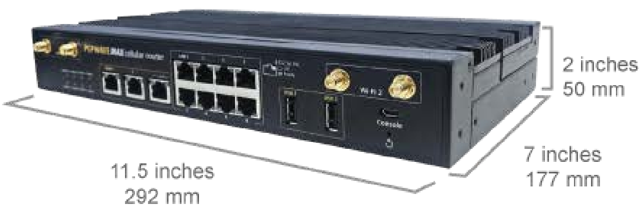
Cellular and Wi-Fi WAN Indicators		
Wi-Fi WAN / Cellular 1 / Cellular 2	OFF	Disabled Intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

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

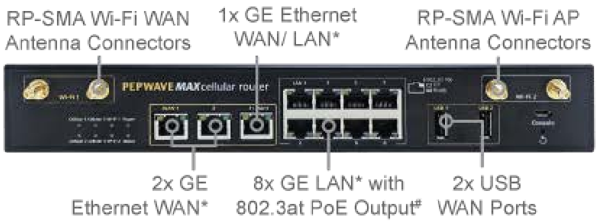
2.16 MAX HD2/4 MBX (CAT-18)

2.16.1 Panel Appearance

HD2/4 MBX (CAT-18)

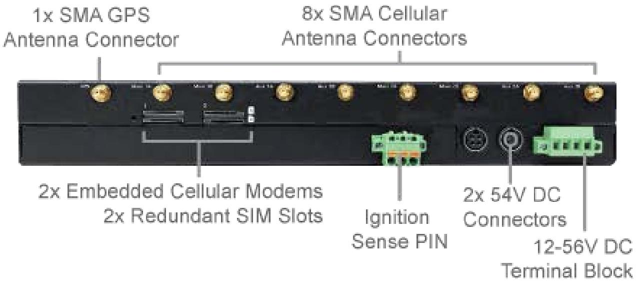

2 inches
50 mm
7 inches
177 mm
11.5 inches
292 mm

Front

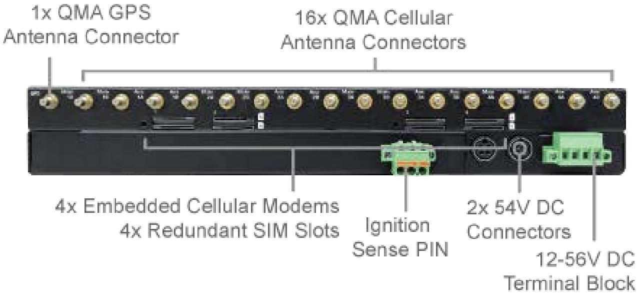

RP-SMA Wi-Fi WAN
Antenna Connectors
1x GE Ethernet
WAN/ LAN*
RP-SMA Wi-Fi AP
Antenna Connectors
2x GE
Ethernet WAN*
8x GE LAN* with
802.3at PoE Output#
2x USB
WAN Ports

Back

HD2 MBX (CAT-18)


1x SMA GPS
Antenna Connector
8x SMA Cellular
Antenna Connectors
2x Embedded Cellular Modems
2x Redundant SIM Slots
Ignition
Sense PIN
2x 54V DC
Connectors
12-56V DC
Terminal Block

HD4 MBX (CAT-18)


1x QMA GPS
Antenna Connector
16x QMA Cellular
Antenna Connectors
4x Embedded Cellular Modems
4x Redundant SIM Slots
Ignition
Sense PIN
2x 54V DC
Connectors
12-56V DC
Terminal Block

2.16.2 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

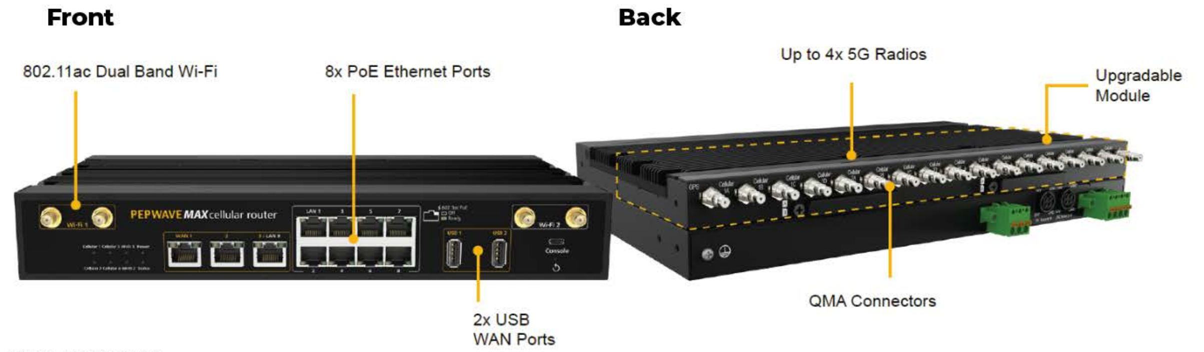
Wi-Fi AP and Wi-Fi WAN Indicators		
Wi-Fi WAN / Cellular 1 / Cellular 2	OFF	Disabled Intermittent
	Blinking slowly	Connecting to network(s)
	Blinking	Connected to network(s) with traffic
	ON	Connected to network(s) without traffic

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

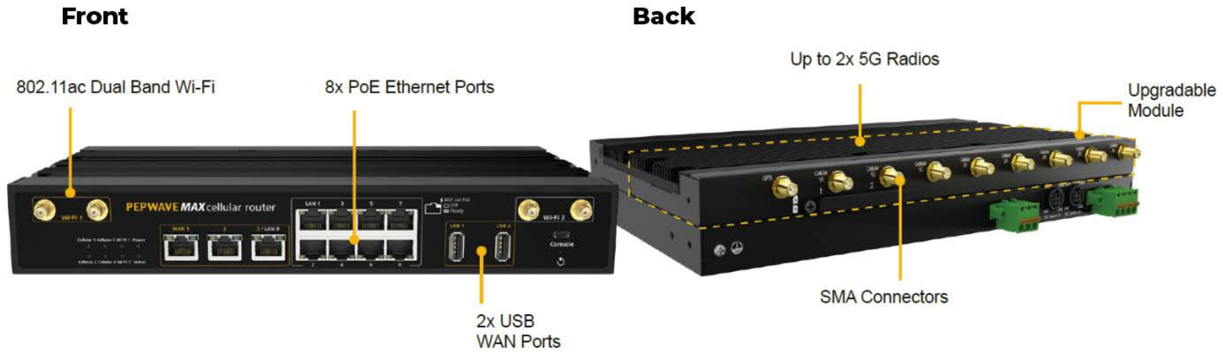
2.17 MAX HD2/4 MBX (5G)

2.17.1 Panel Appearance

HD4 MBX (5G)


Front
Back
802.11ac Dual Band Wi-Fi
8x PoE Ethernet Ports
Up to 4x 5G Radios
Upgradable Module
QMA Connectors
2x USB WAN Ports

HD2 MBX (5G)


Front
Back
802.11ac Dual Band Wi-Fi
8x PoE Ethernet Ports
Up to 2x 5G Radios
Upgradable Module
SMA Connectors
2x USB WAN Ports

2.17.2 LED Indicators

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

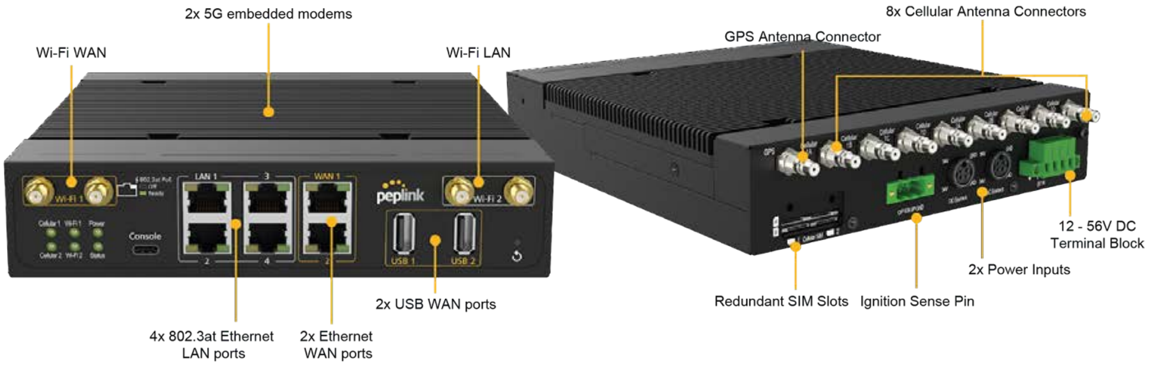
Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

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

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

2.18 MAX MBX Mini

2.18.1 Panel Appearance


2x 5G embedded modems
Wi-Fi WAN
Wi-Fi LAN
8x Cellular Antenna Connectors
GPS Antenna Connector
12 - 56V DC
Terminal Block
2x Power Inputs
2x USB WAN ports
Redundant SIM Slots
Ignition Sense Pin
4x 802.3at Ethernet
LAN ports
2x Ethernet
WAN ports

2.18.2 LED Indicators

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

LED Indicator	
Power LED	OFF – Power off
	GREEN – Power on

LAN Ports	
Green LED	ON – POE Enabled OFF - POE Disabled
Orange LED	Blinking – 10 / 100 / 1000 Mbps with activity
	OFF – No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports

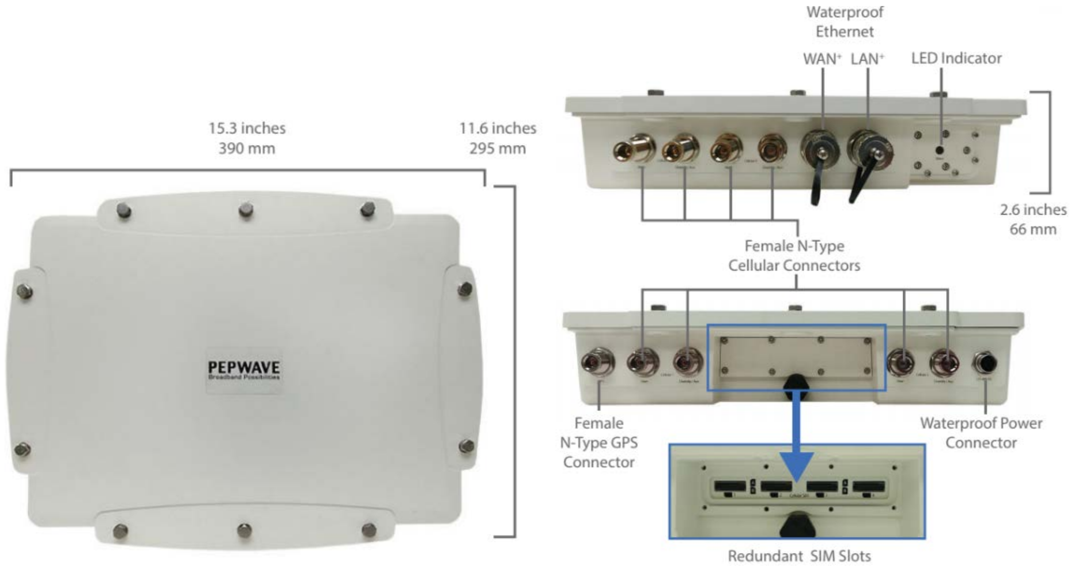
WAN Ports	
Right LED	GREEN – 1000 Mbps
	ORANGE – 100 Mbps
	OFF – 10 Mbps
Left LED	Solid – Port is connected without traffic

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

Console & USB Ports	
Console Port	Reserved for engineering use
USB Ports	For connecting 4G/3G USB modems

2.19 MAX HD4 IP67

2.19.1 Panel Appearance


Waterproof Ethernet
WAN⁺ LAN⁺
LED Indicator
15.3 inches
390 mm
11.6 inches
295 mm
2.6 inches
66 mm
Female N-Type Cellular Connectors
PEPWAVE
Female N-Type GPS Connector
Waterproof Power Connector
Redundant SIM Slots

2.19.2 LED Indicators

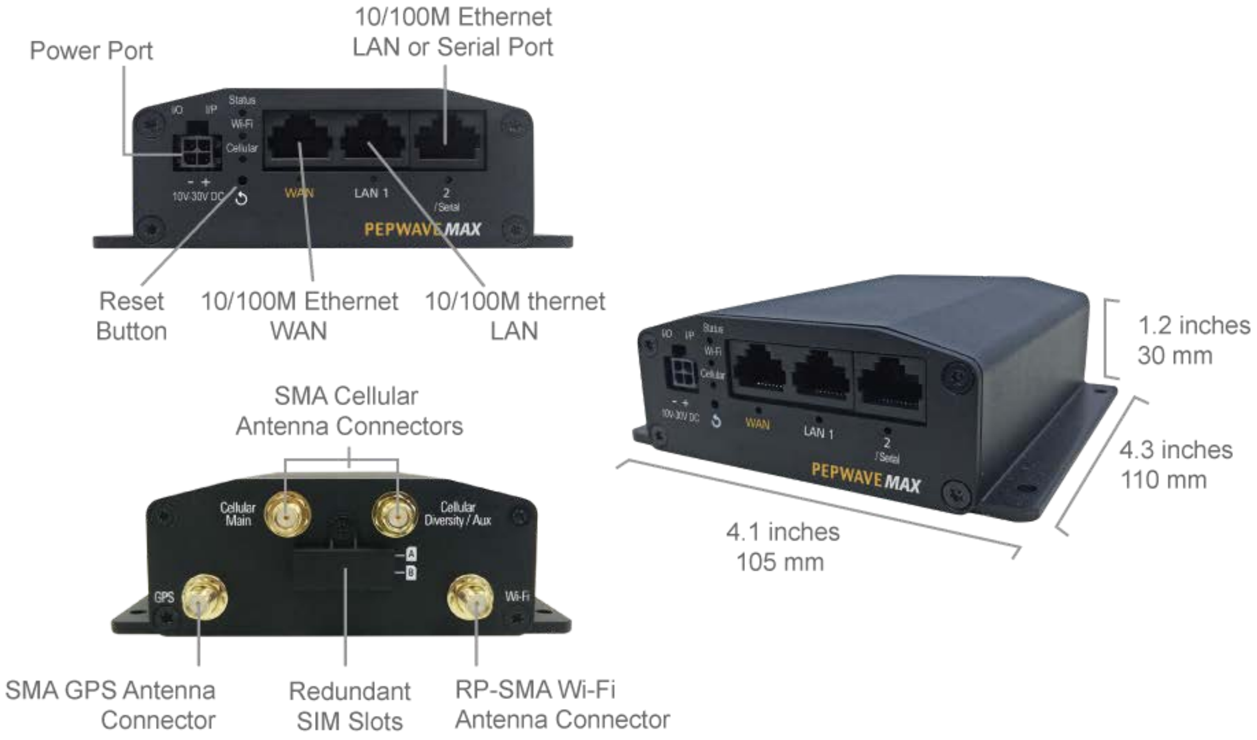
The statuses indicated by the front panel LEDs are as follows:

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

2.20 MAX BR1 Classic

For certification information, please refer to [Appendix B: Declaration]

2.20.1 Panel Appearance


Power Port
10/100M Ethernet LAN or Serial Port
I/O
I/P
Status
Wi-Fi
Cellular
10V-30V DC
WAN
LAN 1
2 / Serial
PEPWAVE MAX
Reset Button
10/100M Ethernet WAN
10/100M thernet LAN
SMA Cellular Antenna Connectors
Cellular Main
Cellular Diversity / Aux
A
B
GPS
Wi-Fi
SMA GPS Antenna Connector
Redundant SIM Slots
RP-SMA Wi-Fi Antenna Connector
1.2 inches 30 mm
4.3 inches 110 mm
4.1 inches 105 mm

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

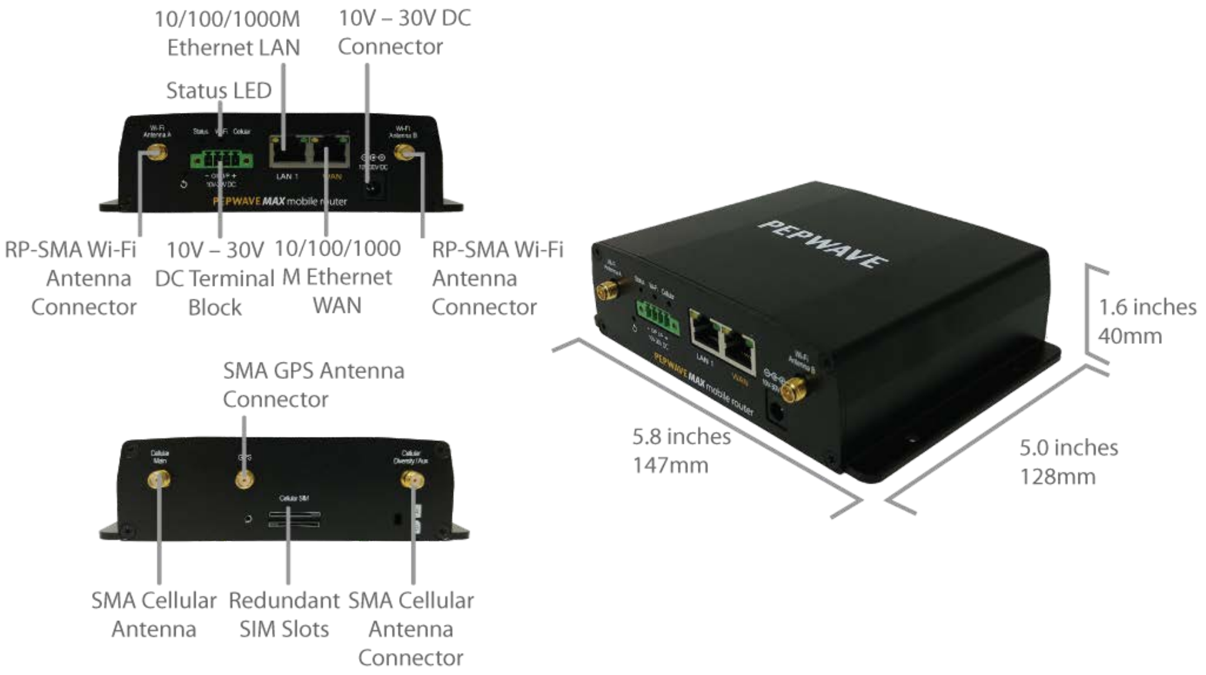
Wi-Fi Indicators		
Wi-Fi	OFF	Disabled intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

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

2.21 MAX BR1 MK2

For certification information, please refer to Appendix B: Declaration

2.21.1 Panel Appearance


10/100/1000M Ethernet LAN
10V – 30V DC Connector
Status LED
RP-SMA Wi-Fi Antenna Connector
10V – 30V DC Terminal Block
10/100/1000 M Ethernet WAN
RP-SMA Wi-Fi Antenna Connector
SMA GPS Antenna Connector
SMA Cellular Antenna
Redundant SIM Slots
SMA Cellular Antenna Connector
1.6 inches 40mm
5.8 inches 147mm
5.0 inches 128mm
PEPWAVE
PEPWAVE MAX mobile router

2.21.2 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

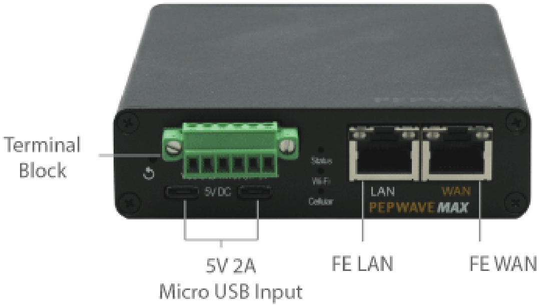
Wi-Fi Indicators		
Wi-Fi	OFF	Disabled intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

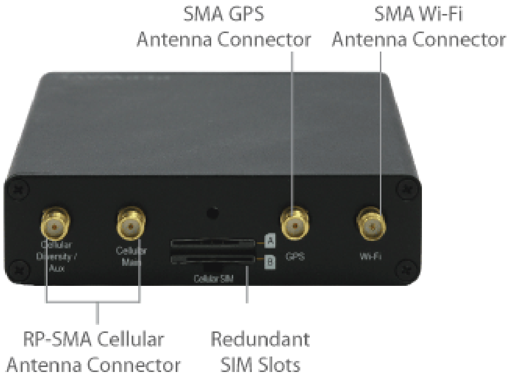
Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

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	Port is not connected
Port Type	Auto MDI/MDI-X ports	

2.22 MAX BR1 Slim

2.22.1 Panel Appearance


Terminal
Block
5V 2A
Micro USB Input
FE LAN
FE WAN
LAN
WAN
PEPWAVE MAX


SMA GPS
Antenna Connector
SMA Wi-Fi
Antenna Connector
RP-SMA Cellular
Antenna Connector
Redundant
SIM Slots

2.22.2 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

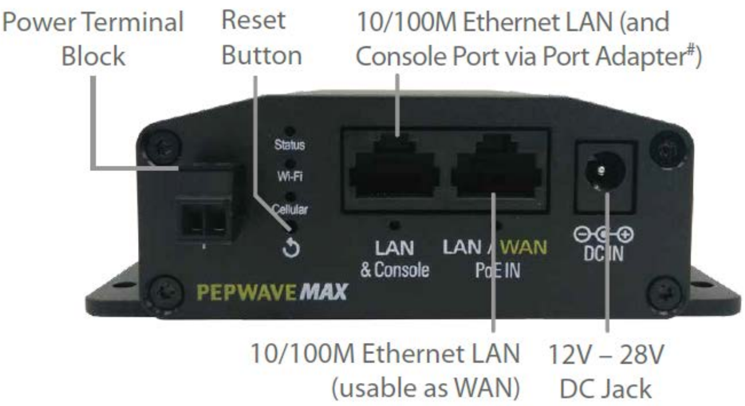
Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

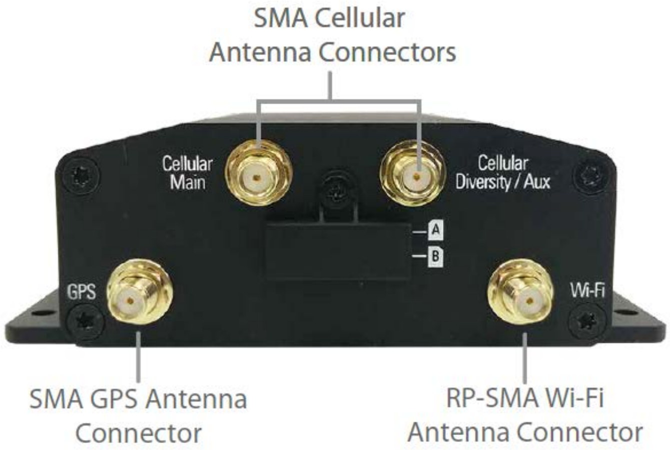
LAN and Ethernet WAN Ports		
Green LED	ON	100 Mbps
	OFF	10 Mbps
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

2.23 MAX BR1 Mini

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

2.23.1 Panel Appearance


Power Terminal Block
Reset Button
10/100M Ethernet LAN (and Console Port via Port Adapter#)
Status
Wi-Fi
Cellular
LAN & Console
LAN / WAN PoE IN
DC IN
PEPWAVE MAX
10/100M Ethernet LAN (usable as WAN)
12V – 28V DC Jack


SMA Cellular Antenna Connectors
Cellular Main
Cellular Diversity / Aux
A
B
GPS
Wi-Fi
SMA GPS Antenna Connector
RP-SMA Wi-Fi Antenna Connector

2.23.2 LED Indicators

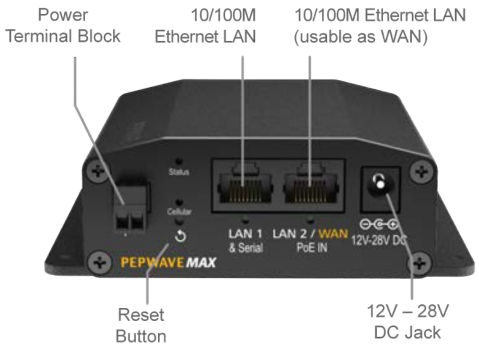
Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

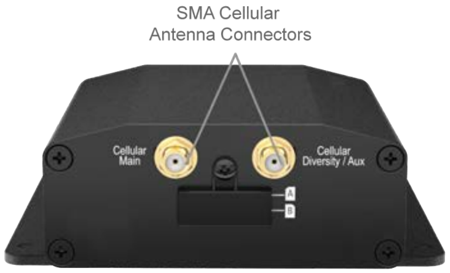
Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

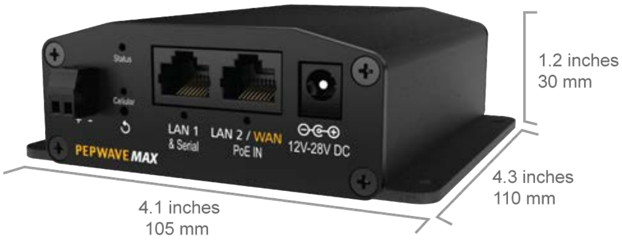
Wi-Fi Indicators		
Wi-Fi	OFF	Disabled intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

2.24 MAX BR1 Mini Core

2.24.1 Panel Appearance


Power
Terminal Block
10/100M
Ethernet LAN
10/100M Ethernet LAN
(usable as WAN)
Status
Cellular
LAN 1
& Serial
LAN 2 / WAN
PoE IN
12V-28V DC
PEPWAVE MAX
Reset
Button
12V – 28V
DC Jack


SMA Cellular
Antenna Connectors
Cellular
Main
Cellular
Diversity / Aux
A
B


1.2 inches
30 mm
4.3 inches
110 mm
4.1 inches
105 mm
Status
Cellular
LAN 1
& Serial
LAN 2 / WAN
PoE IN
12V-28V DC
PEPWAVE MAX

2.24.2 LED Indicators

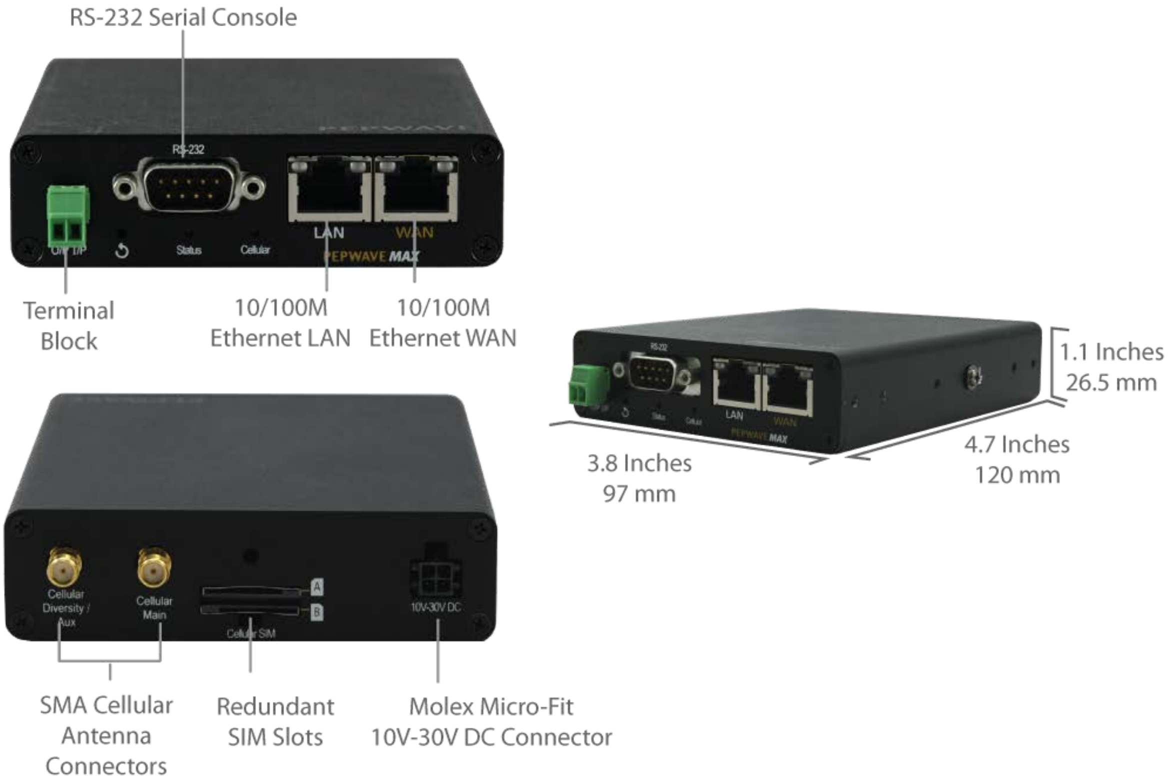
The statuses indicated by the front panel LEDs are as follows:

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
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

2.25 MAX BR1 M2M

2.25.1 Panel Appearance


RS-232 Serial Console
RS-232
LAN
WAN
Status
Cellular
PEPWAVE MAX
Terminal Block
10/100M Ethernet LAN
10/100M Ethernet WAN
1.1 Inches
26.5 mm
3.8 Inches
97 mm
4.7 Inches
120 mm
Cellular Diversity / Aux
Cellular Main
A
B
Cellular SIM
10V-30V DC
SMA Cellular Antenna Connectors
Redundant SIM Slots
Molex Micro-Fit 10V-30V DC Connector

2.25.2 LED Indicators

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

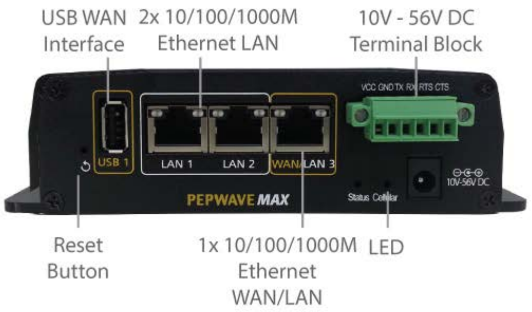
Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

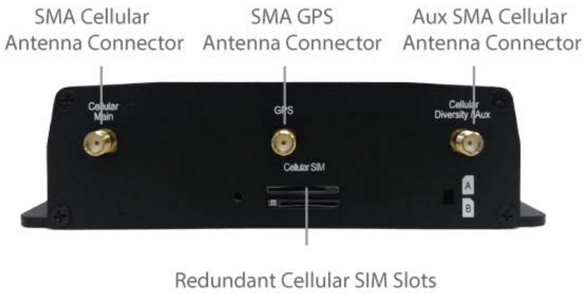
Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

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 ENT

2.26.1 Panel Appearance


USB WAN Interface
2x 10/100/1000M Ethernet LAN
10V - 56V DC Terminal Block
Reset Button
1x 10/100/1000M Ethernet WAN/LAN
LED


SMA Cellular Antenna Connector
SMA GPS Antenna Connector
Aux SMA Cellular Antenna Connector
Redundant Cellular SIM Slots

2.26.2 LED Indicators

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

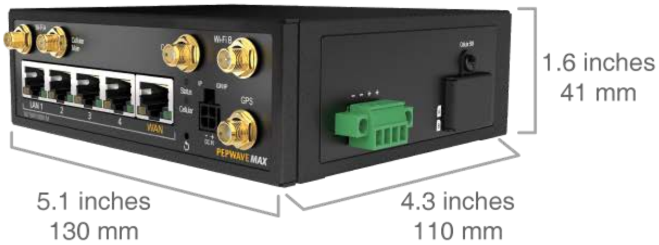
Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

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

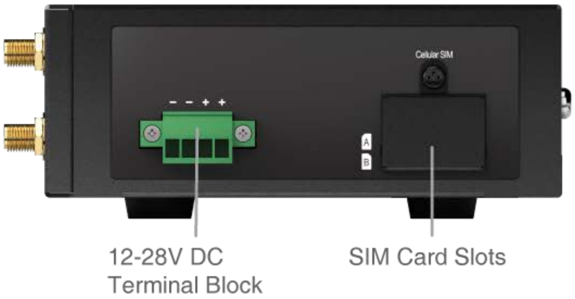
LAN and Ethernet WAN Ports		
Green LED	ON	10 / 100 / 1000 Mbps
Orange LED	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

2.27 MAX BR1 Pro

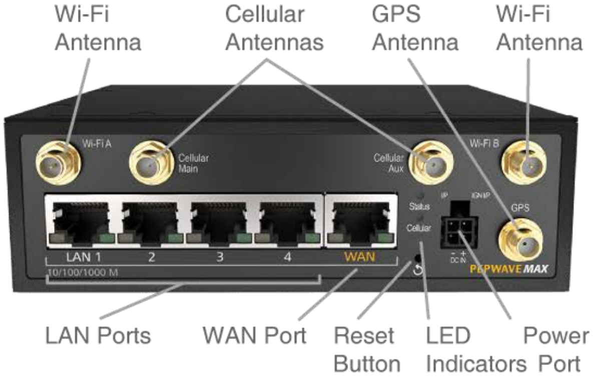
2.27.1 Panel Appearance


1.6 inches
41 mm
5.1 inches
130 mm
4.3 inches
110 mm

Side


12-28V DC
Terminal Block
SIM Card Slots

Front


Wi-Fi
Antenna
Cellular
Antennas
GPS
Antenna
Wi-Fi
Antenna
LAN Ports
WAN Port
Reset
Button
LED
Indicators
Power
Port

Back

2.27.2 LED Indicators

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

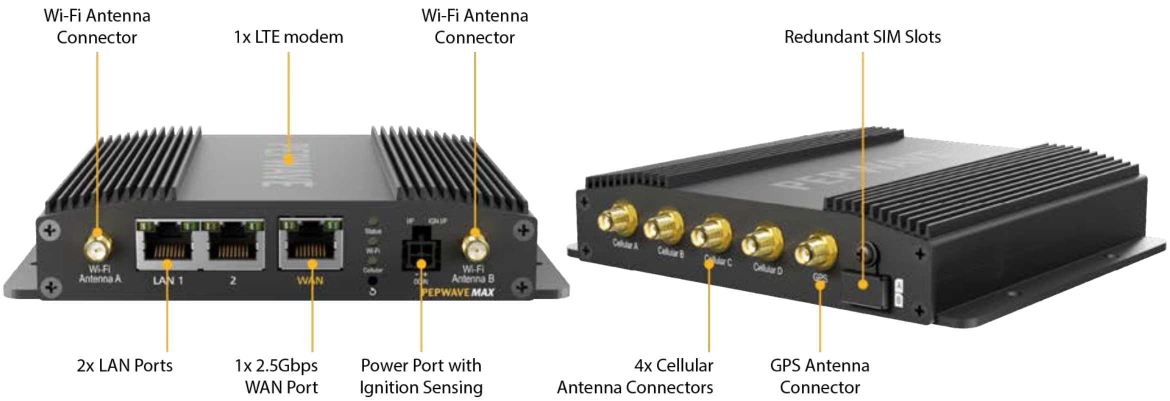
Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

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

2.28 MAX BR1 Pro (CAT-20)

2.28.1 Panel Appearance


Wi-Fi Antenna Connector
1x LTE modem
Wi-Fi Antenna Connector
Redundant SIM Slots
Wi-Fi Antenna A
LAN 1
2
WAN
Wi-Fi Antenna B
PEPWAVE MAX
Cellular A
Cellular B
Cellular C
Cellular D
GPS
2x LAN Ports
1x 2.5Gbps WAN Port
Power Port with Ignition Sensing
4x Cellular Antenna Connectors
GPS Antenna Connector

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

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

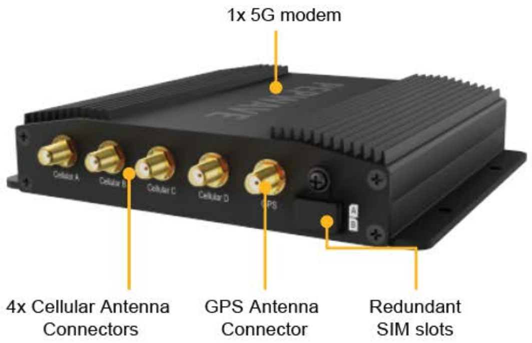
Wi-Fi Indicators		
Wi-Fi / Wi-Fi AP	OFF	Disabled intermittent
	ON	Connected to wireless network(s)

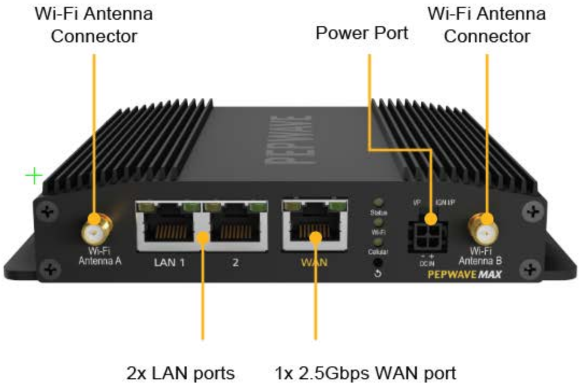
LAN Ports		
Green LED	ON	1000 Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

WAN Port		
Right LED	ON	1000 Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Left 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	

2.29 MAX BR1 Pro 5G

2.29.1 Panel Appearance


1x 5G modem
4x Cellular Antenna Connectors
GPS Antenna Connector
Redundant SIM slots


Wi-Fi Antenna Connector
Power Port
Wi-Fi Antenna Connector
2x LAN ports
1x 2.5Gbps WAN port

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

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

Wi-Fi Indicators		
Wi-Fi / Wi-Fi AP	OFF	Disabled intermittent
	ON	Connected to wireless network(s)

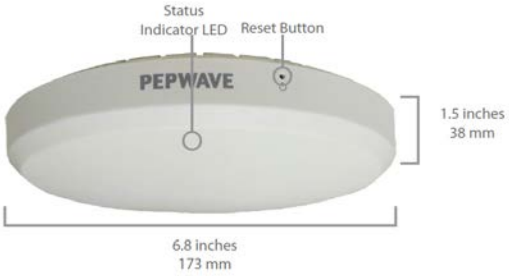
LAN Ports

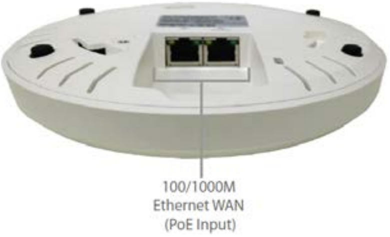
Green LED	ON	1000 Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

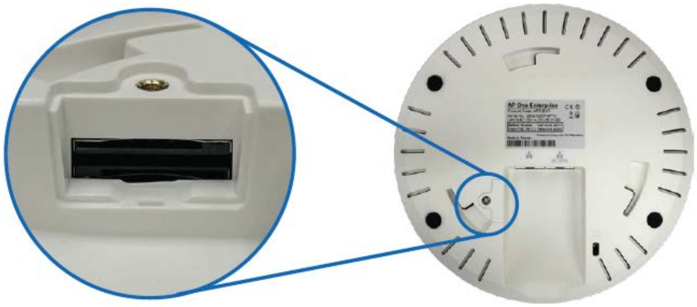
WAN Port		
Right LED	ON	1000 Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Left LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

2.30 MAX Hotspot

2.30.1 Panel Appearance


Status Indicator LED
Reset Button
PEPWAVE
1.5 inches
38 mm
6.8 inches
173 mm


100/1000M
Ethernet WAN
(PoE Input)



Screw Open the Panel to
Reveal Redundant SIM Slots

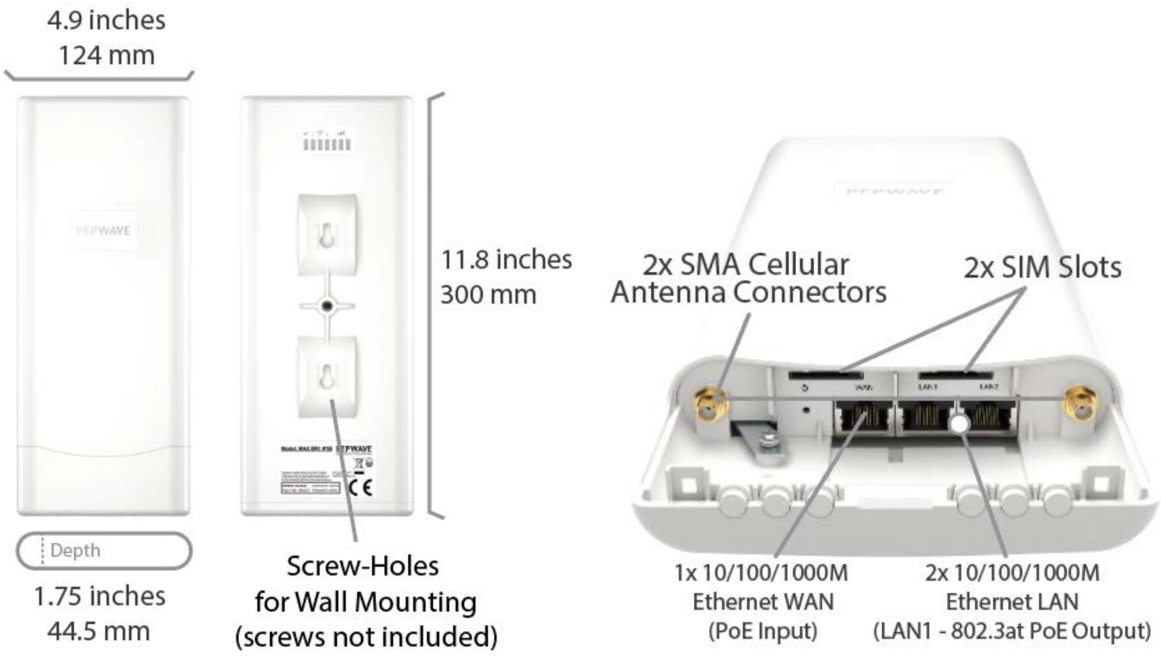
2.30.2 LED Indicators

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

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	

2.31 MAX BR1 IP55

2.31.1 Panel Appearance

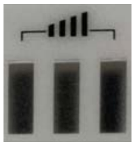

4.9 inches
124 mm
Depth
1.75 inches
44.5 mm
11.8 inches
300 mm
Screw-Holes
for Wall Mounting
(screws not included)
2x SMA Cellular
Antenna Connectors
2x SIM Slots
1x 10/100/1000M
Ethernet WAN
(PoE Input)
2x 10/100/1000M
Ethernet LAN
(LAN1 - 802.3at PoE Output)

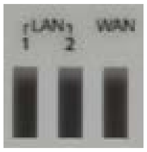
2.31.2 LED Indicators

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

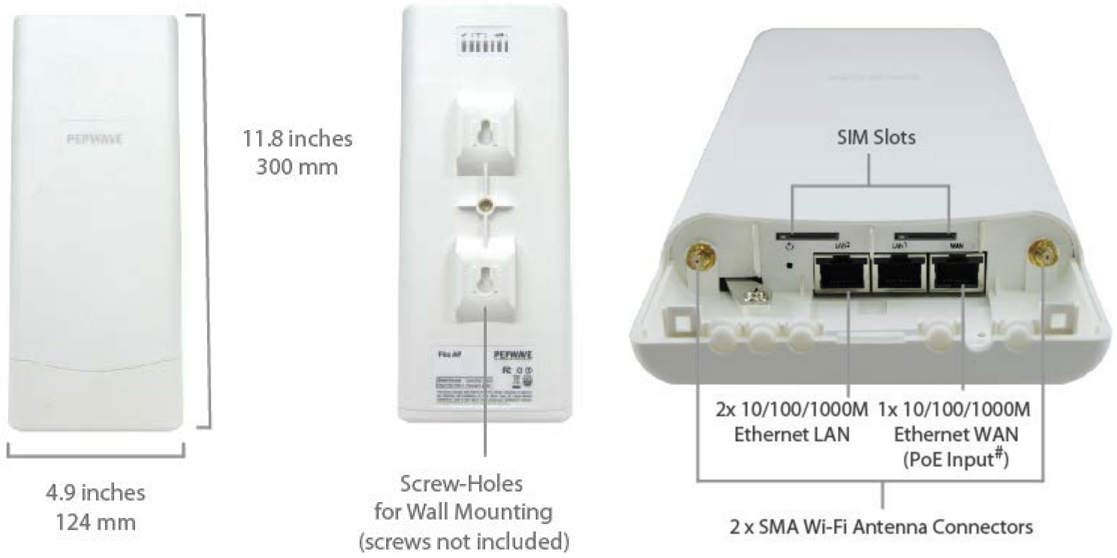
LAN and Ethernet WAN Ports		
Green LED	ON	1000Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

Cellular Indicators		
Cellular 	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

2.32 MAX BR2 IP55

2.32.1 Panel Appearance


11.8 inches
300 mm
4.9 inches
124 mm
Screw-Holes
for Wall Mounting
(screws not included)
SIM Slots
2x 10/100/1000M Ethernet LAN
1x 10/100/1000M Ethernet WAN (PoE Input#)
2 x SMA Wi-Fi Antenna Connectors

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

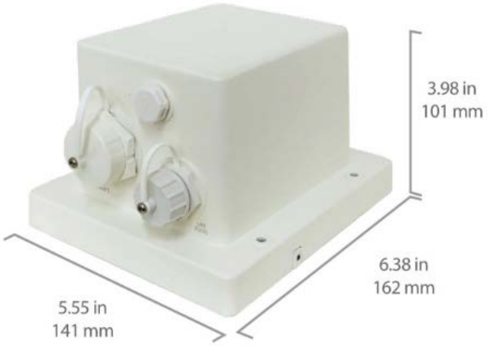
Wi-Fi Indicators		
Wi-Fi	OFF	Disabled Intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

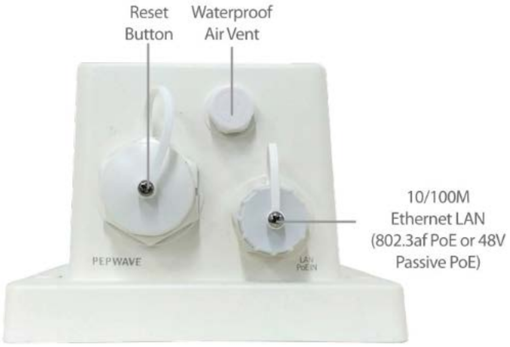
Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	ON	Connecting or connected to network(s)

LAN and Ethernet WAN Ports		
Green LED	ON	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	

2.33 MAX BR1 IP67

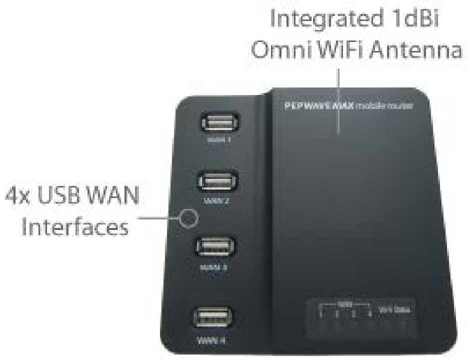
2.33.1 Panel Appearance

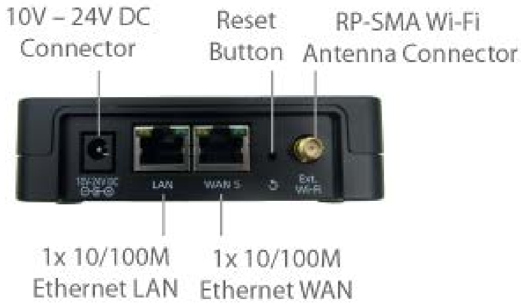

3.98 in
101 mm
6.38 in
162 mm
5.55 in
141 mm


Reset
Button
Waterproof
Air Vent
10/100M
Ethernet LAN
(802.3af PoE or 48V
Passive PoE)
PEPWAVE
LAN
PoE IN

2.34 MAX On-The-Go

2.34.1 Panel Appearance


Integrated 1dBi
Omni WiFi Antenna
4x USB WAN
Interfaces


10V – 24V DC
Connector
Reset
Button
RP-SMA Wi-Fi
Antenna Connector
1x 10/100M
Ethernet LAN
1x 10/100M
Ethernet WAN

2.34.2 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

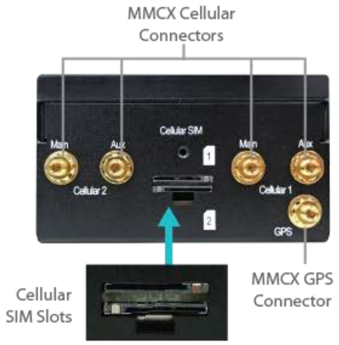
Wi-Fi Indicators		
Wi-Fi	OFF	Disconnected from AP
	Green	Connected to AP

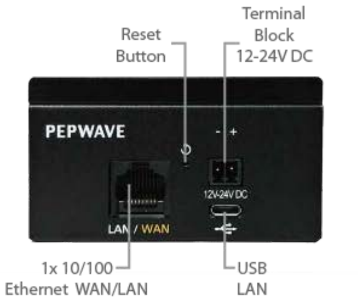
Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Green	Ready

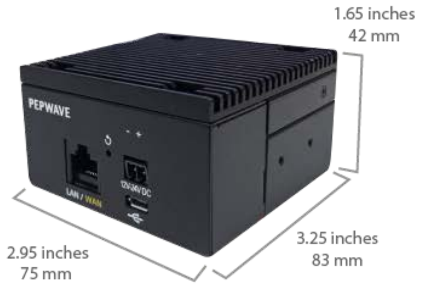
LAN and Ethernet WAN Ports		
Green LED	ON	100 Mbps
	OFF	10 Mbps
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
Port Type	Auto MDI/MDI-X ports	

2.35 SpeedFusion Engine

2.35.1 Panel Appearance

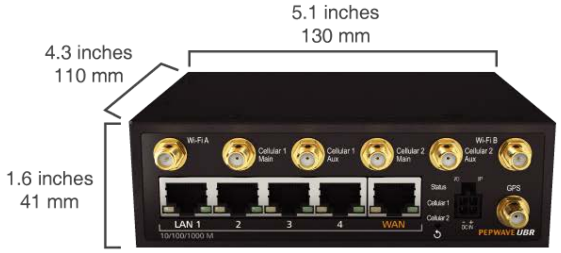

MMCX Cellular Connectors
Main
Aux
Cellular SIM
1
Main
Aux
Cellular 2
Cellular 1
2
GPS
Cellular SIM Slots
MMCX GPS Connector


Reset Button
Terminal Block 12-24V DC
PEPWAVE
12V-24V DC
LAN / WAN
1x 10/100 Ethernet WAN/LAN
USB LAN

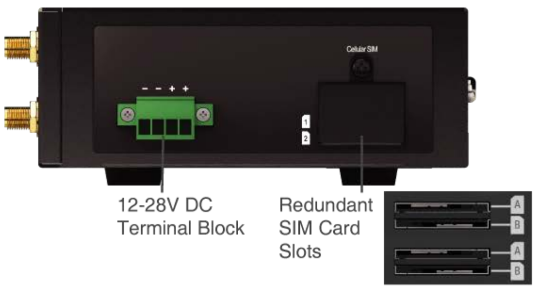

1.65 inches 42 mm
PEPWAVE
LAN / WAN
12V-24V DC
2.95 inches 75 mm
3.25 inches 83 mm

2.36 UBR LTE

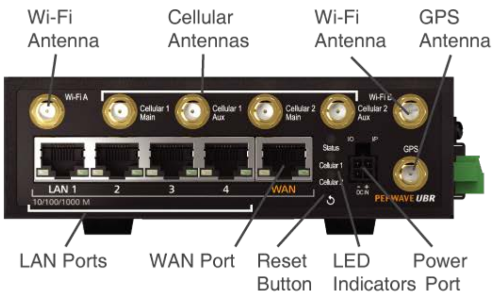
2.36.1 Panel Appearance


5.1 inches 130 mm
4.3 inches 110 mm
1.6 inches 41 mm
Wi-Fi A
Cellular 1 Main
Cellular 1 Aux
Cellular 2 Main
Wi-Fi B
Cellular 2 Aux
GPS
LAN 1
2
3
4
WAN
10/100/1000 M
PEPWAVE UBR

Side


Cellular SIM
1
2
12-28V DC Terminal Block
Redundant SIM Card Slots
A
B
A
B

Front


Wi-Fi Antenna
Cellular Antennas
Wi-Fi Antenna
GPS Antenna
Wi-Fi A
Cellular 1 Main
Cellular 1 Aux
Cellular 2 Main
Cellular 2 Aux
Wi-Fi B
GPS
LAN 1
2
3
4
WAN
10/100/1000 M
PEPWAVE UBR
LAN Ports
WAN Port
Reset Button
LED Indicators
Power Port

Back

2.36.2 LED Indicators

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

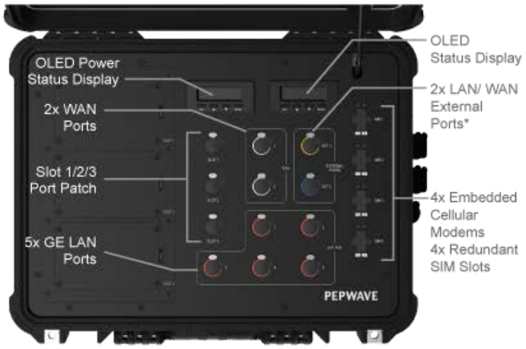
Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking Red	Boot up error
	Green	Ready

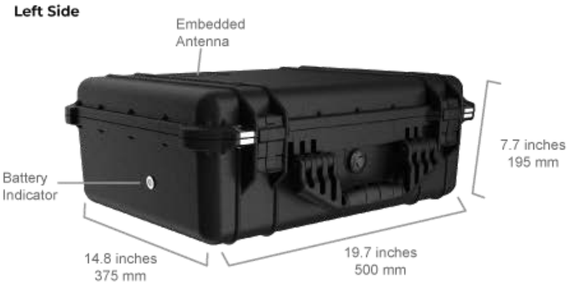
LAN and Ethernet WAN Ports		
Green LED	ON	1000 Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

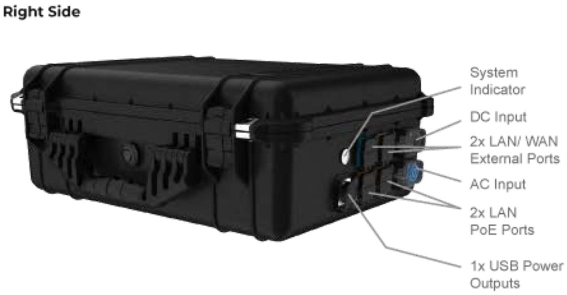
Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	Blinking Slowly	Connecting to network(s)
	Green	Connected to network(s)

2.37 PDX

2.37.1 Panel Appearance


OLED Power
Status Display
2x WAN
Ports
Slot 1/2/3
Port Patch
5x GE LAN
Ports
OLED
Status Display
2x LAN/ WAN
External
Ports*
4x Embedded
Cellular
Modems
4x Redundant
SIM Slots
PEPWAVE


Left Side
Embedded
Antenna
Battery
Indicator
7.7 inches
195 mm
14.8 inches
375 mm
19.7 inches
500 mm


Right Side
System
Indicator
DC Input
2x LAN/ WAN
External Ports
AC Input
2x LAN
PoE Ports
1x USB Power
Outputs

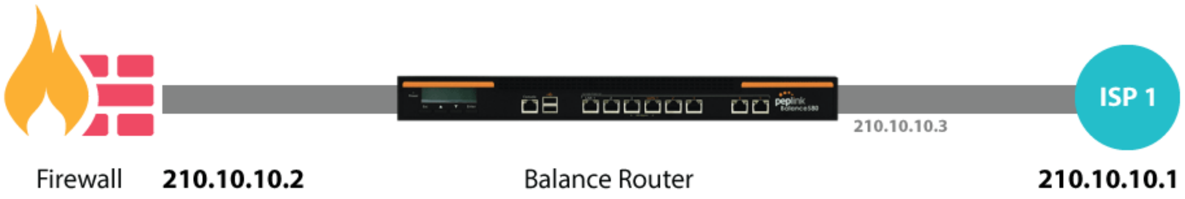
2.37.2 LED Indicators

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



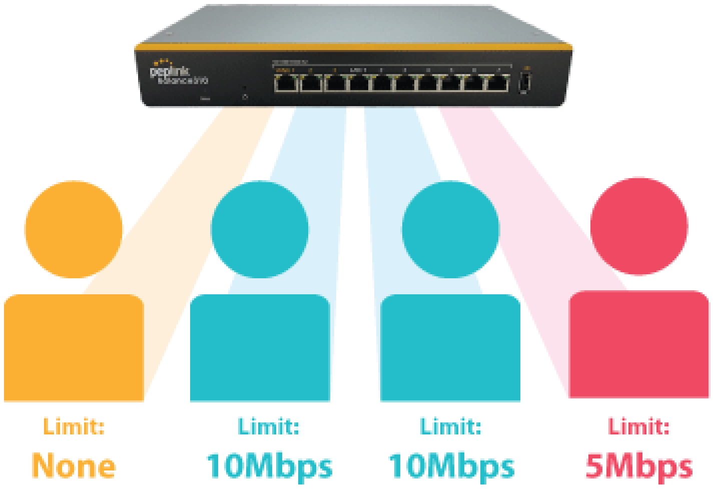
As your organization grows, it may require more bandwidth, but modifying your network can be tedious. In **Drop-in Mode**, you can conveniently install your Peplink router without making any changes to your network. For any reason your Peplink router looses power, the **LAN Bypass** will safely and automatically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

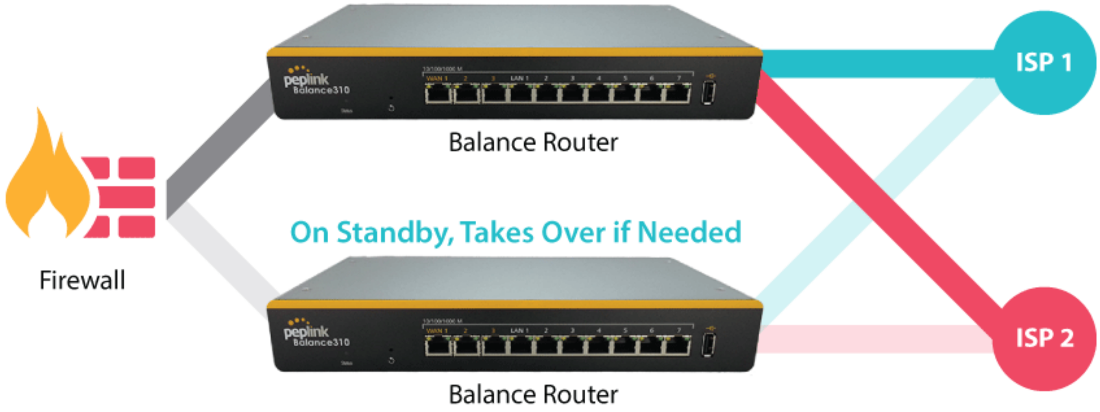
VoIP and videoconferencing are highly sensitive to latency. With QoS, Peplink routers can detect VoIP traffic and assign it the highest priority, giving you crystal-clear calls.

3.3 Per-User Bandwidth Control


Limit:
None
Limit:
10Mbps
Limit:
10Mbps
Limit:
5Mbps

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.

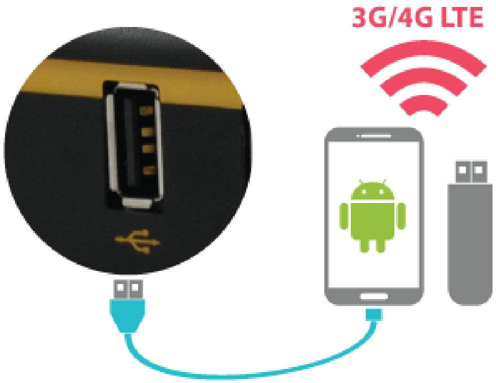
3.4 High Availability via VRRP


ISP 1
Balance Router
Firewall
On Standby, Takes Over if Needed
ISP 2
Balance Router

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)

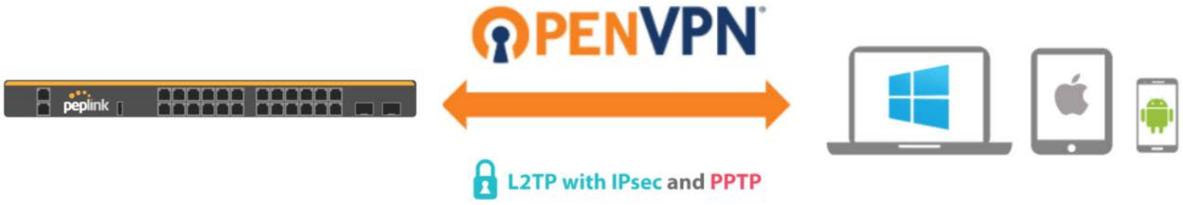
3.5 USB Modem and Android Tethering



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


OPENVPN
peplink
L2TP with IPsec and PPTP

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.

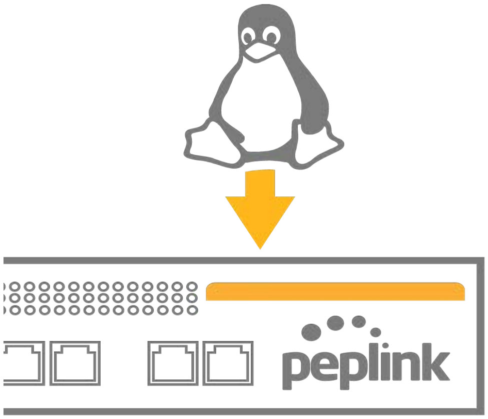
Click here for the full instructions on setting up L2TP with IPsec.
Click here for the full instructions on setting up OpenVPN connections

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 KVM Virtualization



KVM is a virtualisation module that allows administrators using our routers to host a large range of virtual machines. KVM is now supported on some MediaFast / ContentHub routers.

[Click here for the full instructions on how to set up KVM]()
[Click here for the full instructions on how to set up KVM with USB Storage]()

3.9 DPI Engine

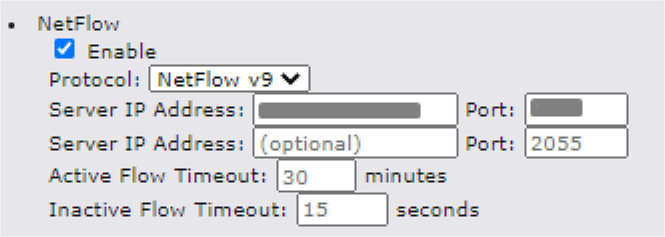
The DPI report written in the updated KB article will show further information on InControl2 through breaking down application categories into subcategories.

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

3.10 NetFlow

NetFlow protocol is used to track network traffic. Tracking information from NetFlow can be sent to the NetFlow collector, which analyzes data and generates reports for review.

Note: To enable this feature, go to https://<Device's IP>/cgi-bin/MANGA/support.cgi

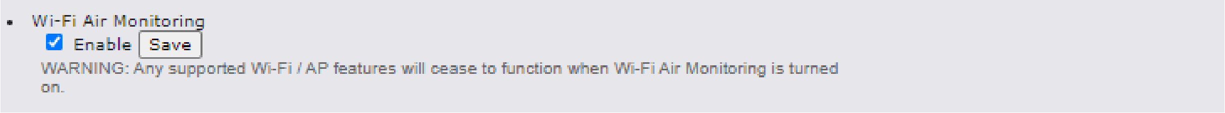


- NetFlow
  ☑ Enable
  Protocol: NetFlow v9
  Server IP Address: [redacted] Port: [redacted]
  Server IP Address: (optional) Port: 2055
  Active Flow Timeout: 30 minutes
  Inactive Flow Timeout: 15 seconds

3.11 Wi-Fi Air Monitoring

Pepwave routers support Wi-Fi “Air Monitoring Mode” which used to troubleshoot remotely and proactively monitor Wi-Fi and WAN performance. The report can be viewed under InControl 2 > Reports > AirProbe Reports after enabling Wi-Fi Air Monitoring.

Note: To enable this feature, go to https://<Device's IP>/cgi-bin/MANGA/support.cgi



- Wi-Fi Air Monitoring
  ☑ Enable
  WARNING: Any supported Wi-Fi / AP features will cease to function when Wi-Fi Air Monitoring is turned on.

3.12 SP Default Configuration

The SP Default Configuration feature written in the updated KB article allows for the provisioning of custom made settings (a.k.a. InControl2 configuration) via the Ethernet LAN port and is ideal for those wanting to do a bulk deployment of many Peplink devices.

Note: If you would like to use this feature, please contact your purchase point (Eg.VAD).

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 5G/4G LTE 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.

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

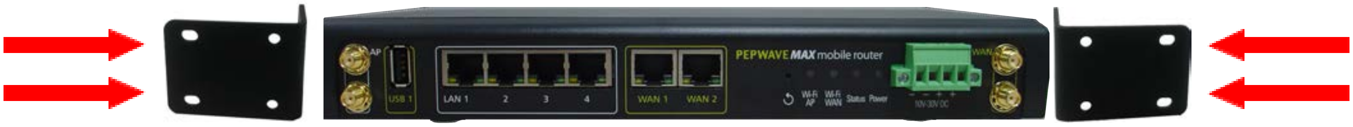
5.1 Wall Mount

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.

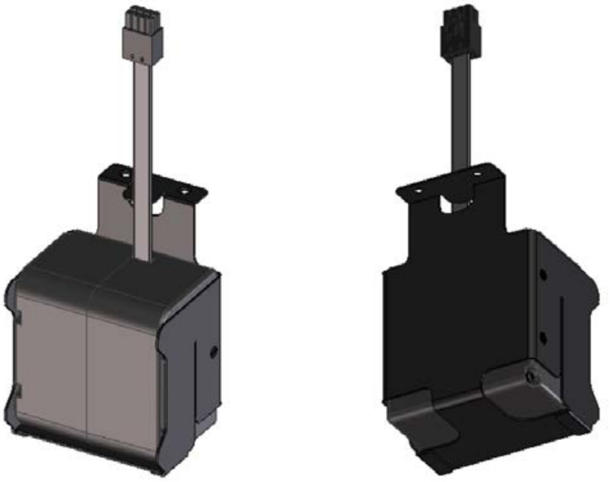

PEPWAVE MAX mobile router
USB 1
LAN 1
2
3
4
WAN 1
WAN 2
Wi-Fi AP
Wi-Fi WAN
Status
Power
10V-30V DC

5.3 IP67 Installation Guide

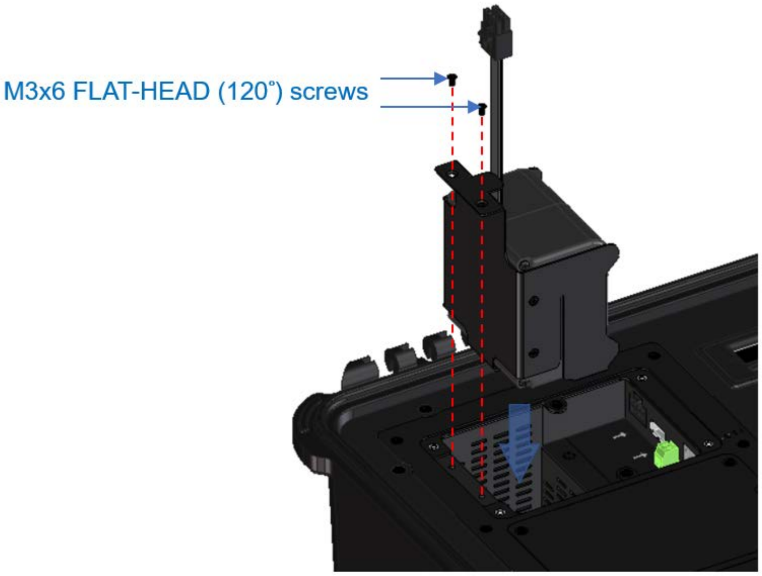
Installation instructions for IP67 devices can be found here:
http://download.peplink.com/manual/IP67_Installation_Guide.pdf

5.4 PDX Accessory Kit Installation Guide

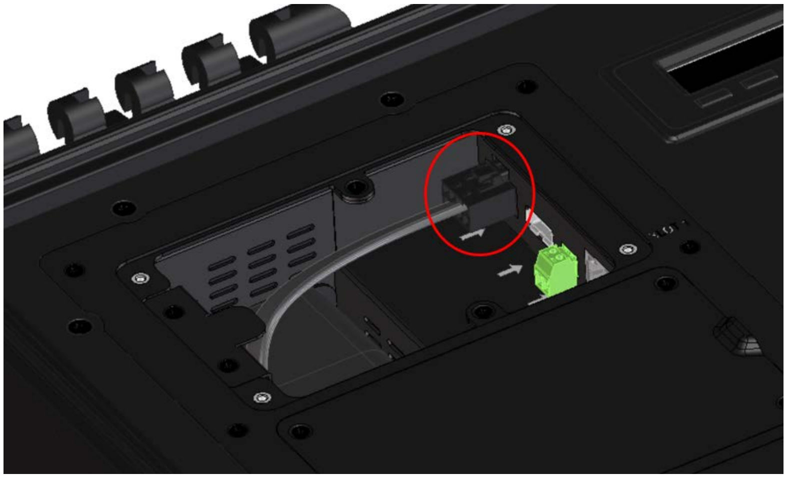
5.4.1 Battery Set appearance



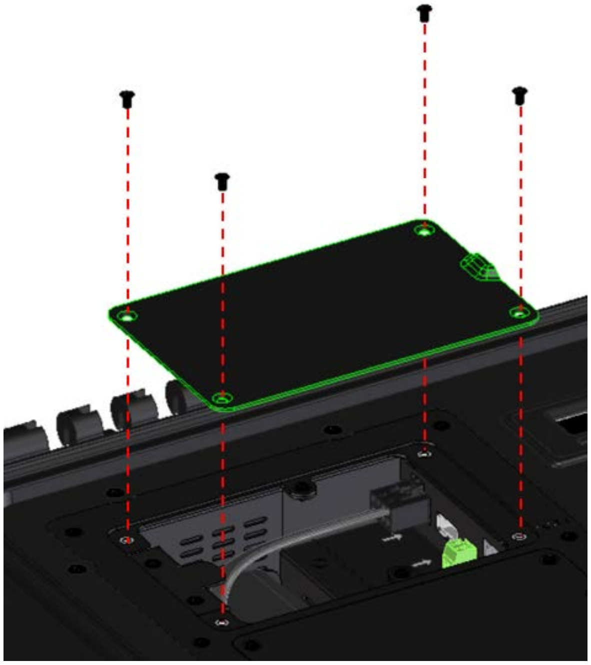
- Step 1: Lock the battery set in the slot with 2 pcs M3 screws.


M3x6 FLAT-HEAD (120˚) screws

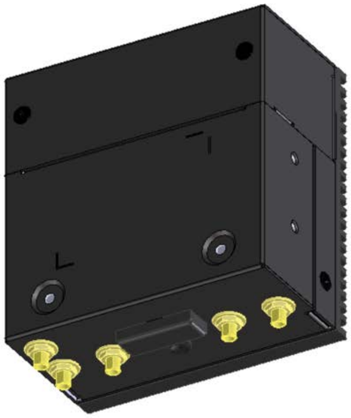
- Step 2: Plug power cable into the socket



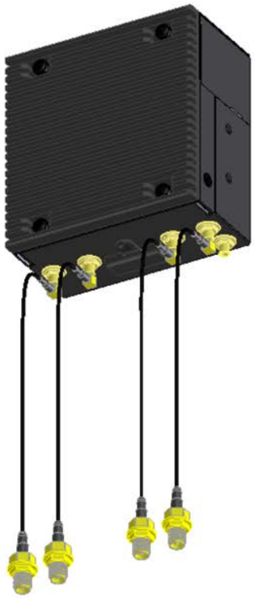
- STEP 3: Lock the slot cover with 4 pcs M3 screws.

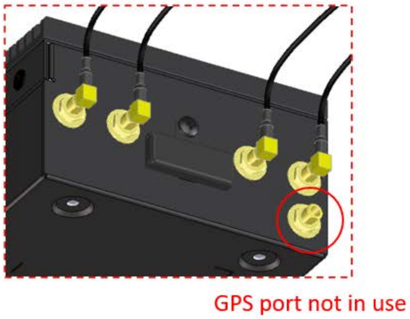


5.4.2 SFE-DUO Set appearance

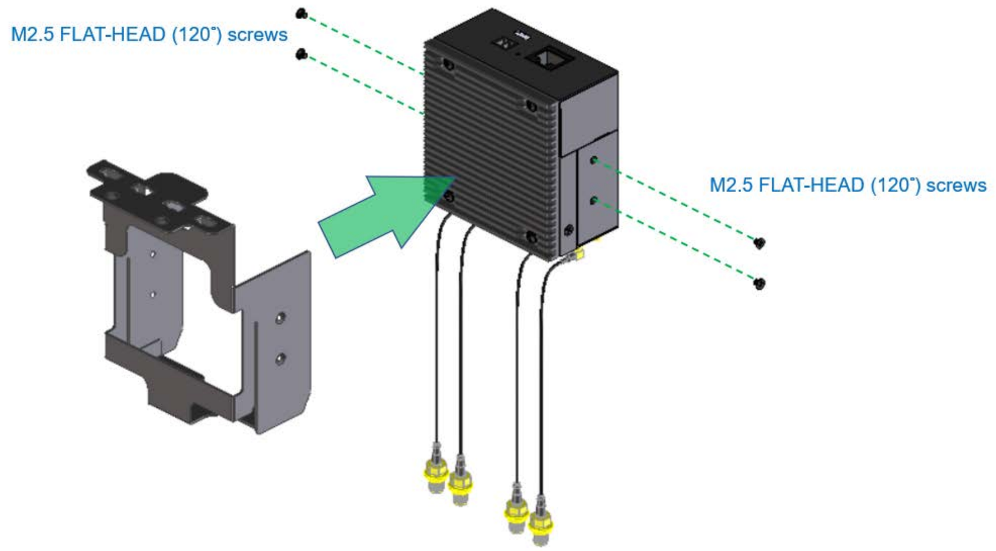


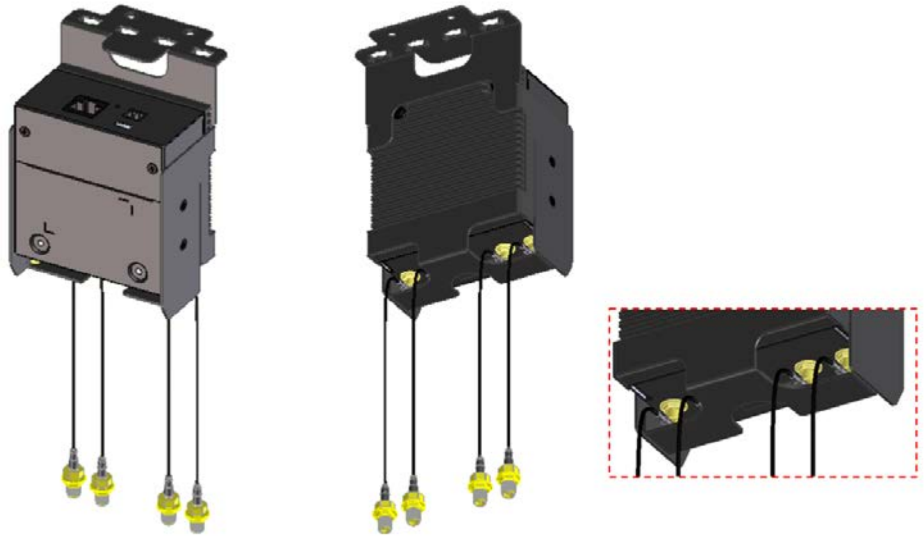
- STEP 1: Assemble SMA cables to the device



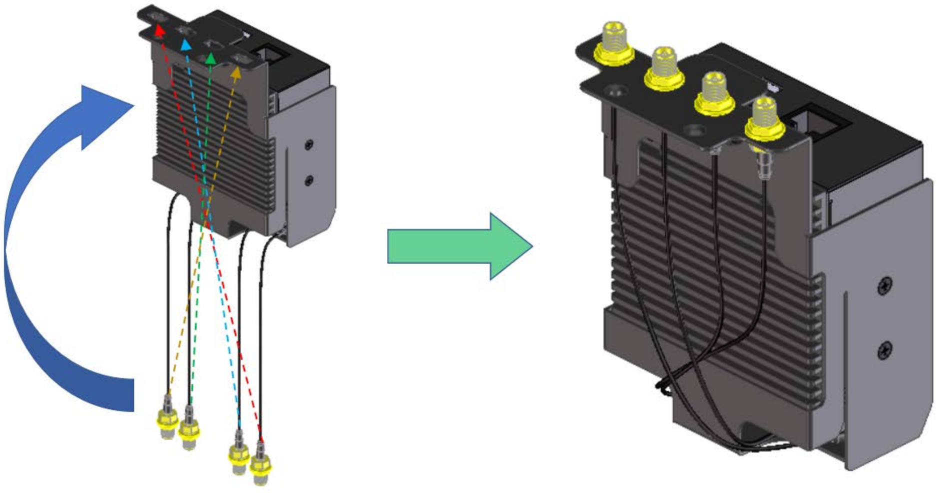

GPS port not in use

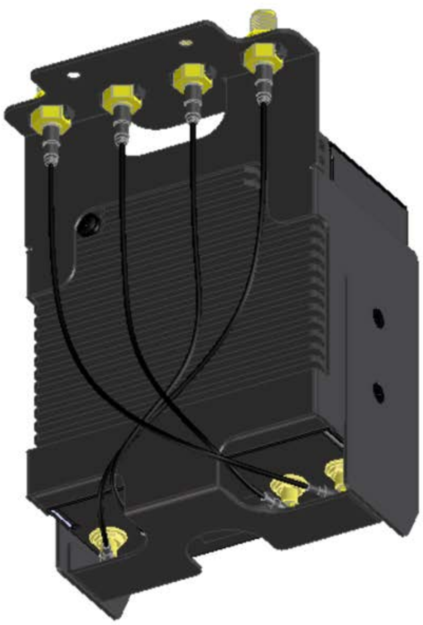
- STEP 2: Assemble bracket to the device

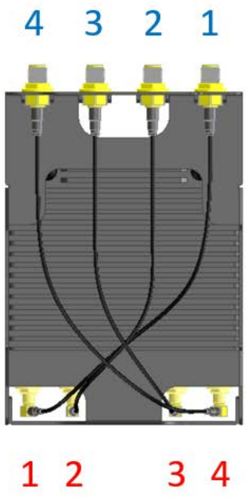

M2.5 FLAT-HEAD (120˚) screws
M2.5 FLAT-HEAD (120˚) screws



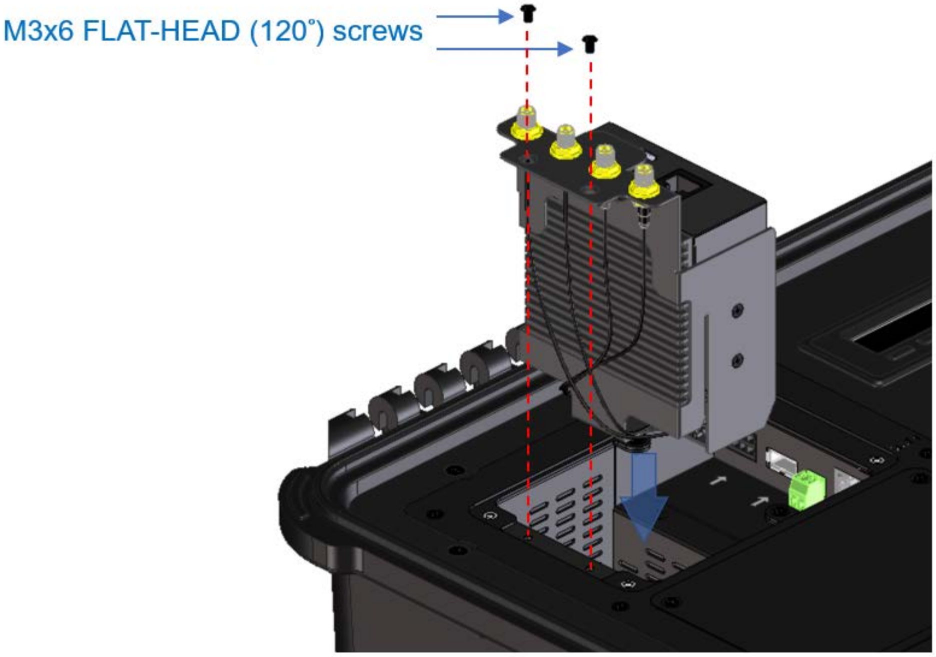
- STEP 3: Assemble SMA connectors to the bracket



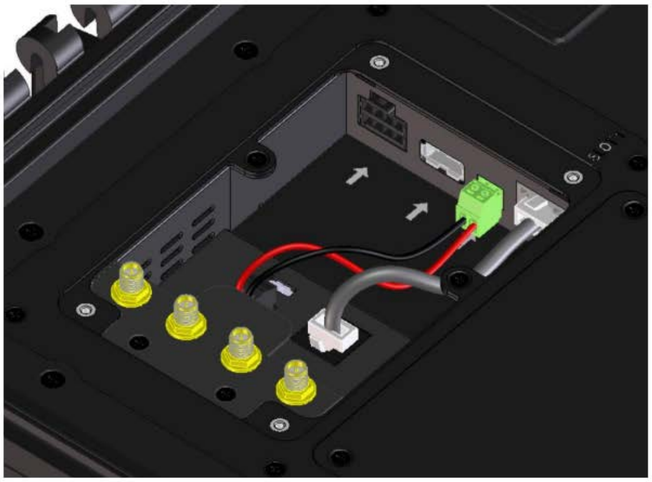


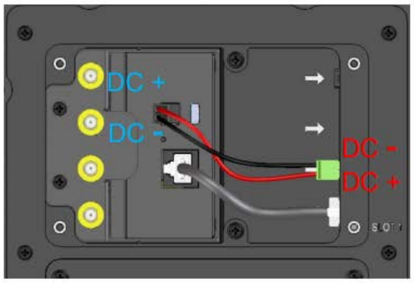


- STEP 4: Lock the SFE-Duo set in the slot with 2 pcs M3 screws.

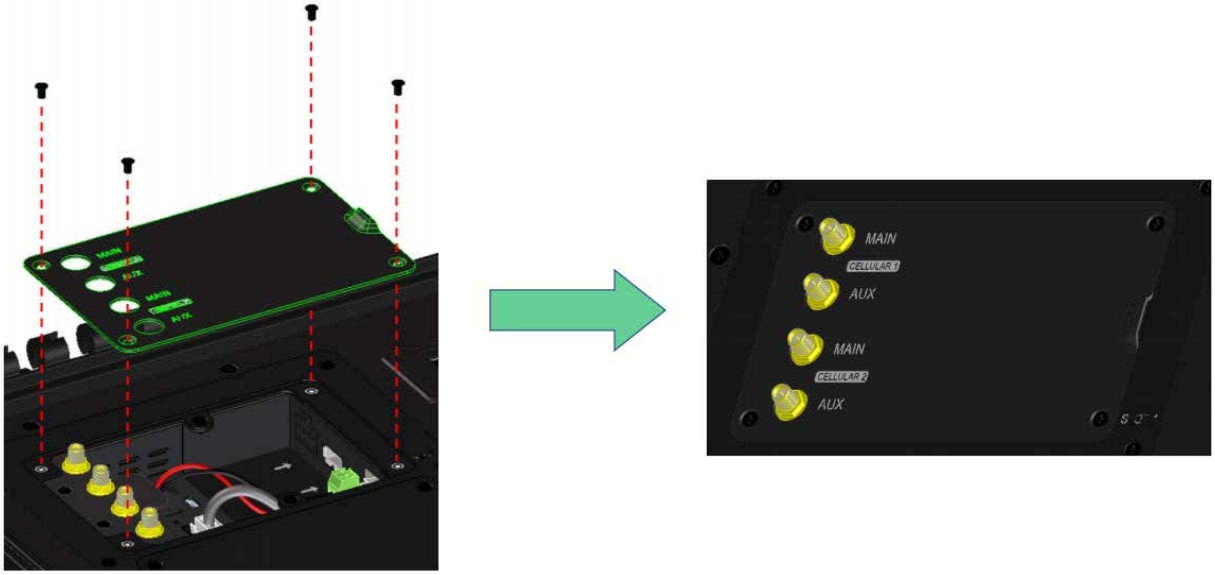

M3x6 FLAT-HEAD (120˚) screws

- STEP 5: Connect DC power & ETH port





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


MAIN
AUX
MAIN
AUX
MAIN
CELLULAR 1
AUX
MAIN
CELLULAR 2
AUX

0

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

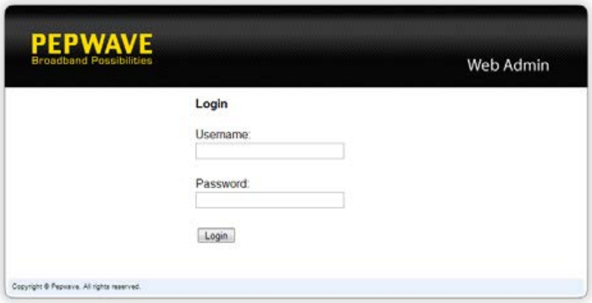
   (This is the default LAN IP address for Pepwave routers.)

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

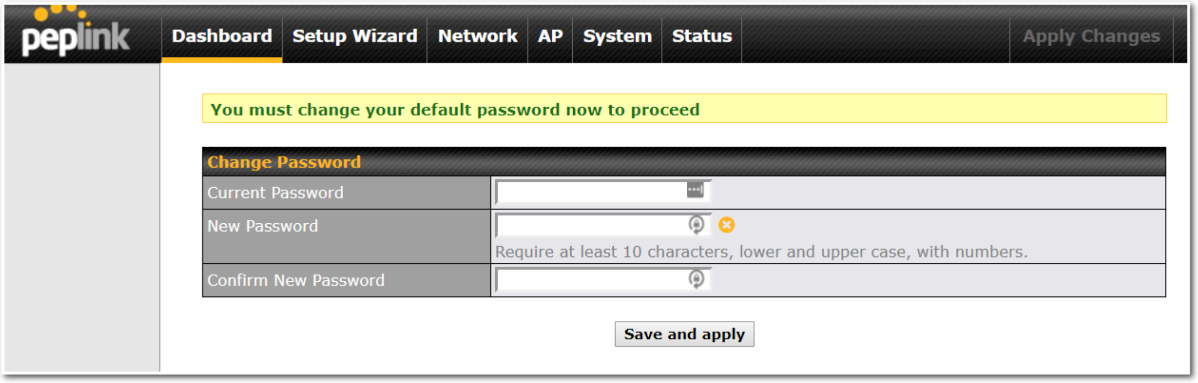
   Username: admin

   Password: admin

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


PEPWAVE
Broadband Possibilities
Web Admin
Login
Username:
Password:
Login
Copyright © Pepwave. All rights reserved.

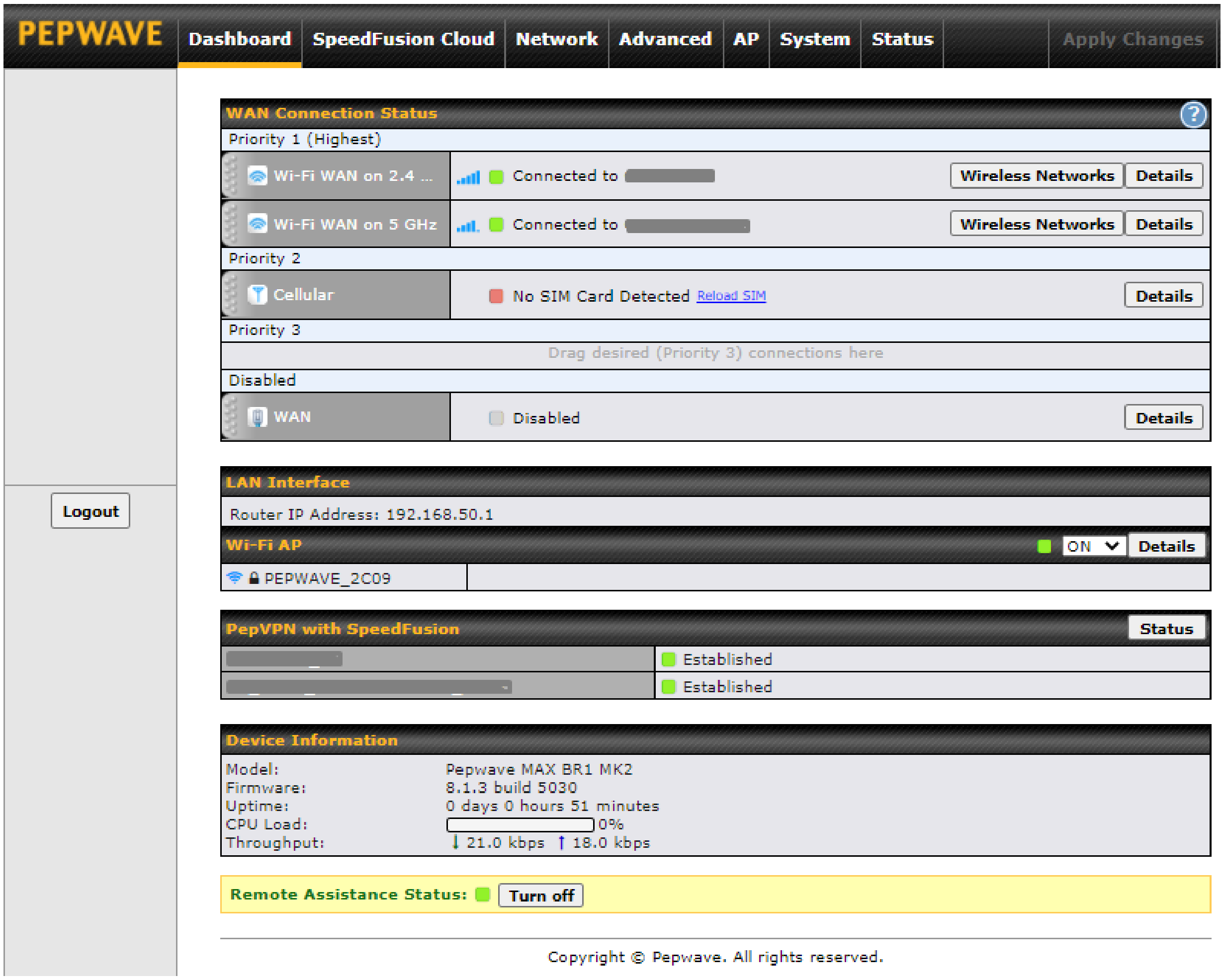
- You must change the default password on the first successful logon.
- Password requirements are: A minimum of 10 lower AND upper case characters, including at least 1 number.
- When HTTP is selected, the URL will be redirected to HTTPS by default.


peplink
Dashboard
Setup Wizard
Network
AP
System
Status
Apply Changes
Save and apply

You must change your default password now to proceed

Change Password	
Current Password	
New Password	Require at least 10 characters, lower and upper case, with numbers.
Confirm New Password	

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


PEPWAVE
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
Apply Changes
Wireless Networks
Details
Reload SIM
Logout
ON
Status
Turn off

WAN Connection Status

Priority 1 (Highest)

Wi-Fi WAN on 2.4 ... 🟩 Connected to [redacted]

Wi-Fi WAN on 5 GHz 🟩 Connected to [redacted]

Priority 2

Cellular 🟥 No SIM Card Detected

Priority 3

Drag desired (Priority 3) connections here

Disabled

WAN ☐ Disabled

LAN Interface

Router IP Address: 192.168.50.1

Wi-Fi AP 🟩

PEPWAVE_2C09

PepVPN with SpeedFusion

[redacted]	🟩 Established
[redacted]	🟩 Established

Device Information

Model:	Pepwave MAX BR1 MK2
Firmware:	8.1.3 build 5030
Uptime:	0 days 0 hours 51 minutes
CPU Load:	0%
Throughput:	↓ 21.0 kbps ↑ 18.0 kbps

Remote Assistance Status: 🟩

Copyright © Pepwave. All rights reserved.

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.**

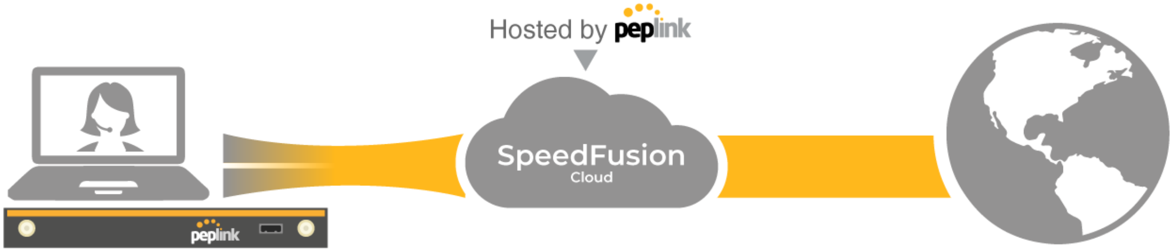
Device Information displays details about the device, including model name, firmware version, and uptime. For further information, please refer to **Section 22.**

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

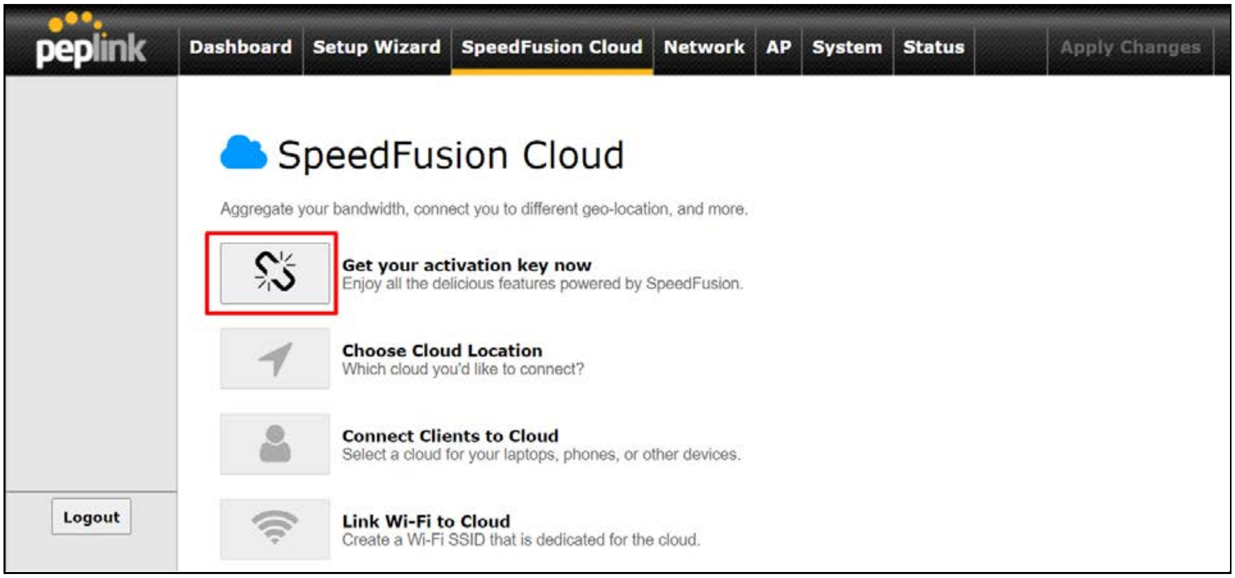
With Peplink products, your device is able to connect to SpeedFusion Cloud without the use of a second endpoint. This service has wide access to a number of SpeedFusion endpoints hosted from around the world, providing your device with unbreakable connectivity wherever you are.*


Hosted by peplink
SpeedFusion
Cloud
peplink

*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 30-day free period with 100GB of SpeedFusion usage upon activation of the SpeedFusion Cloud service. This offer is limited to once per device. To get your activation key please visit SpeedFusion Cloud.


peplink
Dashboard
Setup Wizard
SpeedFusion Cloud
Network
AP
System
Status
Apply Changes
Logout

SpeedFusion Cloud

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

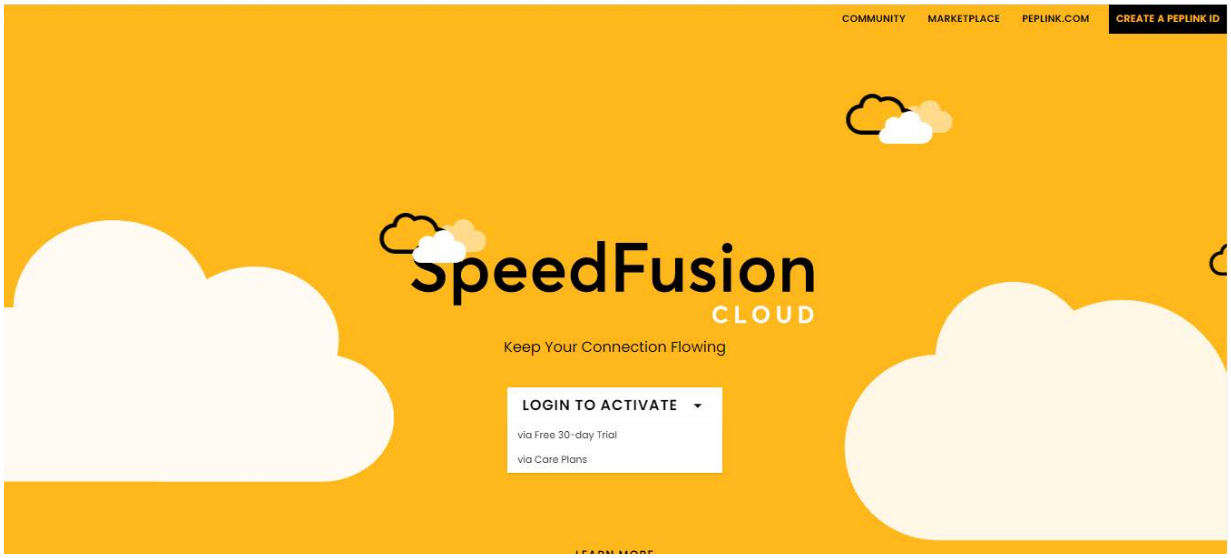
Get your activation key now
Enjoy all the delicious features powered by SpeedFusion.

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

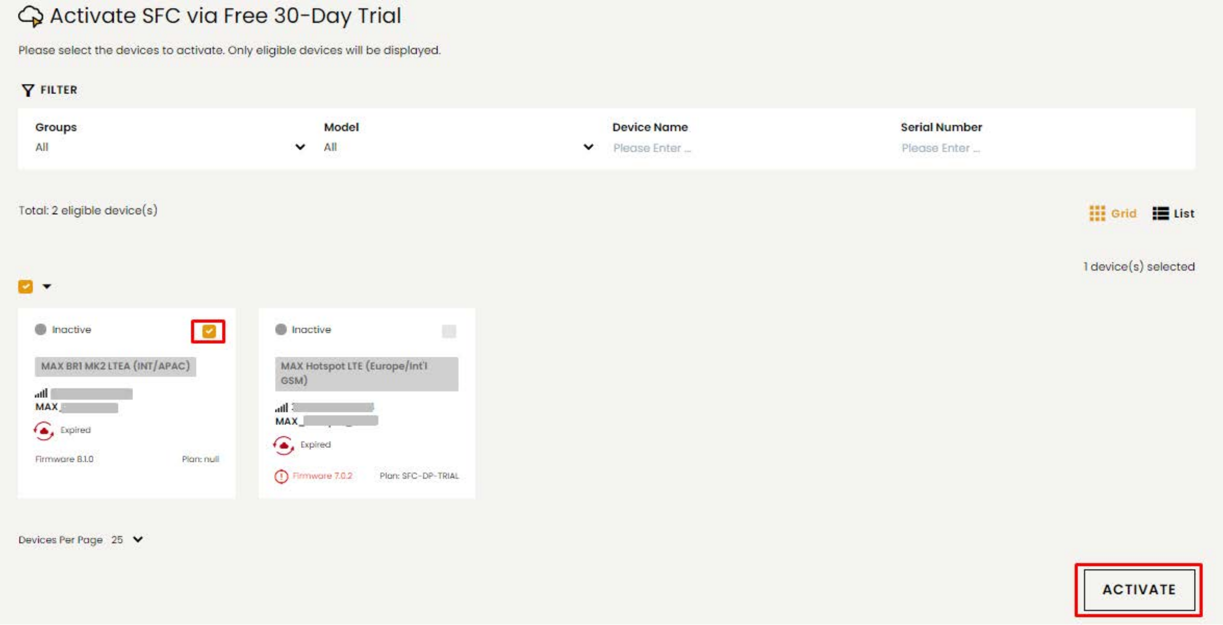
Connect Clients to Cloud
Select a cloud for your laptops, phones, or other devices.

Link Wi-Fi to Cloud
Create a Wi-Fi SSID that is dedicated for the cloud.

Go to activate.speedfusion.com and select the type of SpeedFusion Cloud service, “Via Free 30-days Trial” or “Via Care Plans”, that you would like to activate. Next, register or login to your account.


COMMUNITY
MARKETPLACE
PEPLINK.COM
CREATE A PEPLINK ID
SpeedFusion
CLOUD
Keep Your Connection Flowing
LOGIN TO ACTIVATE
via Free 30-day Trial
via Care Plans

Select the devices that you wish to activate SpeedFusion Cloud on and Click **ACTIVATE**.


Activate SFC via Free 30-Day Trial

Please select the devices to activate. Only eligible devices will be displayed.

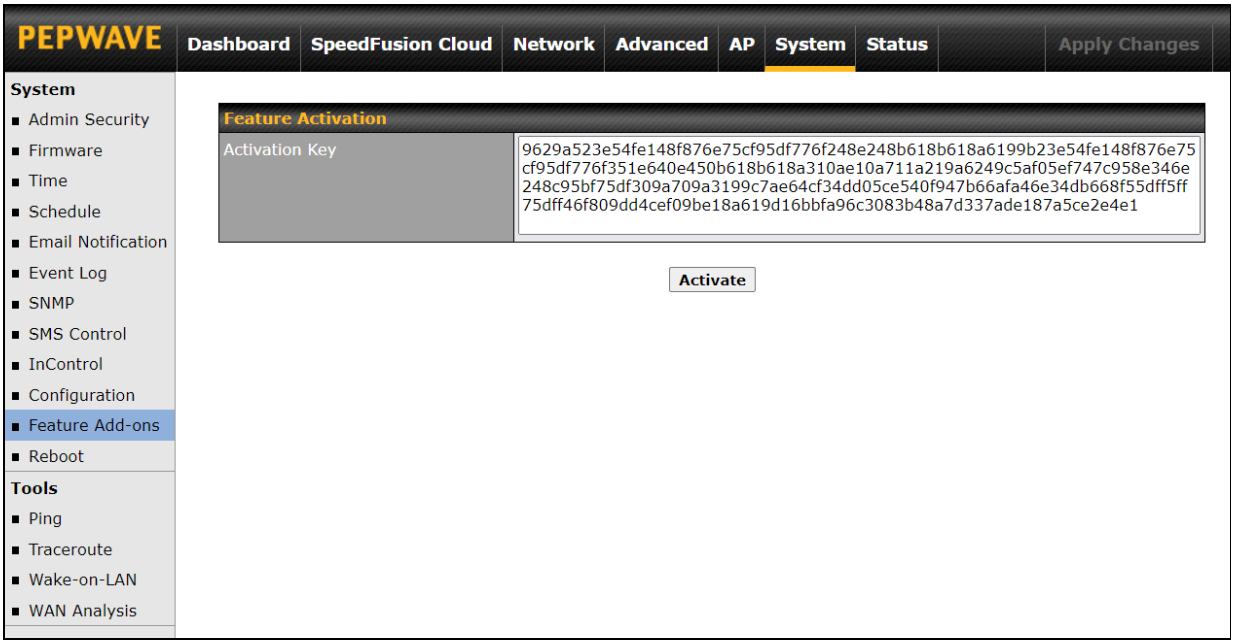
Total: 2 eligible device(s)

1 device(s) selected

FILTER
Groups
All
Model
All
Device Name
Please Enter ...
Serial Number
Please Enter ...
Grid
List
Inactive
MAX BR1 MK2 LTEA (INT/APAC)
[redacted]
MAX [redacted]
Expired
Firmware 8.1.0
Plan: null
Inactive
MAX Hotspot LTE (Europe/Int'l GSM)
[redacted]
MAX [redacted]
Expired
Firmware 7.0.2
Plan: SFC-DP-TRIAL
Devices Per Page 25
ACTIVATE

From **System > Features Add-ons**, paste the license key into the window and click on

Activate once you have received the license key.

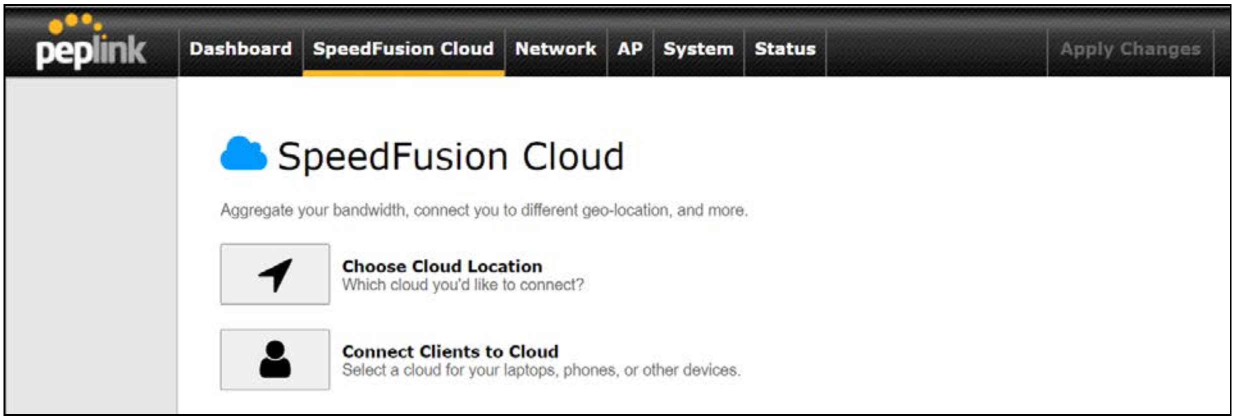

PEPWAVE
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
Apply Changes
System
Admin Security
Firmware
Time
Schedule
Email Notification
Event Log
SNMP
SMS Control
InControl
Configuration
Feature Add-ons
Reboot
Tools
Ping
Traceroute
Wake-on-LAN
WAN Analysis
Activate

Feature Activation

Activation Key	9629a523e54fe148f876e75cf95df776f248e248b618b618a6199b23e54fe148f876e75 cf95df776f351e640e450b618b618a310ae10a711a219a6249c5af05ef747c958e346e 248c95bf75df309a709a3199c7ae64cf34dd05ce540f947b66afa46e34db668f55dff5ff 75dff46f809dd4cef09be18a619d16bbfa96c3083b48a7d337ade187a5ce2e4e1

7.2 Enable SpeedFusion Cloud

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


Dashboard
SpeedFusion Cloud
Network
AP
System
Status
Apply Changes

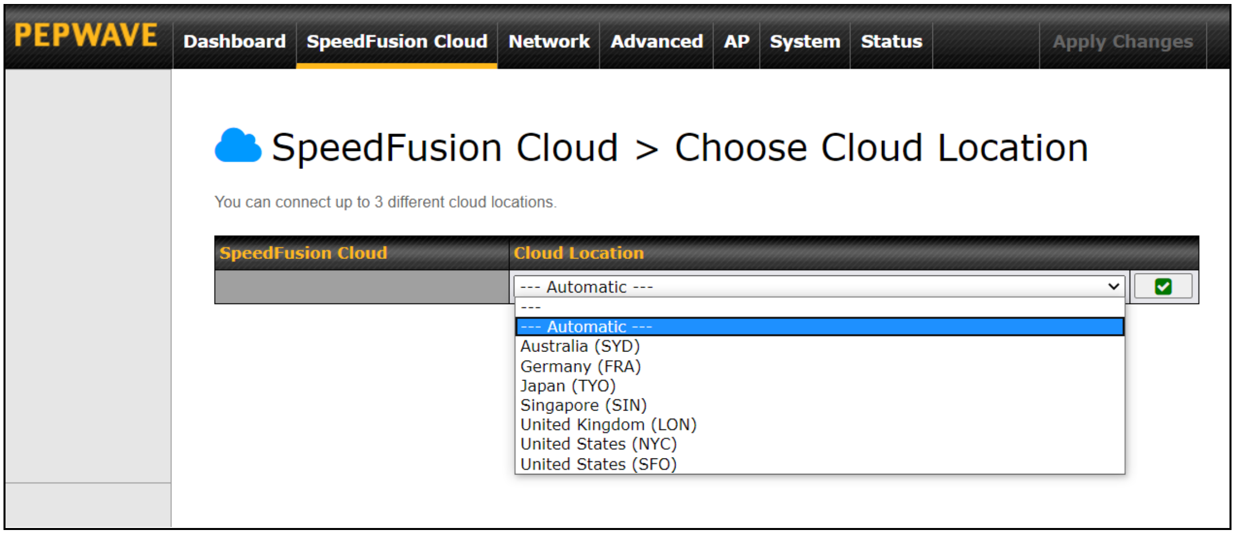
SpeedFusion Cloud

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


PEPWAVE
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
Apply Changes

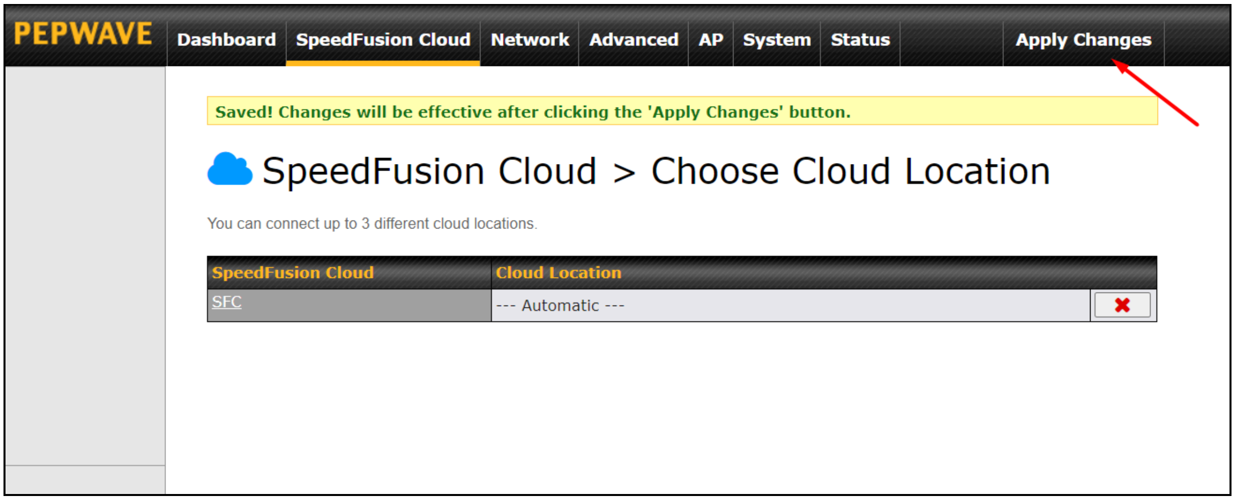
--- Automatic ---
Australia (SYD)
Germany (FRA)
Japan (TYO)
Singapore (SIN)
United Kingdom (LON)
United States (NYC)
United States (SFO)

SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

SpeedFusion Cloud	Cloud Location
	--- Automatic --- ☑

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

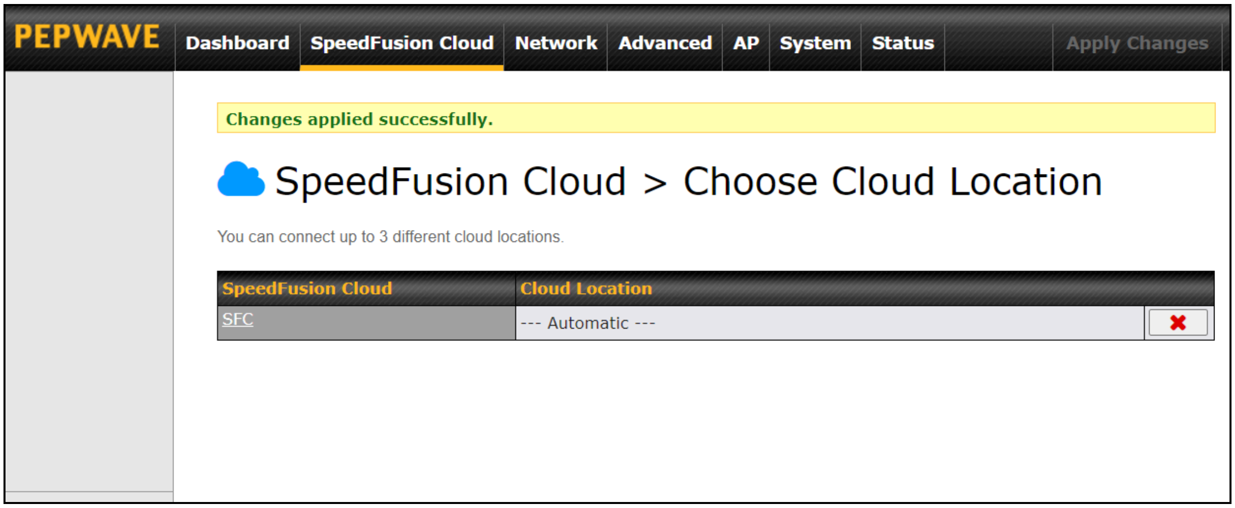

PEPWAVE
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
Apply Changes

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

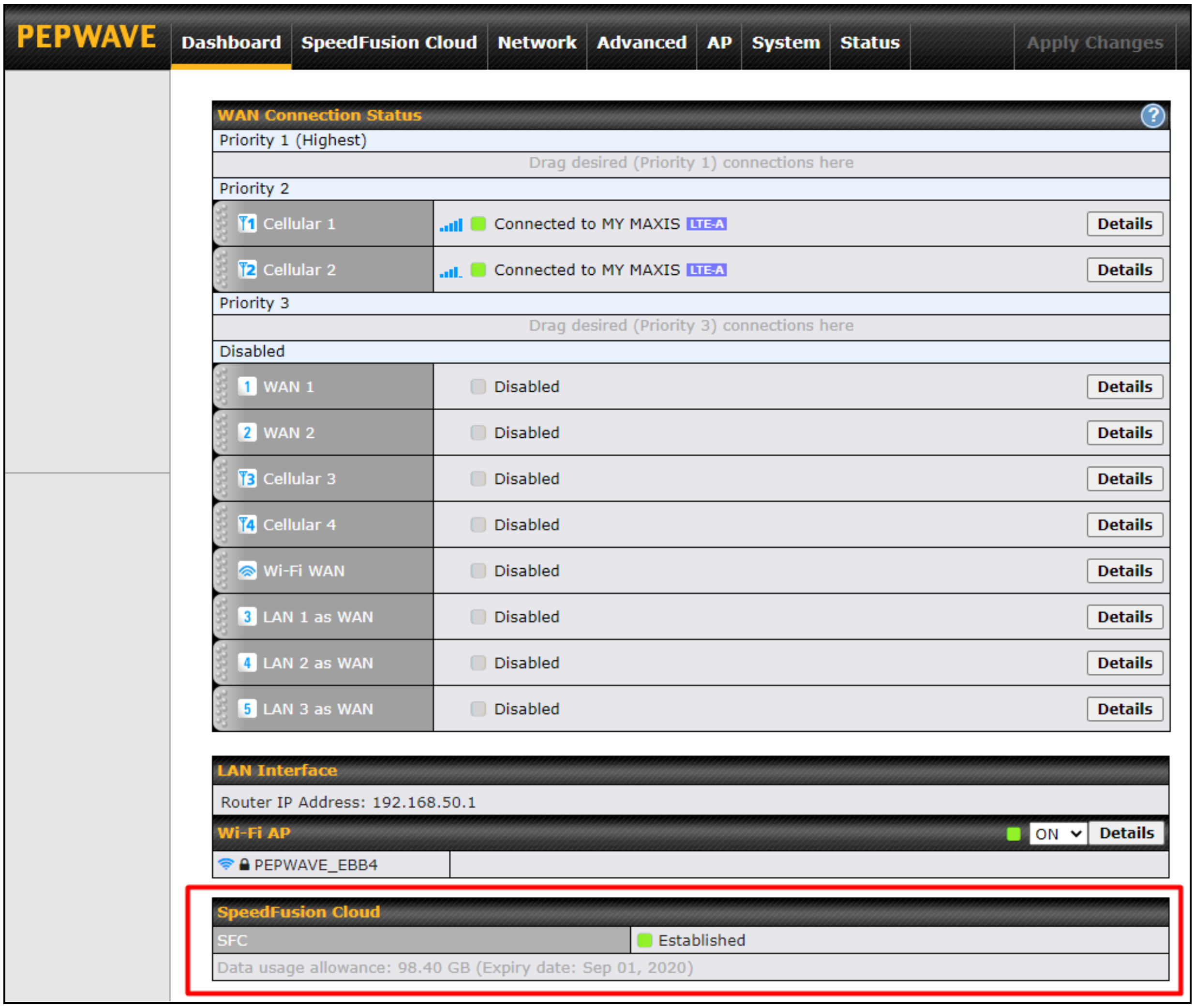
Changes applied successfully.

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		
Cellular 1	🟩 Connected to MY MAXIS LTE-A	Details
Cellular 2	🟩 Connected to MY MAXIS LTE-A	Details
Priority 3		
	Drag desired (Priority 3) connections here	
Disabled		
WAN 1	Disabled	Details
WAN 2	Disabled	Details
Cellular 3	Disabled	Details
Cellular 4	Disabled	Details
Wi-Fi WAN	Disabled	Details
LAN 1 as WAN	Disabled	Details
LAN 2 as WAN	Disabled	Details
LAN 3 as WAN	Disabled	Details

LAN Interface

Router IP Address: 192.168.50.1

Wi-Fi AP 🟩 ON Details

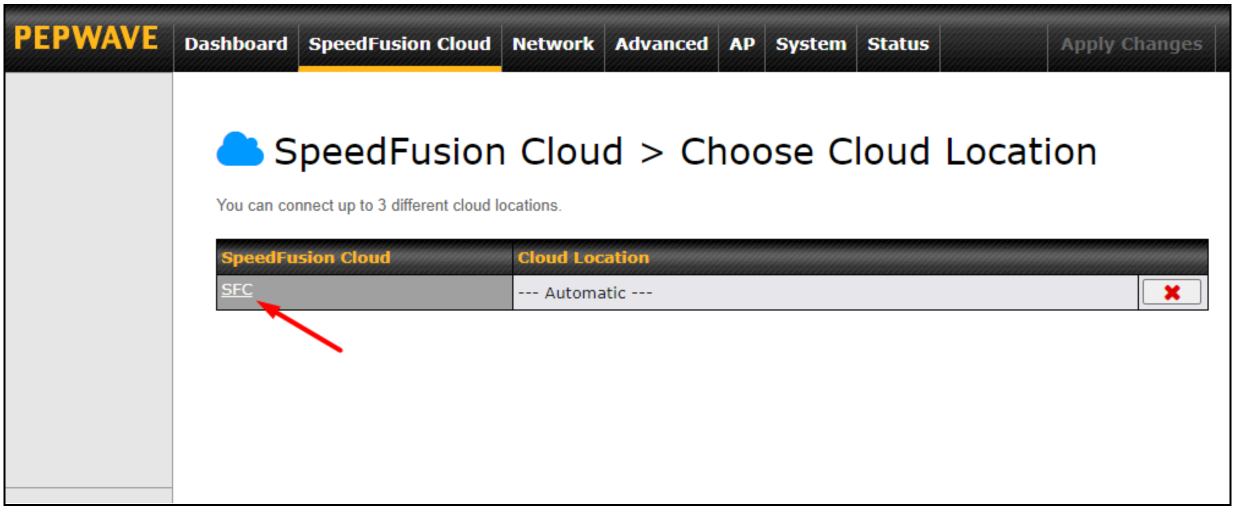
PEPWAVE_EBB4

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**.

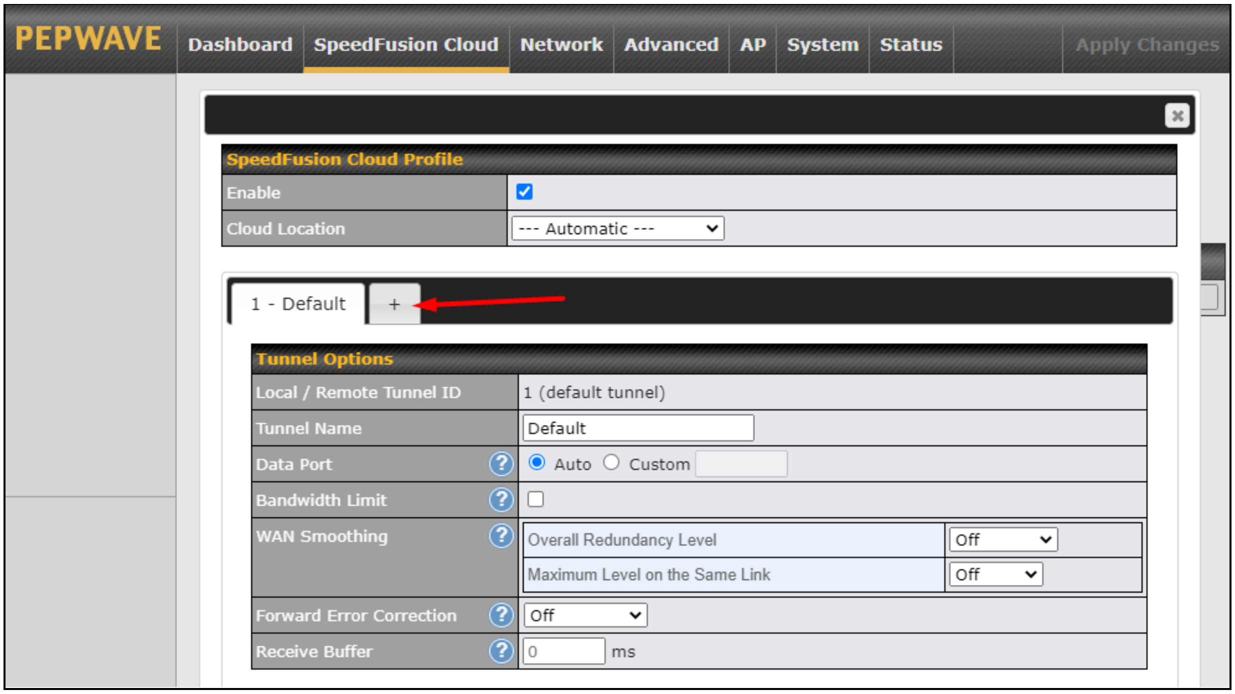

PEPWAVE
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
Apply Changes

SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

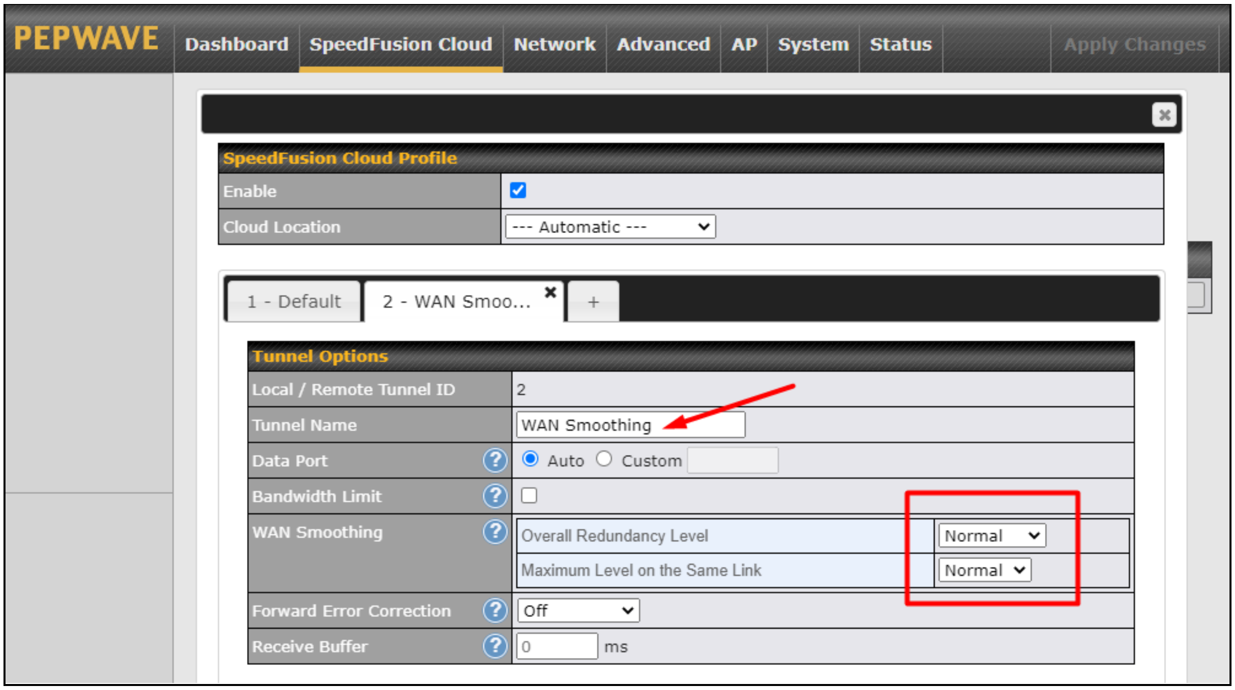
SpeedFusion Cloud	Cloud Location
SFC	--- Automatic ---

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
1 - Default
+

SpeedFusion Cloud Profile	
Enable	☑
Cloud Location	--- Automatic ---

Tunnel Options	
Local / Remote Tunnel ID	1 (default tunnel)
Tunnel Name	Default
Data Port	● Auto ○ Custom
Bandwidth Limit	☐
WAN Smoothing	Overall Redundancy Level: Off Maximum Level on the Same Link: Off
Forward Error Correction	Off
Receive Buffer	0 ms


PEPWAVE
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
Apply Changes

SpeedFusion Cloud Profile

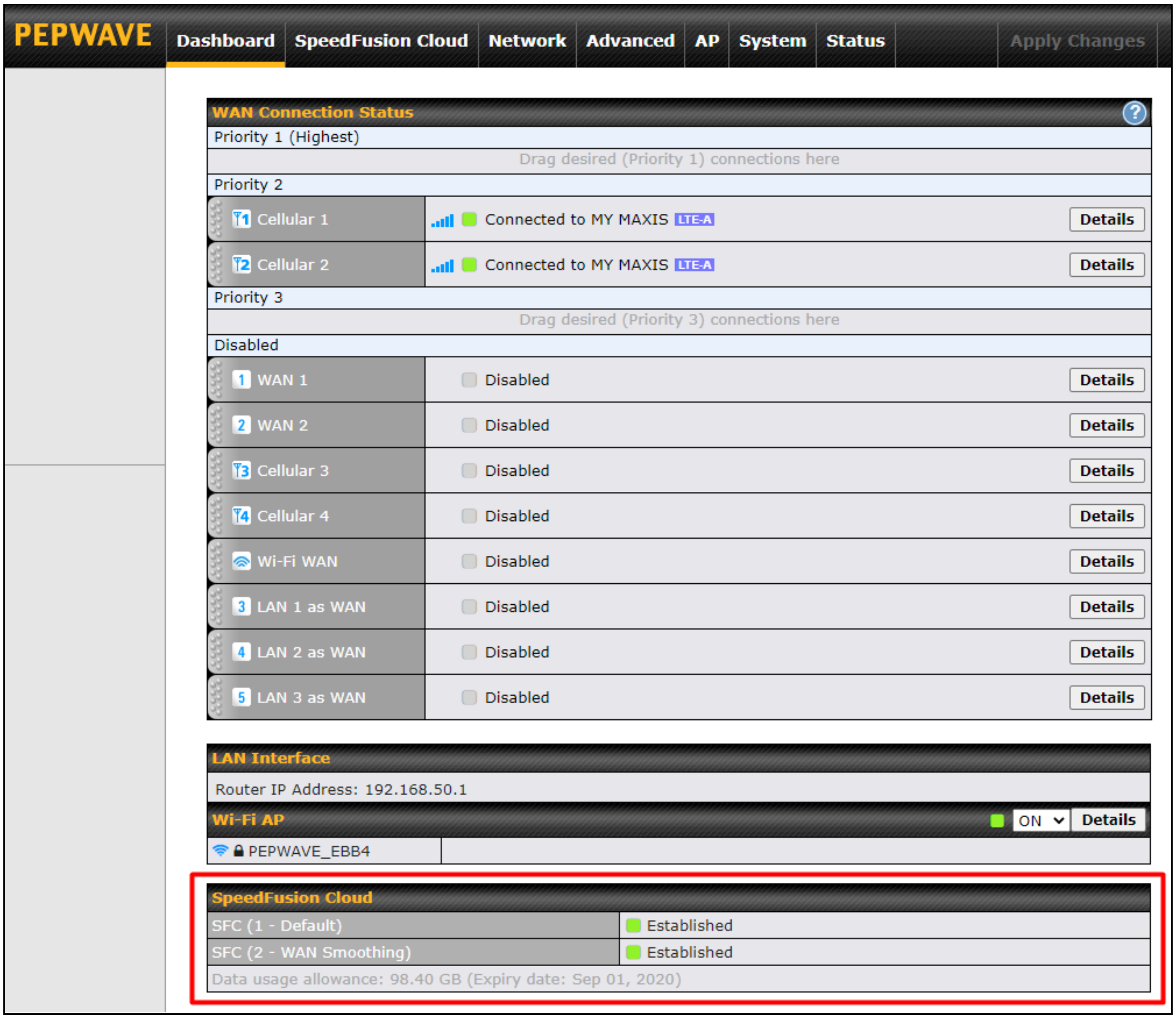
Enable	☑
Cloud Location	--- Automatic ---

1 - Default
2 - WAN Smoo...
+

Tunnel Options

Local / Remote Tunnel ID	2
Tunnel Name	WAN Smoothing
Data Port	● Auto ○ Custom
Bandwidth Limit	☐
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.



WAN Connection Status

Priority 1 (Highest)

Drag desired (Priority 1) connections here

Priority 2

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

Priority 3

Drag desired (Priority 3) connections here

Disabled

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

LAN Interface

Router IP Address: 192.168.50.1

Wi-Fi AP 🟩 ON Details

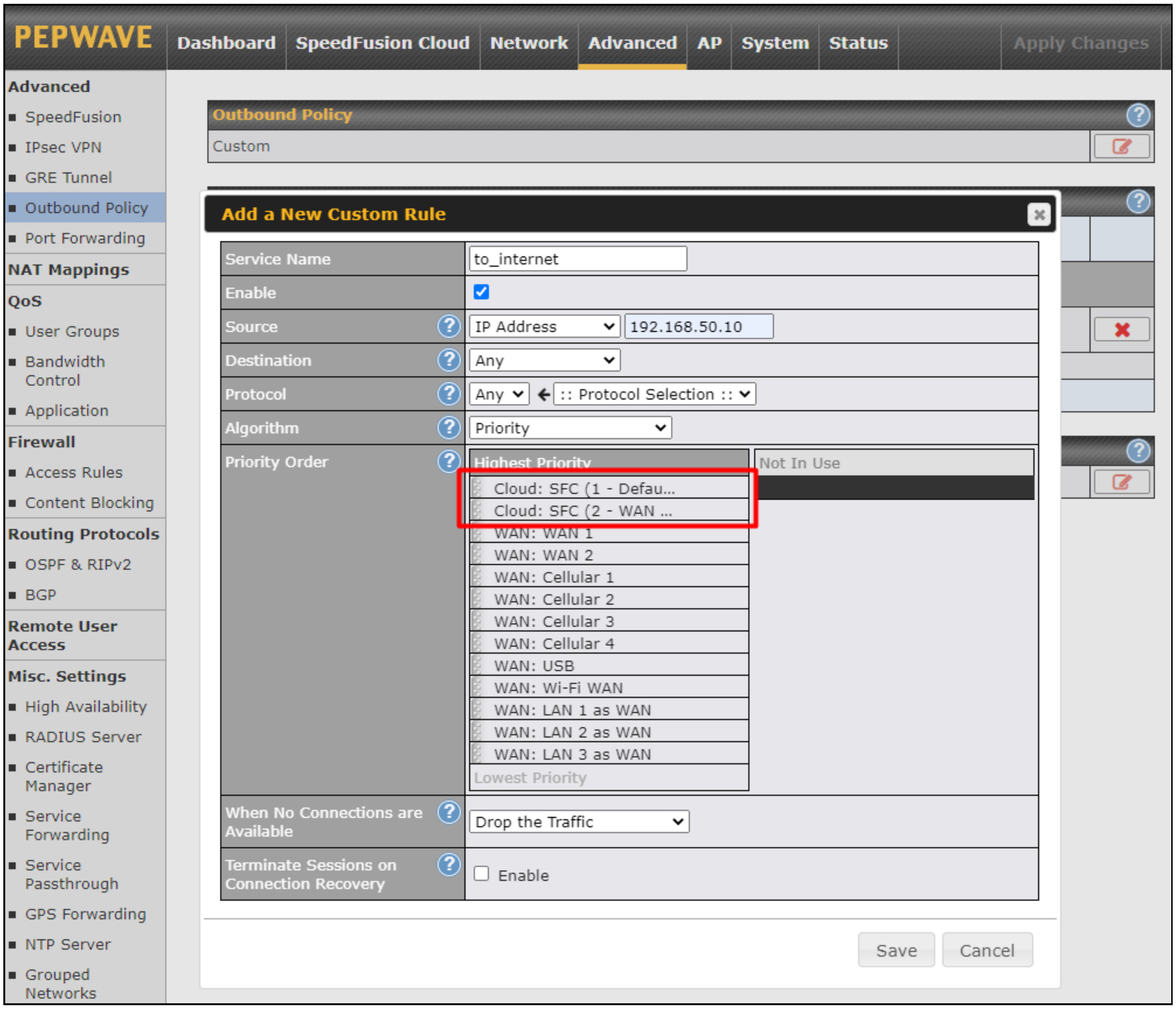
PEPWAVE_EBB4

SpeedFusion Cloud

SFC (1 - Default)	🟩 Established
SFC (2 - WAN Smoothing)	🟩 Established

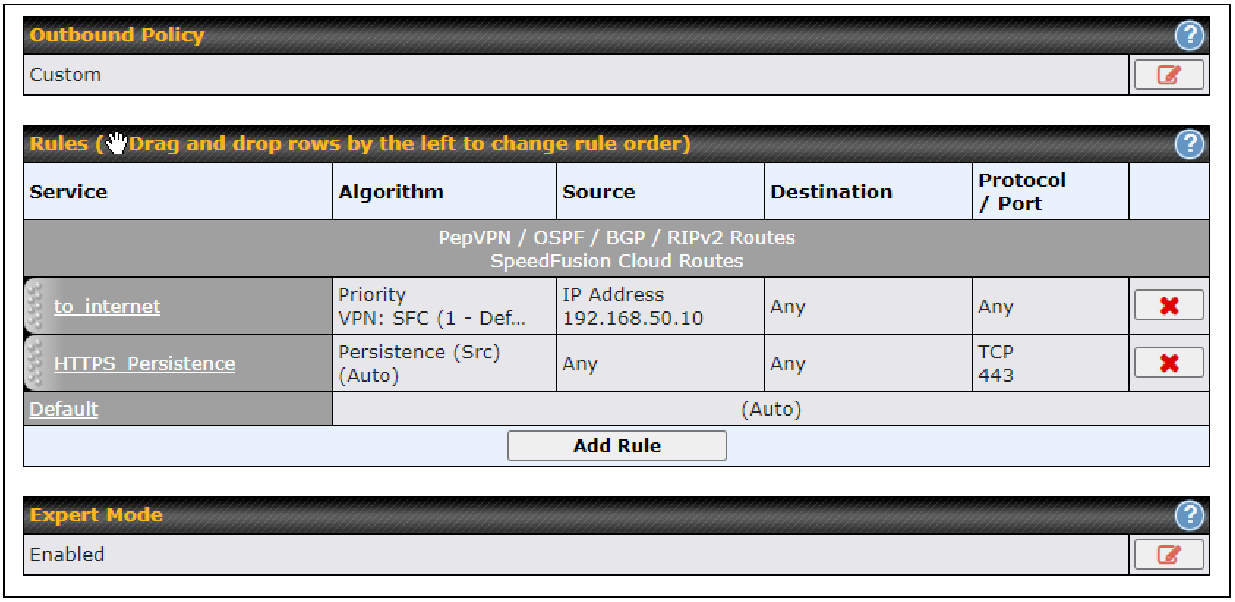
Data usage allowance: 98.40 GB (Expiry date: Sep 01, 2020)

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
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
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
Save
Cancel

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



Outbound Policy

Custom

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

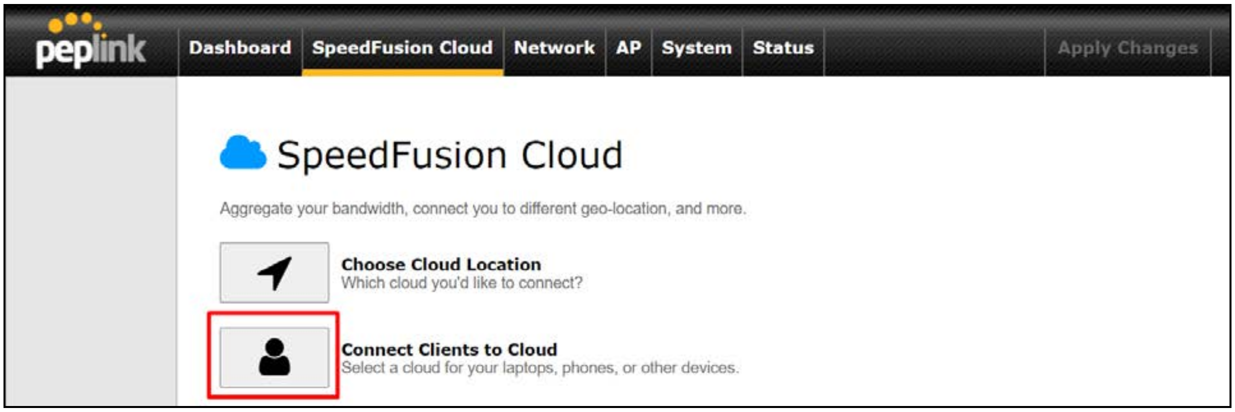
Service	Algorithm	Source	Destination	Protocol / Port	
PepVPN / OSPF / BGP / RIPv2 Routes SpeedFusion Cloud Routes					
to_internet	Priority VPN: SFC (1 - Def...	IP Address 192.168.50.10	Any	Any	✖
HTTPS_Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	✖
Default	(Auto)				

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**.



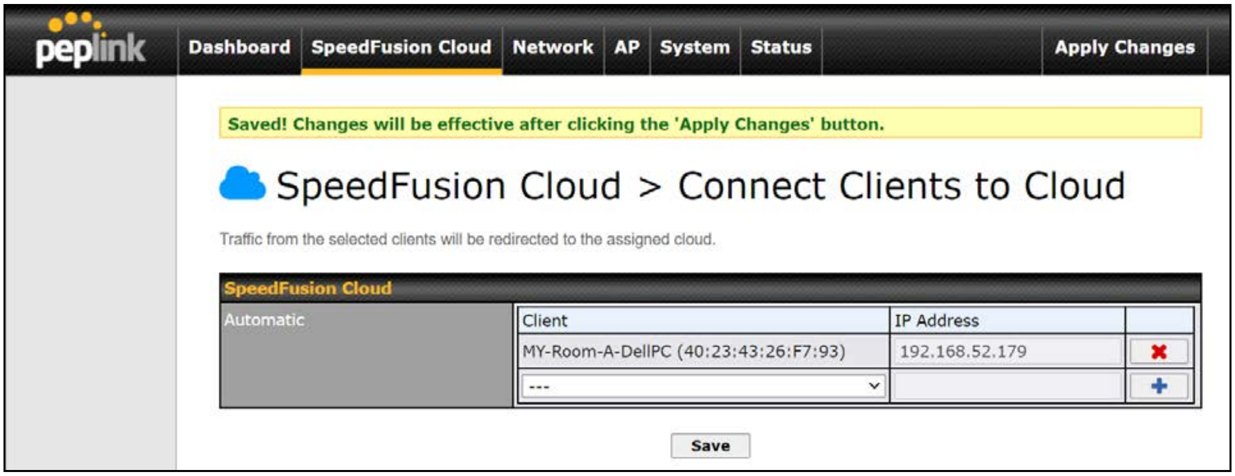
SpeedFusion Cloud

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.


peplink
Dashboard
SpeedFusion Cloud
Network
AP
System
Status
Apply Changes

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

SpeedFusion Cloud > Connect Clients to Cloud

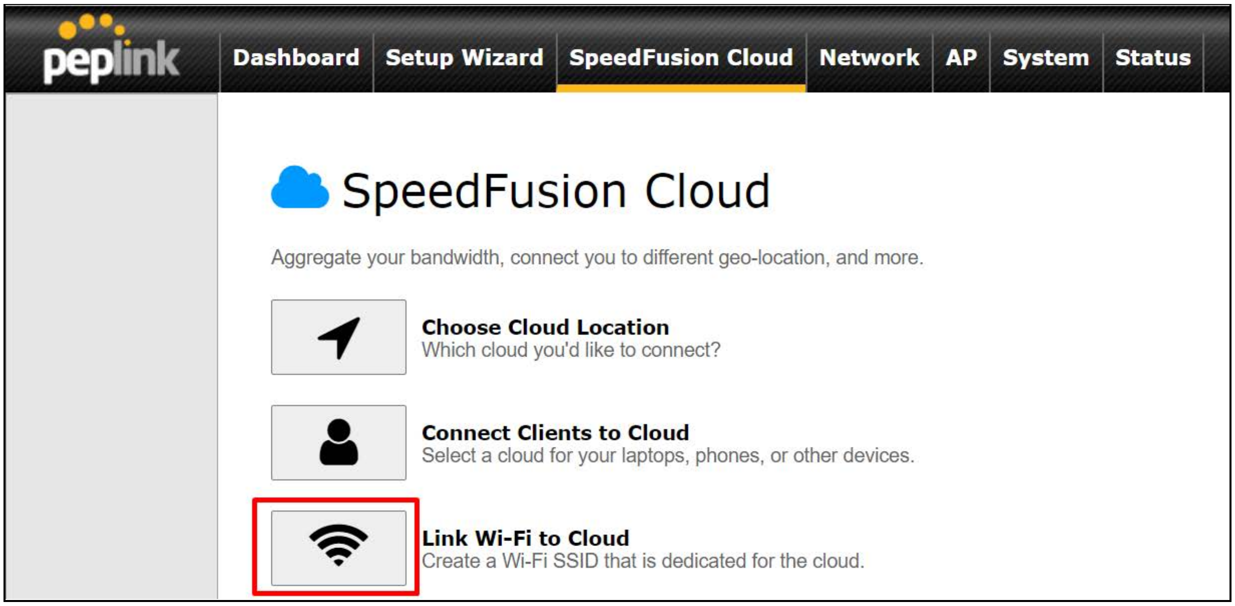
Traffic from the selected clients will be redirected to the assigned cloud.

SpeedFusion Cloud	Client	IP Address	
Automatic	MY-Room-A-DellPC (40:23:43:26:F7:93)	192.168.52.179	✖
	---		+

Save

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**.


peplink
Dashboard
Setup Wizard
SpeedFusion Cloud
Network
AP
System
Status

SpeedFusion Cloud

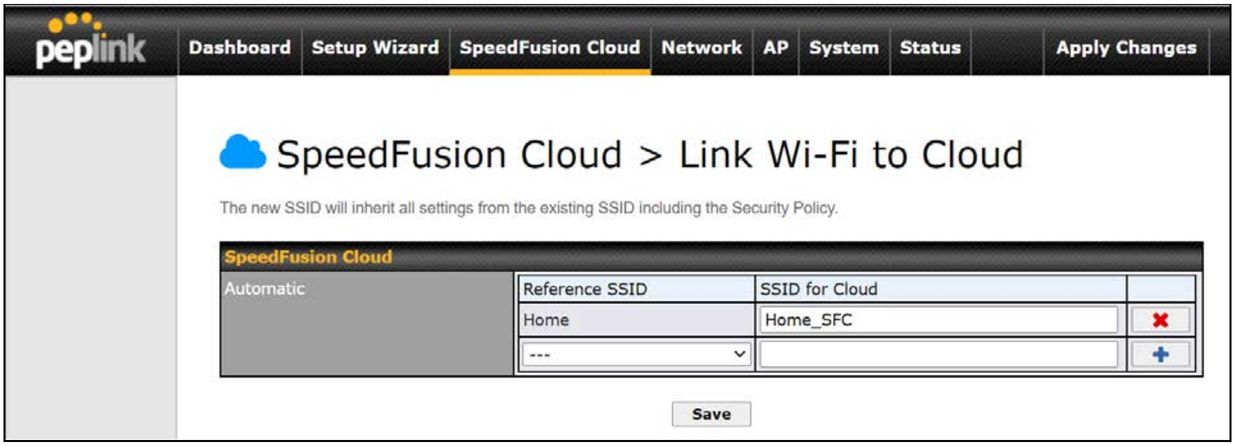
Aggregate your bandwidth, connect you to different geo-location, and more.

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

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

Link Wi-Fi to Cloud
Create a Wi-Fi SSID that is dedicated for the cloud.

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**.


Dashboard
Setup Wizard
SpeedFusion Cloud
Network
AP
System
Status
Apply Changes

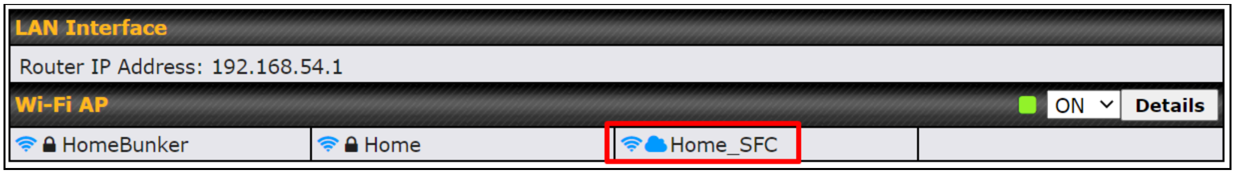
SpeedFusion Cloud > Link Wi-Fi to Cloud

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

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

Save

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



LAN Interface

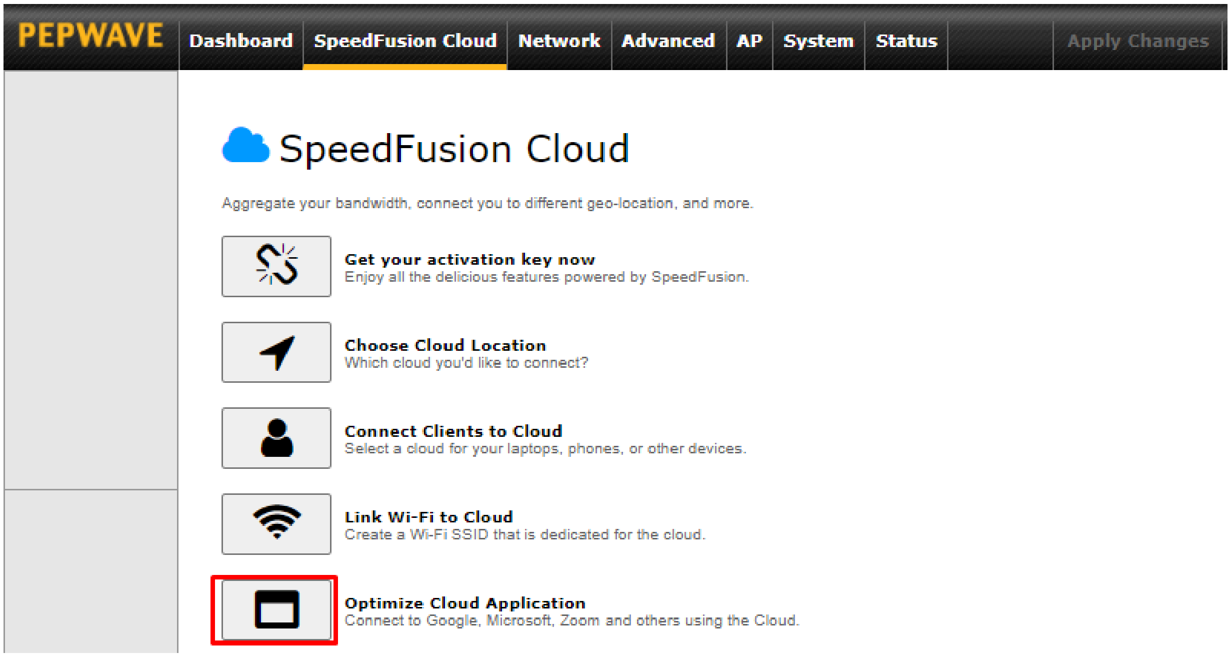
Router IP Address: 192.168.54.1

Wi-Fi AP

HomeBunker	Home	Home_SFC	

7.5 Optimize Cloud Application

Optimize Cloud Application allows you to route Internet traffic to SpeedFusion Cloud based on the application. Go to **SpeedFusion Cloud > Optimize Cloud Application**.


PEPWAVE
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
Apply Changes

SpeedFusion Cloud

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

Get your activation key now
Enjoy all the delicious features powered by SpeedFusion.

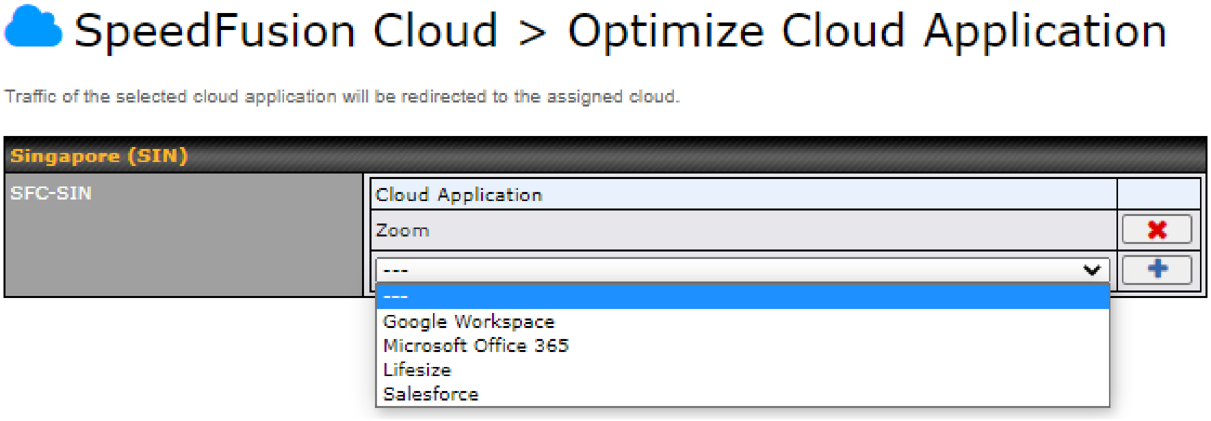
Choose Cloud Location
Which cloud you'd like to connect?

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

Link Wi-Fi to Cloud
Create a Wi-Fi SSID that is dedicated for the cloud.

Optimize Cloud Application
Connect to Google, Microsoft, Zoom and others using the Cloud.

Select a Cloud application to route through SpeedFusion Cloud from the drop down list **>** Click ➕ **>** Save > Apply Changes. Click the ✖ to remove a selected Cloud application to route through SpeedFusion Cloud.


SpeedFusion Cloud > Optimize Cloud Application

Traffic of the selected cloud application will be redirected to the assigned cloud.

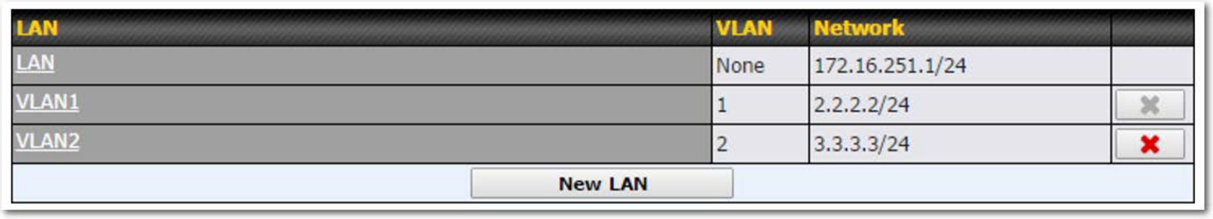
Singapore (SIN)		
SFC-SIN	Cloud Application	
	Zoom	✖
	---	➕

Google Workspace
Microsoft Office 365
Lifesize
Salesforce

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:

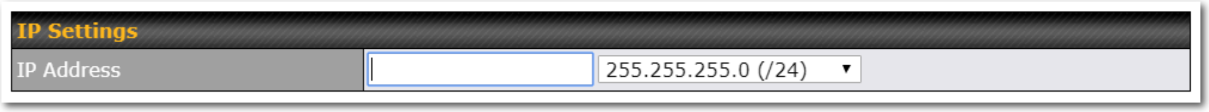


LAN	VLAN	Network	
LAN	None	172.16.251.1/24	
VLAN1	1	2.2.2.2/24	✖
VLAN2	2	3.3.3.3/24	✖

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”.

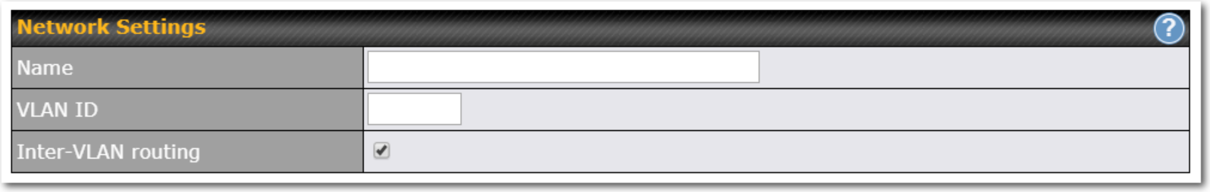
Alternatively, a red “X” means that there are no settings using the VLAN. You can delete that VLAN by clicking the red “X”

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



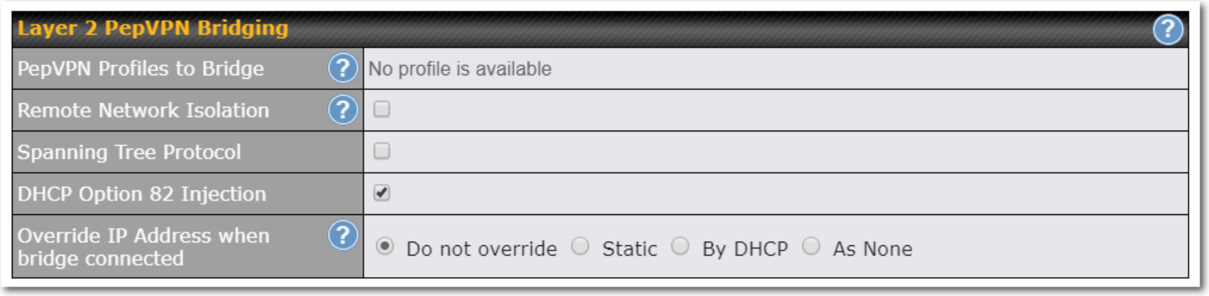
IP Settings	
IP Address	255.255.255.0 (/24)

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



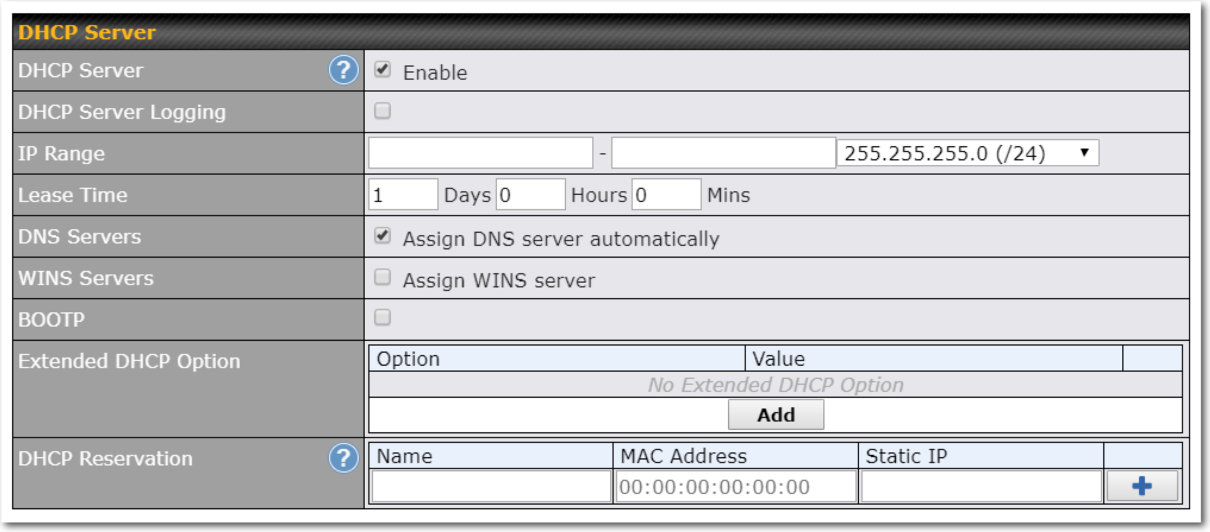
Network Settings	
Name	
VLAN ID	
Inter-VLAN routing	☑

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



Layer 2 PepVPN Bridging	
PepVPN Profiles to Bridge	No profile is available
Remote Network Isolation	☐
Spanning Tree Protocol	☐
DHCP Option 82 Injection	☑
Override IP Address when bridge connected	● Do not override ○ Static ○ By DHCP ○ As None

Layer 2 PepVPN Bridging	
PepVPN Profiles to Bridge	The remote network of the selected PepVPN profiles will be bridged with this local LAN, creating a Layer 2 PepVPN, they will be connected and operate like a single LAN, and any broadcast or multicast packets will be sent over the VPN.
Remote Network Isolation	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.
Spanning Tree Protocol	Click the box will enable STP for this layer 2 profile bridge.
Override IP Address when bridge connected	Select "Do not override" if the LAN IP address and local DHCP server should remain unchanged after the Layer 2 PepVPN is up. If you choose to override IP address when the VPN is connected, the device will not act as a router, and most Layer 3 routing functions will cease to work.
DHCP Option 82	Click on the question Mark if you want to enable DHCP Option 82. 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.

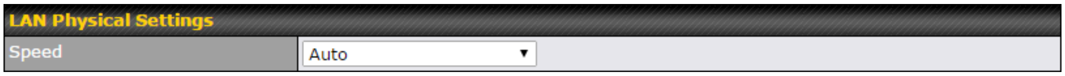


DHCP Server

DHCP Server	☑ Enable
DHCP Server Logging	☐
IP Range	- 255.255.255.0 (/24)
Lease Time	1 Days 0 Hours 0 Mins
DNS Servers	☑ Assign DNS server automatically
WINS Servers	☐ Assign WINS server
BOOTP	☐
Extended DHCP Option	Option, Value No Extended DHCP Option Add
DHCP Reservation	Name, MAC Address, Static IP 00:00:00:00:00:00

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

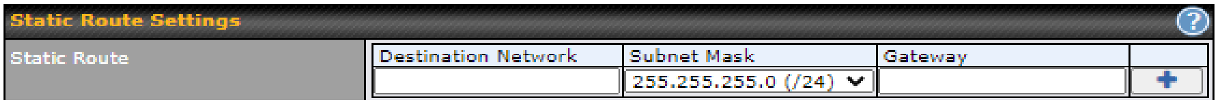
	pass additional configuration information to LAN hosts. To define an extended DHCP option, click the **Add** button, choose the option to define and enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option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



LAN Physical Settings

Speed: Auto ▾

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

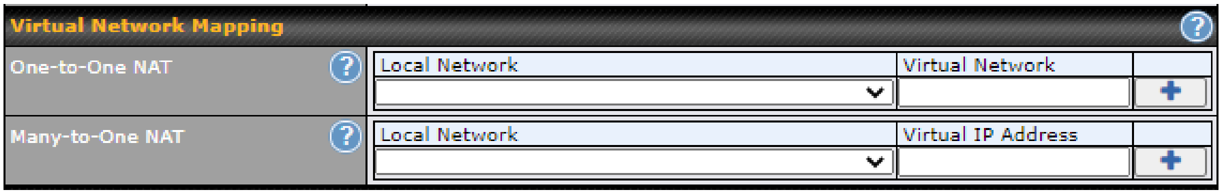


Static Route Settings

Static Route	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.

[A] - Advanced feature, please click the ? button on the top right hand corner of the Static Route section to activate and configure Virtual Network Mapping to resolve network address conflict with remote peers.



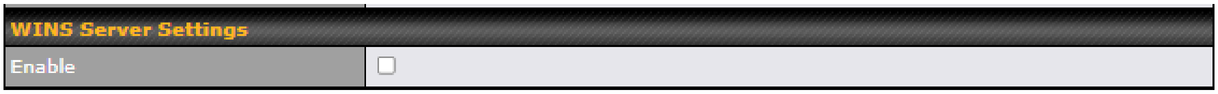
Virtual Network Mapping			
One-to-One NAT	Local Network	Virtual Network	
			+
Many-to-One NAT	Local Network	Virtual IP Address	
			+

In case of a network address conflict with remote peers (i.e. PepVPN / IPsec VPN / IP Forwarding WAN are considered as remote connections), you can define Virtual Network Mapping to resolve it.

Note: OSPF & RIPv2 settings should be updated as well to avoid advertising conflicted networks.

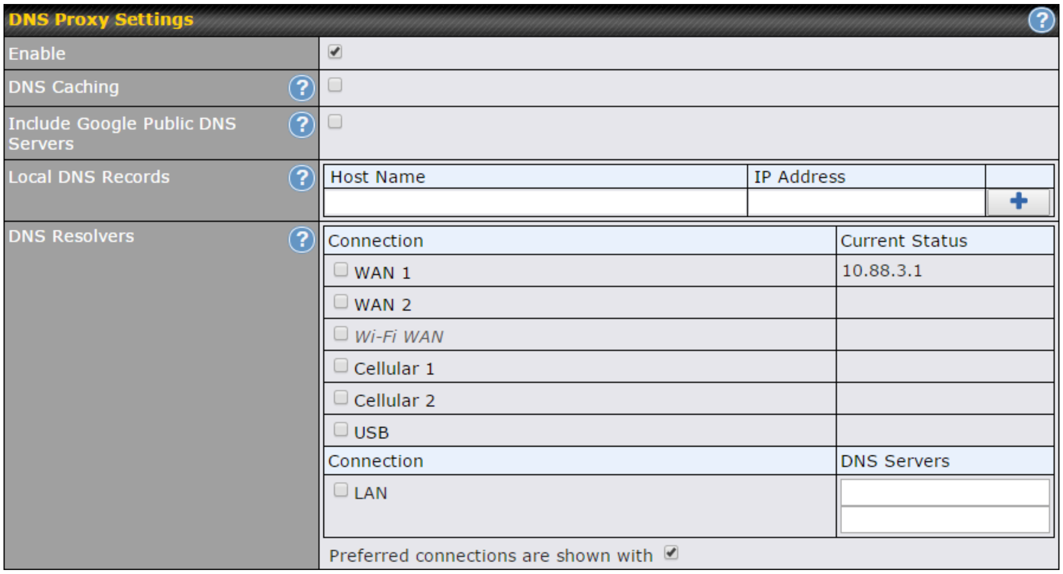
For further details on virtual network mapping watch this video:
https://youtu.be/C1FMdZCn3Z8

Virtual Network Mapping	
One-to-One NAT	Every IP Address in the Local Network has a corresponding unique Virtual IP Address for NAT. Traffic originating from the Local Network to remote connections will be SNAT'ed and behave like coming from the defined Virtual Network. While traffic initiated by remote peers to the Virtual Network will be DNAT'ed accordingly.
Many-to-One NAT	The subnet range defined in Local Network will be mapped to a single Virtual IP Address for NAT. Traffic can only be initiated from local to remote, and these traffic will be NAT'ed and behaves like coming from the same Virtual IP Address.



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

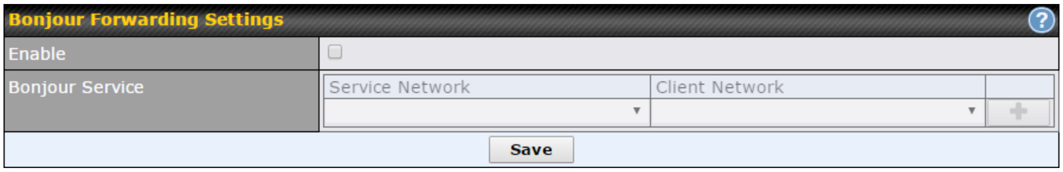
Enable	☑
DNS Caching	☐
Include Google Public DNS Servers	☐
Local DNS Records	Host Name | IP Address
DNS Resolvers	Connection | Current Status ☐ WAN 1 | 10.88.3.1 ☐ WAN 2 ☐ *Wi-Fi WAN* ☐ Cellular 1 ☐ Cellular 2 ☐ USB Connection | DNS Servers ☐ LAN Preferred connections are shown with ☑

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

	resolver IP address(es). Queries will be forwarded to the selected connections' resolvers. If all of the selected connections are down, queries will be forwarded to all resolvers on healthy WAN connections.

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

Finally, if needed, configure Bonjour forwarding, Apple's zero configuration networking protocol. Once VLAN configuration is complete, click **Save** to store your changes.

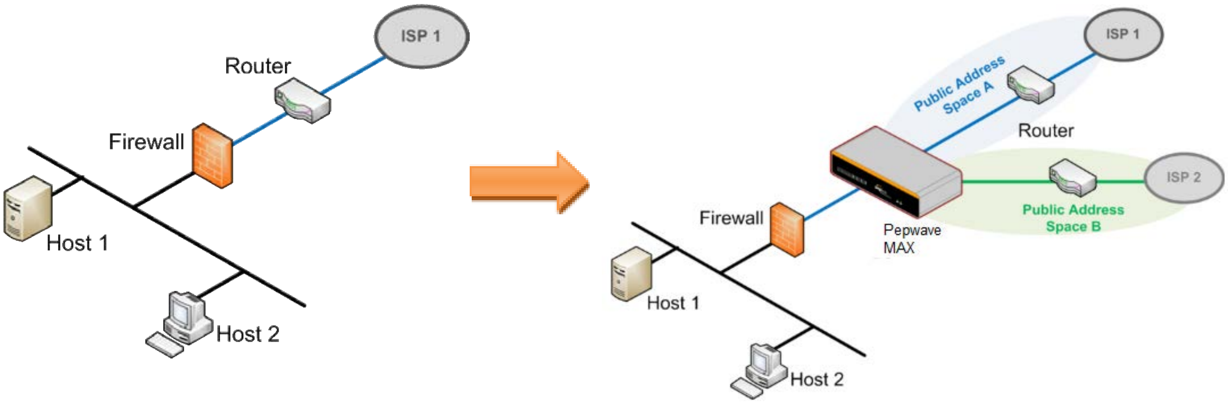

Bonjour Forwarding Settings
?
Enable
☐
Bonjour Service
Service Network
Client Network
+
Save

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

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:

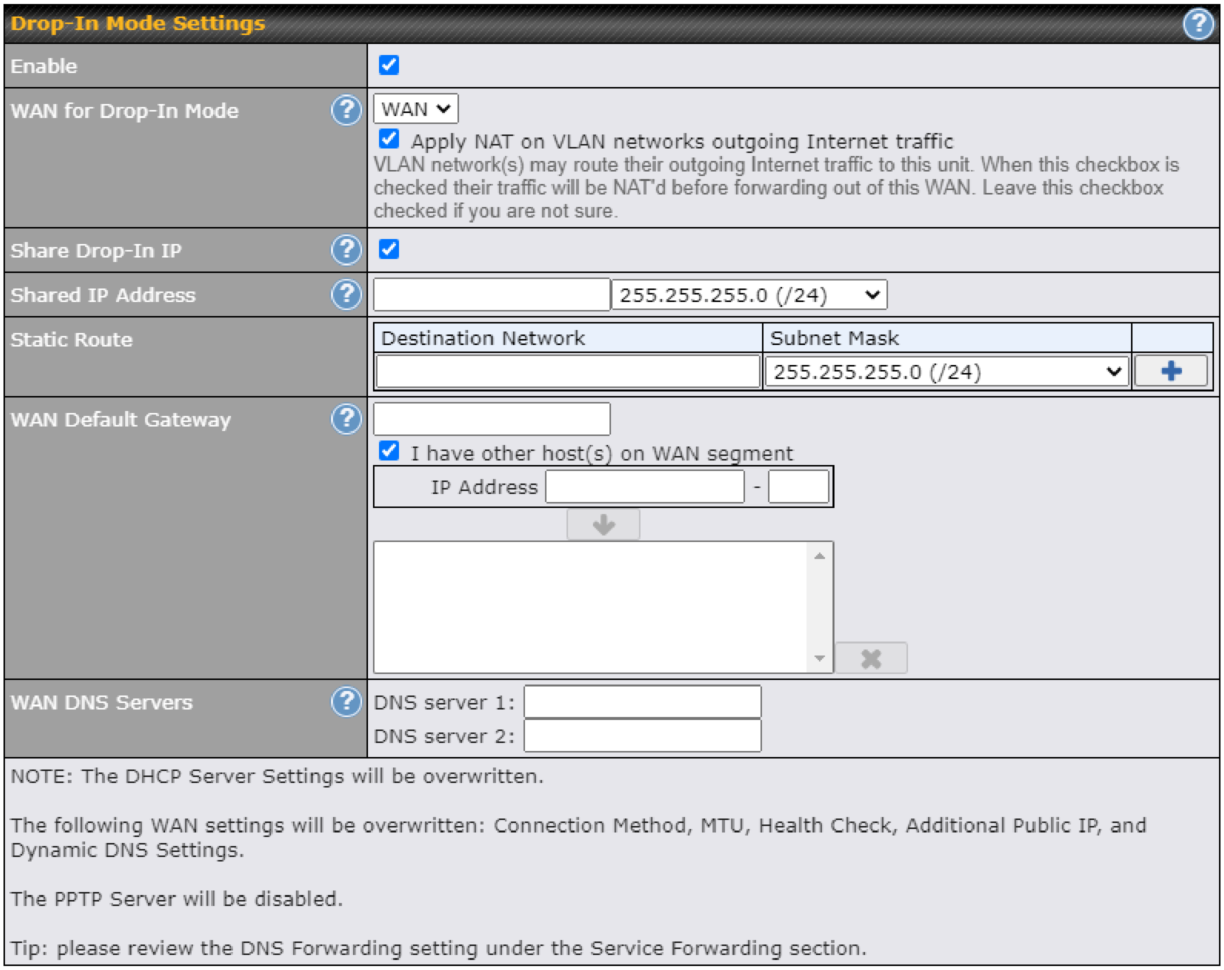


Check the box Enable to enable the Drop-in Mode. After enabling this feature and selecting the WAN for Drop-in mode, various settings including the WAN's connection method and IP address will be automatically updated.

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 ☑

WAN for Drop-In Mode: WAN

☑ 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.

Share Drop-In IP ☑

Shared IP Address: 255.255.255.0 (/24)

Static Route:

Destination Network	Subnet Mask
	255.255.255.0 (/24)

WAN Default Gateway:

☑ I have other host(s) on WAN segment

IP Address -

WAN DNS Servers:

DNS server 1:

DNS server 2:

NOTE: The DHCP Server Settings will be overwritten.

The following WAN settings will be overwritten: Connection Method, MTU, Health Check, Additional Public IP, and Dynamic DNS Settings.

The PPTP Server will be disabled.

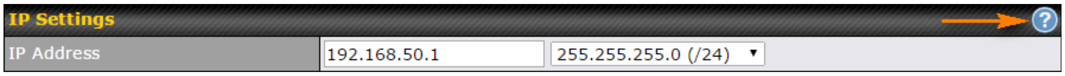
Tip: please review the DNS Forwarding setting under the Service Forwarding section.

Drop-in Mode Settings	
Enable	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.
WAN for Drop-In Mode	Select the WAN port to be used for drop-in mode. If **WAN** is selected, the high availability feature will be disabled automatically.
Shared Drop-In IP^{A}	When this option is enabled, the passthrough IP address will be used to connect to WAN hosts (email notification, remote syslog, etc.). The 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.). 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 proxy, etc.).
Shared IP	Access to this IP address will be passed through to the LAN port if this device is

Address[A]	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.)
WAN Default Gateway	Enter the WAN router's IP address in this field. If there are more hosts in addition to the router on the WAN segment, click the ? button next to "WAN Default Gateway" and check the other **host(s) on the WAN segment** box and enter the IP address of the hosts that need to access LAN devices or be accessed by others.
WAN DNS Servers	Enter the selected WAN's corresponding DNS server IP addresses.

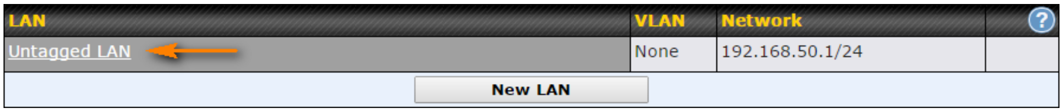
[A] - Advanced feature, please click the ? button on the top right-hand corner to activate.

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



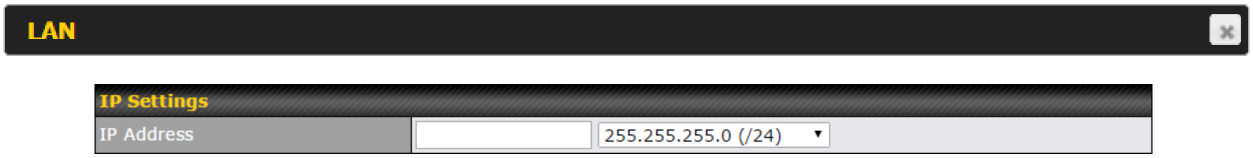
IP Settings		
IP Address	192.168.50.1	255.255.255.0 (/24) ▾

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.



LAN	VLAN	Network
Untagged LAN	None	192.168.50.1/24

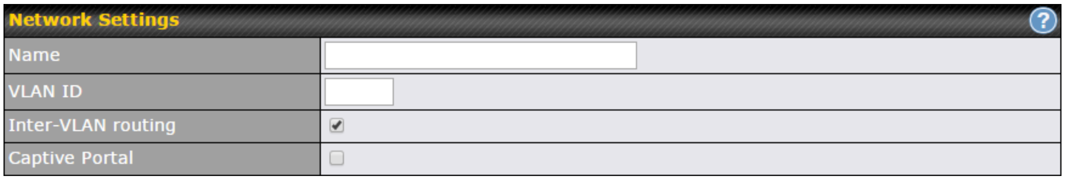
The following settings are displayed when creating a new LAN or editing an existing LAN.



LAN

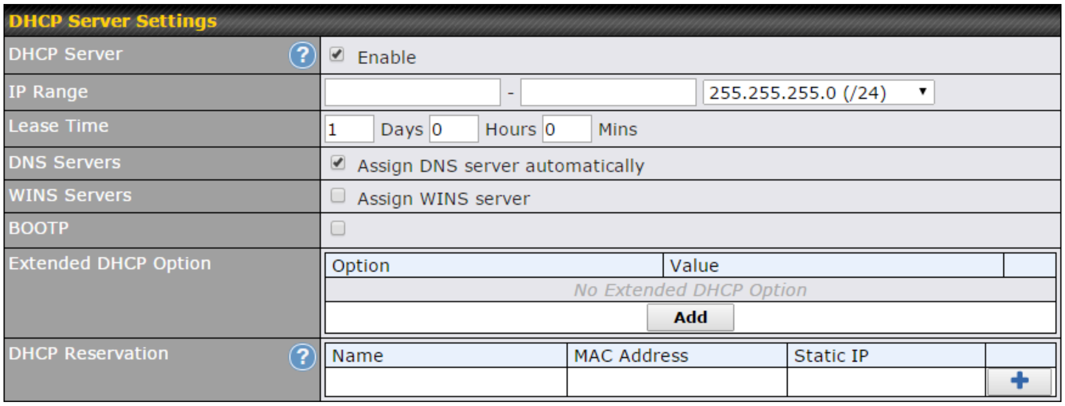
IP Settings		
IP Address		255.255.255.0 (/24) ▾

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



Network Settings	
Name	
VLAN ID	
Inter-VLAN routing	☑
Captive Portal	☐

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

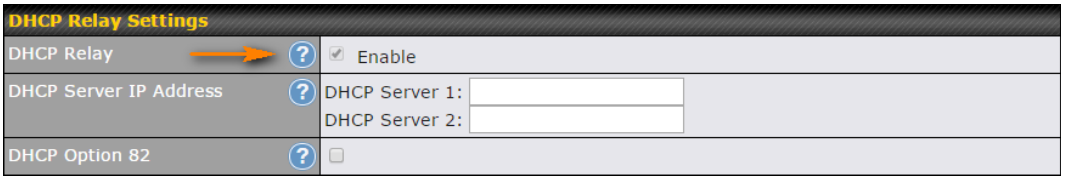


DHCP Server Settings	
DHCP Server	☑ Enable
IP Range	- 255.255.255.0 (/24)
Lease Time	1 Days 0 Hours 0 Mins
DNS Servers	☑ Assign DNS server automatically
WINS Servers	☐ Assign WINS server
BOOTP	☐
Extended DHCP Option	Option / Value No Extended DHCP Option Add
DHCP Reservation	Name / MAC Address / Static IP +

DHCP Server Settings	
DHCP Server	When this setting is enabled, the Pepwave router's DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Pepwave router's DHCP server can prevent IP address collisions on the LAN. To enable DHCP bridge relay, please click the ? icon on this menu item.
IP Range & Subnet Mask	These settings allocate a range of IP addresses that will be assigned to LAN computers by the Pepwave router's DHCP server.
Lease Time	This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of **Lease Time**, the assigned IP address will no longer be valid and the IP address assignment must be renewed.

DNS Servers	This option allows you to input the DNS server addresses to be offered to DHCP clients. If **Assign DNS server automatically** is selected, the Pepwave router's built-in DNS server address (i.e., LAN IP address) will be offered.
WINS Servers	This option allows you to specify the Windows Internet Name Service (WINS) server. You may choose to use the built-in WINS server or external WINS servers. When this unit is connected using SpeedFusion^{TM}, other VPN peers can share this unit's built-in WINS server by entering this unit's LAN IP address in their **DHCP WINS Servers** setting. Therefore, all PC clients in the VPN can resolve the NetBIOS names of other clients in remote peers. If you have enabled this option, a list of WINS clients will be displayed at **Status>WINS Clients**.
BOOTP	Check this box to enable BOOTP on older networks that still require it.
Extended DHCP Option	In addition to standard DHCP options (e.g. DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts. To define an extended DHCP option, click the **Add** button, choose the option to define, and then enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only.
DHCP Reservation	This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses. The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses. **Name** (an optional field) allows you to specify a name to represent the device. MAC addresses should be in the format of **00:AA:BB:CC:DD:EE**. Press ➕ to create a new record. Press ✖ to remove a record. Reserved clients information can be imported from the **Client List**, located at **Status>Client List**. For more details, please refer to **Section 22.3.**

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



DHCP Relay Settings	
DHCP Relay	☑ Enable
DHCP Server IP Address	DHCP Server 1: DHCP Server 2:
DHCP Option 82	☐

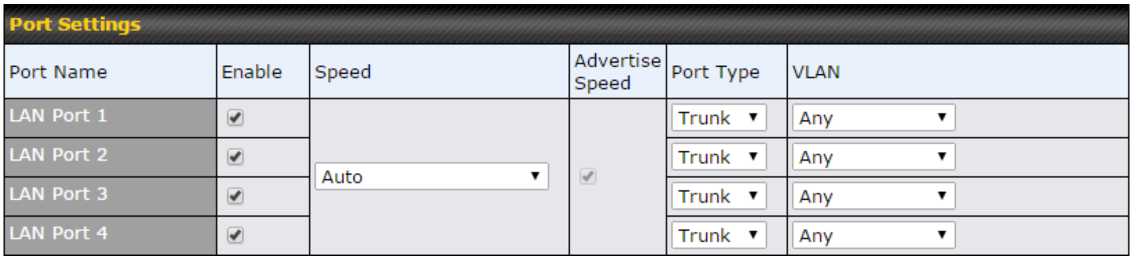
DHCP Relay Settings	
Enable	Check this box to turn on DHCP relay. Click the ? icon to disable DHCP relay.
DHCP Server IP	Enter the IP addresses of one or two DHCP servers in the provided fields. The DHCP servers entered here will receive relayed DHCP requests from the LAN. For

Address	active-passive DHCP server configurations, enter active and passive DHCP server relay IP addresses in **DHCP Server 1** and **DHCP Server 2.**
DHCP Option 82	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**



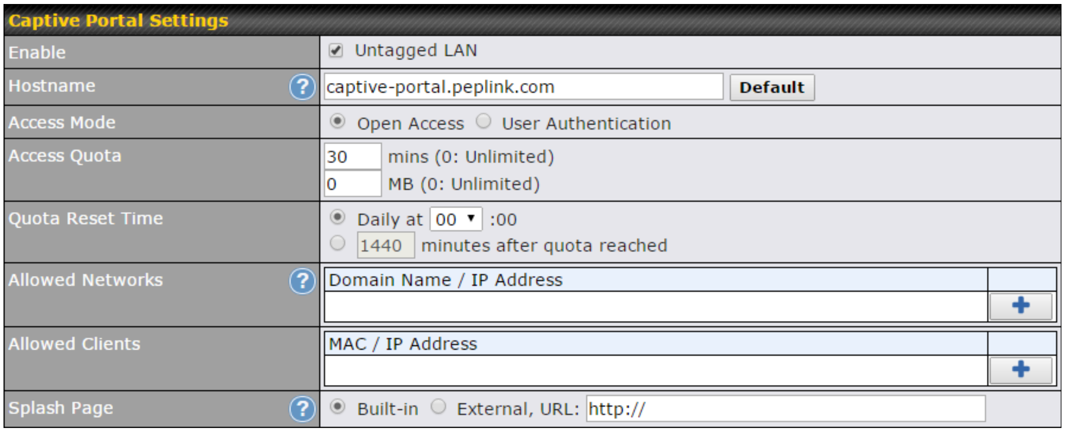
Port Settings

Port Name	Enable	Speed	Advertise Speed	Port Type	VLAN
LAN Port 1	☑	Auto	☑	Trunk	Any
LAN Port 2	☑			Trunk	Any
LAN Port 3	☑			Trunk	Any
LAN Port 4	☑			Trunk	Any

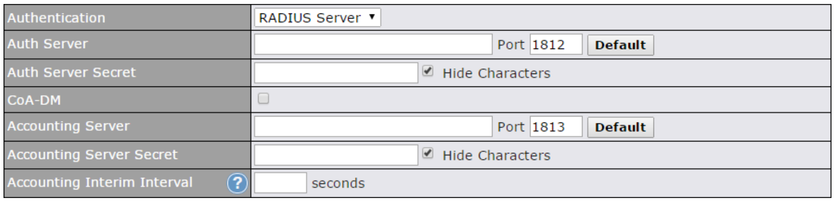
On this screen, you can enable specific ports, as well as determine the speed of the LAN ports, whether each port is a trunk or access port, can well as which VLAN each link belongs to, if any.

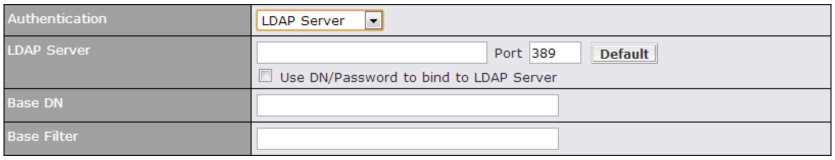
8.3 Captive Portal

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**.

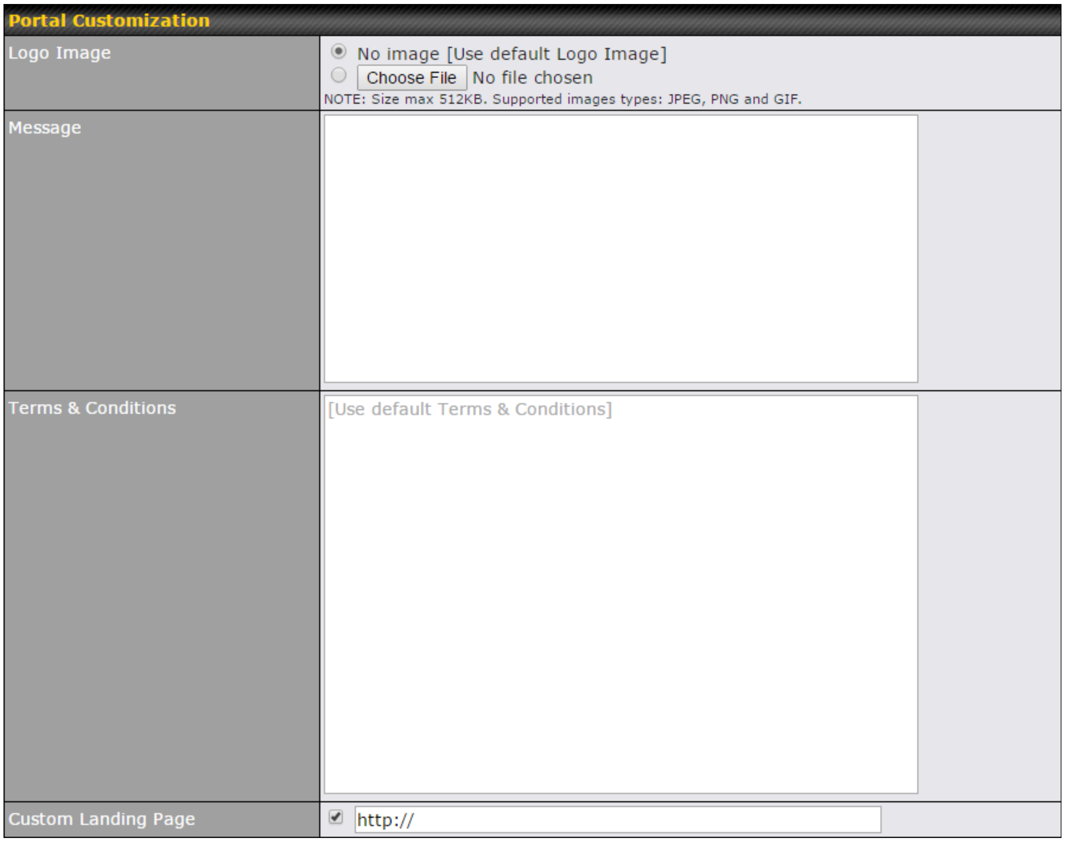


Captive Portal Settings	
Enable	☑ Untagged LAN
Hostname	captive-portal.peplink.com Default
Access Mode	● Open Access ○ User Authentication
Access Quota	30 mins (0: Unlimited) 0 MB (0: Unlimited)
Quota Reset Time	● Daily at 00 :00 ○ 1440 minutes after quota reached
Allowed Networks	Domain Name / IP Address
Allowed Clients	MAC / IP Address
Splash Page	● Built-in ○ External, URL: 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: Port 1812 Default Auth Server Secret: ☑ Hide Characters CoA-DM: ☐ Accounting Server: Port 1813 Default Accounting Server Secret: ☑ Hide Characters Accounting Interim Interval: 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: Port 389 Default ☐ Use DN/Password to bind to LDAP Server Base DN Base Filter Fill in the necessary information to complete your connection to the server and enable authentication.
Access Quota	Set a time and data cap to each user's Internet usage.
Quota Reset Time	This menu determines how your usage quota resets. Setting it to **Daily** will reset it at a specified time every day. Setting a number of **minutes after quota reached** establish a timer for each user that begins after the quota has been reached.
Allowed Networks	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.
Allowed Clients	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.
Splash Page	Here, you can choose between using the Pepwave router's built-in captive portal and redirecting clients to a URL you define.

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



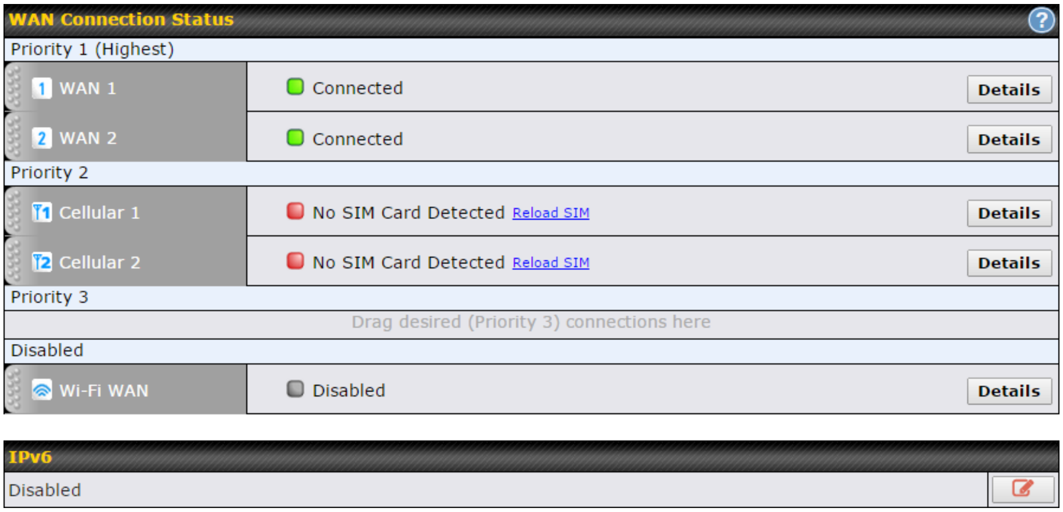
Portal Customization

Logo Image	● No image [Use default Logo Image] ○ Choose File No file chosen NOTE: Size max 512KB. Supported images types: JPEG, PNG and GIF.
Message	
Terms & Conditions	[Use default Terms & Conditions]
Custom Landing Page	☑ http://

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

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	Details
2 WAN 2	🟩 Connected	Details
Priority 2		
T1 Cellular 1	🟥 No SIM Card Detected Reload SIM	Details
T2 Cellular 2	🟥 No SIM Card Detected Reload SIM	Details
Priority 3		
Drag desired (Priority 3) connections here		
Disabled		
Wi-Fi WAN	⬜ Disabled	Details

IPv6

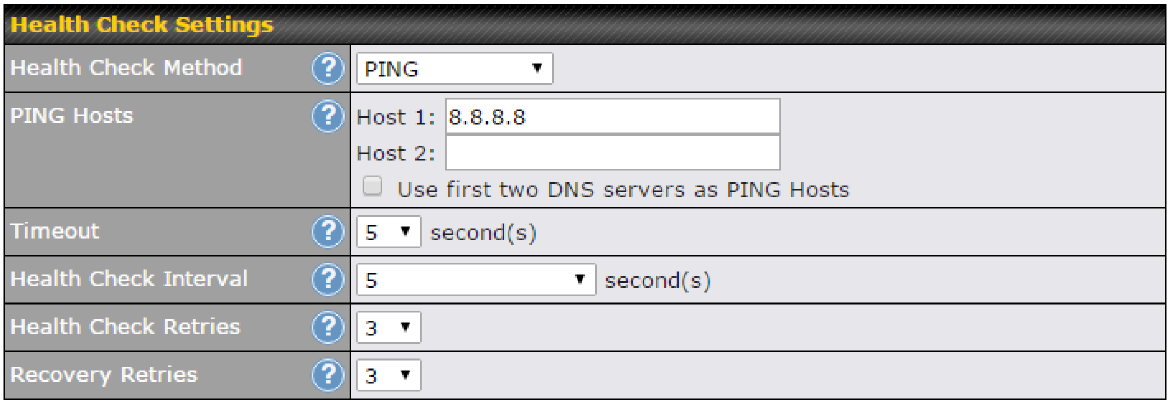
Disabled

To able a particular WAN connection, drag on the appropriate WAN by holding the left mouse button, move it the **Disabled** row, and drop it by releasing the mouse button.

You can also set priorities on the **Dashboard**. Click the **Details** button in the corresponding row to modify the connection setting.

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

9.1 Ethernet WAN



Health Check Settings

Health Check Method: PING

PING Hosts: Host 1: 8.8.8.8
Host 2:
☐ Use first two DNS servers as PING Hosts

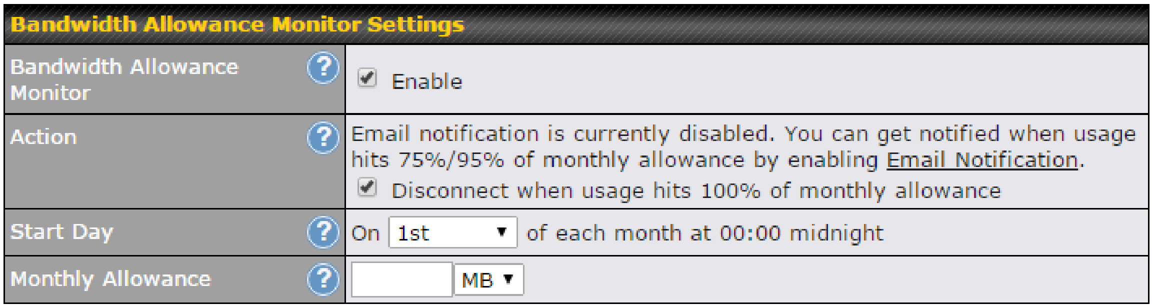
Timeout: 5 second(s)

Health Check Interval: 5 second(s)

Health Check Retries: 3

Recovery Retries: 3

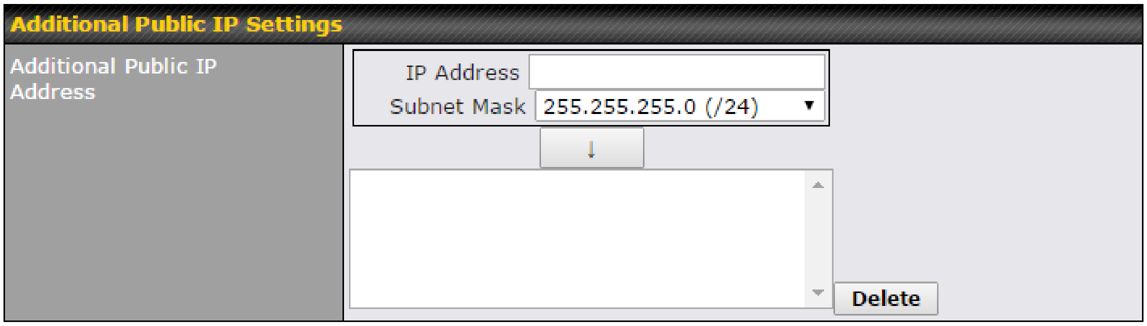
Health Check Settings	
Health Check Method	This field specifies the Health Check method to be used for this WAN connection. ● Disabled - The WAN connection is always considered to be up and will not be treated as down for any IP routing errors. ● PING - ICMP PING packets will be issued to test connectivity with configurable target IP addresses or host names. ● DNS Lookup - DNS lookups will be issued to test the connectivity with configurable target DNS server IP addresses. ● HTTP - HTTP connections will be issued to test the connectivity with configurable URLs and strings to match. Default: DNS Lookup.
PING Hosts	These fields are for specifying the target IP addresses or host names where ICMP Ping packets will be sent to for health check. 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. The connection is considered to be up if ping responses are received from any one of the ping hosts.
Timeout	If a health check test cannot be completed within the specified amount of time, the test will be treated as failed.
Health Check Interval	This is the time interval between each health check test.
Health Check Retries	This is the number of consecutive check failures before treating a connection as down.
Recovery Retries	This is the number of responses required after a health check failure before treating a connection as up again.



Bandwidth Allowance Monitor Settings

Bandwidth Allowance Monitor	☑ Enable
Action	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification. ☑ Disconnect when usage hits 100% of monthly allowance
Start Day	On 1st ▾ of each month at 00:00 midnight
Monthly Allowance	MB ▾

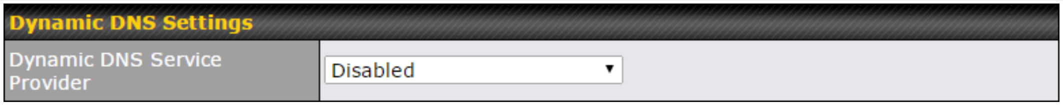
Bandwidth Allowance Monitor Settings	
Bandwidth Allowance Monitor	Check the box *Enable* to enable bandwidth usage monitoring on this WAN connection for each billing cycle. When this option is not enabled, bandwidth usage of each month is still being tracked but no action will be taken.
Action	If Email Notification is enabled, you will receive an email notification when usage hits 75% and 95% of the monthly allowance. 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.
Start Day	This option allows you to select which day of the month a billing cycle starts.
Monthly Allowance	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) ▾

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 ▾

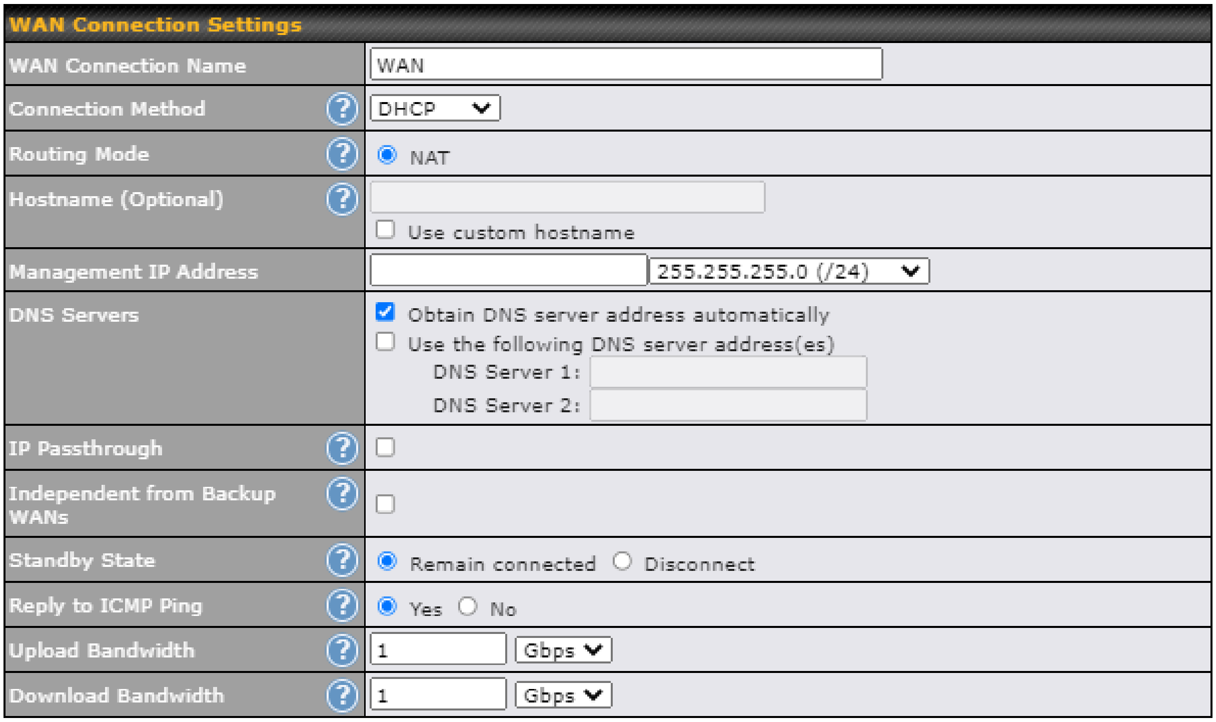
Dynamic DNS Settings	
Dynamic DNS Service Provider	This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers: ● changeip.com ● dyndns.org ● no-ip.org ● tzo.com ● DNS-O-Matic Select **Disabled** to disable this feature. See **Section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

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.).



WAN Connection Settings	
WAN Connection Name	WAN
Connection Method	DHCP
Routing Mode	● NAT
Hostname (Optional)	☐ Use custom hostname
Management IP Address	255.255.255.0 (/24)
DNS Servers	☑ Obtain DNS server address automatically ☐ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
IP Passthrough	☐
Independent from Backup WANs	☐
Standby State	● Remain connected ○ Disconnect
Reply to ICMP Ping	● Yes ○ No
Upload Bandwidth	1 Gbps
Download Bandwidth	1 Gbps

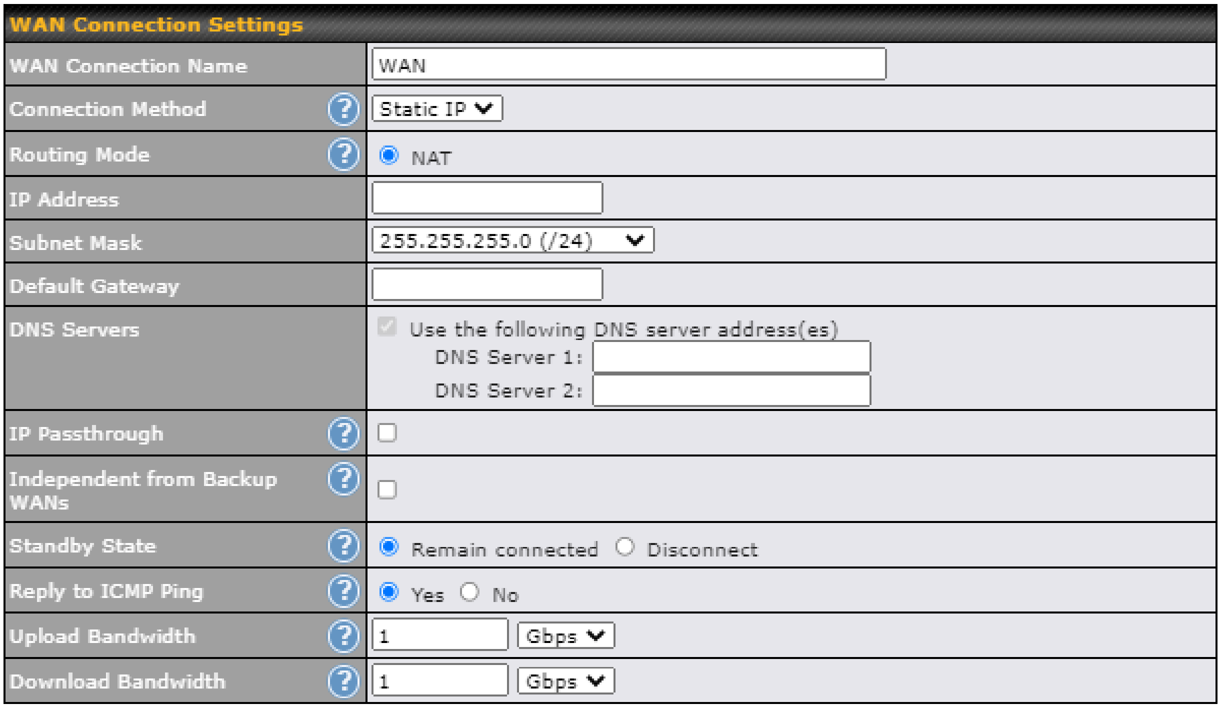
DHCP Connection Settings

Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help ? icon in this field, you can display the **IP Forwarding** option, if your network requires it.
Hostname (Optional)	If your service provider's DHCP server requires you to supply a hostname value upon acquiring an IP address, you may enter the value here. If your service provider does not provide you with the value, you can safely bypass this option.
Management IP Address	**Management IP Address** is available for configuration when you click the link in the help ? icon via the Hostname. This option allows you to configure the management IP address for the DHCP WAN connection.
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.
IP Passthrough	When this **IP Passthrough** option is active, after the ethernet WAN connection is up, the router's DHCP server will offer the connection's IP address to one LAN client. All incoming or outgoing traffic will be routed without NAT. Regardless the WAN connection's state, the router always binds to the LAN IP address (Default: 192.168.50.1). So when the ethernet WAN is connected, the LAN client could access the router's web admin by manually configuring its IP address to the same subnet as the router's LAN IP address (e.g. 192.168.50.10). Note: when this option is firstly enabled, the LAN client may not be able to refresh its IP address to the ethernet WAN IP address in a timely fashion. The LAN client may have to manually renew its IP address from DHCP server. After this option is enabled, the DHCP lease time will be 2 minutes. I.e. the LAN client could refresh its IP address and access the network at most one minute after the ethernet WAN connection goes up.
Independent from Backup WANs	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.

Standby State	This option allows you to choose whether to remain connected when this WAN connection is no longer in the highest priority and has entered the standby state. When **Remain connected** is chosen, upon bringing up this WAN connection to active, it will be immediately available for use. If this WAN connection is charged by connection time, you may want to set this option to **Disconnect** so that connection will be made only when needed. PepVPN may use connected standby WAN for failover if link failure detected on the higher priority WAN, you can set this option to Disconnect to avoid data passing through.
Reply to ICMP PING	If the checkbox is **unticked**, this option is disabled and the system will not reply to any ICMP ping echo requests to the WAN IP addresses of this WAN connection. Default: **ticked** (Yes)
Upload Bandwidth	This field refers to the maximum upload speed. This value is referenced when default weight is chosen for outbound traffic and traffic prioritization. A correct value can result in effective traffic prioritization and efficient use of upstream bandwidth.
Download Bandwidth	This field refers to the maximum download speed. Default weight control for outbound traffic will be adjusted according to this value.

9.1.2 Static IP Connection

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

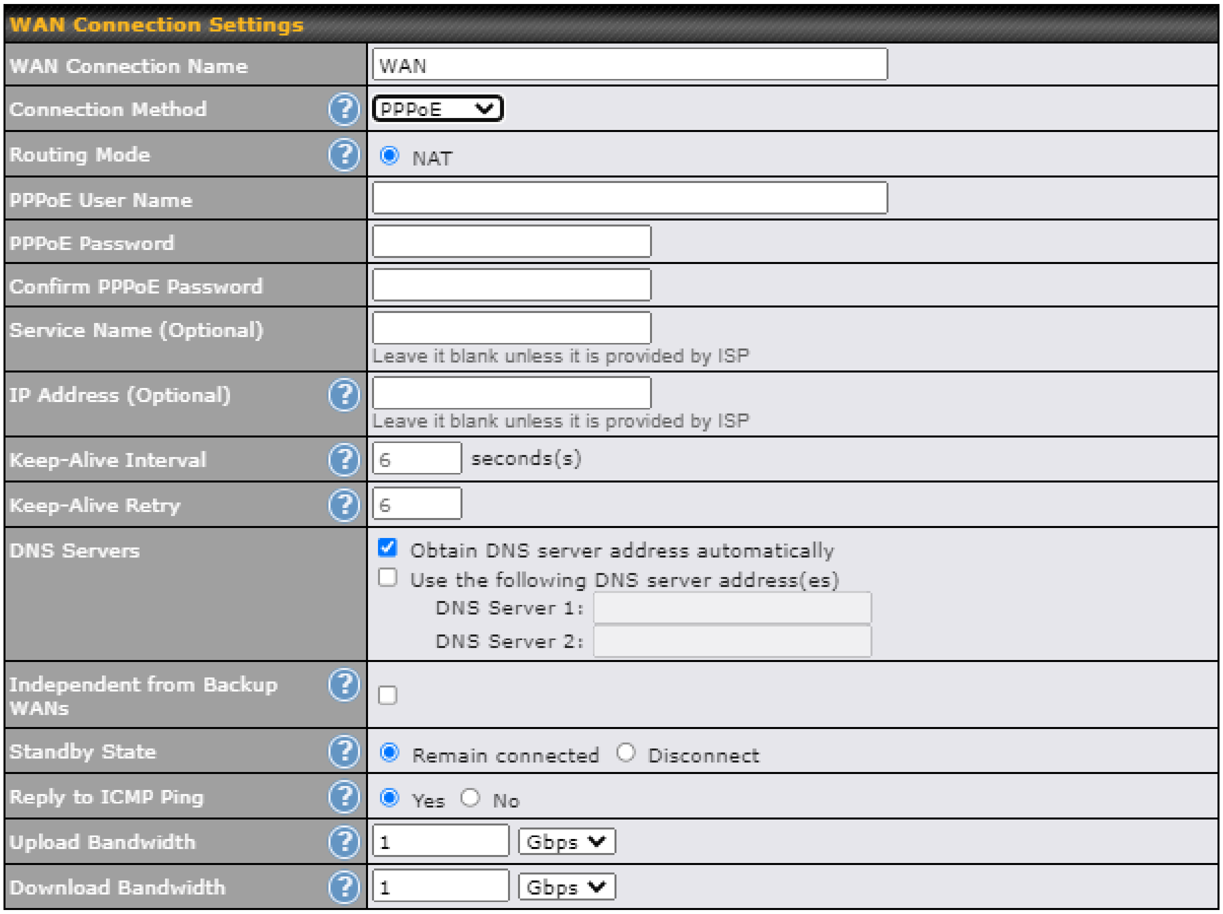


WAN Connection Settings	
WAN Connection Name	WAN
Connection Method	Static IP
Routing Mode	● NAT
IP Address	
Subnet Mask	255.255.255.0 (/24)
Default Gateway	
DNS Servers	☑ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
IP Passthrough	☐
Independent from Backup WANs	☐
Standby State	● Remain connected ○ Disconnect
Reply to ICMP Ping	● Yes ○ No
Upload Bandwidth	1 Gbps
Download Bandwidth	1 Gbps

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.

9.1.3 PPPoE Connection

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



WAN Connection Settings

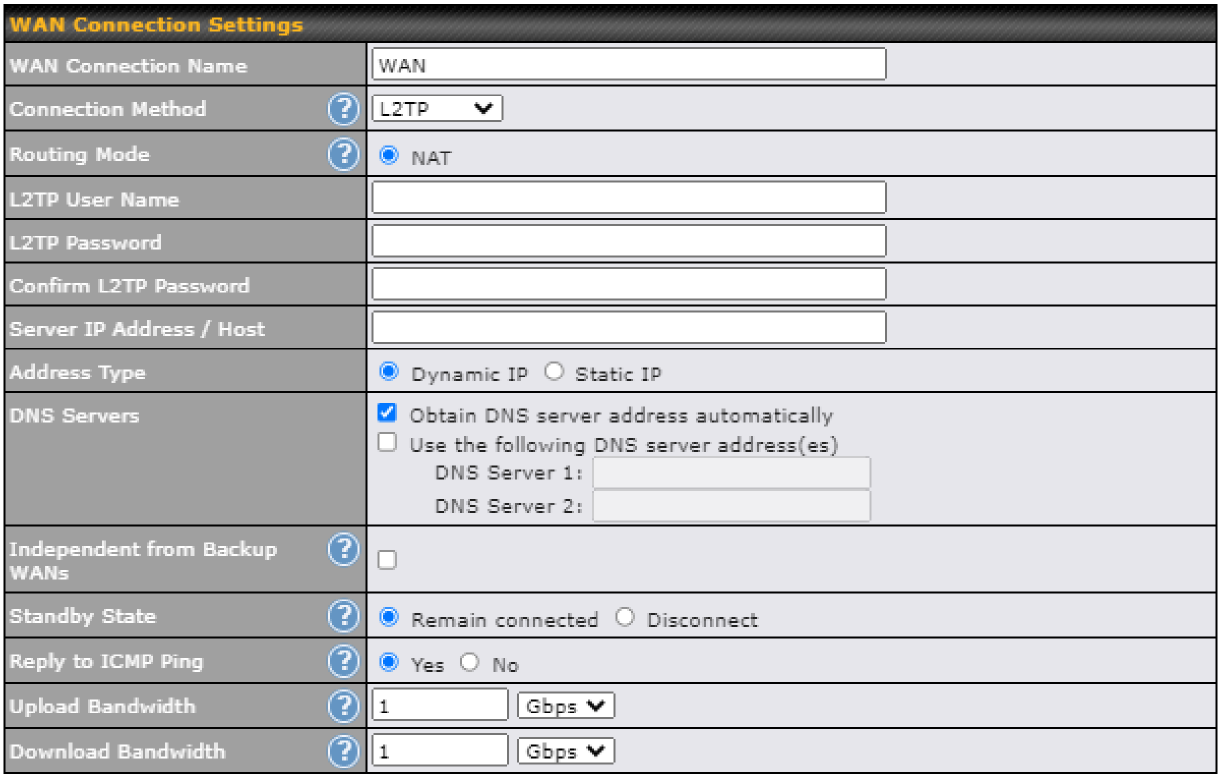
WAN Connection Name	WAN
Connection Method	PPPoE
Routing Mode	● NAT
PPPoE User Name	
PPPoE Password	
Confirm PPPoE Password	
Service Name (Optional)	Leave it blank unless it is provided by ISP
IP Address (Optional)	Leave it blank unless it is provided by ISP
Keep-Alive Interval	6 seconds(s)
Keep-Alive Retry	6
DNS Servers	☑ Obtain DNS server address automatically ☐ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
Independent from Backup WANs	☐
Standby State	● Remain connected ○ Disconnect
Reply to ICMP Ping	● Yes ○ No
Upload Bandwidth	1 Gbps
Download Bandwidth	1 Gbps

PPPoE Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.
PPPoE Username / Password	Enter the required information in these fields in order to connect via PPPoE to the ISP. The parameter values are determined by and can be obtained from the ISP.
Confirm PPPoE Password	Verify your password by entering it again in this field.
Service Name (Optional)	Service name is provided by the ISP. **Note: Leave this field blank unless it is provided by your ISP.**
IP Address	If your ISP provides a PPPoE IP address, enter it here.

(Optional)	**Note: Leave this field blank unless it is provided by your ISP.**
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers being assigned by the WAN DHCP server to be used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned from the DHCP server.) When **Use the following DNS server address(es)** is selected, you may enter custom DNS server addresses for this WAN connection into the **DNS Server 1** and **DNS Server 2** fields.

9.1.4 L2TP Connection

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



WAN Connection Settings

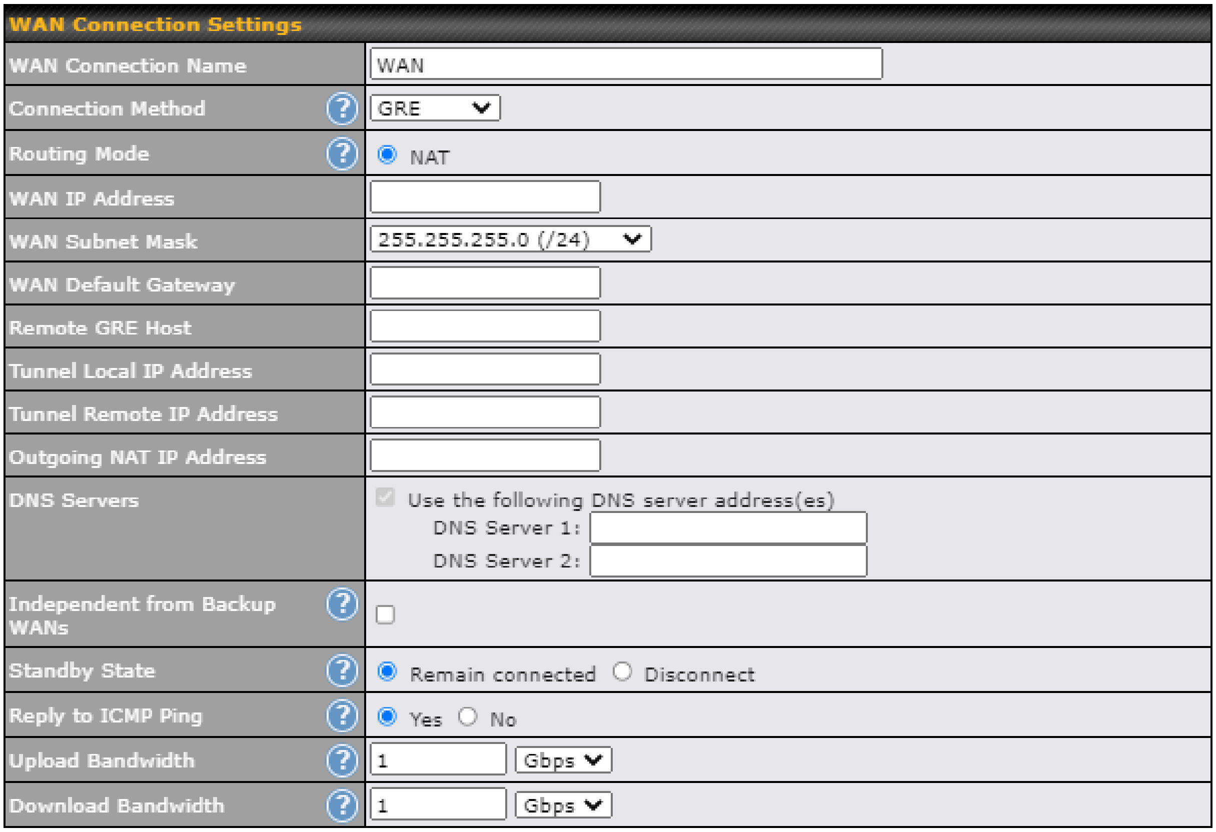
WAN Connection Name	WAN
Connection Method	L2TP
Routing Mode	● NAT
L2TP User Name	
L2TP Password	
Confirm L2TP Password	
Server IP Address / Host	
Address Type	● Dynamic IP ○ Static IP
DNS Servers	☑ Obtain DNS server address automatically ☐ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
Independent from Backup WANs	☐
Standby State	● Remain connected ○ Disconnect
Reply to ICMP Ping	● Yes ○ No
Upload Bandwidth	1 Gbps
Download Bandwidth	1 Gbps

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

	WAN connection. (The DNS servers are obtained along with the WAN IP address assigned from the PPPoE server.) When **Use the following DNS server address(es)** is selected, you can enter custom DNS server addresses for this WAN connection into the **DNS server 1** and **DNS server 2** fields.

9.1.5 GRE Connection

This connection method is suitable if your ISP provides a static WAN IP and Tunnel IP via GRE.

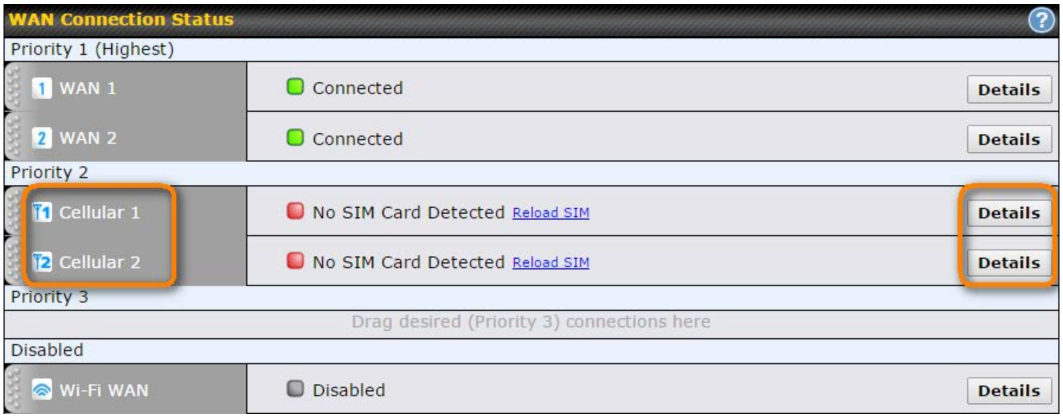


WAN Connection Settings	
WAN Connection Name	WAN
Connection Method	GRE
Routing Mode	● NAT
WAN IP Address	
WAN Subnet Mask	255.255.255.0 (/24)
WAN Default Gateway	
Remote GRE Host	
Tunnel Local IP Address	
Tunnel Remote IP Address	
Outgoing NAT IP Address	
DNS Servers	☑ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
Independent from Backup WANs	☐
Standby State	● Remain connected ○ Disconnect
Reply to ICMP Ping	● Yes ○ No
Upload Bandwidth	1 Gbps
Download Bandwidth	1 Gbps

L2TP 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.

WAN 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.
Remote GRE Host	This field allows you to enter the IP address of the remote GRE.
Tunnel Local IP Address	This field allows you to enter the IP address of the local tunnel for the GRE tunnel connection.
Tunnel Remote IP Address	This field allows you to enter the IP address of the remote tunnel for the GRE tunnel connection.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting **Obtain DNS server address automatically** results in the DNS servers assigned by the PPPoE server to be used for outbound DNS lookups over the WAN connection. (The DNS servers are obtained along with the WAN IP address assigned from the PPPoE server.) When **Use the following DNS server address(es)** is selected, you can enter custom DNS server addresses for this WAN connection into the **DNS server 1** and **DNS server 2** fields.

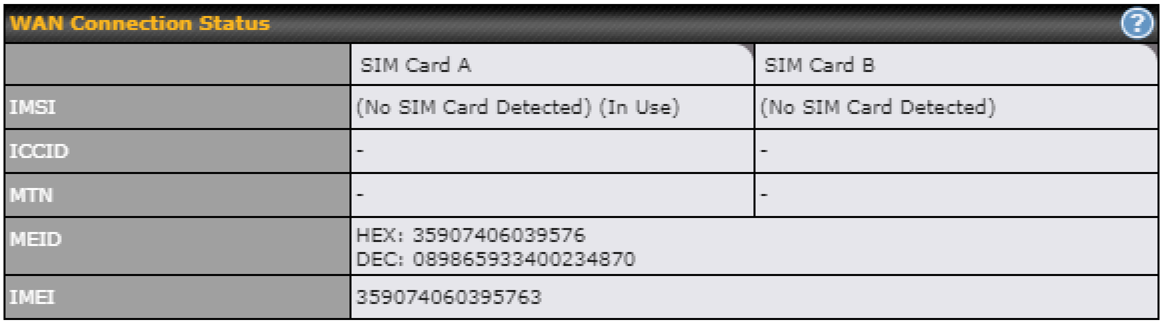
9.2 Cellular WAN



WAN Connection Status

Priority 1 (Highest)		
1 WAN 1	🟩 Connected	Details
2 WAN 2	🟩 Connected	Details
Priority 2		
Cellular 1	🟥 No SIM Card Detected Reload SIM	Details
Cellular 2	🟥 No SIM Card Detected Reload SIM	Details
Priority 3		
	Drag desired (Priority 3) connections here	
Disabled		
Wi-Fi WAN	● Disabled	Details

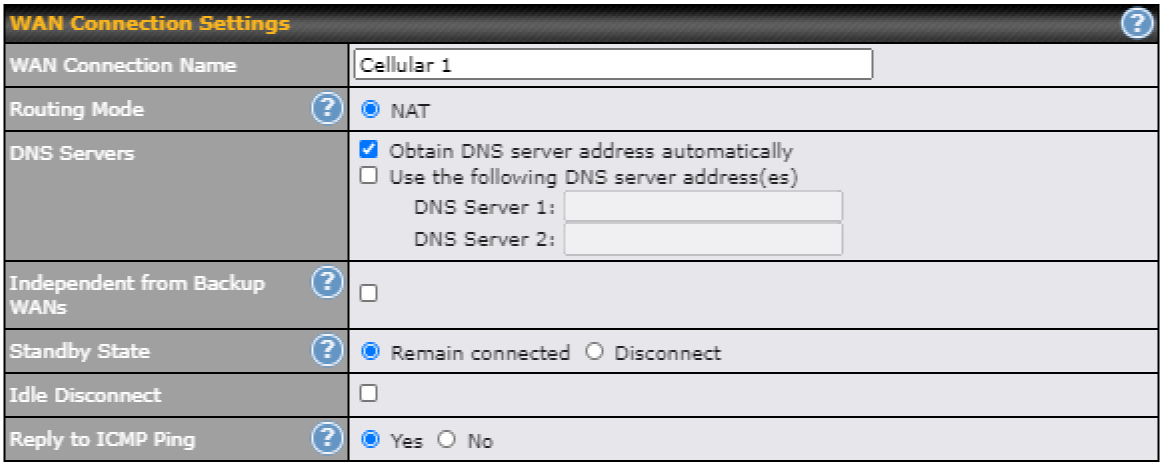
To access cellular WAN settings, click **Network>WAN>Details**.



WAN Connection Status

	SIM Card A	SIM Card B
IMSI	(No SIM Card Detected) (In Use)	(No SIM Card Detected)
ICCID	-	-
MTN	-	-
MEID	HEX: 35907406039576 DEC: 089865933400234870	
IMEI	359074060395763	

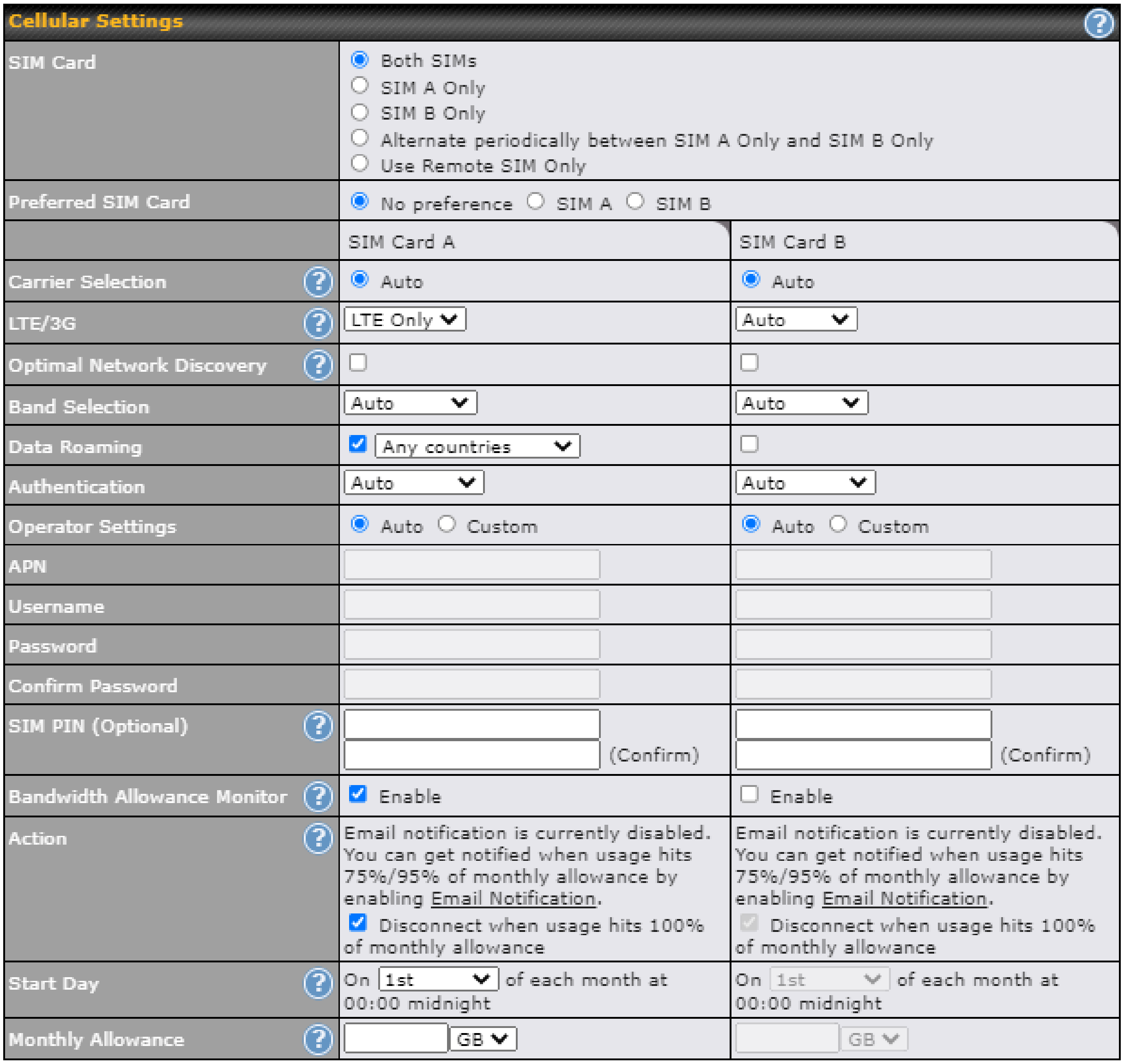
WAN Connection Status	
IMSI	This is the International Mobile Subscriber Identity which uniquely identifies the SIM card. This is applicable to 3G modems only.
ICCID	This is a unique number assigned to a SIM card used in a cellular device.
MEID	Some Pepwave routers support both HSPA and EV-DO. For Sprint or Verizon Wireless EV-DO users, a unique MEID identifier code (in hexadecimal format) is used by the carrier to associate the EV-DO device with the user. This information is presented in hex and decimal format.
IMEI	This is the unique ID for identifying the modem in GSM/HSPA mode.



WAN Connection Settings	
WAN Connection Name	Cellular 1
Routing Mode	● NAT
DNS Servers	☑ Obtain DNS server address automatically ☐ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
Independent from Backup WANs	☐
Standby State	● Remain connected ○ Disconnect
Idle Disconnect	☐
Reply to ICMP Ping	● Yes ○ No

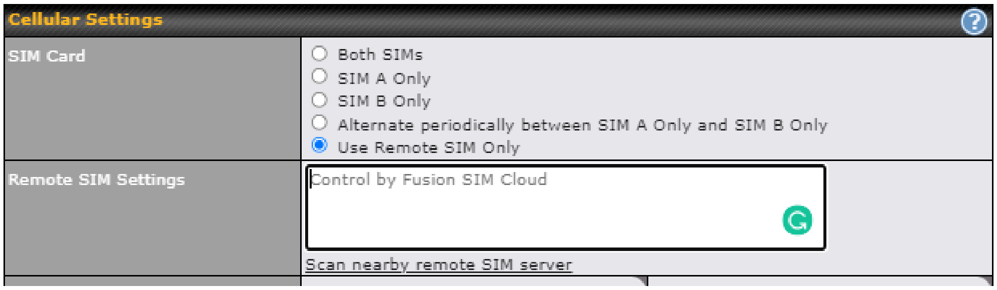
Connection Settings	
WAN Connection Name	Indicate a name you wish to give this WAN connection
Routing Mode	This option allows you to select the routing method to be used in routing IP frames via the WAN connection. The mode can be either NAT (Network Address Translation) or IP Forwarding. In the case if you need to choose IP Forwarding for your scenario. Click the ? button to enable IP Forwarding.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting Obtain DNS server address automatically results in the DNS servers assigned by the 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.
Independent from Backup WANs	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.
Standby State	This option allows you to choose whether to remain connected or disconnected when this WAN connection is no longer in the highest priority and has entered the standby state. When **Remain connected** is chosen, bringing up this WAN connection to active makes it immediately available for use.

Idle Disconnect	If this is checked, the connection will disconnect when idle after the configured Time value. This option is disabled by default.



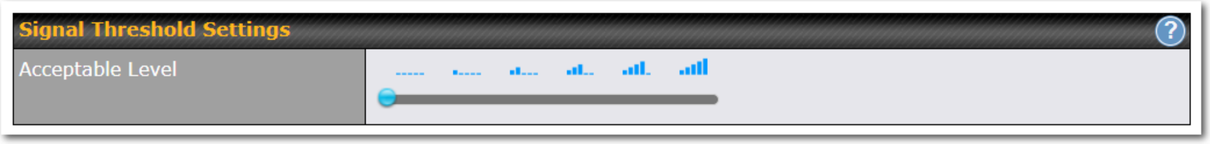
Cellular Settings		
SIM Card	● Both SIMs ○ SIM A Only ○ SIM B Only ○ Alternate periodically between SIM A Only and SIM B Only ○ Use Remote SIM Only	
Preferred SIM Card	● No preference ○ SIM A ○ SIM B	
	SIM Card A	SIM Card B
Carrier Selection	● Auto	● Auto
LTE/3G	LTE Only	Auto
Optimal Network Discovery	☐	☐
Band Selection	Auto	Auto
Data Roaming	☑ Any countries	☐
Authentication	Auto	Auto
Operator Settings	● Auto ○ Custom	● Auto ○ Custom
APN		
Username		
Password		
Confirm Password		
SIM PIN (Optional)	(Confirm)	(Confirm)
Bandwidth Allowance Monitor	☑ Enable	☐ Enable
Action	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification. ☑ Disconnect when usage hits 100% of monthly allowance	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification. ☑ Disconnect when usage hits 100% of monthly allowance
Start Day	On 1st of each month at 00:00 midnight	On 1st of each month at 00:00 midnight
Monthly Allowance	GB	GB

Cellular Settings	
SIM Card	IIndicate which SIM card this cellular WAN will use. Only applies to cellular WAN with redundant SIM cards. For routers that support the SIM Injector, you may select the "Use Remote SIM Only" to provision a SIM from a SIM Injector. Further details on the SIM Injector found is available here: https://www.peplink.com/products/sim-injector/.
Preferred SIM	If "**Both SIMs**" were selected on the above field, then you can designate the priority

Card	of the SIM card slots here.
Remote SIM Settings	If “**Use Remote SIM Only**” is selected in the SIM card section, the **Remote SIM Settings** will be shown.  Cellular Settings SIM Card: ○ Both SIMs ○ SIM A Only ○ SIM B Only ○ Alternate periodically between SIM A Only and SIM B Only ● Use Remote SIM Only Remote SIM Settings: Control by Fusion SIM Cloud Scan nearby remote SIM server You may need to enable the remote SIM Host settings in the Remote SIM management, see the **section 22.10** or **Appendix B** for more details on FusionSIM. After that, click on “**Scan nearby remote SIM server**” to show the serial number(s) of the connected SIM Injector(s). If you want to select a specific SIM, in the Cellular Settings, type “**:**” and then the number of the SIM slot, eg.1111-2222-3333:7.
LTE/3G	This drop-down menu allows restricting cellular to particular band. Click the ? button to enable the selection of specific bands.
Optimal Network Discovery	Cellular WANs 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.
Band Selection	When set to **Auto**, 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.
Data Roaming	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.
Authentication	Choose from **PAP Only** or **CHAP Only** to use those authentication methods exclusively. Select **Auto** to automatically choose an authentication method.
Operator Settings	This setting allows you to configure the APN settings of your connection. If **Auto** is selected, the mobile operator should be detected automatically. The connected device will be configured and connection will be made automatically. If there is any difficulty in making connection, you may select **Custom** to enter your carrier’s **APN**, **Login**, **Password**, and **Dial Number** settings manually. The correct values can be obtained from your carrier. The default and recommended setting is **Auto**.

APN / Login / Password / SIM PIN	When **Auto** is selected, the information in these fields will be filled automatically. Select **Custom** to customize these parameters. The parameter values are determined by and can be obtained from the ISP.
Bandwidth Allowance Monitor	Check the box Enable to enable bandwidth usage monitoring on this WAN connection for each billing cycle. When this option is not enabled, bandwidth usage of each month is still being tracked but no action will be taken.
Action	If email notification is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance. If **Disconnect when usage hits 100% of monthly allowance** is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume connection unless this option has been turned off or the usage has been reset when a new billing cycle starts.
Start Day	This option allows you to define which day of the month each billing cycle begins.
Monthly Allowance	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

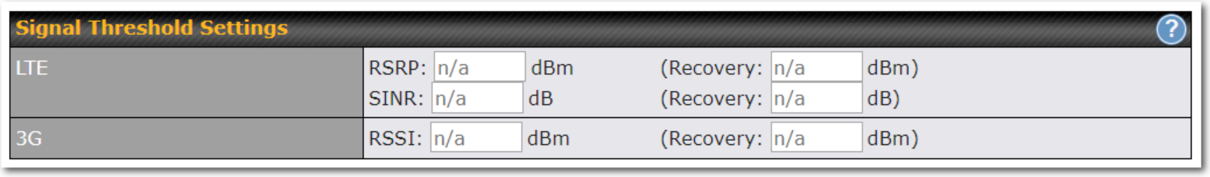
Signal Threshold Settings



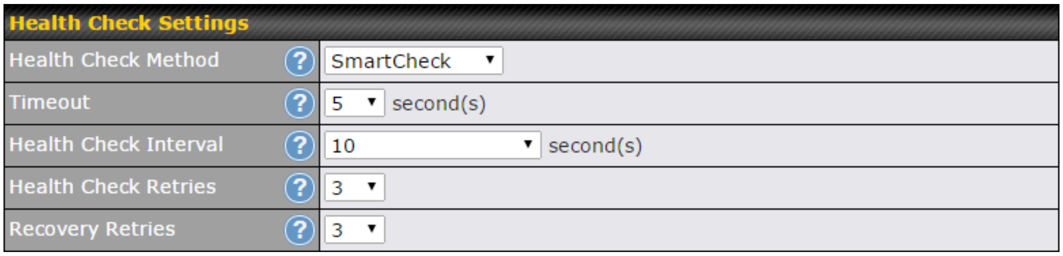
If signal threshold is defined, this connection will be treated as down when a weaker than threshold signal is determined.
The following values are used by the threshold scale:

	0 bars	1 bar	2 bars	3 bars	4 bars	5 bars
LTE / RSSRP	-140	-128	-121	-114	-108	-98
3G / RSSI	-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.

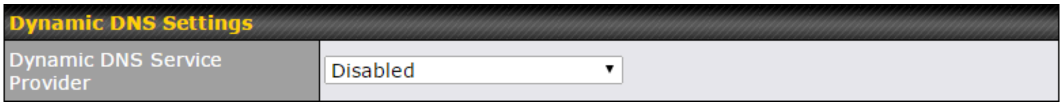

Signal Threshold Settings

LTE	RSRP: n/a dBm	(Recovery: n/a dBm)
	SINR: n/a dB	(Recovery: n/a dB)
3G	RSSI: n/a dBm	(Recovery: n/a dBm)



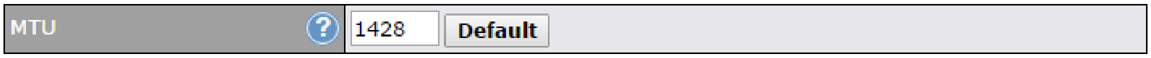
Health Check Settings	
Health Check Method	SmartCheck
Timeout	5 second(s)
Health Check Interval	10 second(s)
Health Check Retries	3
Recovery Retries	3

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



Dynamic DNS Settings	
Dynamic DNS Service Provider	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.

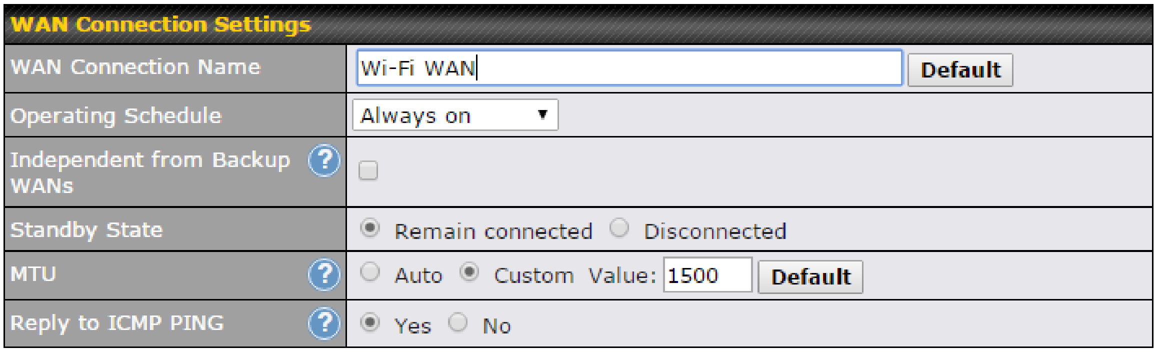


MTU	1428 Default

MTU	
MTU	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**.

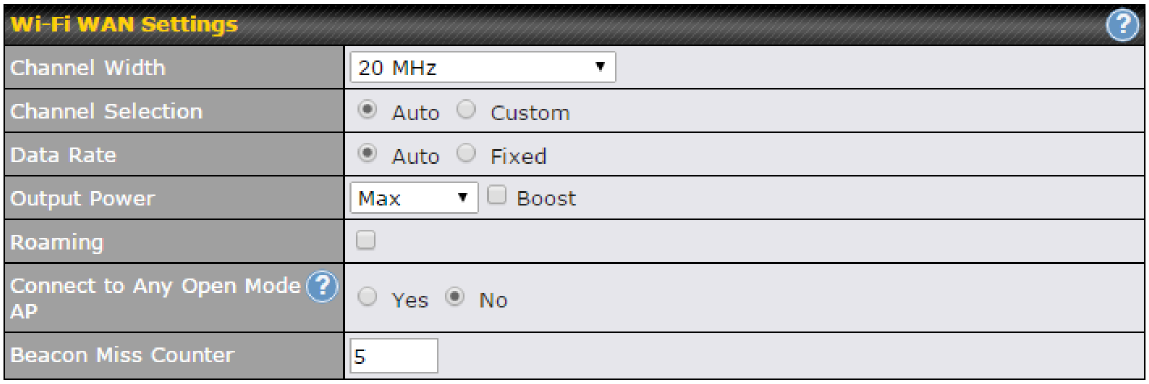


WAN Connection Settings

WAN Connection Name	Wi-Fi WAN Default
Operating Schedule	Always on
Independent from Backup WANs	☐
Standby State	● Remain connected ○ Disconnected
MTU	○ Auto ● Custom Value: 1500 Default
Reply to ICMP PING	● Yes ○ No

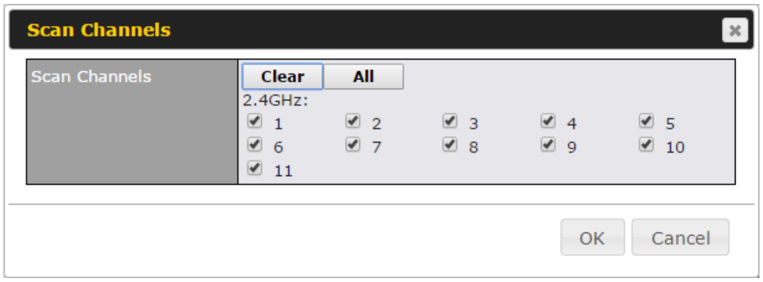
WAN Connection Settings	
WAN Connection Name	Enter a name to represent this WAN connection.
Operating Schedule	Click the drop-down menu to apply a time schedule to this interface.
Independent from Backup WANs	If this is checked, the connection will be working independent from other Backup WAN connections. 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.
Standby State	This setting specifies the state of the WAN connection while in standby. The available options are **Remain Connected** (hot standby) and **Disconnect** (cold standby).
MTU	This setting specifies the maximum transmission unit. By default, MTU is set to **Custom 1440**. You may adjust the MTU value by editing the text field. Click **Default** to restore the default MTU value. Select **Auto** and the appropriate MTU value will be automatically detected. The auto-detection will run each time the

	WAN connection establishes
Reply to ICMP PING	If this setting is disabled, the WAN connection will not respond to ICMP ping requests. By default, this setting is enabled.

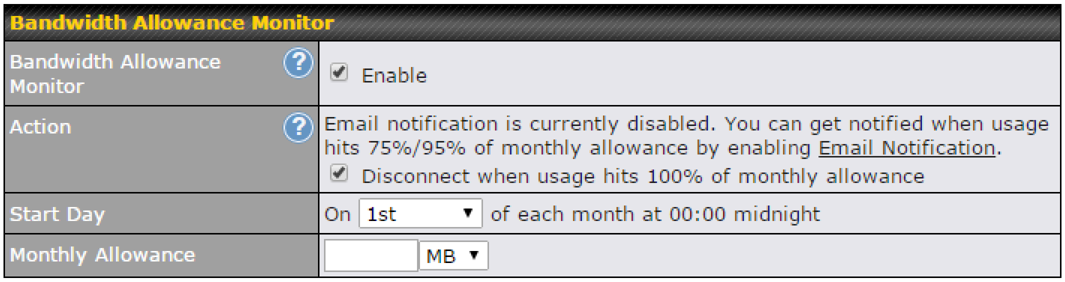


Wi-Fi WAN Settings

Channel Width	20 MHz ▾
Channel Selection	● Auto ○ Custom
Data Rate	● Auto ○ Fixed
Output Power	Max ▾ ☐ Boost
Roaming	☐
Connect to Any Open Mode AP ?	○ Yes ● No
Beacon Miss Counter	5

Wi-Fi WAN Settings	
Channel Width	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
Channel Selection	Determine whether the channel will be automatically selected. If you select custom, the following table will appear:  **Scan Channels** Scan Channels: Clear All 2.4GHz: ☑ 1 ☑ 2 ☑ 3 ☑ 4 ☑ 5 ☑ 6 ☑ 7 ☑ 8 ☑ 9 ☑ 10 ☑ 11 OK Cancel
Data Rate	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.
Output Power	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.
Roaming	Checking this box will enable Wi-Fi roaming. Click the ? icon for additional options.
Connect to Any Open Mode AP	This option is to specify whether the Wi-Fi WAN will connect to any open mode access points it finds.

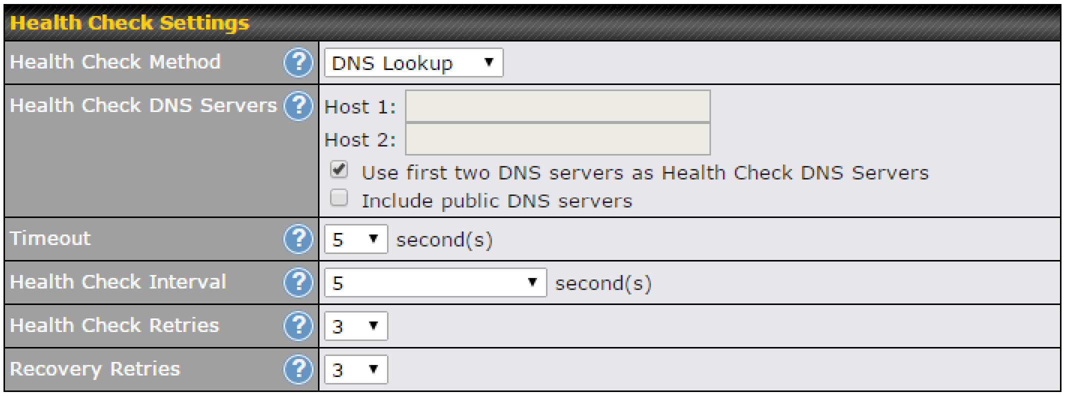
Beacon Miss Counter	This sets the threshold for the number of missed beacons.



Bandwidth Allowance Monitor

Bandwidth Allowance Monitor	☑ Enable
Action	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification. ☑ Disconnect when usage hits 100% of monthly allowance
Start Day	On 1st ▾ of each month at 00:00 midnight
Monthly Allowance	MB ▾

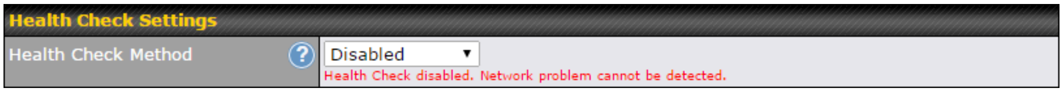
Bandwidth Allowance Monitor	
Action	If enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance. If **Disconnect when usage hits 100% of monthly allowance** is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance.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



Health Check Settings

Health Check Method	DNS Lookup ▾
Health Check DNS Servers	Host 1: Host 2: ☑ Use first two DNS servers as Health Check DNS Servers ☐ Include public DNS servers
Timeout	5 ▾ second(s)
Health Check Interval	5 ▾ second(s)
Health Check Retries	3 ▾
Recovery Retries	3 ▾

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



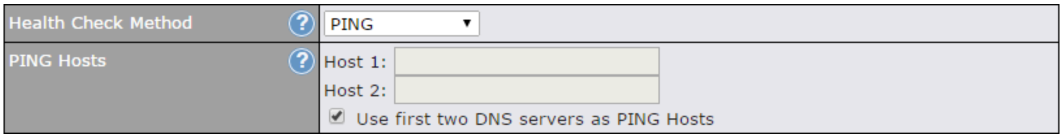
Health Check Settings

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

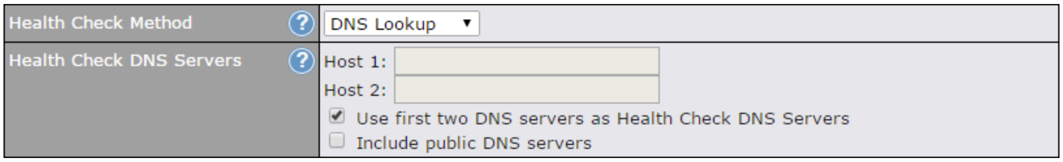
PING Hosts: Host 1: Host 2:

☑ Use first two DNS servers as PING Hosts

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

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

Health Check Method: DNS Lookup



Health Check Method: DNS Lookup

Health Check DNS Servers: Host 1: Host 2:

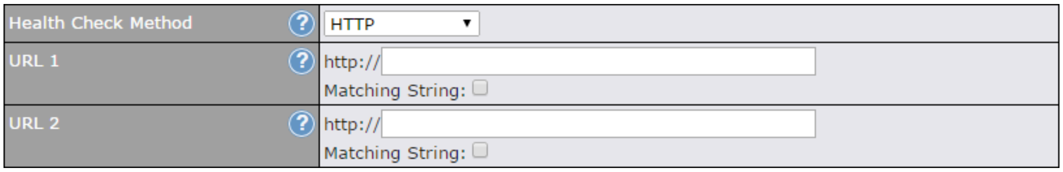
☑ Use first two DNS servers as Health Check DNS Servers

☐ Include public DNS servers

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

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

Health Check Method: HTTP

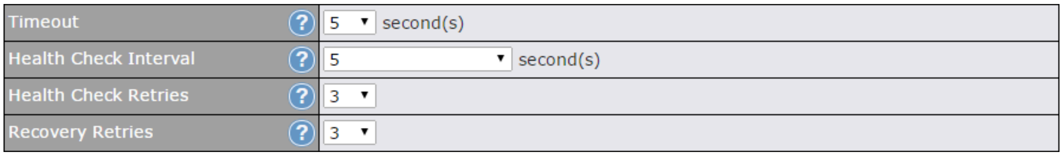


Health Check Method	HTTP
URL 1	http:// Matching String: ☐
URL 2	http:// Matching String: ☐

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

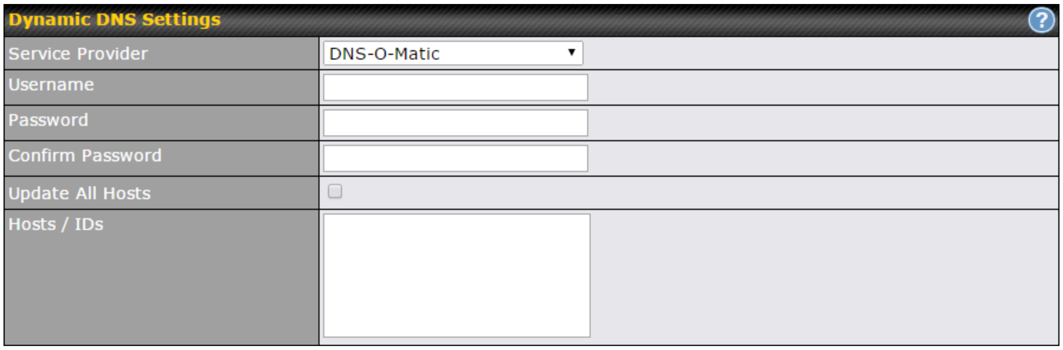
URL1	**WAN Settings>WAN Edit>Health Check Settings>URL1** The URL will be retrieved when performing an HTTP health check. When **String to Match** is left blank, a health check will pass if the HTTP return code is between 200 and 299 **(**Note: HTTP redirection codes 301 or 302 are treated as failures). When **String to Match** is 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 Pepwave MAX will treat the corresponding WAN connection as down. Default health retries is set to **3**. Using the default **Health Retries** setting of **3**, the corresponding WAN connection will be treated as down after three consecutive timeouts.
Recovery Retries	This setting specifies the number of consecutive successful ping/DNS lookup responses that must be received before the Pepwave MAX treats a previously down WAN connection as up again. By default, **Recover Retries** is set to **3**. Using the default setting, a WAN connection that is treated as down will be considered as up again upon receiving three consecutive successful ping/DNS lookup responses.



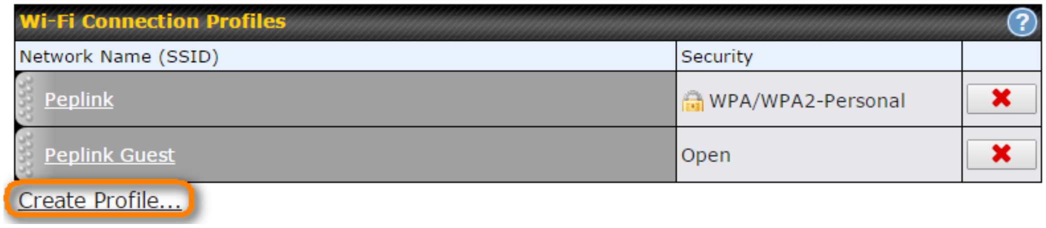
Dynamic DNS Settings	
Service Provider	DNS-O-Matic
Username	
Password	
Confirm Password	
Update All Hosts	☐
Hosts / IDs	

Dynamic DNS Settings	
Service Provider	This setting specifies the dynamic DNS service provider to be used for the WAN. Supported providers are: ● changeip.com ● dyndns.org ● no-ip.org ● tzo.com ● DNS-O-Matic Select **Disabled** to disable this feature.
User ID / User / Email	This setting specifies the registered user name for the dynamic DNS service.
Password / Pass / TZO Key	This setting specifies the password for the dynamic DNS service.
Update All Hosts	Check this box to automatically update all hosts.
Hosts / Domain	This setting specifies a list of hostnames or domains to be associated with the public Internet IP address of the WAN connection.

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

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.

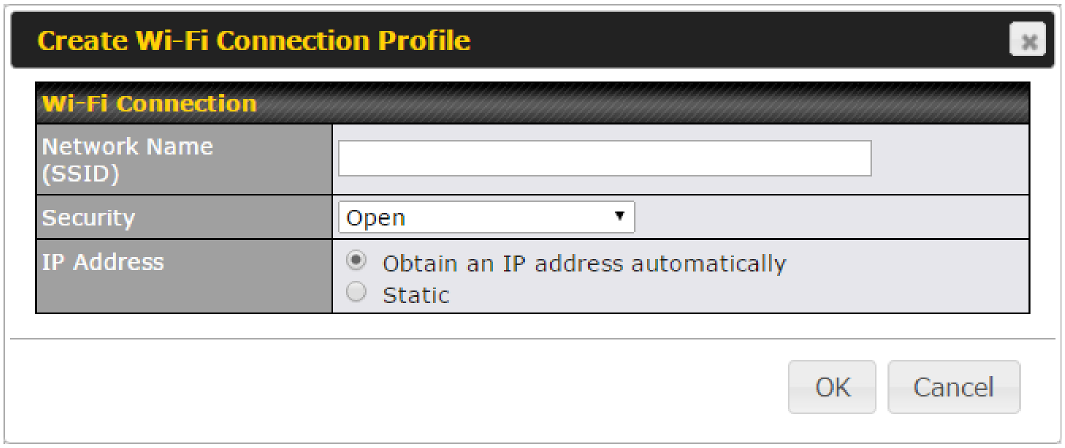


Wi-Fi Connection Profiles

Network Name (SSID)	Security	
Peplink	WPA/WPA2-Personal	✖
Peplink Guest	Open	✖

Create Profile…

This will open a window similar to the one shown below



Create Wi-Fi Connection Profile

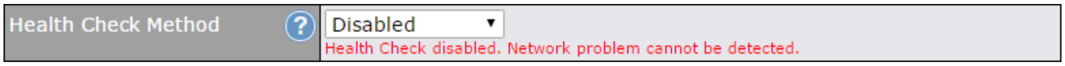
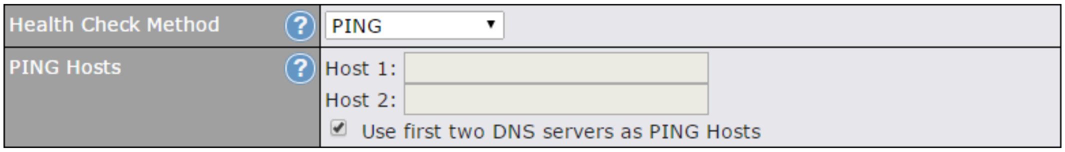
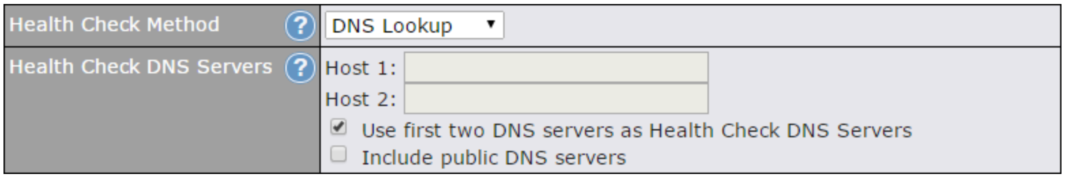
Wi-Fi Connection

Network Name (SSID)	
Security	Open
IP Address	● Obtain an IP address automatically ○ Static

Wi-Fi Connection Profile Settings	
Type	Select whether the network will connect automatically or manually.
Network Name (SSID)	Enter a name to represent this Wi-Fi connection.
Security	This option allows you to select which security policy is used for this wireless network. Available options: ● **Open** ● **WPA3 -Personal (AES:CCMP)** ● **WPA2/WPA3 -Personal (AES:CCMP)** ● **WPA2 – Personal: AES:CCMP** ● **WPA2 – Enterprise: AES: CCMP** ● **WPA/ WPA2 – Personal: TKIP/AES:CCMP** ● **WPA/ WPA2 – ENterprise: TKIP/AES:CCMP**

9.4 WAN Health Check

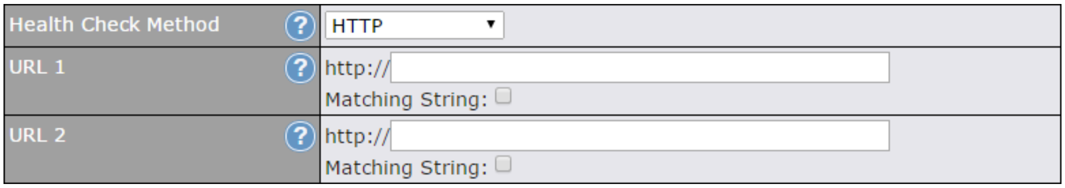
To ensure traffic is routed to healthy WAN connections only, the Pepwave router can periodically check the health of each WAN connection. The health check settings for each WAN connection can be independently configured via **Network>WAN>Details**.

Health Check Settings	
Method	This setting specifies the health check method for the WAN connection. This value can be configured as **Disabled**, **PING**, **DNS Lookup**, or **HTTP**. The default method is **DNS Lookup**. For mobile Internet connections, the value of **Method** can be configured as **Disabled** or **SmartCheck**.
Health Check Disabled	
 Health Check Method: Disabled Health Check disabled. Network problem cannot be detected.	
When **Disabled** is chosen in the **Method** field, the WAN connection will always be considered as up. The connection will **NOT** be treated as down in the event of IP routing errors.	
Health Check Method: PING	
 Health Check Method: PING PING Hosts: Host 1: Host 2: ☑ Use first two DNS servers as PING Hosts	
ICMP ping packets will be issued to test the connectivity with a configurable target IP address or hostname. A WAN connection is considered as up if ping responses are received from either one or both of the ping hosts.	
PING Hosts	This setting specifies IP addresses or hostnames with which connectivity is to be tested via ICMP ping. If **Use first two DNS servers as Ping Hosts** is checked, the target ping host will be the first DNS server for the corresponding WAN connection. Reliable ping hosts with a high uptime should be considered. By default, the first two DNS servers of the WAN connection are used as the ping hosts.
Health Check Method: DNS Lookup	
 Health Check Method: DNS Lookup Health Check DNS Servers: Host 1: Host 2: ☑ Use first two DNS servers as Health Check DNS Servers ☐ Include public DNS servers	
DNS lookups will be issued to test connectivity with target DNS servers. The connection will be treated as up if DNS responses are received from one or both of the servers, regardless of whether the result was positive or negative.	

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

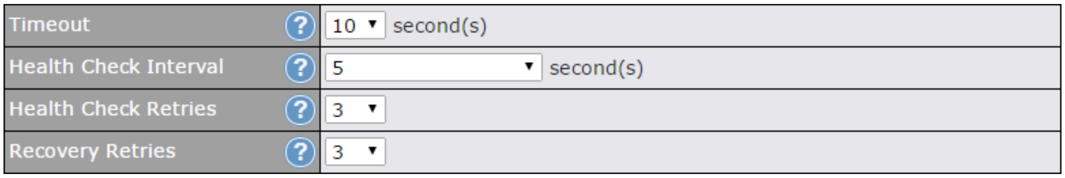
Health Check Method: HTTP

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



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

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.

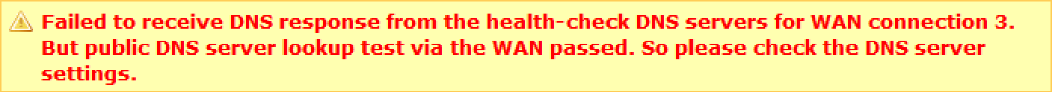


Timeout: 10 second(s)
Health Check Interval: 5 second(s)
Health Check Retries: 3
Recovery Retries: 3

Other Health Check Settings

Timeout	This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is **5 seconds**.
Health Check	This setting specifies the time interval in seconds between ping or DNS lookup

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

Automatic Public DNS Server Check on DNS Test Failure
When the health check method is set to **DNS Lookup** and health checks fail, the Pepwave router will automatically perform DNS lookups on public DNS servers. If the tests are successful, the WAN may not be down, but rather the target DNS server malfunctioned. You will see the following warning message on the main page:  ⚠ Failed to receive DNS response from the health-check DNS servers for WAN connection 3. But public DNS server lookup test via the WAN passed. So please check the DNS server settings.

9.5 Dynamic DNS Settings

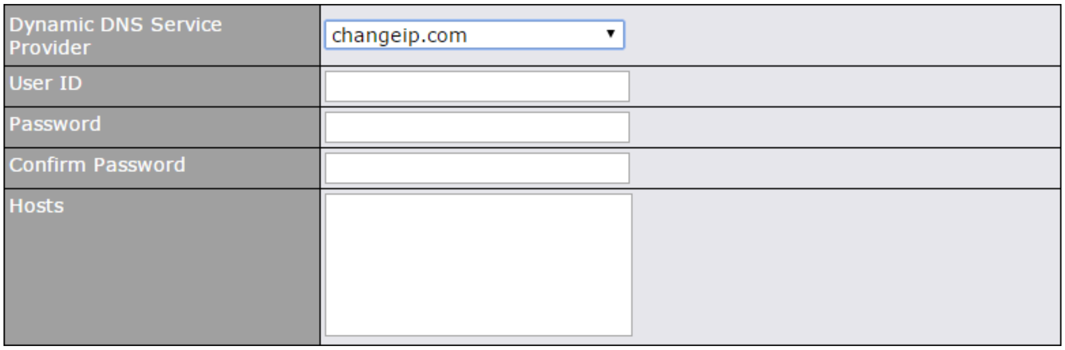
Pepwave routers are capable of registering the domain name relationships to dynamic DNS service providers. Through registration with dynamic DNS service provider(s), the default public Internet IP address of each WAN connection can be associated with a host name. With dynamic DNS service enabled for 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.



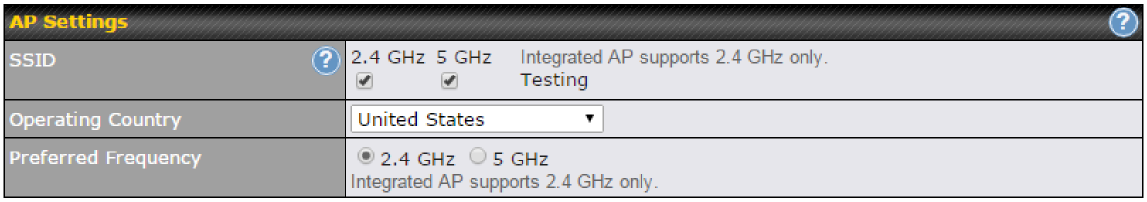
Dynamic DNS Service Provider	changeip.com ▾
User ID	
Password	
Confirm Password	
Hosts	

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

Important Note
In order to use dynamic DNS services, appropriate host name registration(s) and a valid account with a supported dynamic DNS service provider are required. A dynamic DNS update is performed whenever a WAN's IP address changes (e.g., the IP is changed after a DHCP IP refresh, reconnection, etc.). Due to dynamic DNS service providers' policy, a dynamic DNS host will automatically expire if the host record has not been updated for a long time. Therefore the Pepwave router performs an update every 23 days, even if a WAN's IP address has not changed.

10 Advanced Wi-Fi Settings

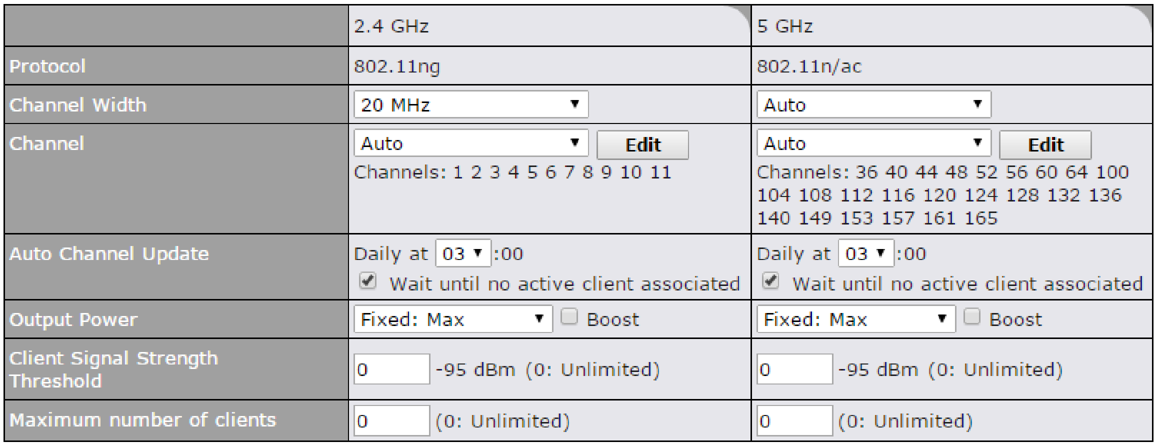
Wi-Fi settings can be configured at **Advanced>Wi-Fi Settings** (or **AP>Settings** on some models). Note: Menus displayed can vary by model.



AP Settings	
SSID	2.4 GHz ☑ 5 GHz ☑ Integrated AP supports 2.4 GHz only. Testing
Operating Country	United States
Preferred Frequency	● 2.4 GHz ○ 5 GHz Integrated AP supports 2.4 GHz only.

AP Settings	
SSID	You can select the wireless networks for 2.4 GHz or 5 GHz separately for each SSID.
Operating Country	This drop-down menu specifies the national/regional regulations which the Wi-Fi radio should follow. ● 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). ● If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW). **N**ote: Users are required to choose an option suitable to local laws and regulations.
Preferred Frequency	Indicate the preferred frequency to use for clients to connect.

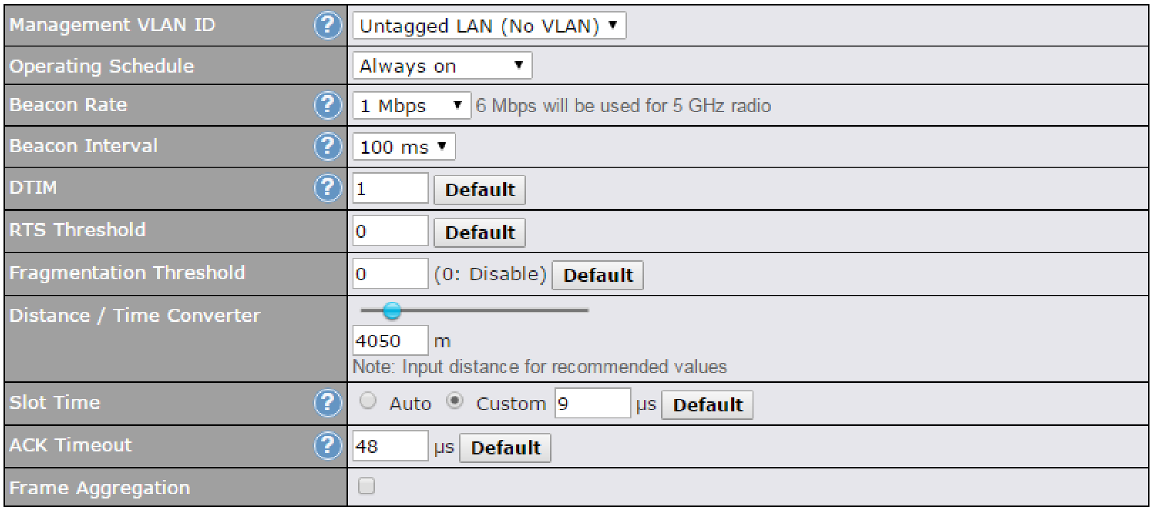
Important Note
Per FCC regulation, the country selection is not available on all models marketed in the US. All US models are fixed to US channels only.



	2.4 GHz	5 GHz
Protocol	802.11ng	802.11n/ac
Channel Width	20 MHz ▾	Auto ▾
Channel	Auto ▾ Edit Channels: 1 2 3 4 5 6 7 8 9 10 11	Auto ▾ 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 ☑ Wait until no active client associated	Daily at 03 ▾ :00 ☑ Wait until no active client associated
Output Power	Fixed: Max ▾ ☐ Boost	Fixed: Max ▾ ☐ 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)	
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 Width	Available options are **20 MHz**, **40 MHz**, and **Auto (20/40 MHz)** . Default is **Auto (20/40 MHz),** which allows both widths to be used simultaneously.
Channel	This option allows you to select which 802.11 RF channel will be utilized. **Channel 1 (2.412 GHz)** is selected by default.
Auto Channel Update	Indicate the time of day at which update automatic channel selection.
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.
Client Signal Strength Threshold	Clients with signal strength lower than this value will not be allowed to connect.
Maximum number of clients	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**.

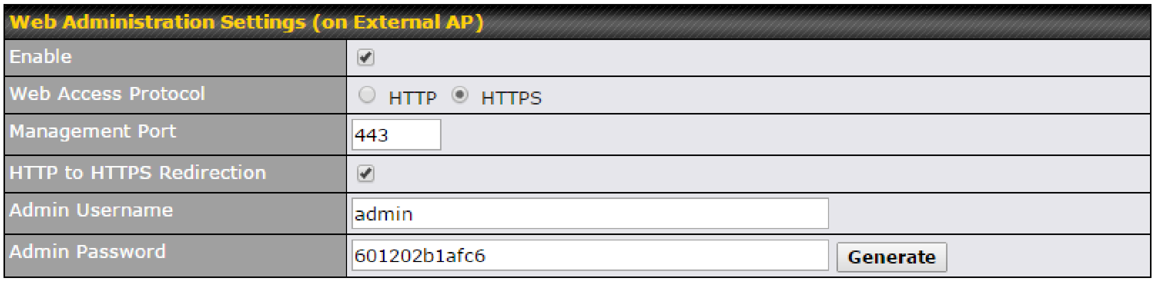


Management VLAN ID	Untagged LAN (No VLAN) ▾
Operating Schedule	Always on ▾
Beacon Rate	1 Mbps ▾ 6 Mbps will be used for 5 GHz radio
Beacon Interval	100 ms ▾
DTIM	1 Default
RTS Threshold	0 Default
Fragmentation Threshold	0 (0: Disable) Default
Distance / Time Converter	4050 m Note: Input distance for recommended values
Slot Time	○ Auto ● Custom 9 µs Default
ACK Timeout	48 µs Default
Frame Aggregation	☐

Advanced AP Settings	
Management VLAN ID	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. Note: Change this value with caution as alterations may result in loss of connection to the AP Controller.
Operating Schedule	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.
Beacon Rate A	This option is for setting the transmit bit rate for sending a beacon. By default, **1Mbps** is selected.
Beacon Interval A	This option is for setting the time interval between each beacon. By default, **100ms** is selected.
DTIM A	This field allows you to set the frequency for the beacon to include delivery traffic indication messages. The interval is measured in milliseconds. The default value is set to **1 ms**.
RTS Threshold A	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.
Fragmentation Threshold A	This setting determines the maximum size of a packet before it gets fragmented into multiple pieces.
Distance / Time Convertor	Select the range you wish to cover with your Wi-Fi, and the router will make recommendations for the Slot Time and ACK Timeout.
Slot Time A	This field is for specifying the unit wait time before transmitting a packet. By default, this field is set to **9 µs**.

ACK Timeout [A]	This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to **48 μs**.
Frame Aggregation [A]	This option allows you to enable frame aggregation to increase transmission throughput.

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

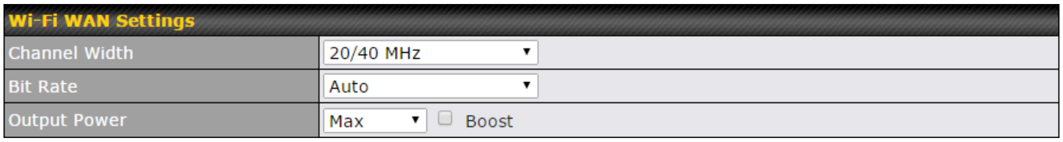


Web Administration Settings (on External AP)

Enable	☑
Web Access Protocol	○ HTTP ● HTTPS
Management Port	443
HTTP to HTTPS Redirection	☑
Admin Username	admin
Admin Password	601202b1afc6 Generate

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

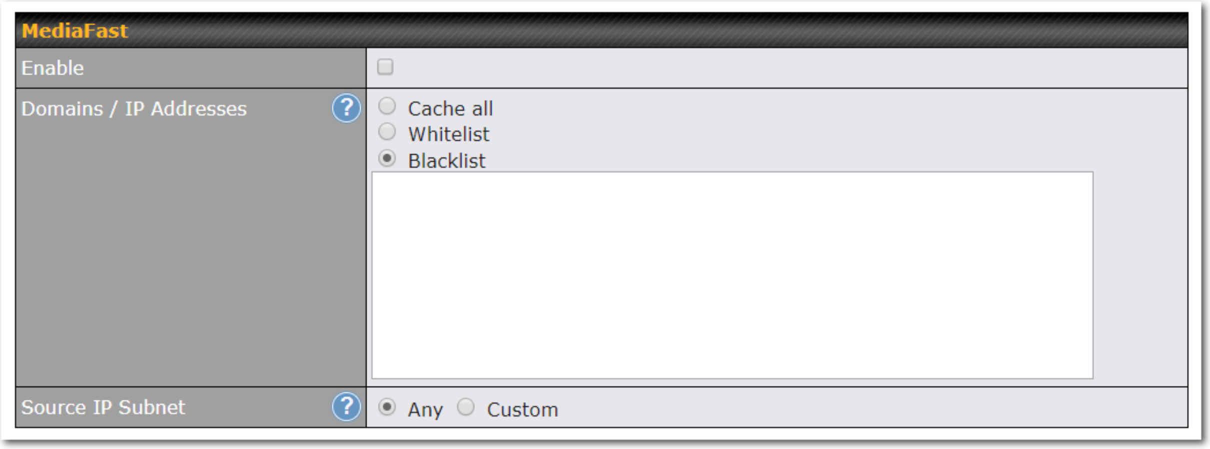
Wi-Fi WAN Settings	
Channel Width	Available options are **20/40 MHz** and **20 MHz**. Default is **20/40 MHz,** which allows both widths to be used simultaneously.
Bit Rate	This option allows you to select a specific bit rate for data transfer over the device's Wi-Fi network. By default, **Auto** is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

11 MediaFast Configuration

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

11.1 Setting Up MediaFast Content Caching

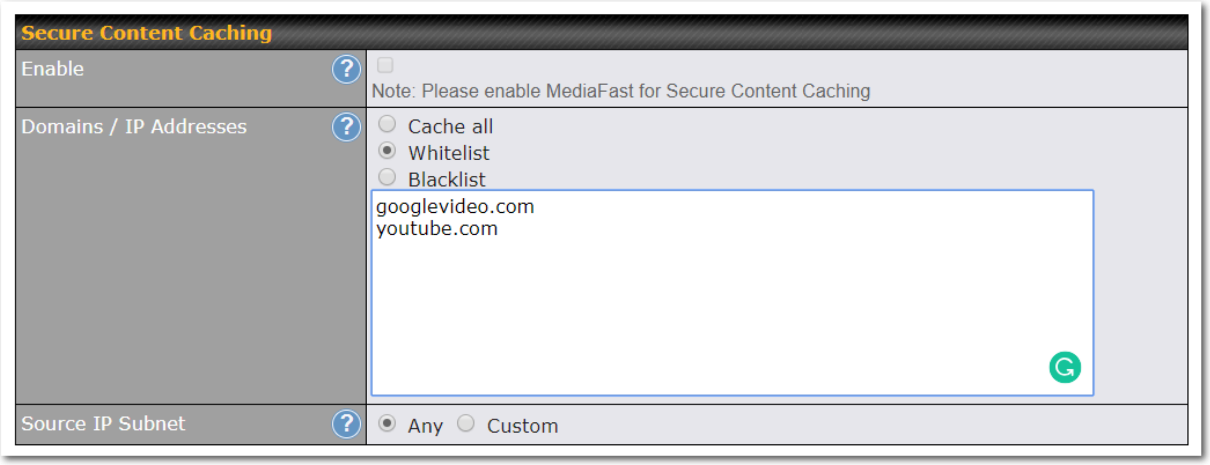
To access MediaFast content caching settings, select **Advanced>Cache Control**



MediaFast

Enable	☐
Domains / IP Addresses	○ Cache all ○ Whitelist ● Blacklist
Source IP Subnet	● Any ○ Custom

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

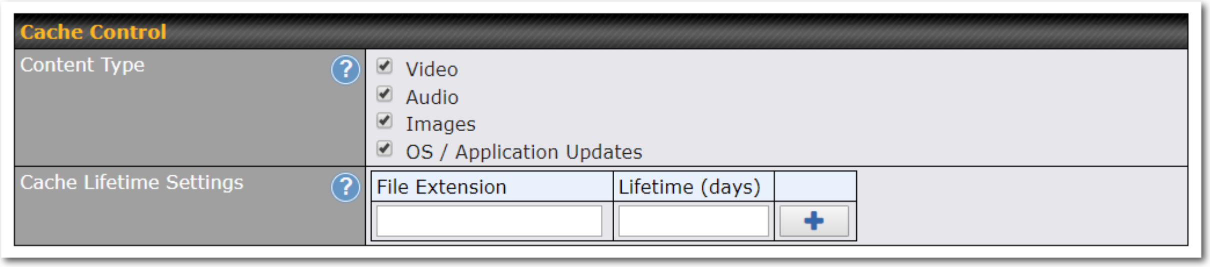


Secure Content Caching

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 cachting 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/



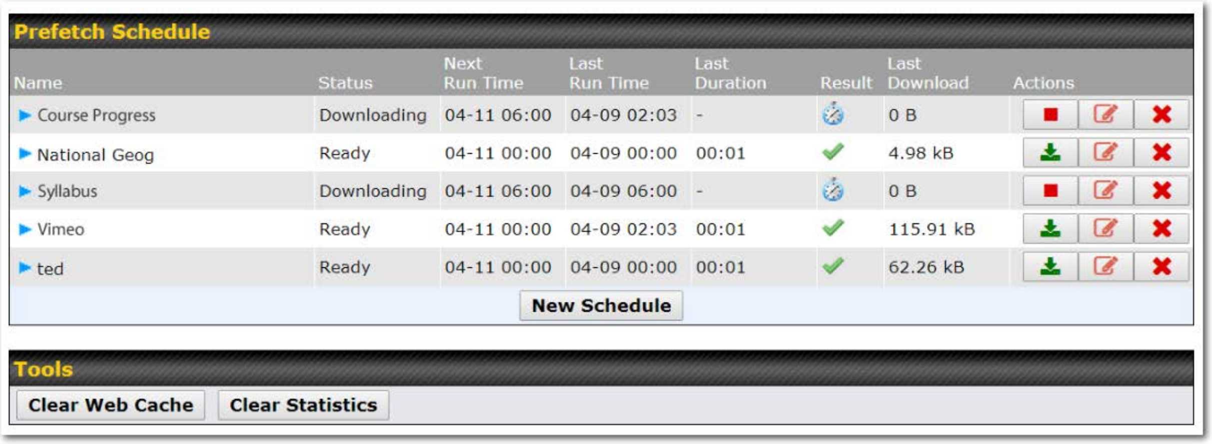
Cache Control

Content Type	☑ Video ☑ Audio ☑ Images ☑ OS / Application Updates
Cache Lifetime Settings	File Extension / Lifetime (days)

Cache Control	
Content Type	Check these boxes to cache the listed content types or leave boxes unchecked to disable caching for the listed types.
Cache Lifetime Settings	Enter a file extension, such as JPG or DOC. Then enter a lifetime in days to specify how long files with that extension will be cached. Add or delete entries using the controls on the right.

11.2 Scheduling Content Prefetching

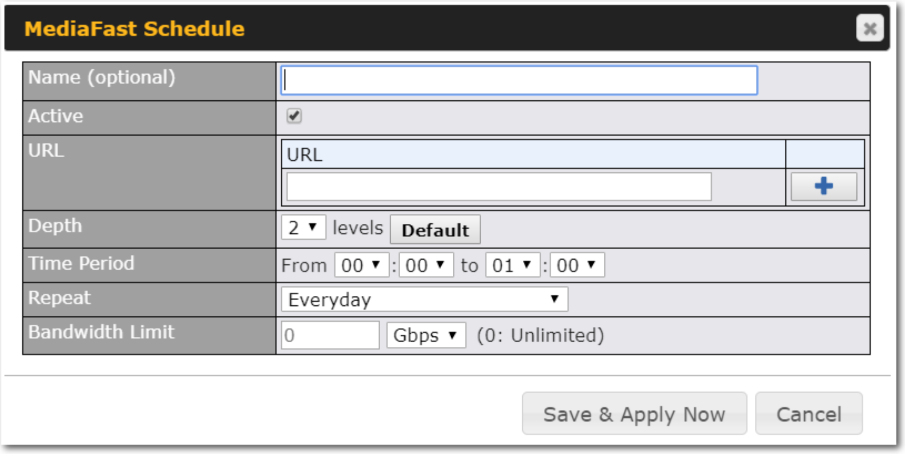
Content prefetching allows you to download content on a schedule that you define, which can help to preserve network bandwidth during busy times and keep costs down. To access MediaFast content prefetching settings, select **Advanced >Prefetch Schedule**.



Prefetch Schedule

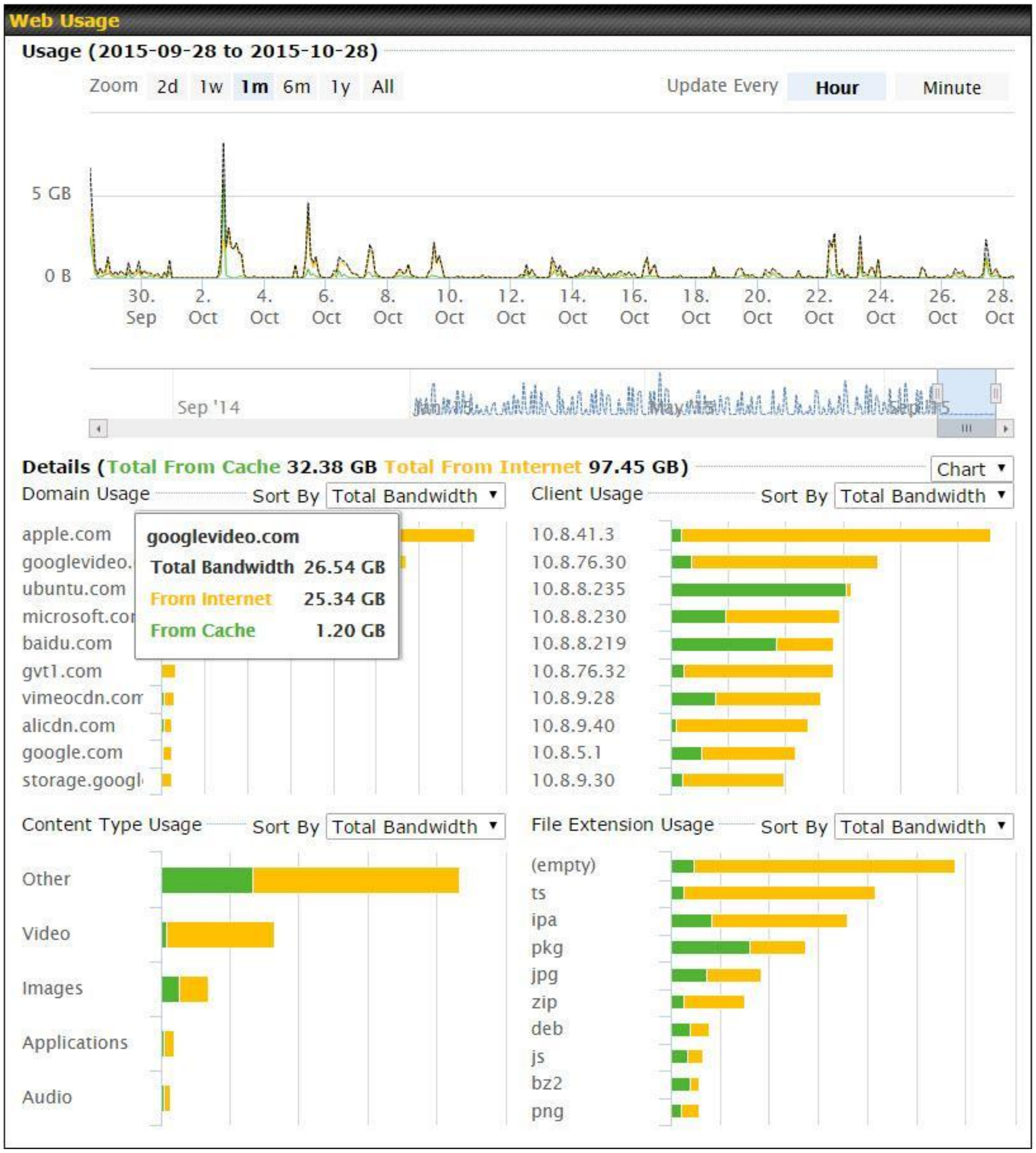
Name	Status	Next Run Time	Last Run Time	Last Duration	Result	Last Download	Actions
▶ Course Progress	Downloading	04-11 06:00	04-09 02:03	-	⏱	0 B	■ ✎ ✖
▶ National Geog	Ready	04-11 00:00	04-09 00:00	00:01	✓	4.98 kB	⬇ ✎ ✖
▶ Syllabus	Downloading	04-11 06:00	04-09 06:00	-	⏱	0 B	■ ✎ ✖
▶ Vimeo	Ready	04-11 00:00	04-09 02:03	00:01	✓	115.91 kB	⬇ ✎ ✖
▶ ted	Ready	04-11 00:00	04-09 00:00	00:01	✓	62.26 kB	⬇ ✎ ✖

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

	To delete a scheduled download, click ✖.
New Schedule	Click to begin creating a new scheduled download. Clicking the button will cause the following screen to appear: MediaFast Schedule Name (optional): Active: ☑ URL: URL 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.

11.3 Viewing MediaFast Statistics

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


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

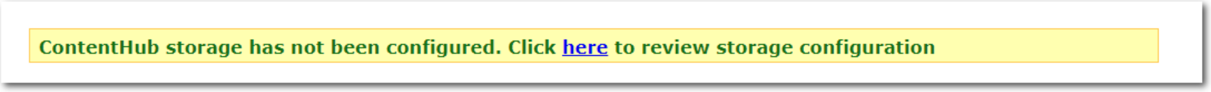
12 ContentHub

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.

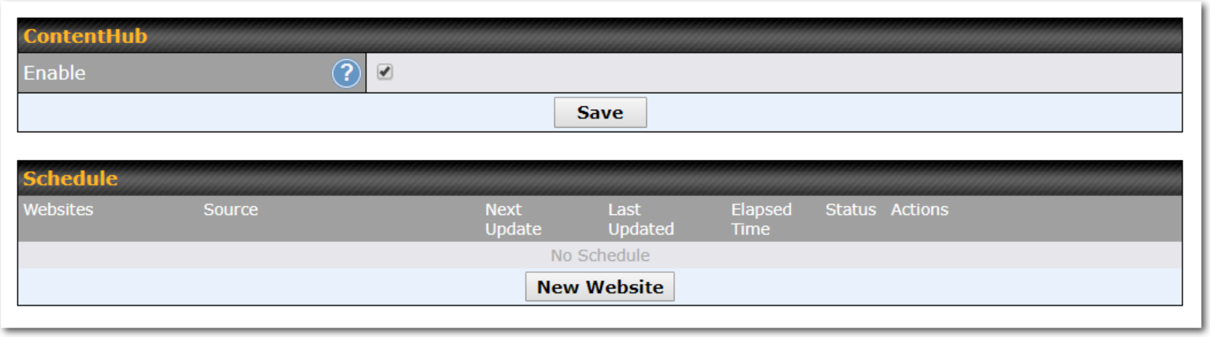
12.1 Configuring the ContentHub

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



ContentHub storage has not been configured. Click here to review storage configuration

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



ContentHub

Enable	☑

Schedule

Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions
No Schedule						

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

To configure a website or application as content, follow the steps below.

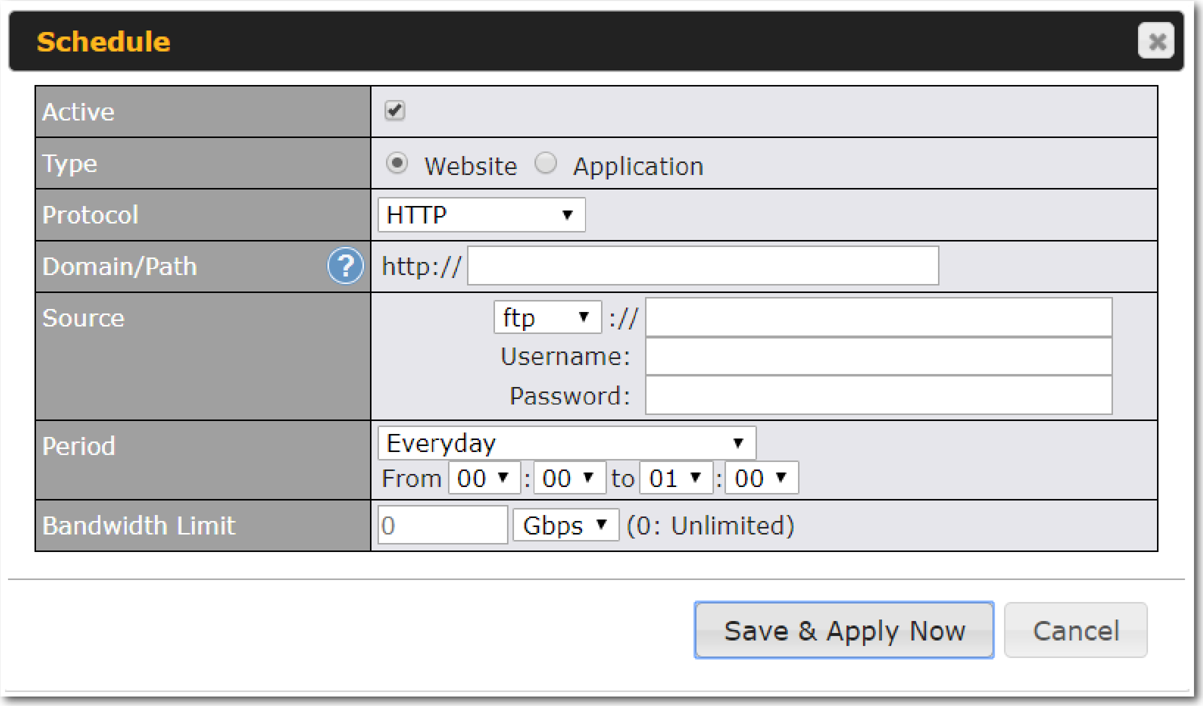
Configure a website for ContentHub

This option allows you to sync a website to the Pepwave 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 you sync it with ContentHub.

Click **New Website** and a window with the following configuration options will appear:

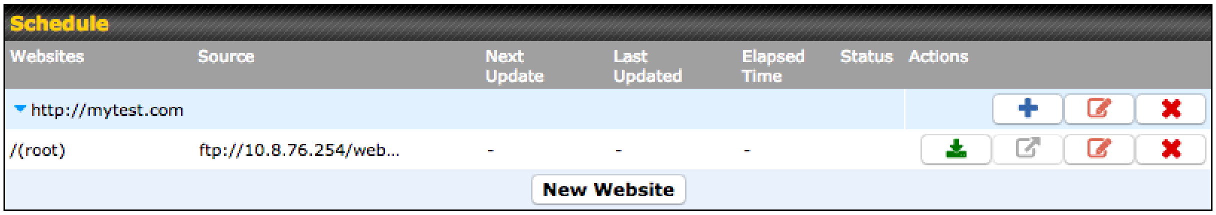


Schedule

Active	☑
Type	● Website ○ Application
Protocol	HTTP ▾
Domain/Path	http://
Source	ftp ▾ :// Username: Password:
Period	Everyday ▾ From 00 ▾ : 00 ▾ to 01 ▾ : 00 ▾
Bandwidth Limit	0 Gbps ▾ (0: Unlimited)

Schedule	
Active	Checking the box toggles the activation of the content.
Type	Select the type of content: Website or Application.
Protocol	Configure the protocol to be used: HTTP, HTTPS or both.
Domain/Path	Enter the URL for the ContenHub to use as the domain name for client access (such as http://mytest.com).
Method	Only applicable for **Application** type content. Choose between sync or file upload.
Source	Enter the details of the server that the content will be downloaded from. Enter credentials under **Username** and **Password**.
Period	This field determines how often the router will search for updates to the source content.
Bandwidth Limit	Set a bandwidth limit for clients.

Click “**Save & Apply Now**” to activate the changes. A screenshot of the display after configuration is shown below:

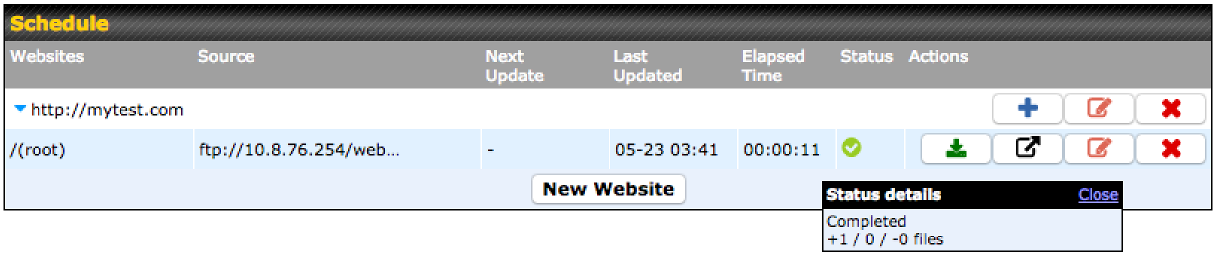


Schedule

Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions
▾ http://mytest.com						
/(root)	ftp://10.8.76.254/web...	-	-	-		

The content will be synced regularly according to the time set in the **Period** that was configured earlier.

If you want to activate the sync manually, you can click the “ ⬇ ” icon. The “Status” column will display the sync progress. When the sync is completed, a summary will be displayed, as shown in the screenshot below:



Schedule

Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions
▾ http://mytest.com						
/(root)	ftp://10.8.76.254/web...	-	05-23 03:41	00:00:11	✓	

Status details

Completed
+1 / 0 / -0 files

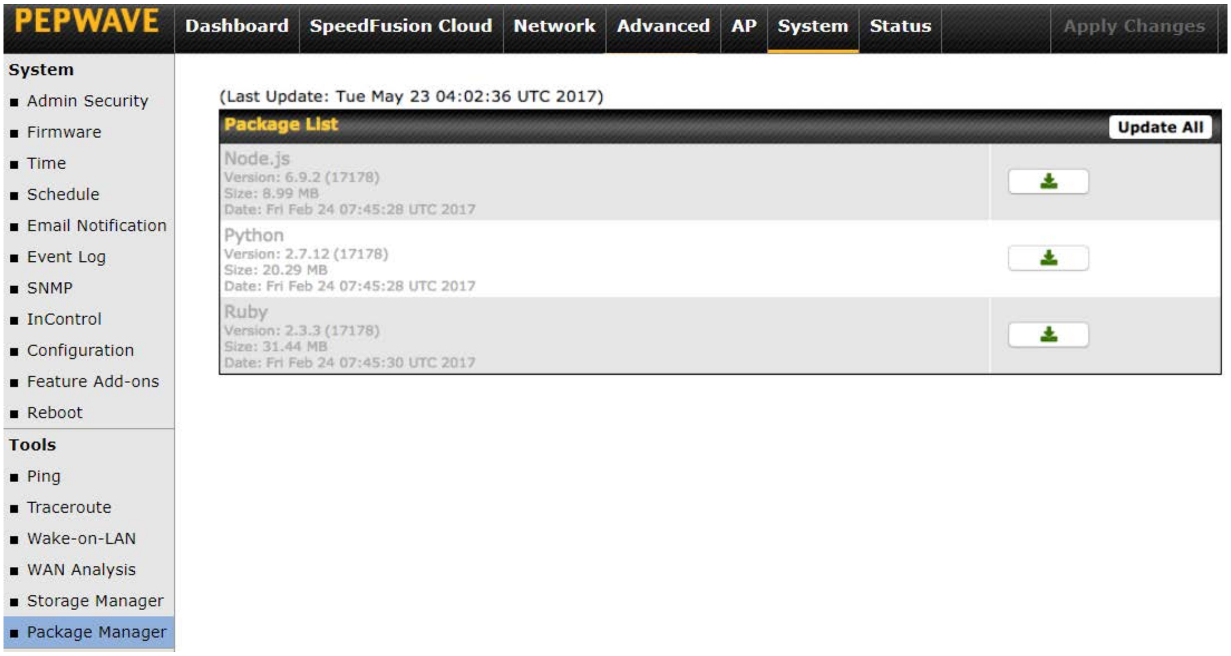
To access the content, open a browser in the MFA’s client and enter the domain details that were configured earlier (such as http://mytest.com).

Configure an application for ContentHub

MediaFast routers allow you to configure and publish any application from the router itself by using one of the supported frameworks below:

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

Install the desired framework under “Package Manager” as shown below:


PEPWAVE
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
Apply Changes
System
Admin Security
Firmware
Time
Schedule
Email Notification
Event Log
SNMP
InControl
Configuration
Feature Add-ons
Reboot
Tools
Ping
Traceroute
Wake-on-LAN
WAN Analysis
Storage Manager
Package Manager
Package List
Update All

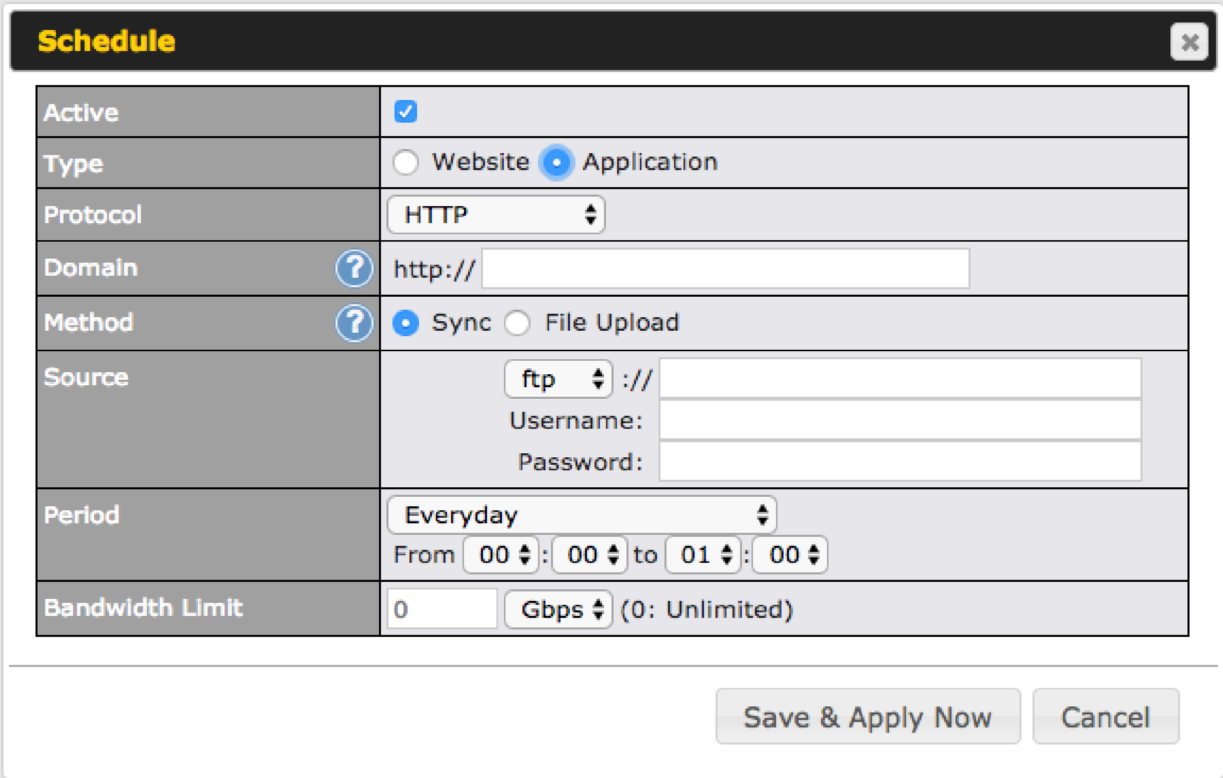
(Last Update: Tue May 23 04:02:36 UTC 2017)

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, change the ”Type” to “Application” and configure the website.



Schedule

Active	☑
Type	○ Website ● Application
Protocol	HTTP
Domain	http://
Method	● Sync ○ File Upload
Source	ftp :// Username: Password:
Period	Everyday From 00 : 00 to 01 : 00
Bandwidth Limit	0 Gbps (0: Unlimited)

The setting is the same as the Website type (refer to the description in the section above).

Application type content need to be packed as explained below:

1. Implement two bash script files, start.sh and stop.sh in the 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 the application files and the bash script to .tar.gz format.
3. Upload this tar file to the router.

13 Docker

MediaFast enabled routers can host Docker containers when running Firmware 7.1 or later.

Docker is an open platform for developing, shipping, and running applications.

From Firmware version 7.1.0 and upwards, it is possible to install and run Docker Containers on your Pepwave routers with MediaFast, such as the MAX HD2 and the MAX HD4.

Due to the nature of Docker and its unlimited variables, this feature is supported by Pepwave up to the point of creating a running Docker Container.

Information about Docker can be found on the Docker Documentation site:

https://docs.docker.com/ 2

This will allow you to run a file sharing platform (ownCloud), a web server (WordPress, Joomla!) , a learning platform (Moodle), or a visualisation tool for viewing large scale data (Kibana).

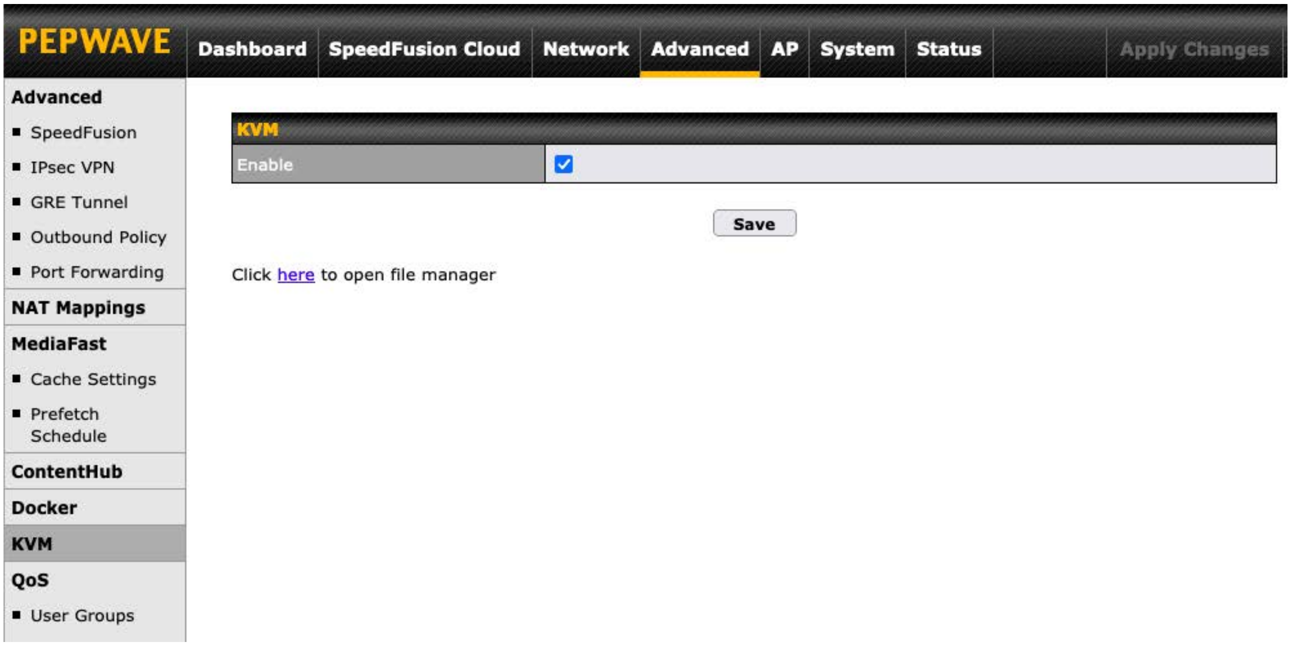
When creating a new Docker Container, the Pepwave router will search through the Docker Hub repository. https://hub.docker.com/explore/ 7

For detailed configuration instructions, refer to our knowledge base:

https://forum.peplink.com/t/how-to-run-a-docker-application-on-a-peplink-mediafast-router/16021

14 KVM

MediaFast enabled routers now support KVM. Users will have to download and install Virtual Machine Manager to manage the KVM virtual machines. Through this, users are able to virtualise a Linux environment.


PEPWAVE
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
Apply Changes
Advanced
SpeedFusion
IPsec VPN
GRE Tunnel
Outbound Policy
Port Forwarding
NAT Mappings
MediaFast
Cache Settings
Prefetch Schedule
ContentHub
Docker
KVM
QoS
User Groups
Save

KVM	
Enable	☑

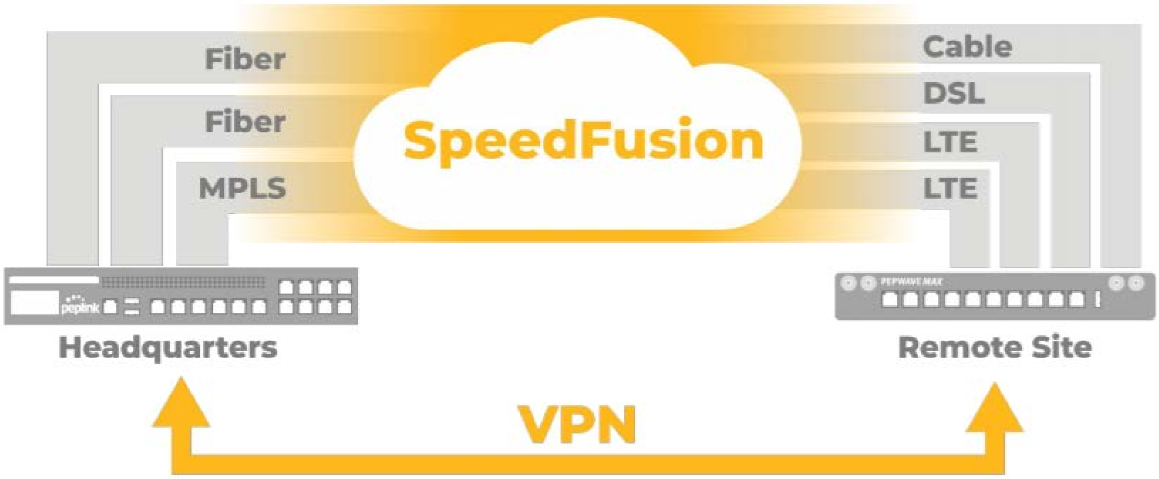
Click here to open file manager

For detailed configuration instructions, refer to our knowledge base articles:

1. [How to install a Virtual Machine on Peplink/Pepwave - MediaFast/ContentHub Routers]()

2. [How to Install Virtual Machine with USB storage on Peplink/Pepwave - MediaFast/ContentHub Routers]()

15 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.

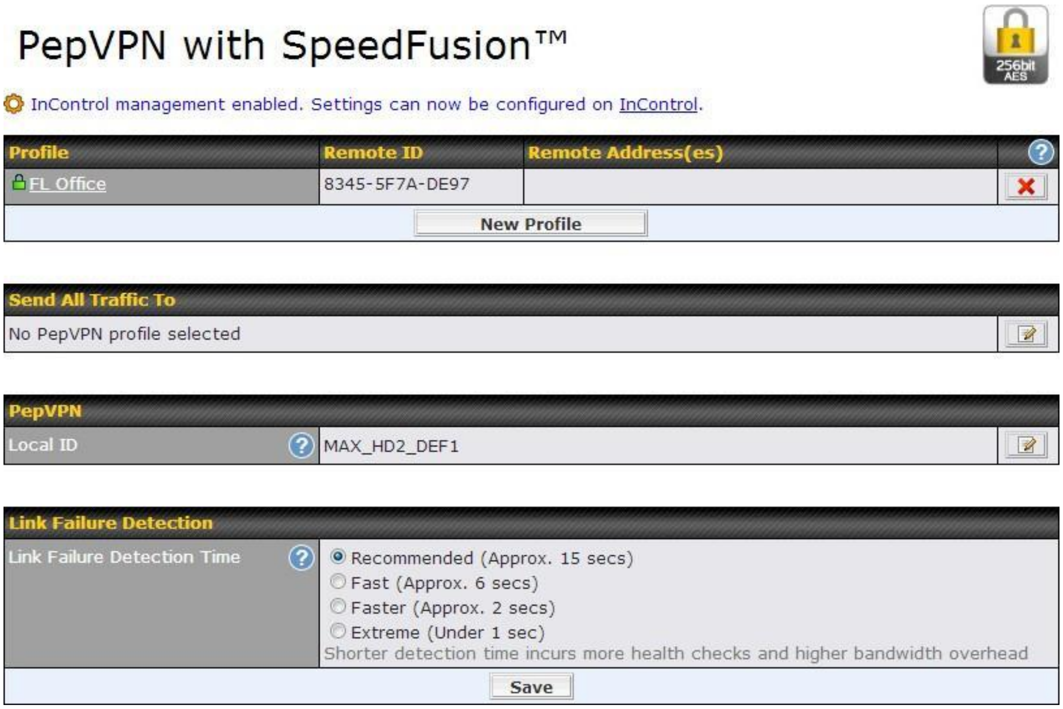
Pepwave routers can aggregate all WAN connections' bandwidth for routing SpeedFusion™ traffic. Unless all the WAN connections of one site are down, Pepwave routers can keep the VPN up and running.

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.

15.1 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	

Send All Traffic To

No PepVPN profile selected

PepVPN

Local ID	MAX_HD2_DEF1

Link Failure Detection

Link Failure Detection Time

● Recommended (Approx. 15 secs)
○ Fast (Approx. 6 secs)
○ Faster (Approx. 2 secs)
○ Extreme (Under 1 sec)

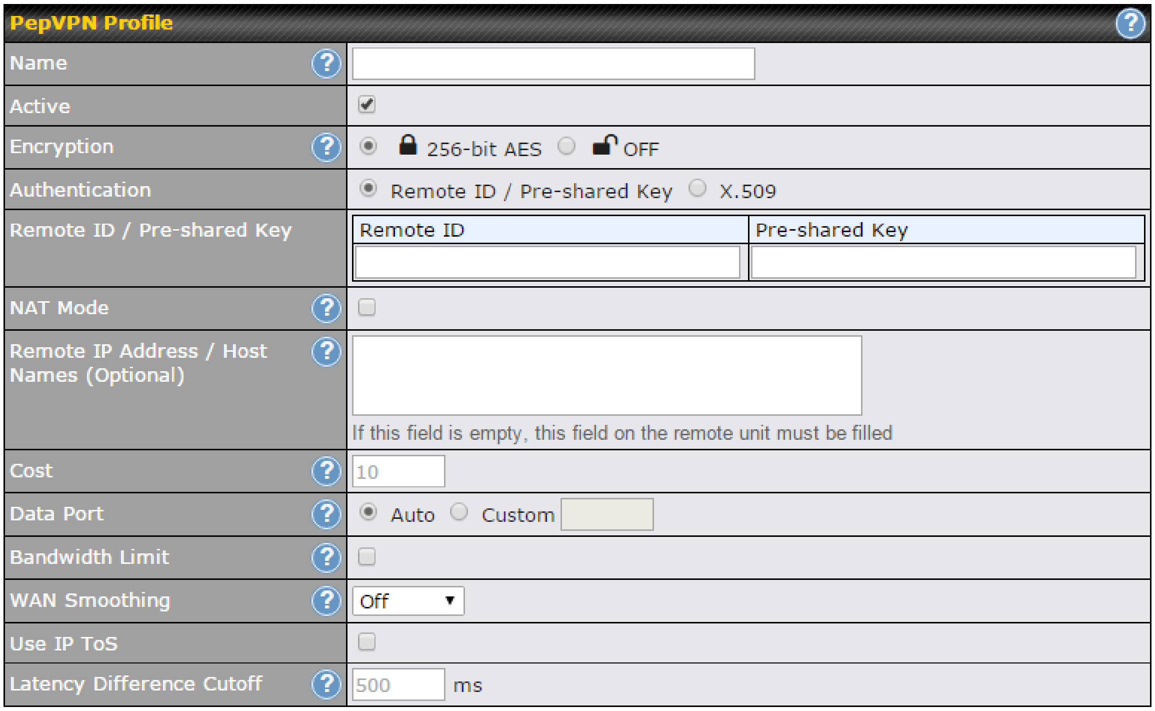
Shorter detection time incurs more health checks and higher bandwidth overhead

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 Pepwave or Peplink device via the available WAN connections. Each profile is for making a VPN connection with one remote Pepwave or Peplink Device.



PepVPN Profile

Name	
Active	☑
Encryption	● 256-bit AES ○ OFF
Authentication	● Remote ID / Pre-shared Key ○ X.509
Remote ID / Pre-shared Key	Remote ID Pre-shared Key
NAT Mode	☐
Remote IP Address / Host Names (Optional)	If this field is empty, this field on the remote unit must be filled
Cost	10
Data Port	● Auto ○ Custom
Bandwidth Limit	☐
WAN Smoothing	Off
Use IP ToS	☐
Latency Difference Cutoff	500 ms

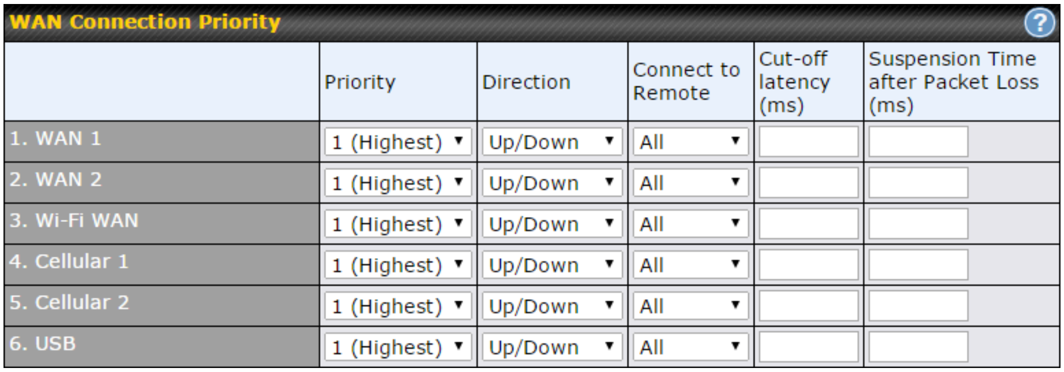
PepVPN Profile Settings	
Name	This field is for specifying a name to represent this profile. The name can be any combination of alphanumeric characters (0-9, A-Z, a-z), underscores (_), dashes (-), and/or non-leading/trailing spaces ( ).
Active	When this box is checked, this VPN connection profile will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

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

^{A} - Advanced feature, please click the ? button on the top right-hand corner to activate.

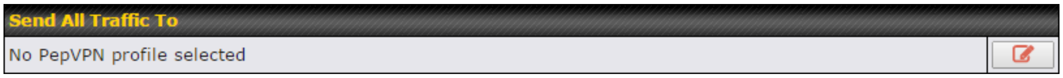
To enable Layer 2 Bridging between PepVPN profiles, navigate to **Network>LAN>Basic Settings>*LAN Profile Name*** and refer to instructions in section 9.1



WAN Connection Priority ?

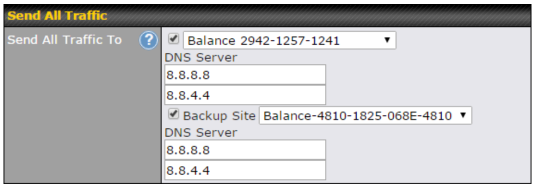
	Priority	Direction	Connect to Remote	Cut-off latency (ms)	Suspension Time after Packet Loss (ms)
1. WAN 1	1 (Highest) ▾	Up/Down ▾	All ▾		
2. WAN 2	1 (Highest) ▾	Up/Down ▾	All ▾		
3. Wi-Fi WAN	1 (Highest) ▾	Up/Down ▾	All ▾		
4. Cellular 1	1 (Highest) ▾	Up/Down ▾	All ▾		
5. Cellular 2	1 (Highest) ▾	Up/Down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

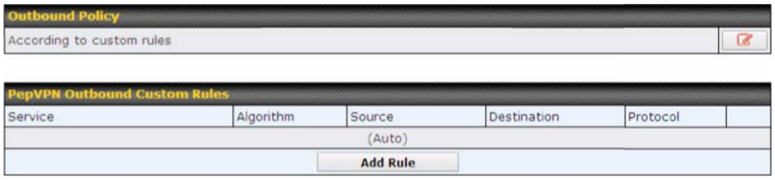
8.8.8.8

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.

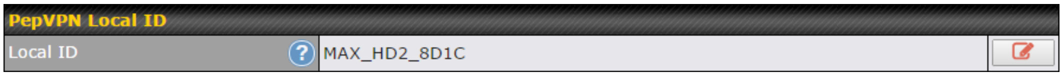


Outbound Policy

According to custom rules

PepVPN Outbound Custom Rules

Service	Algorithm	Source	Destination	Protocol
(Auto)				

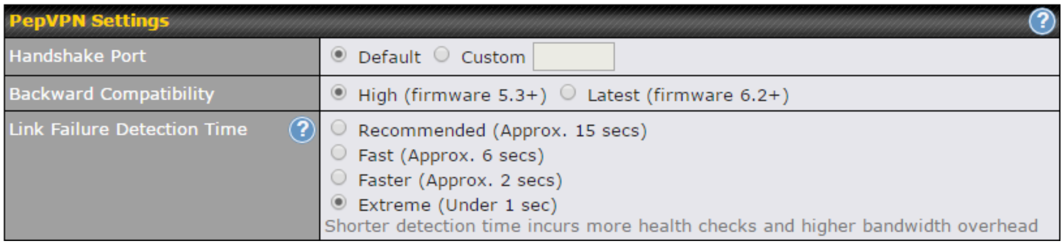


PepVPN Local ID

Local ID: MAX_HD2_8D1C

PepVPN Local ID

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



PepVPN Settings

Handshake Port: ● Default ○ Custom

Backward Compatibility: ● High (firmware 5.3+) ○ Latest (firmware 6.2+)

Link Failure Detection Time:
○ Recommended (Approx. 15 secs)
○ Fast (Approx. 6 secs)
○ Faster (Approx. 2 secs)
● Extreme (Under 1 sec)
Shorter detection time incurs more health checks and higher bandwidth overhead

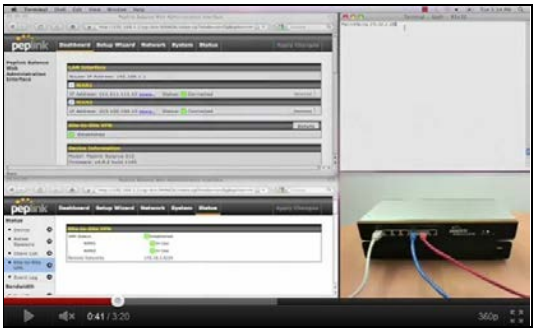
PepVPN Settings

Handshake Port^{A}	To designate a custom handshake port (TCP), click the **custom** radio button and enter the port number you wish to designate.
Backward Compatibility	Determine the level of backward compatibility needed for PepVPN tunnels. The use of the **Latest** setting is recommended as it will improve the performance and resilience of SpeedFusion connections.
Link Failure Detection Time	The bonded VPN can detect routing failures on the path between two sites over each WAN connection. Failed WAN connections will not be used to route VPN traffic. Health check packets are sent to the remote unit to detect any failure. The more frequently checks are sent, the shorter the detection time, although more

	bandwidth will be consumed. When **Recommended** (default) is selected, a health check packet is sent every five seconds, and the expected detection time is 15 seconds. When **Fast** is selected, a health check packet is sent every three seconds, and the expected detection time is six seconds. When **Faster** is selected, a health check packet is sent every second, and the expected detection time is two seconds. When **Extreme** is selected, a health check packet is sent every 0.1 second, and the expected detection time is less than one second.

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

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

Tip
Want to know more about VPN sub-second session failover? Visit our YouTube Channel for a video tutorial!  http://youtu.be/TLQgdpPSY88

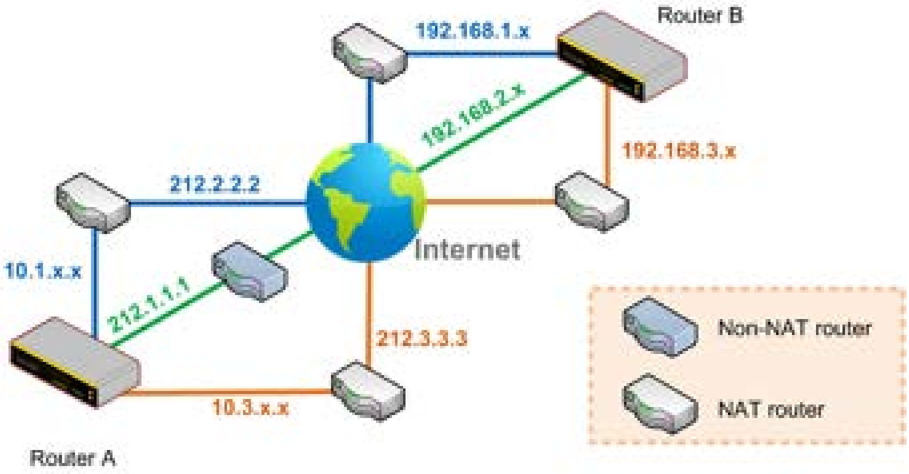
15.2 The Pepwave Router Behind a NAT Router

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.

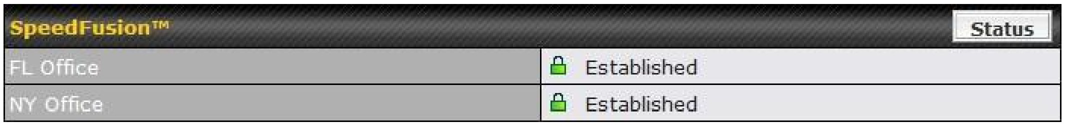
See the following diagram for an example of this setup in use:



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.

15.3 SpeedFusion™ Status

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



SpeedFusion™	Status
FL Office	🔒 Established
NY Office	🔒 Established

After clicking the **Status** button at the top right corner of the SpeedFusion^{TM} table, you will be forwarded to **Status>SpeedFusion^{TM}**, 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^{TM} network is a single non-NAT IP network. Avoid duplicating subnets in your sites to prevent connectivity problems when accessing those subnets.

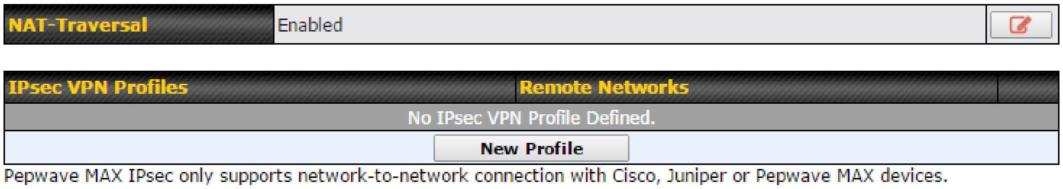
16 IPsec VPN

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.

16.1 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.**

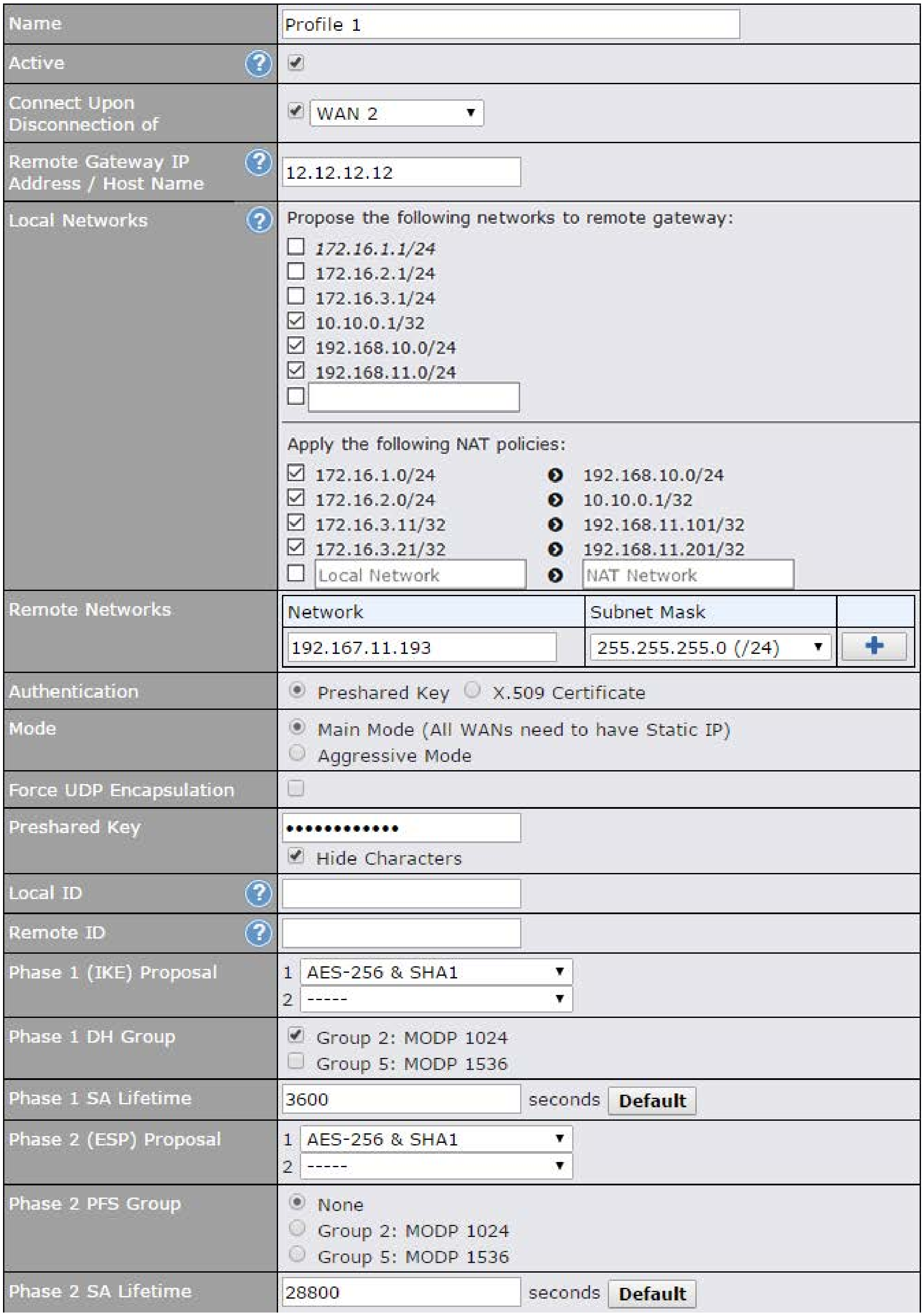


NAT-Traversal	Enabled

IPsec VPN Profiles	Remote Networks
No IPsec VPN Profile Defined.	

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

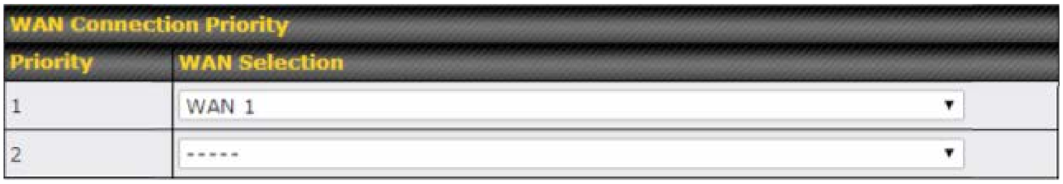
A **NAT-Traversal** option and list of defined **IPsec VPN** profiles will be shown. **NAT-Traversal** should be enabled if your system is behind a NAT router. Click the **New Profile** button to create new IPsec VPN profiles that make VPN connections to remote Pepwave, Cisco, or Juniper routers via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



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

IPsec VPN Settings	
Name	This field is for specifying a local name to represent this connection profile.
Active	When this box is checked, this IPsec VPN connection profile will be enabled. Otherwise, it will be disabled.
Connect Upon Disconnection of	Check this box and select a WAN to connect to this VPN automatically when the specified WAN is disconnected.
Remote Gateway IP Address / Host Name	Enter the remote peer's public IP address. For **Aggressive Mode**, this is optional.
Local Networks	Enter the local LAN subnets here. If you have defined static routes, they will be shown here. Using NAT, you can map a specific local network / IP address to another, and the packets received by remote gateway will appear to be coming from the mapped network / IP address. This allow you to establish IPsec connection to a remote site that has one or more subnets overlapped with local site. Two types of NAT policies can be defined: One-to-One NAT policy: if the defined subnet in Local Network and NAT Network has the same size, for example, policy "192.168.50.0/24 > 172.16.1.0/24" will translate the local IP address 192.168.50.10 to 172.16.1.10 and 192.168.50.20 to 172.16.1.20. This is a bidirectional mapping which means clients in remote site can initiate connection to the local clients using the mapped address too. Many-to-One NAT policy: if the defined NAT Network on the right hand side is an IP address (or having a network prefix /32), for example, policy "192.168.1.0/24 > 172.168.50.1/32" will translate all clients in 192.168.1.0/24 network to 172.168.50.1. This is a unidirectional mapping which means clients in remote site will not be able to initiate connection to the local clients.
Remote Networks	Enter the LAN and subnets that are located at the remote site here.
Authentication	To access your VPN, clients will need to authenticate by your choice of methods. Choose between the **Preshared Key** and **X.509 Certificate** methods of authentication.
Mode	Choose **Main Mode** if both IPsec peers use static IP addresses. Choose **Aggressive Mode** if one of the IPsec peers uses dynamic IP addresses.

Force UDP Encapsulation	For forced UDP encapsulation regardless of NAT-traversal, tick this checkbox.
Pre-shared Key	This defines the peer authentication pre-shared key used to authenticate this VPN connection. The connection will be up only if the pre-shared keys on each side match.
Remote Certificate (pem encoded)	Available only when **X.509 Certificat**e is chosen as the **Authentication** method, this field allows you to paste a valid X.509 certificate.
Local ID	In **Main Mode**, this field can be left blank. In **Aggressive Mode**, if **Remote Gateway IP Address** is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.
Remote ID	In **Main Mode**, this field can be left blank. In **Aggressive Mode**, if **Remote Gateway IP Address** is filled on this end and the peer end, this field can be left blank. Otherwise, this field is typically a U-FQDN.
Phase 1 (IKE) Proposal	In **Main Mode**, this allows setting up to six encryption standards, in descending order of priority, to be used in initial connection key negotiations. In **Aggressive Mode**, only one selection is permitted.
Phase 1 DH Group	This is the Diffie-Hellman group used within IKE. This allows two parties to establish a shared secret over an insecure communications channel. The larger the group number, the higher the security. **Group 2**: **1024-bit** is the default value. **Group 5**: **1536-bit** is the alternative option.
Phase 1 SA Lifetime	This setting specifies the lifetime limit of this Phase 1 Security Association. By default, it is set at **3600** seconds.
Phase 2 (ESP) Proposal	In **Main Mode**, this allows setting up to six encryption standards, in descending order of priority, to be used for the IP data that is being transferred. In **Aggressive Mode**, only one selection is permitted.
Phase 2 PFS Group	Perfect forward secrecy (PFS) ensures that if a key was compromised, the attacker will be able to access only the data protected by that key. **None** - Do not request for PFS when initiating connection. However, since there is no valid reason to refuse PFS, the system will allow the connection to use PFS if requested by the remote peer. This is the default value. **Group 2**: 1024-bit Diffie-Hellman group. The larger the group number, the higher the security. **Group 5**: **1536-bit** is the third option.
Phase 2 SA Lifetime	This setting specifies the lifetime limit of this Phase 2 Security Association. By default, it is set at **28800** seconds.



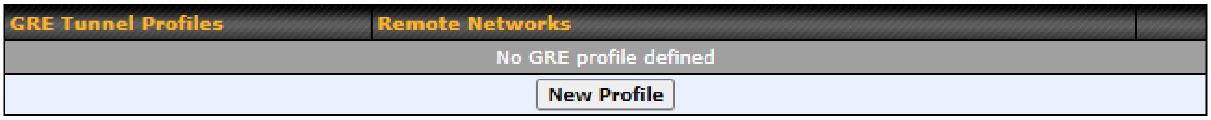
Priority	WAN Selection
1	WAN 1
2	-----

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

16.2 GRE Tunnel

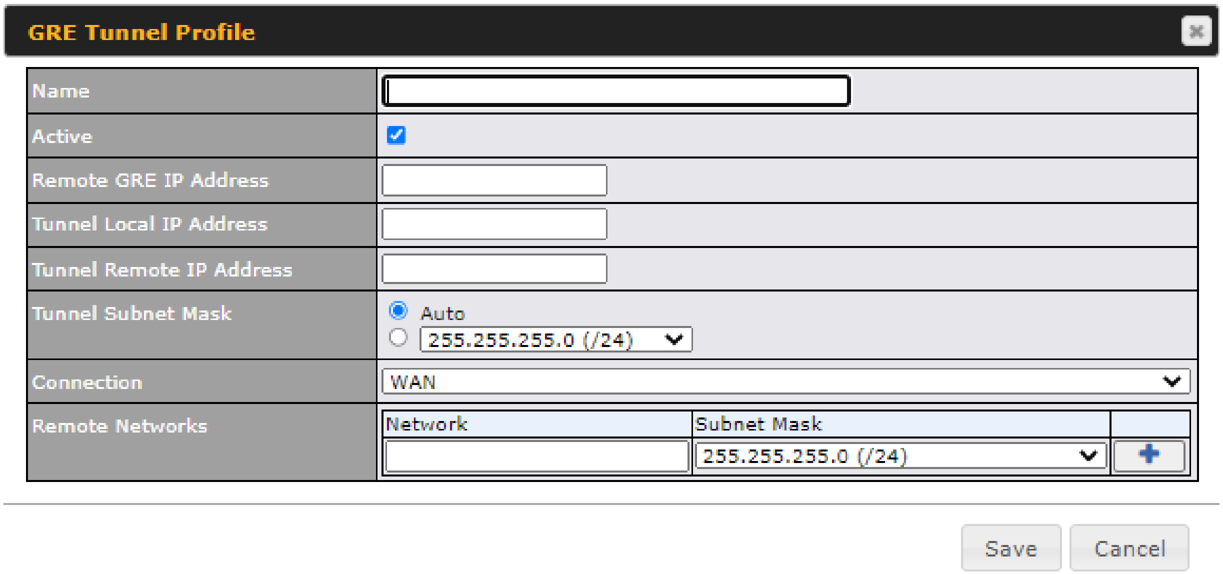
Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. A GRE tunnel is similar to IPSec or PepVPN.

To configure a GRE Tunnel, navigate to **Advanced > GRE Tunnel**.



GRE Tunnel Profiles	Remote Networks	
No GRE profile defined		

Click the **New Profile** button to create new GRE tunnel profiles that establish tunnel connections to remote tunnel endpoints via available WAN connections. To edit the profiles, click on its associated connection name in the leftmost column.



GRE Tunnel Profile

Name	
Active	☑
Remote GRE IP Address	
Tunnel Local IP Address	
Tunnel Remote IP Address	
Tunnel Subnet Mask	● Auto ○ 255.255.255.0 (/24)
Connection	WAN
Remote Networks	Network: (empty); Subnet Mask: 255.255.255.0 (/24)

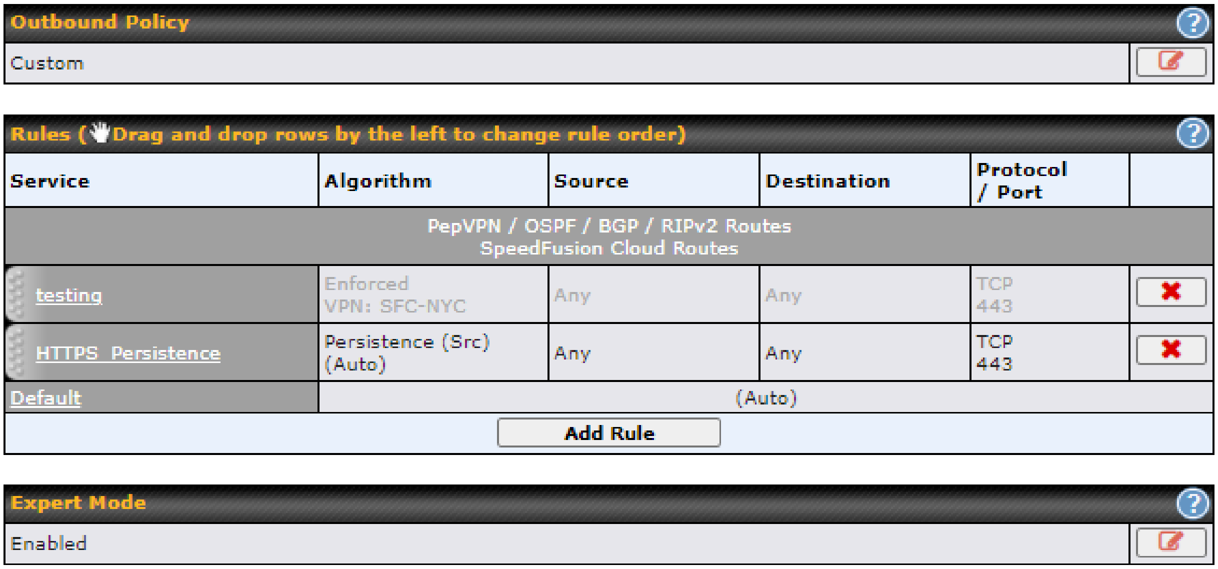
GRE Tunnel Profile Settings	
Name	This field is for specifying a name to represent this GRE Tunnel connection profile.
Active	When this box is checked, this GRE Tunnel connection profile will be enabled. Otherwise, it will be disabled.
Remote GRE IP Address	This field is for entering the remote GRE's IP address
Tunnel Local IP Address	This field is for specifying the tunnel source IP address.
Tunnel Remote IP Address	This field is for specifying the tunnel destination IP address
Tunnel Subnet Mask	This field is to select the subnet mask that is to be used for the GRE tunnel.
Connection	Select the appropriate WAN connection from the drop-down menu.
Remote Networks	Input the LAN and subnets that are located at the remote site here.

17 Outbound Policy

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 by the left to change rule order)

Service	Algorithm	Source	Destination	Protocol / Port	
PepVPN / OSPF / BGP / RIPv2 Routes SpeedFusion Cloud Routes					
testing	Enforced VPN: SFC-NYC	Any	Any	TCP 443	✖
HTTPS_Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	✖
Default	(Auto)				

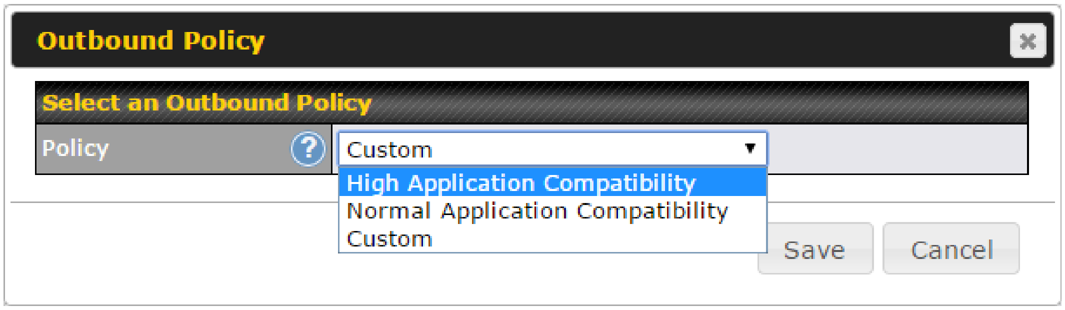
Expert Mode

Enabled

17.1 Outbound Policy

Outbound policies for managing and load balancing outbound traffic are located at

Advanced>Outbound Policy> or **Advanced>PepVPN>Outbound Policy.** Click the button beside the **Outbound Policy** box:



Outbound Policy
Select an Outbound Policy
High Application Compatibility
Normal Application Compatibility
Custom
Save
Cancel

Policy: Custom

There are three main selections for the outbound traffic policy:

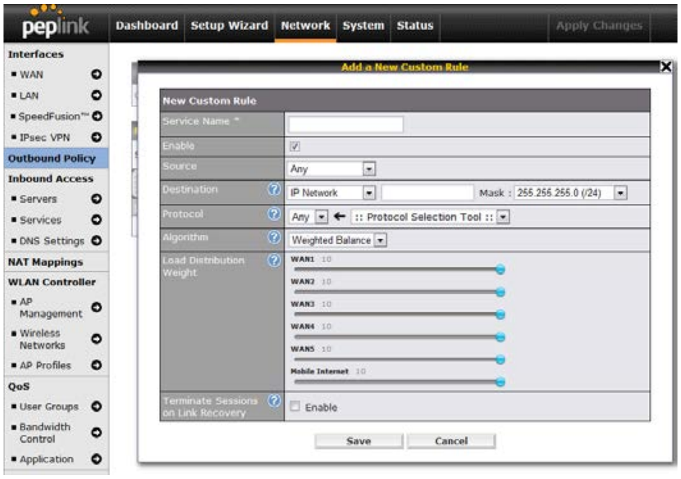
- High Application Compatibility
- Normal Application Compatibility
- Custom

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

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

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

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


peplink
Dashboard
Setup Wizard
Network
System
Status
Apply Changes
Interfaces
WAN
LAN
SpeedFusion™
IPsec VPN
Outbound Policy
Inbound Access
Servers
Services
DNS Settings
NAT Mappings
WLAN Controller
AP Management
Wireless Networks
AP Profiles
QoS
User Groups
Bandwidth Control
Application
Save
Cancel

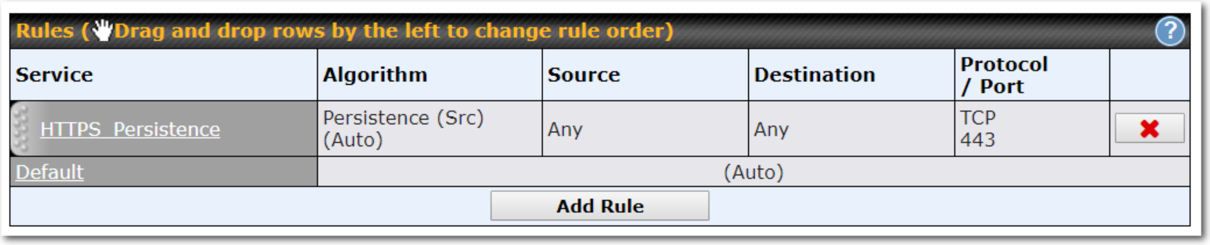
Add a New Custom Rule

New Custom Rule	
Service Name *	
Enable	☑
Source	Any
Destination	IP Network; Mask : 255.255.255.0 (/24)
Protocol	Any ← :: Protocol Selection Tool ::
Algorithm	Weighted Balance
Load Distribution Weight	WAN1 10 WAN2 10 WAN3 10 WAN4 10 WAN5 10 Mobile Internet 10
Terminate Sessions on Link Recovery	☐ Enable

http://youtu.be/rKH4AS_bQnE

17.2 Adding Rules for Outbound Policy

The menu underneath enables you to define Outbound policy rules:

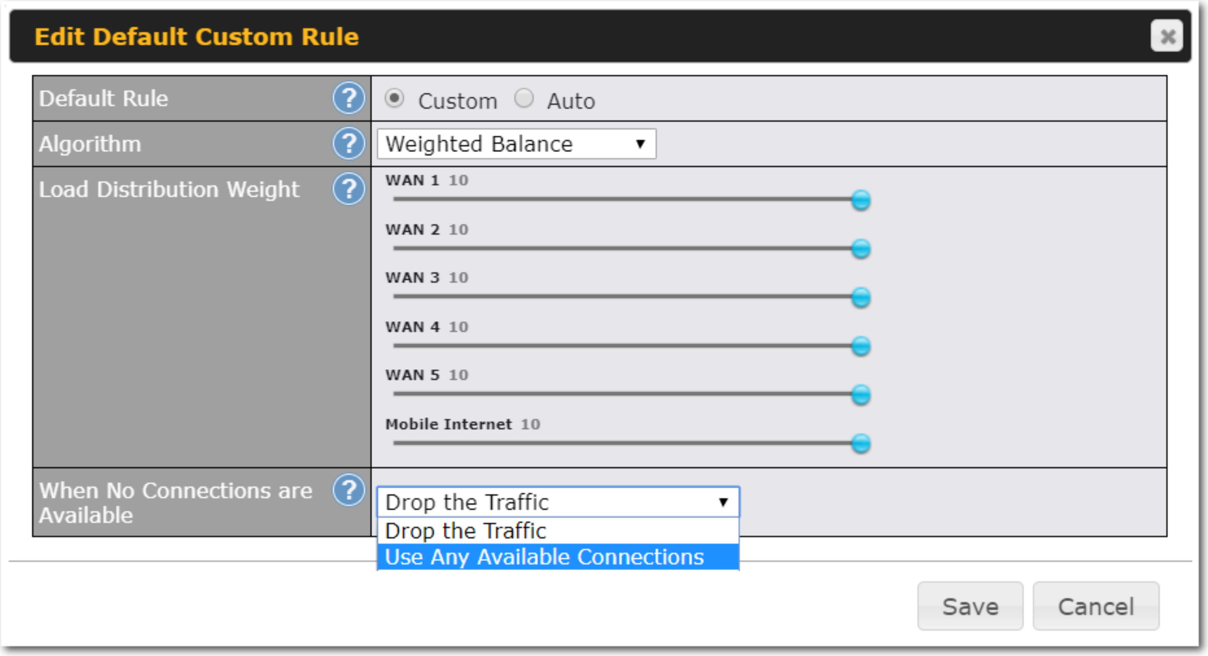


Rules (Drag and drop rows by the left to change rule order)

Service	Algorithm	Source	Destination	Protocol / Port	
HTTPS_Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	✖
Default	(Auto)				
	Add Rule				

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

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

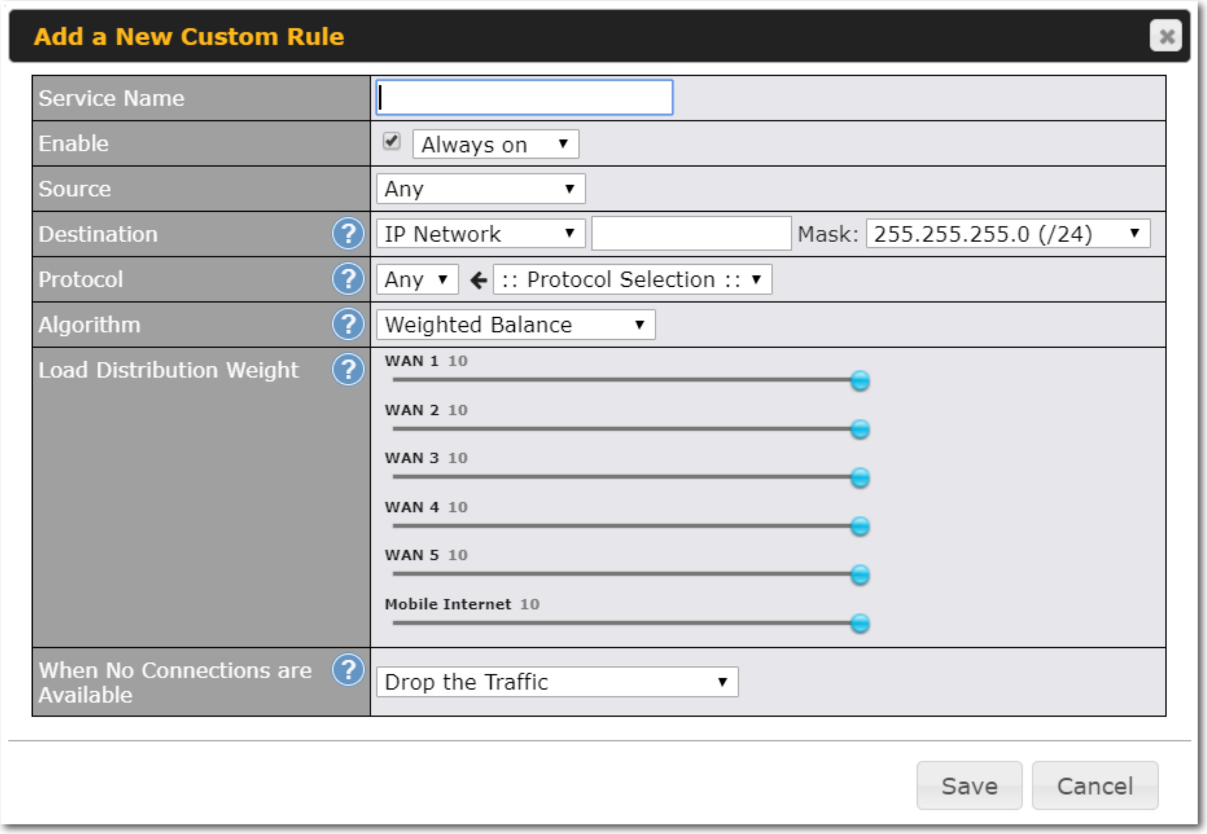


Edit Default Custom Rule

Default Rule	● Custom ○ Auto
Algorithm	Weighted Balance ▾
Load Distribution Weight	WAN 1 10 WAN 2 10 WAN 3 10 WAN 4 10 WAN 5 10 Mobile Internet 10
When No Connections are Available	Drop the Traffic ▾ Drop the Traffic Use Any Available Connections

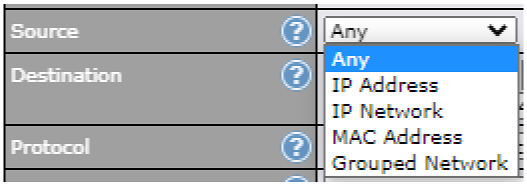
By default, **Auto** is selected as the **Default Rule**. You can select **Custom** to change the algorithm to be used. Please refer to the upcoming sections for the details on the available algorithms.

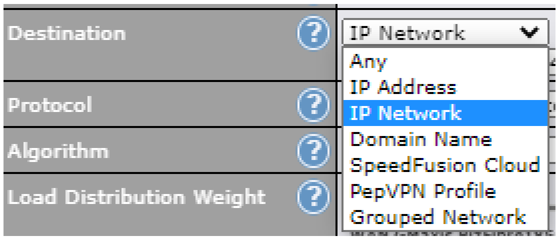
To create a custom rule, click **Add Rule** at the bottom of the table.



Add a New Custom Rule

Service Name	
Enable	☑ Always on
Source	Any
Destination	IP Network Mask: 255.255.255.0 (/24)
Protocol	Any ← :: Protocol Selection ::
Algorithm	Weighted Balance
Load Distribution Weight	WAN 1 10 WAN 2 10 WAN 3 10 WAN 4 10 WAN 5 10 Mobile Internet 10
When No Connections are Available	Drop the Traffic

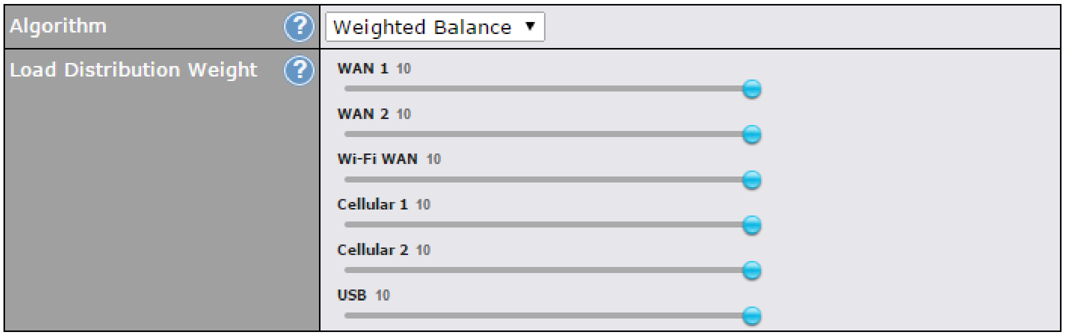
New Custom Rule Settings	
Service Name	This setting specifies the name of the outbound traffic rule.
Enable	This setting specifies whether the outbound traffic rule takes effect. When **Enable** is checked, the rule takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When **Enable** is unchecked, the rule does not take effect: the Pepwave router disregards the other parameters of the rule. Click the drop-down menu next to the checkbox to apply a time schedule to this custom rule.
Source	This setting specifies the source IP Address, IP Network, MAC Address or Grouped Network for traffic that matches the rule.  Source: Any Any IP Address IP Network MAC Address Grouped Network Destination Protocol
Destination	This setting specifies the destination IP address, IP network, Domain name, SpeedFusion Cloud, PepVPN Profile or Grouped network for traffic that matches the rule.

	 Destination Protocol Algorithm Load Distribution Weight IP Network Any IP Address IP Network Domain Name SpeedFusion Cloud PepVPN Profile Grouped Network If **Domain Name** is chosen and a domain name, such as *foobar.com*, is entered, any outgoing accesses to *foobar.com* and **.foobar.com* will match this criterion. You may enter a wildcard (.*) at the end of a domain name to match any host with a name having the domain name in the middle. If you enter *foobar.*,* for example, *www.foobar.com*, *www.foobar.co.jp*, or *foobar.co.uk* will also match. Placing wildcards in any other position is not supported. Note: if a server has one Internet IP address and multiple server names, and if one of the names is defined here, access to any one of the server names will also match this rule.
Protocol and Port	This setting specifies the IP protocol and port of traffic that matches this rule. Via a drop-down menu, the following protocols can be specified: ● Any ● TCP ● UDP ● IP ● DSCP Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.) After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remains manually modifiable.
Algorithm	This setting specifies the behavior of the Pepwave router for the custom rule. One of the following values can be selected (Note that some Pepwave routers provide only some of these options): ● Weighted Balance ● Persistence ● Enforced ● Priority ● Overflow ● Least Used ● Lowest Latency ● Fastest Response Time For a full explanation of each Algorithm, please see the following article: https://forum.peplink.com/t/exactly-how-do-peplinks-load-balancing-algorithmns-work/8059
Load Distribution Weight	This is to define the outbound traffic weight ratio for each WAN connection.

When No connections are available	This field allows you to configure the default action when all the selected Connections are not available. **Drop the Traffic** - Traffic will be discarded. **Use Any Available Connections** - Traffic will be routed to any available Connection, even it is not selected in the list. **Fall-through to Next Rule** - Traffic will continue to match the next Outbound Policy rule just like this rule is inactive.
Terminate Sessions on Connection Recovery	This setting specifies whether to terminate existing IP sessions on a less preferred WAN connection in the event that a more preferred WAN connection is recovered. This setting is applicable to the **Priority** algorithms. By default, this setting is disabled. In this case, existing IP sessions will not be terminated or affected when any other WAN connection is recovered. When this setting is enabled, existing IP sessions may be terminated when another WAN connection is recovered, such that only the preferred healthy WAN connection(s) is used at any point in time.

17.2.1 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:
WAN 1 10
WAN 2 10
Wi-Fi WAN 10
Cellular 1 10
Cellular 2 10
USB 10

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

For example, with the following weight settings:

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

- USB: 10

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

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

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

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

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

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

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

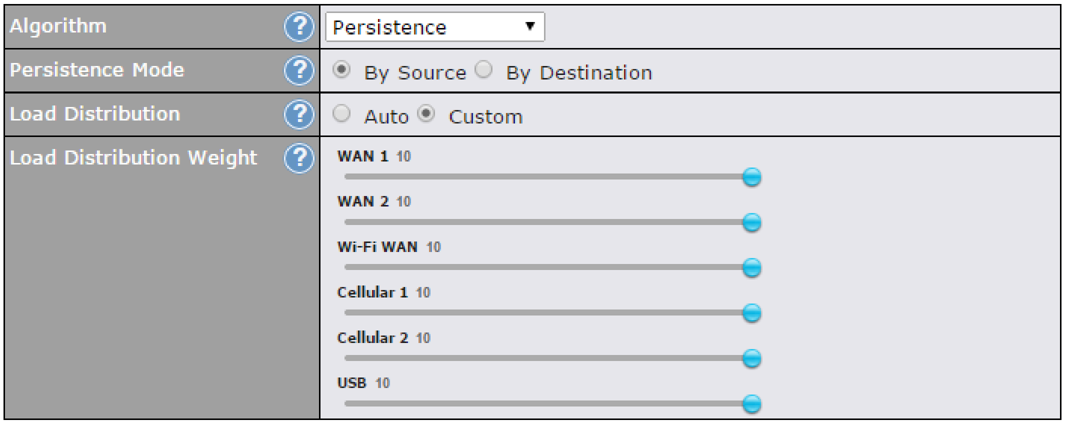
17.2.2 Algorithm: Persistence

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	● By Source ○ By Destination
Load Distribution	○ Auto ● Custom
Load Distribution Weight	WAN 1 10 WAN 2 10 Wi-Fi WAN 10 Cellular 1 10 Cellular 2 10 USB 10

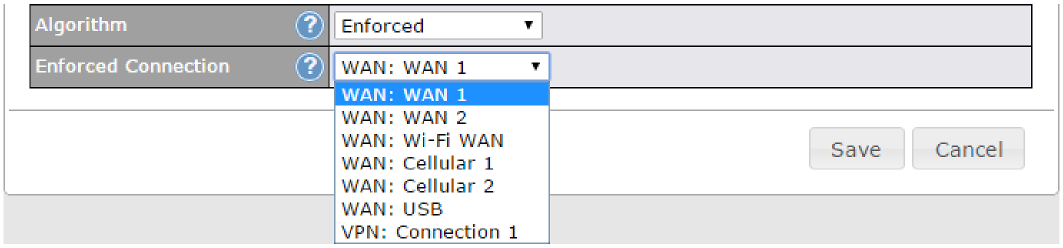
There are two persistent modes: **By Source** and **By Destination**.

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

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

17.2.3 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**.



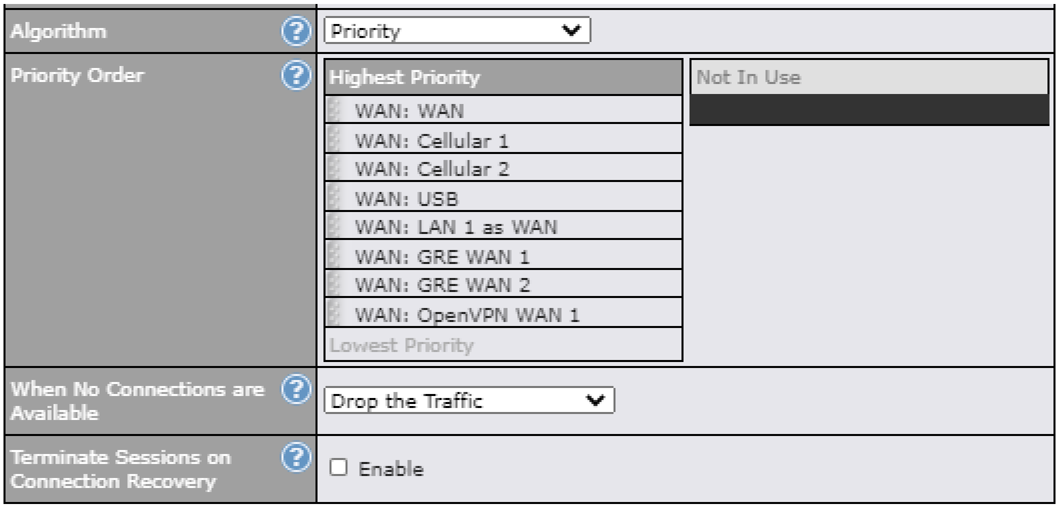
Algorithm: Enforced

Enforced Connection: WAN: WAN 1

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^{TM} connection.

17.2.4 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.



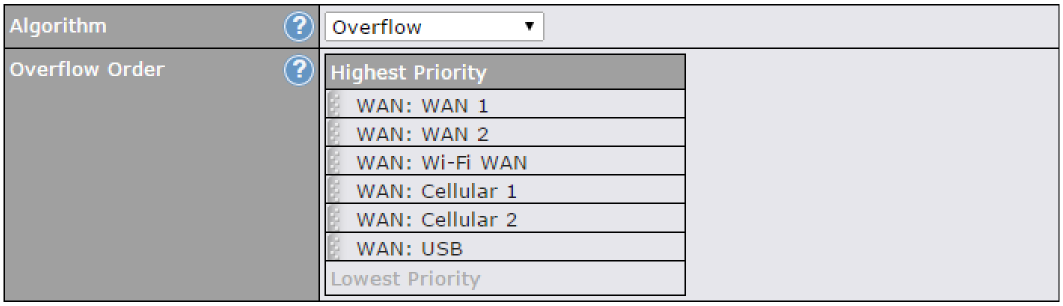
Algorithm	Priority
Priority Order	Highest Priority WAN: WAN WAN: Cellular 1 WAN: Cellular 2 WAN: USB WAN: LAN 1 as WAN WAN: GRE WAN 1 WAN: GRE WAN 2 WAN: OpenVPN WAN 1 Lowest Priority Not In Use
When No Connections are Available	Drop the Traffic
Terminate Sessions on Connection Recovery	☐ Enable

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

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

17.2.5 Algorithm: Overflow

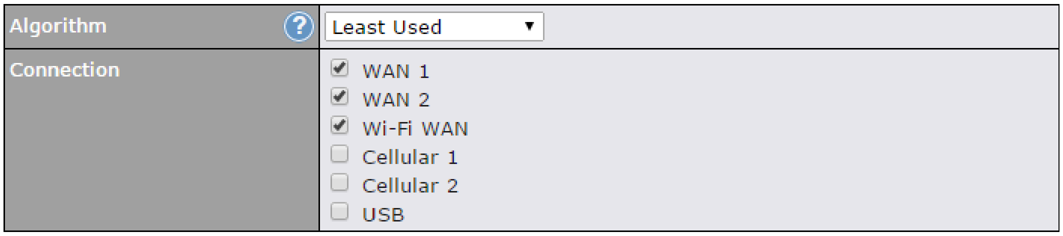
The traffic matching this rule will be routed through the healthy WAN connection that has the highest priority and is not in full load. When this connection gets saturated, new sessions will be routed to the next healthy WAN connection that is not in full load.



Algorithm	Overflow
Overflow Order	Highest Priority WAN: WAN 1 WAN: WAN 2 WAN: Wi-Fi WAN WAN: Cellular 1 WAN: Cellular 2 WAN: USB Lowest Priority

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.

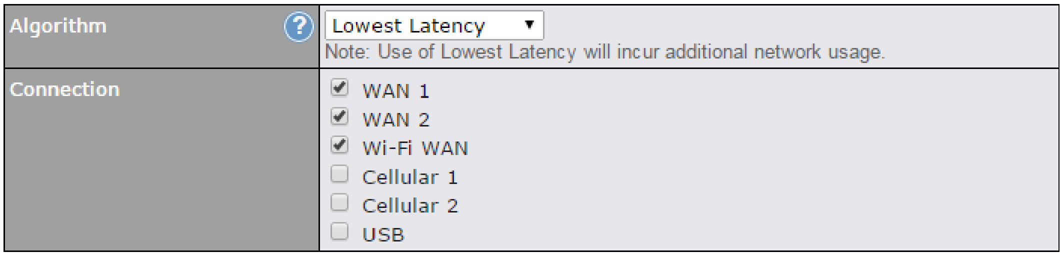
17.2.6 Algorithm: Least Used



Algorithm	Least Used
Connection	☑ WAN 1 ☑ WAN 2 ☑ Wi-Fi WAN ☐ Cellular 1 ☐ Cellular 2 ☐ USB

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.

17.2.7 Algorithm: Lowest Latency



Algorithm	Lowest Latency Note: Use of Lowest Latency will incur additional network usage.
Connection	☑ WAN 1 ☑ WAN 2 ☑ Wi-Fi WAN ☐ Cellular 1 ☐ Cellular 2 ☐ USB

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.

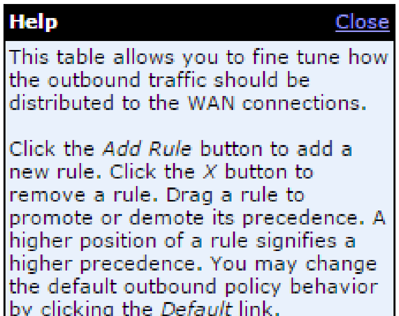
Tip

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.

17.2.8 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**.



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.

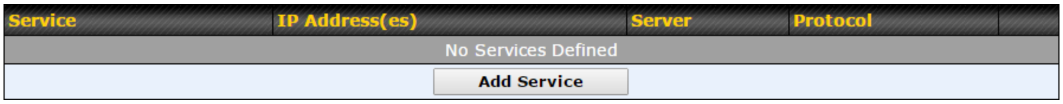
In Expert Mode, a new special rule, **SpeedFusion^{TM} Routes**, is displayed in the **Custom Rules** table. This rule represents all SpeedFusion^{TM} routes learned from remote VPN peers. By default, this bar is on the top of all custom rules. This position means that traffic for remote VPN subnets 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^{TM} routes.

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

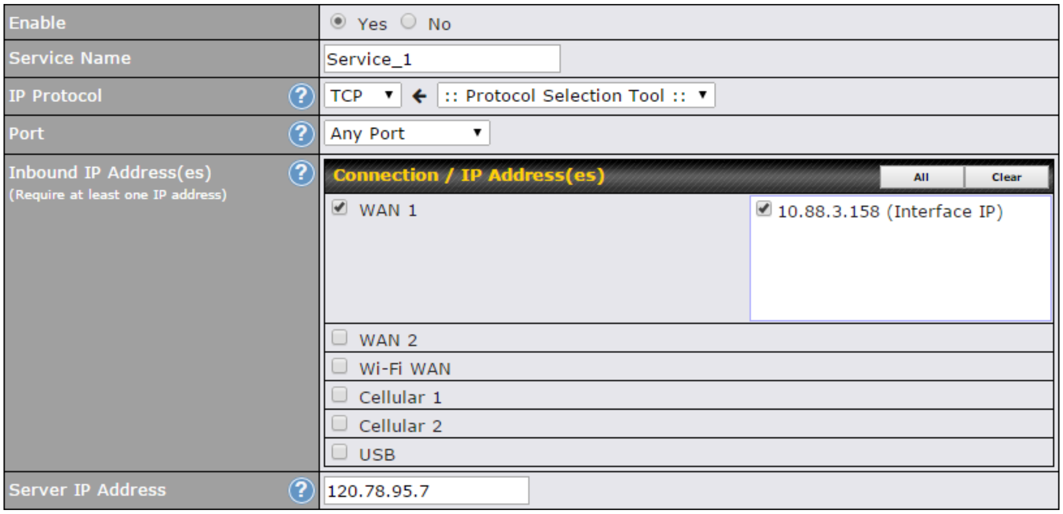
18 Port Forwarding

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**.



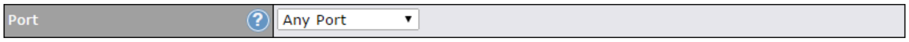
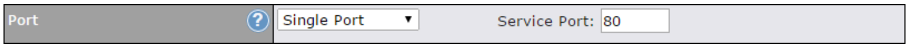
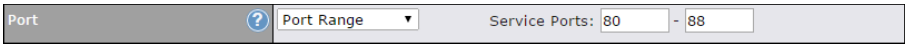
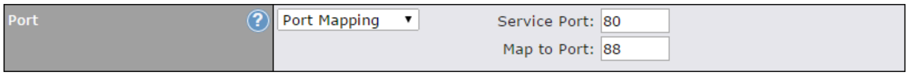
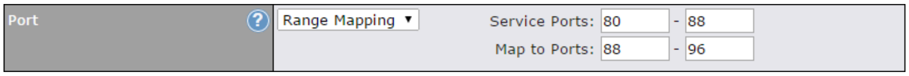
Service	IP Address(es)	Server	Protocol
No Services Defined			
Add Service			

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



Enable	● Yes ○ No
Service Name	Service_1
IP Protocol	TCP ← :: Protocol Selection Tool ::
Port	Any Port
Inbound IP Address(es) (Require at least one IP address)	Connection / IP Address(es) — All, Clear ☑ WAN 1 — ☑ 10.88.3.158 (Interface IP) ☐ WAN 2 ☐ Wi-Fi WAN ☐ Cellular 1 ☐ Cellular 2 ☐ USB
Server IP Address	120.78.95.7

Port Forwarding Settings	
Enable	This setting specifies whether the inbound service takes effect. When **Enable** is checked, the inbound service takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When this setting is disabled, the inbound service does not take effect: the Pepwave router disregards the other parameters of the rule.
Service Name	This setting identifies the service to the system administrator. Valid values for this setting consist of only alphanumeric and underscore "_" characters.

IP Protocol	The **IP Protocol** setting, along with the **Port** setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Traffic that is received by the Pepwave router via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the **Servers** setting. Please see below for details on the **Port** and **Servers** settings. Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and a single port number of common Internet services (e.g. HTTP, HTTPS, etc.). After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remain manually modifiable.
Port	The **Port** setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners: **Any Port**, **Single Port**, **Port Range**, **Port Map**, and **Range Mapping**  Port ? Any Port **Any Port**: all traffic that is received by the Pepwave router via the specified protocol is forwarded to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Any Port**, all TCP traffic is forwarded to the configured servers.  Port ? Single Port Service Port: 80 **Single Port**: traffic that is received by the Pepwave router via the specified protocol at the specified port is forwarded via the same port to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Single Port** and **Service Port** 80, TCP traffic received on port 80 is forwarded to the configured servers via port 80.  Port ? Port Range Service Ports: 80 - 88 **Port Range**: traffic that is received by the Pepwave router via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Range** and **Service Ports** 80-88, TCP traffic received on ports 80 through 88 is forwarded to the configured servers via the respective ports.  Port ? Port Mapping Service Port: 80 Map to Port: 88 **Port Mapping**: traffic that is received by Pepwave router via the specified protocol at the specified port is forwarded via a different port to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Mapping**, **Service Port** 80, and **Map to Port** 88, TCP traffic on port 80 is forwarded to the configured servers via port 88. (Please see below for details on the **Servers** setting.)  Port ? Range Mapping Service Ports: 80 - 88 Map to Ports: 88 - 96 **Range Mapping**: traffic that is received by the Pepwave router via the specified protocol at the specified port range is forwarded via a different port to the servers specified by the **Servers** setting.

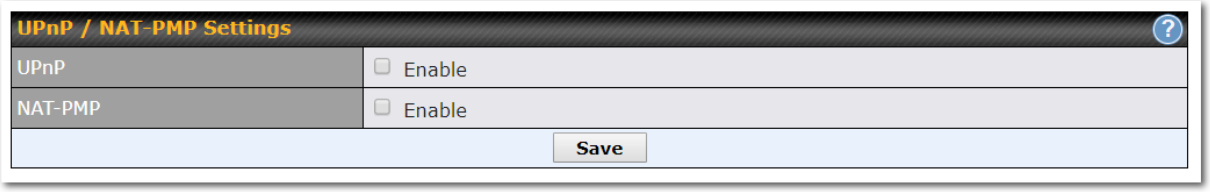
Inbound IP Address(es)	This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed.
Server IP Address	This setting specifies the LAN IP address of the server that handles the requests for the service.

18.1 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.

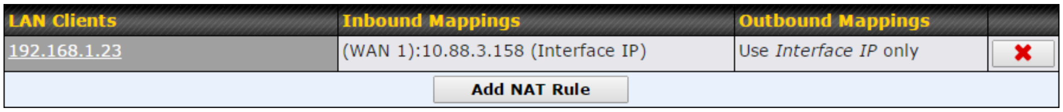


UPnP / NAT-PMP Settings	
UPnP	☐ Enable
NAT-PMP	☐ Enable

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

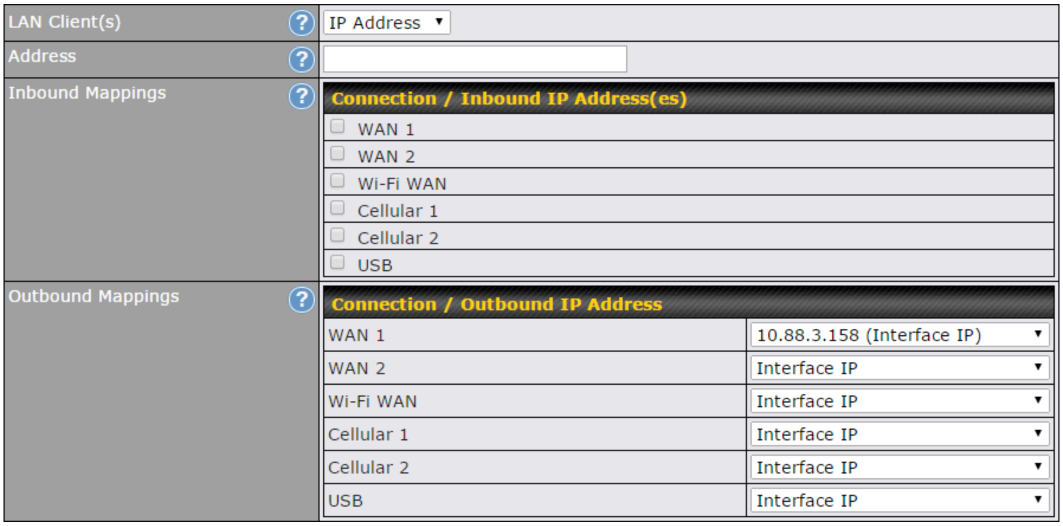
19 NAT Mappings

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	✖

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



LAN Client(s)	IP Address
Address	

Inbound Mappings

Connection / Inbound IP Address(es)
☐ WAN 1
☐ WAN 2
☐ Wi-Fi WAN
☐ Cellular 1
☐ Cellular 2
☐ USB

Outbound Mappings

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

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

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

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

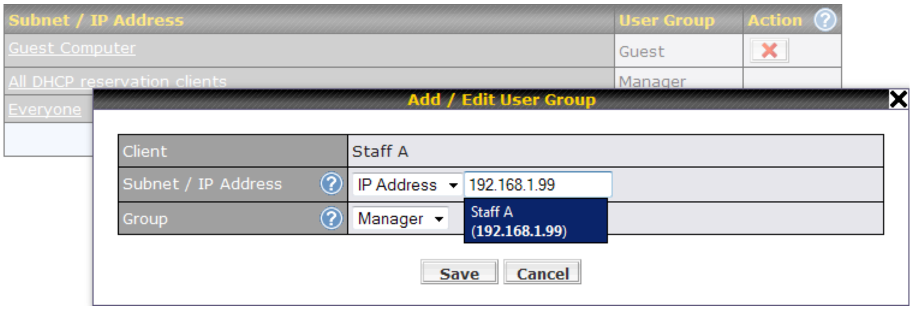
20 QoS

20.1 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

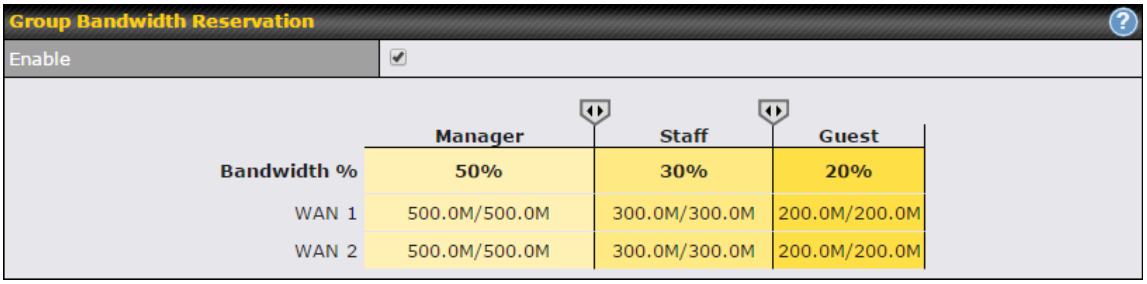
Client	Staff A
Subnet / IP Address	IP Address 192.168.1.99
Group	Manager

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

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

20.2 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

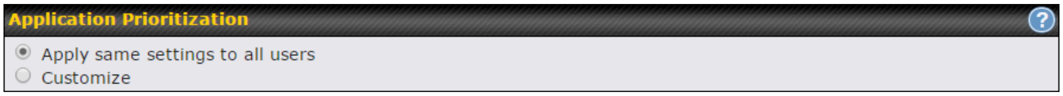
Enable ☑

	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

20.3 Application

20.3.1 Application Prioritization

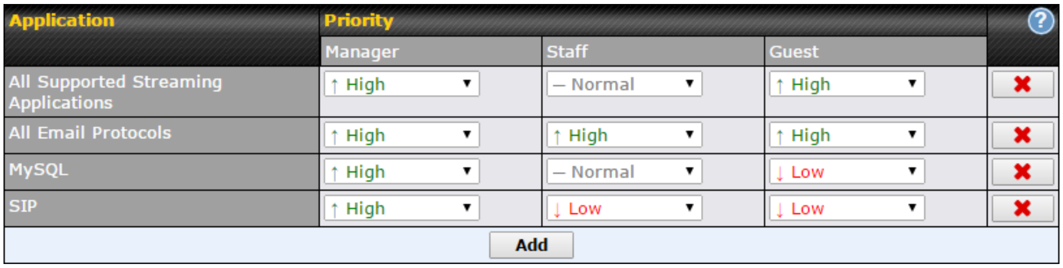
On many Pepwave routers, you can choose whether to apply the same prioritization settings to all user groups or customize the settings for each group.



Application Prioritization

● Apply same settings to all users
○ 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.

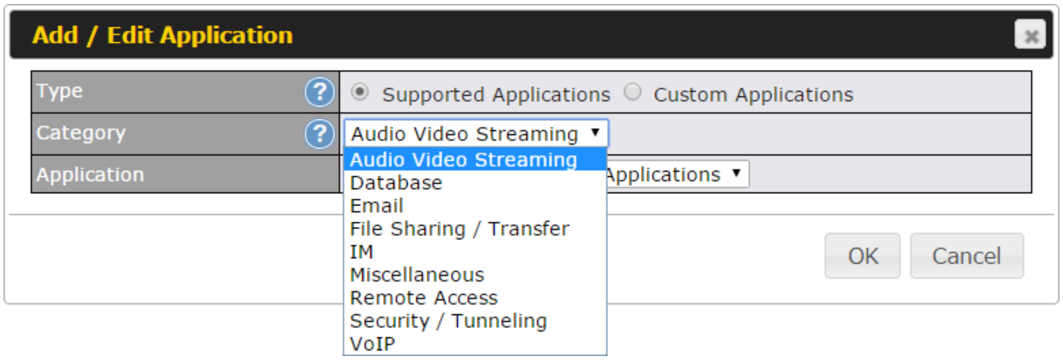


Application	Priority: Manager	Priority: Staff	Priority: Guest	
All Supported Streaming Applications	↑ High	— Normal	↑ High	✖
All Email Protocols	↑ High	↑ High	↑ High	✖
MySQL	↑ High	— Normal	↓ Low	✖
SIP	↑ High	↓ Low	↓ Low	✖

20.3.2 Prioritization for Custom Applications

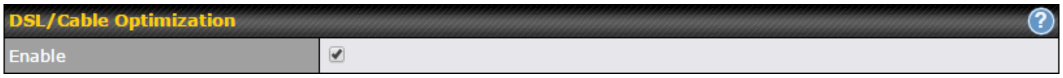
Click the **Add** button to define a custom application. Click the button ✖ in the **Action** column to delete the custom application in the corresponding row.

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.


Add / Edit Application
Type
● Supported Applications ○ Custom Applications
Category
Audio Video Streaming ▼
Audio Video Streaming
Database
Email
File Sharing / Transfer
IM
Miscellaneous
Remote Access
Security / Tunneling
VoIP
Application
Applications ▼
OK
Cancel

20.3.3 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.


DSL/Cable Optimization

Enable ☑

21 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.

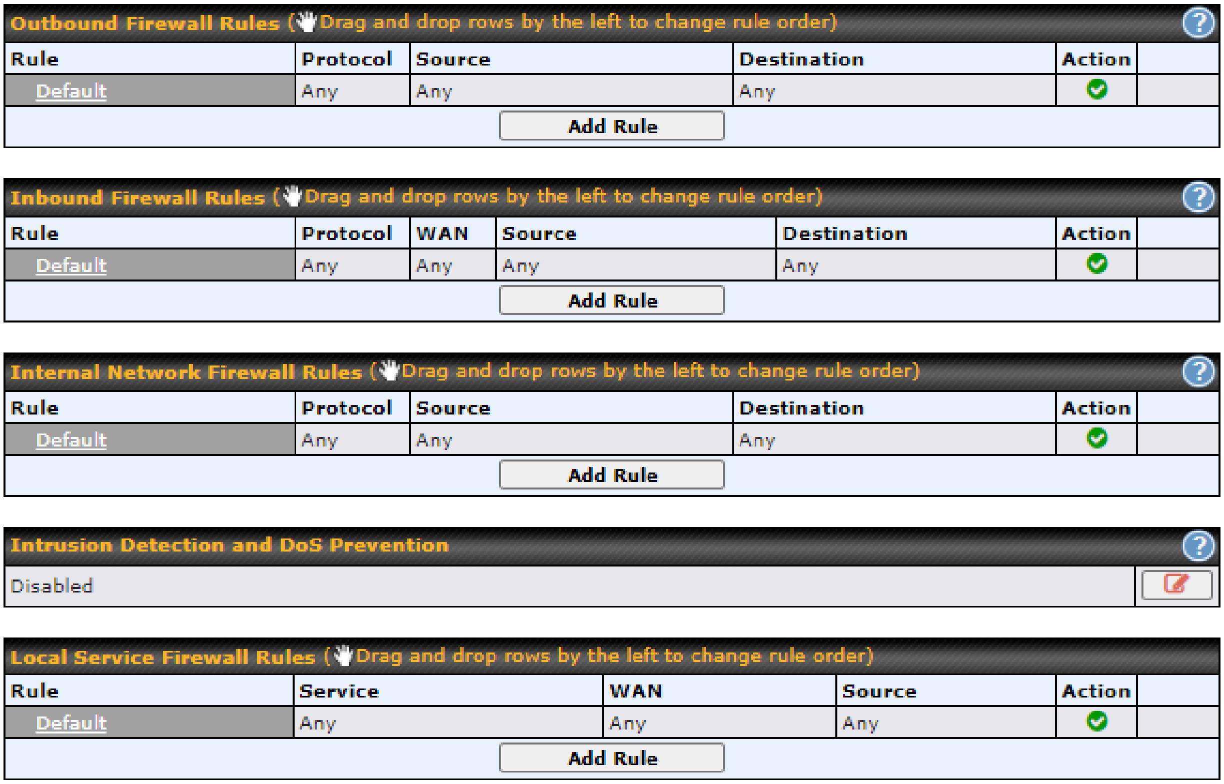
The firewall functionality of Pepwave routers supports the selective filtering of data traffic in both directions:

- Outbound (LAN to WAN)
- Inbound (WAN to LAN)
- Internal Network (VLAN to VLAN)

The firewall also supports the following functionality:

- Intrusion detection and DoS prevention
- Web blocking

With SpeedFusion^{TM} 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)

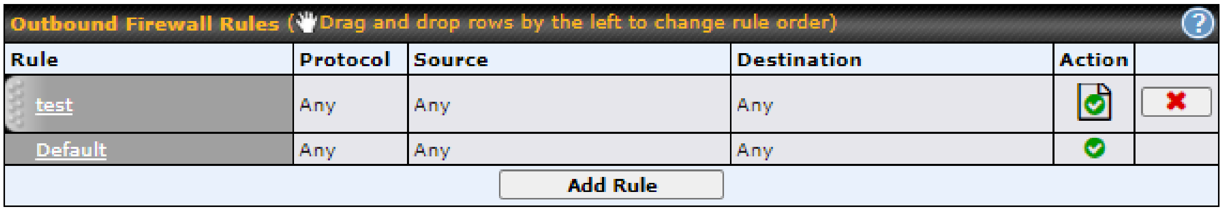
Rule	Service	WAN	Source	Action	
Default	Any	Any	Any	✓	

Add Rule

21.1 Outbound and Inbound Firewall Rules

21.1.1 Access Rules

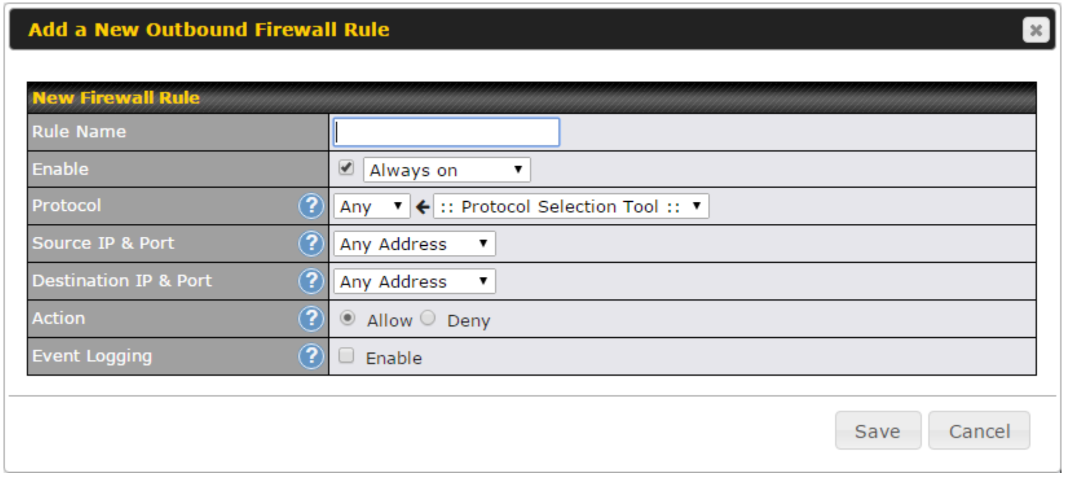
The outbound firewall settings are located at **Advanced>Firewall>Access Rules>Outbound Firewall Rules.**



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	✓	

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

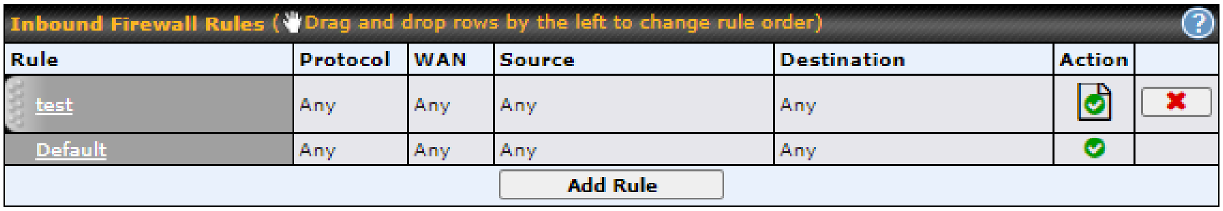


Add a New Outbound Firewall Rule

New Firewall Rule

Rule Name	
Enable	☑ Always on
Protocol	Any ← :: Protocol Selection Tool ::
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	● Allow ○ Deny
Event Logging	☐ Enable

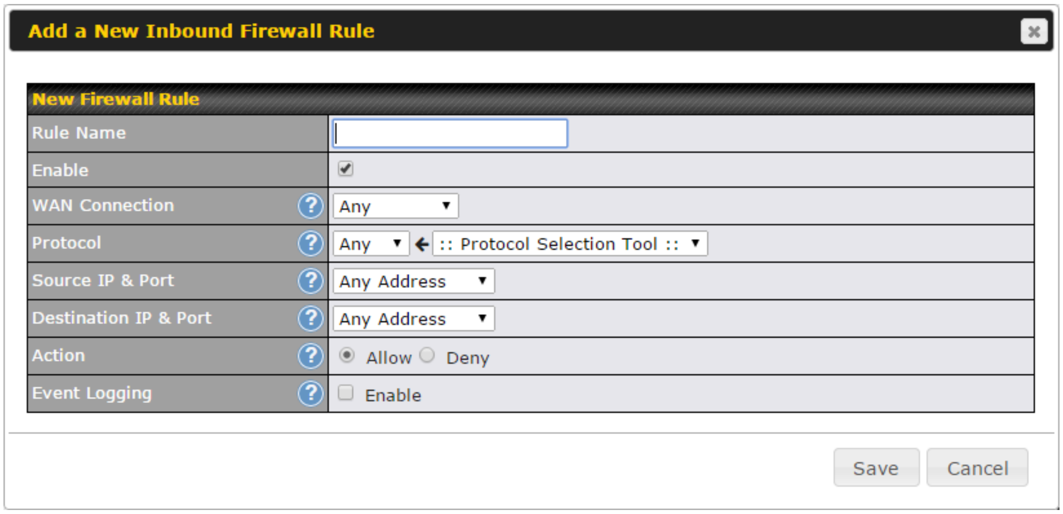
Inbound firewall settings are located at **Advanced>Firewall>Access Rules>Inbound Firewall Rules.**



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	✓	

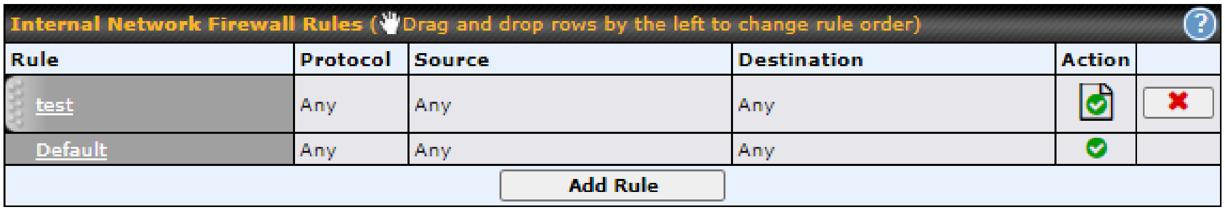
Click **Add Rule** to display the following screen:



Add a New Inbound Firewall Rule

New Firewall Rule	
Rule Name	
Enable	☑
WAN Connection	Any
Protocol	Any ← :: Protocol Selection Tool ::
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	● Allow ○ Deny
Event Logging	☐ Enable

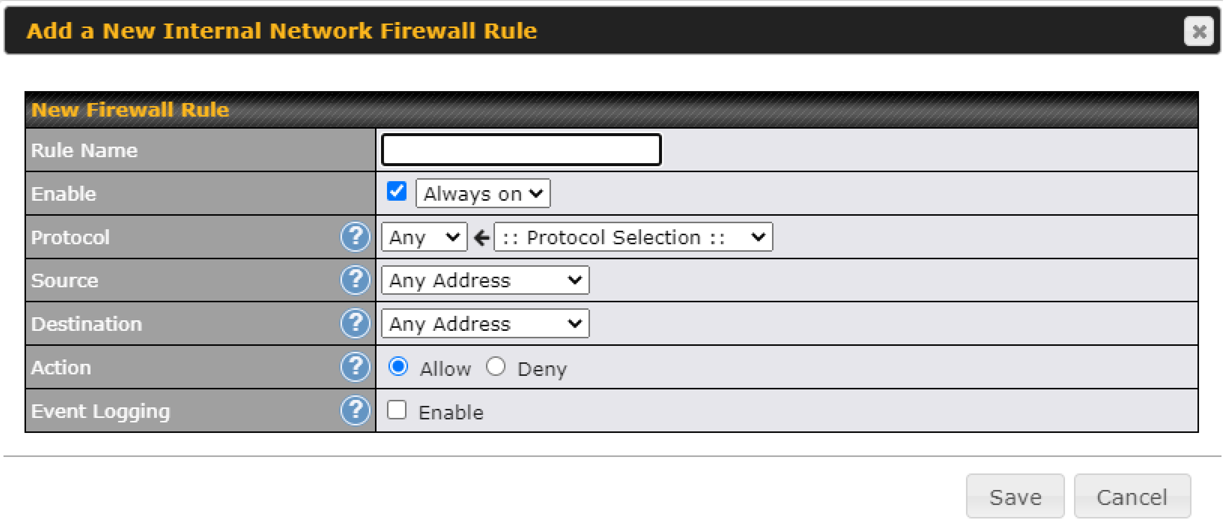
Internal Network firewall settings are located at **Advanced>Firewall>Access Rules>Internal Network Firewall Rules.**



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

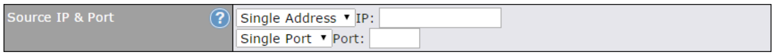
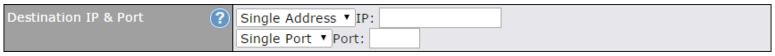
Rule	Protocol	Source	Destination	Action	
test	Any	Any	Any	✓	✗
Default	Any	Any	Any	✓	

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



Add a New Internal Network Firewall Rule

New Firewall Rule	
Rule Name	
Enable	☑ Always on
Protocol	Any ← :: Protocol Selection ::
Source	Any Address
Destination	Any Address
Action	● Allow ○ Deny
Event Logging	☐ Enable

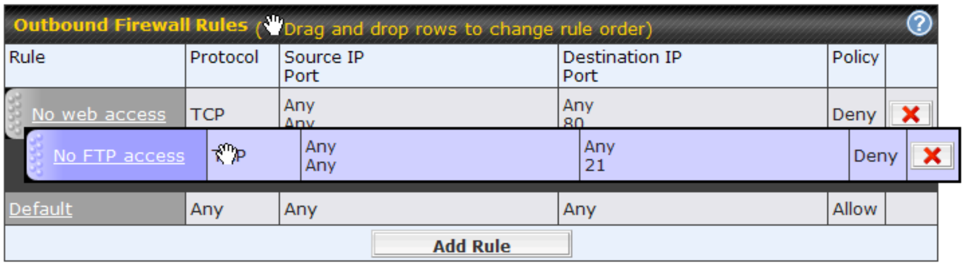
Inbound / Outbound / Internal Network Firewall Settings	
Rule Name	This setting specifies a name for the firewall rule.
Enable	This setting specifies whether the firewall rule should take effect. If the box is checked, the firewall rule takes effect. If the traffic matches the specified protocol/IP/port, 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. Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule.
WAN Connection (Inbound)	Select the WAN connection that this firewall rule should apply to.
Protocol	This setting specifies the protocol to be matched. Via a drop-down menu, the following protocols can be specified: ● **Any** ● **TCP** ● **UDP** ● **ICMP** ● **DSCP** ● **IP** Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.) After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remains manually modifiable.
Source IP & Port	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 **Source IP & Port** setting, as indicated by the following screenshot:  Source IP & Port Single Address ▾ IP: Single Port ▾ Port: In addition, a single port, or a range of ports, can be specified for the **Source IP & Port** settings.
Destination IP & Port	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 **Destination IP & Port** setting, as indicated by the following screenshot:  Destination IP & Port Single Address ▾ IP: Single Port ▾ Port: In addition, a single port, or a range of ports, can be specified for the **Destination IP & Port** settings.
Action	This setting specifies the action to be taken by the router upon encountering traffic

	that matches the both of the following: - Source IP & port - Destination IP & port With the value of **Allow** for the **Action** setting, the matching traffic passes through the router (to be routed to the destination). If the value of the **Action** setting is set to **Deny**, the matching traffic does not pass through the router (and is discarded).
Event Logging	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 - **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.



Outbound Firewall Rules (Drag and drop rows to change rule order)

Rule	Protocol	Source IP Port	Destination IP Port	Policy	
No web access	TCP	Any Any	Any 80	Deny	✖
No FTP access	P	Any Any	Any 21	Deny	✖
Default	Any	Any	Any	Allow	

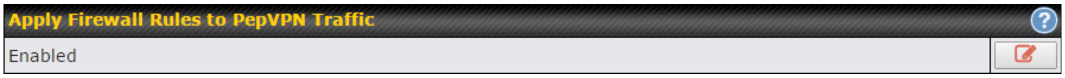
To remove a rule, click the ✖ button.

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 Outbound, Inbound and Internal Network access.

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.

21.1.2 Apply Firewall Rules to PepVpn Traffic

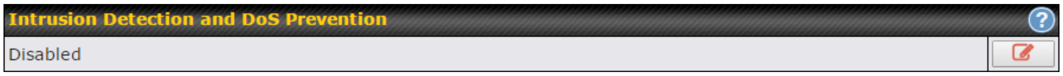


Apply Firewall Rules to PepVPN Traffic

Enabled

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.

21.1.3 Intrusion Detection and DoS Prevention



Intrusion Detection and DoS Prevention

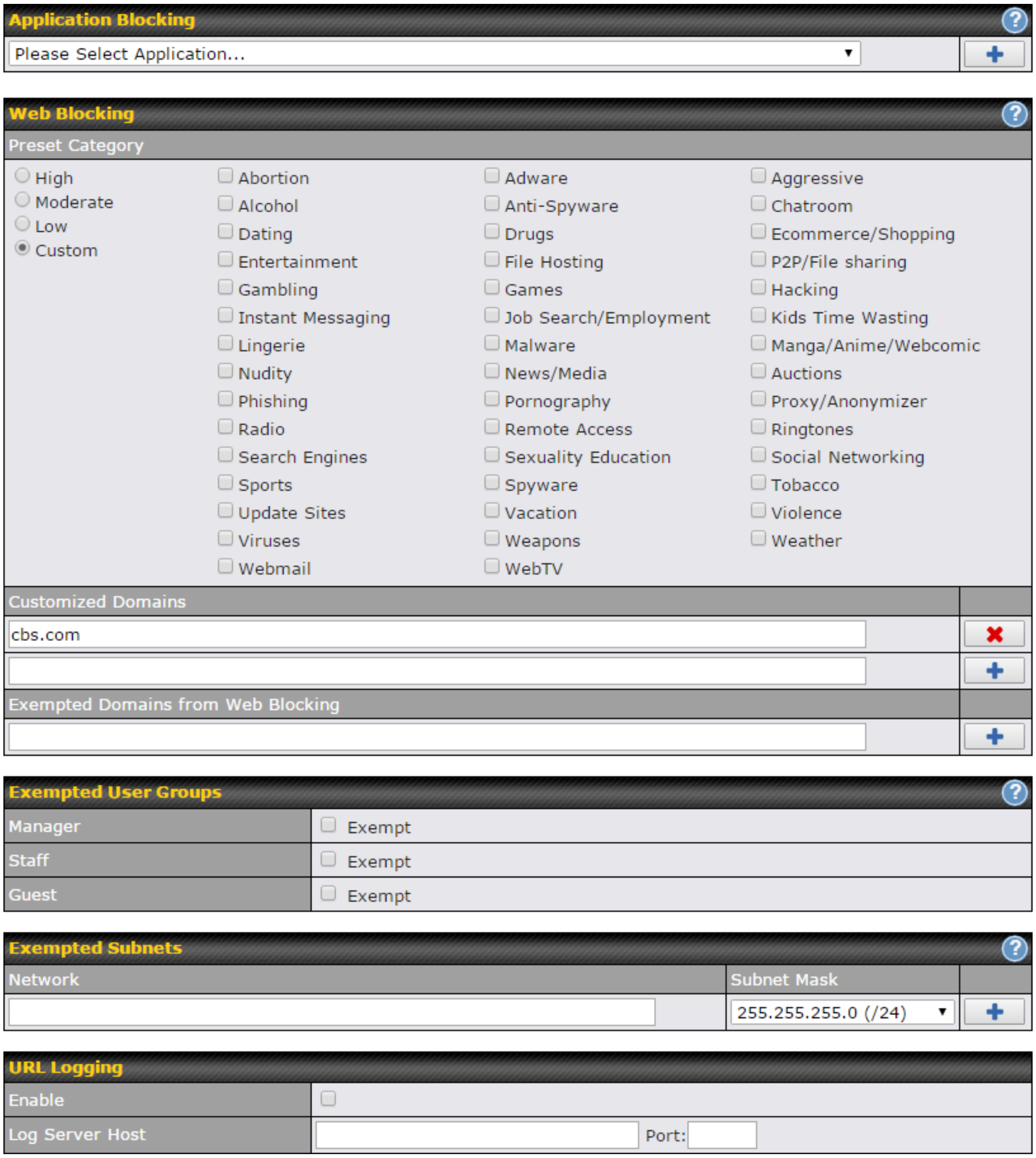
Disabled

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

21.2 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	☐ Exempt
Staff	☐ Exempt
Guest	☐ Exempt

Exempted Subnets

Network	Subnet Mask
	255.255.255.0 (/24)

URL Logging

Enable	☐
Log Server Host	Port:

21.2.1 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.

21.2.2 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.

21.2.3 Customized Domains

Enter an appropriate website address, and the Pepwave MAX will block and disallow LAN/PPTP/SpeedFusionTM 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 Pepwave MAX will inspect and look for blocked domain names on all HTTP traffic. Secure web (HTTPS) traffic is not supported.

21.2.4 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.

21.2.5 Exempted Subnets

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

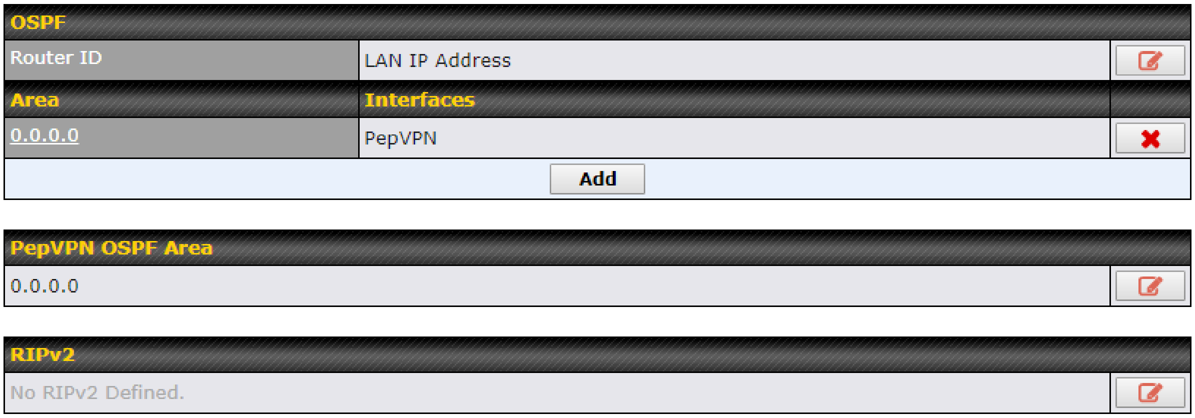
21.2.6 URL Logging

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

22 Routing Protocols

22.1 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:

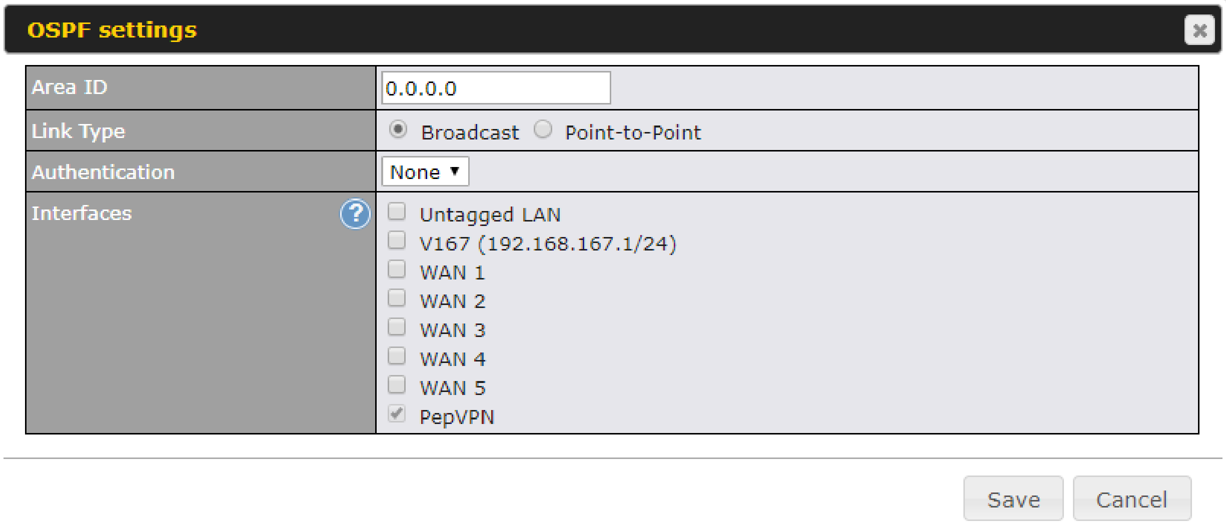


OSPF		
Router ID	LAN IP Address	✎
Area	**Interfaces**	
0.0.0.0	PepVPN	✖
	Add	

PepVPN OSPF Area	
0.0.0.0	✎

RIPv2	
No RIPv2 Defined.	✎

OSPF	
Router ID	This field determines the ID of the router. By default, this is specified as the WAN IP address. If you want to specify your own ID, enter it into the **Custom** field.
Area	This is an overview of the OSPF areas that you have defined. Clicking on the name under Area allows you to configure the connection. To define a new area, click Add. To delete an existing area, click on the ✖.

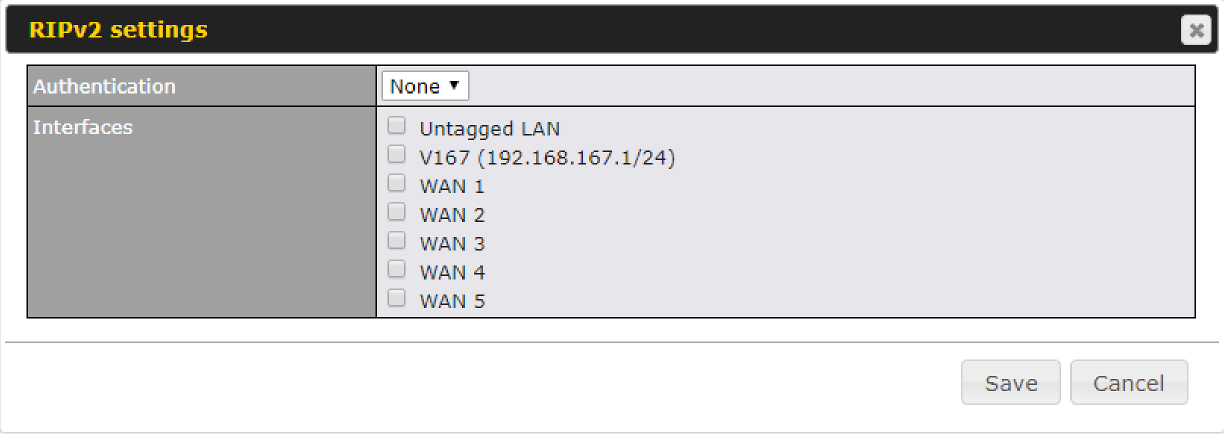


OSPF settings

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

OSPF Settings	
Area ID	Assign a name to be applied to this group. Machines linked to this group will send and receive related OSPF packets, while unlinked machines will ignore them.
Link Type	Choose the type of network that this area will use.
Authentication	If an authentication method is used, select one from this drop-down menu. Available options are **MD5** and **Text**. Authentication key(s) may be input next to the drop-down menu after selecting an authentication method.
Interfaces	Select the interface(s) that this area will use to listen to and deliver OSPF packets.

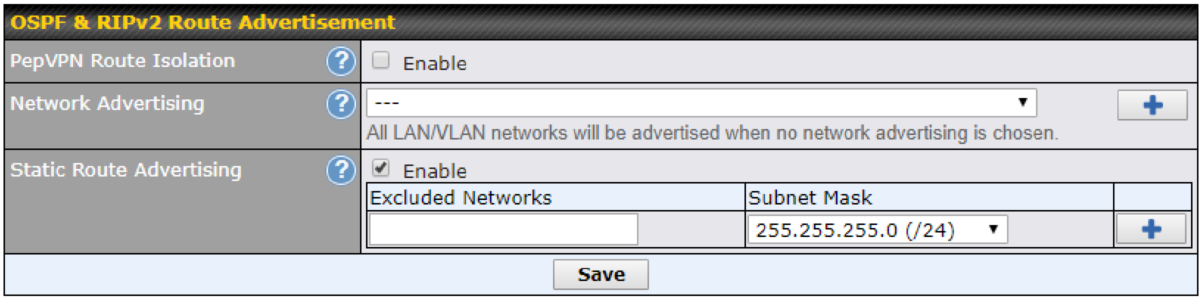
To access RIPv2 settings, click on ✎.



RIPv2 settings

Authentication	None ▾
Interfaces	☐ Untagged LAN ☐ V167 (192.168.167.1/24) ☐ WAN 1 ☐ WAN 2 ☐ WAN 3 ☐ WAN 4 ☐ WAN 5

RIPv2 Settings	
Authentication	If an authentication method is used, select one from this drop-down menu. Available options are **MD5** and **Text**. Authentication key(s) may be input next to the drop-down menu after selecting an authentication method.
Interfaces	Select the interface(s) that this area will use to listen to and deliver RIPv2 packets.



OSPF & RIPv2 Route Advertisement

PepVPN Route Isolation: ☐ Enable

Network Advertising: ---

All LAN/VLAN networks will be advertised when no network advertising is chosen.

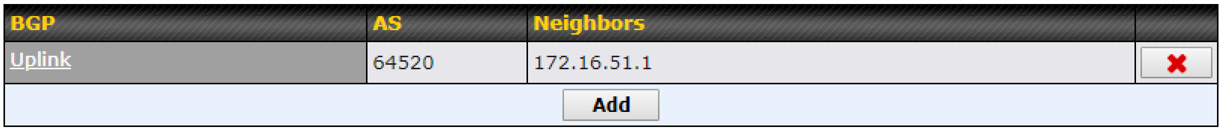
Static Route Advertising: ☑ Enable

Excluded Networks	Subnet Mask
	255.255.255.0 (/24)

OSPF & RIPv2 Route Advertisement	
PepVPN Route Isolation	Isolate PepVPN peers from each other. Received PepVPN routes will not be forwarded to other PepVPN peers to reduce bandwidth consumption..
Network Advertising	Networks to be advertised over OSPF & RIPv2. If no network is selected, all LAN / VLAN networks will be advertised by default.
Static Route Advertising	Enabling OSPF & RIPv2 Route Advertising allows it to advertise LAN static routes over OSPF & RIPv2. Static routes on the Excluded Networks table will not be advertised.

22.2 BGP

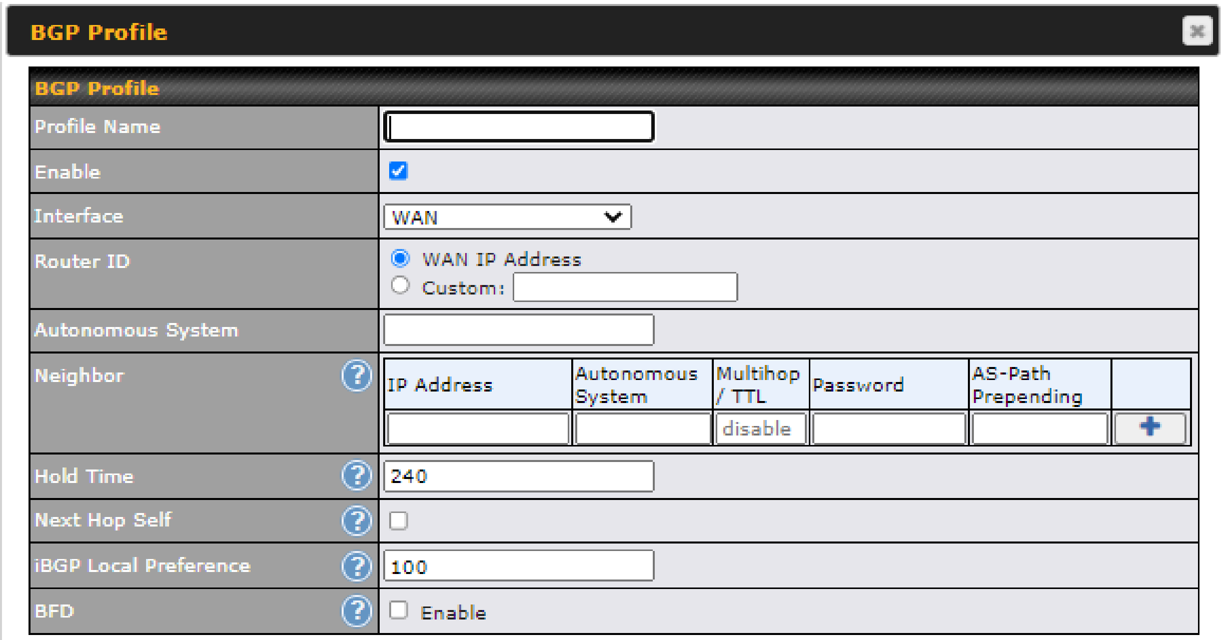
Click the **Network** tab along the top bar, and then click the **BGP** item on the sidebar to configure BGP.



BGP	AS	Neighbors	
Uplink	64520	172.16.51.1	✗

Click the "x" to delete a BGP profile.

Click "**Add**" to create a new BGP profile.



BGP Profile

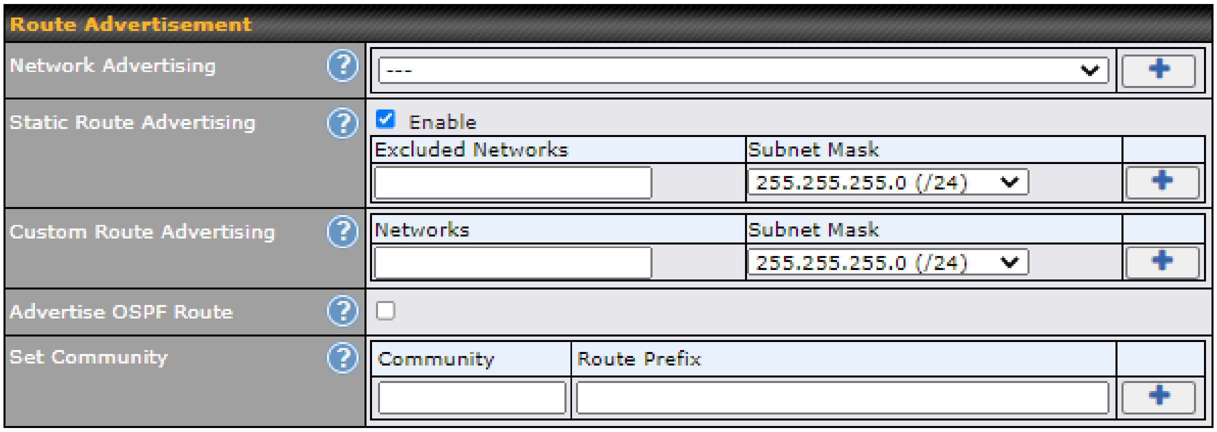
BGP Profile

Profile Name	
Enable	☑
Interface	WAN
Router ID	● WAN IP Address ○ Custom:
Autonomous System	
Neighbor	
Hold Time	240
Next Hop Self	☐
iBGP Local Preference	100
BFD	☐ Enable

IP Address	Autonomous System	Multihop / TTL	Password	AS-Path Prepending	
		disable			+

BGP	
Name	This field specifies the name that represents this profile.
Enable	When this box is checked, this BGP profile will be enabled. If it is left unchecked, it will be disabled.
Interface	The interface in which the BGP neighbor is located.
Autonomous System	The Autonomous System Number (ASN) assigned to this profile.
Neighbor	BGP Neighbors and their details.
IP address	The IP address of the Neighbor.
Autonomous System	The Neighbor's ASN.
Multihop/TTL	This field determines the Time-to-live (TTL) of BGP packets. Leave this field blank if the BGP neighbor is directly connected, otherwise you must specify a TTL value. This option should be used if the configured Neighbor's IP address does not match the selected Interface's network subnets. The TTL value must be between 2 to 255.
Password	(Optional) Assign a password for MD5 authentication of BGP sessions.
AS-Path Prepending:	AS path to be prepended to the routes received from this Neighbor. Values must be ASN and separated by commas. For example: inputting "64530,64531" will prepend "64530, 64531" to received routes.

Hold Time	Wait time in seconds for a keepalive message from a Neighbor before considering the BGP connection as stalled. The value must be either 0 (infinite hold time) or between 3 and 65535 inclusively. Default: 240
Next Hop Self	Enable this option to advertise your own source address as the next hop when propagating routes.
iBGP Local Preference	This is the metric advertised to iBGP Neighbors to indicate the preference for external routes. The value must be between 0 to 4294967295 inclusively. Default: 100
BFD	Enable this option to add Bidirectional Forwarding Detection for path failure. All directly connected Neighbors that use the same physical interface share the same BFD settings. All mulithop Neighbors share the same multihop BFD settings. You can configure BFD settings in the BGP profile listing page after this option is enabled.

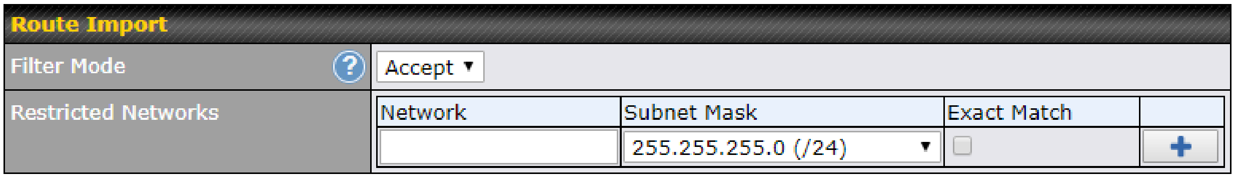


Route Advertisement

Network Advertising	---
Static Route Advertising	☑ Enable Excluded Networks / Subnet Mask: 255.255.255.0 (/24)
Custom Route Advertising	Networks / Subnet Mask: 255.255.255.0 (/24)
Advertise OSPF Route	☐
Set Community	Community / Route Prefix

Network Advertising	Select the Networks that will be advertised to the BGP Neighbor.
Static Route Advertising	Enable this option to advertise static LAN routes. Static routes that match the Excluded Networks table will not be advertised.
Custom Route Advertising	Additional routes to be advertised to the BGP Neighbor.
Advertise OSPF Route	When this box is checked, every learnt OSPF route will be advertised.
Set Community	Assign a prefix to a Community. Community:

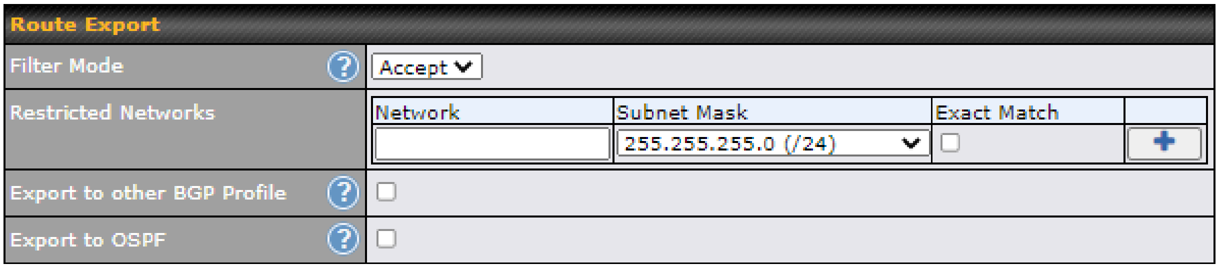
	Two numbers in new-format. e.g. 65000:21344 Well-known communities: no-export 65535:65281 no-advertise 65535:65282 no-export-subconfed 65535:65283 no-peer 65535:65284 Route Prefix: Comma separated networks. e.g. 172.168.1.0/24,192.168.1.0/28



Route Import

Filter Mode	Accept			
Restricted Networks	Network	Subnet Mask	Exact Match	
		255.255.255.0 (/24)	☐	+

Filter Mode	This field allows for the selection of the filter mode for route import. **None**: All BGP routes will be accepted. **Accept**: Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected. **Reject**: Routes in "Restricted Networks" will be rejected, routes not in the list will be accepted.
Restricted Networks	This field specifies the network(s) in the “route import” entry. **Exact Match:** When this box is checked, only routes with the same Network and Subnet Mask will be filtered. Otherwise, routes within the Networks and Subnets will be filtered.



Route Export

Filter Mode	Accept			
Restricted Networks	Network	Subnet Mask	Exact Match	
		255.255.255.0 (/24)	☐	+
Export to other BGP Profile	☐			
Export to OSPF	☐			

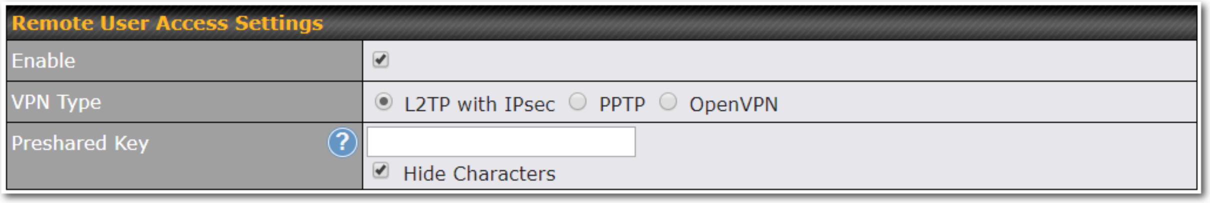
Filter Mode	This field allows for the selection of the filter mode for route export. **None**: All BGP routes will be accepted. **Accept**: Routes in "Restricted Networks" will be accepted, routes not in the list will

	be rejected. **Reject**: Routes in "Restricted Networks" will be rejected, routes not in the list will be accepted.
Restricted Networks	This field specifies the network(s) in the “route export” entry. **Exact Match:** When this box is checked, only routes with the same Network and Subnet Mask will be filtered. Otherwise, routes within the Networks and Subnets will be filtered.
Export to other BGP Profile	When this box is checked, routes learnt from this BGP profile will be exported to other BGP profiles.
Export to OSPF	When this box is checked, routes learnt from this BGP profile will be exported to the OSPF routing protocol.

23 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 Pepwave 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.

23.1 L2TP with IPsec



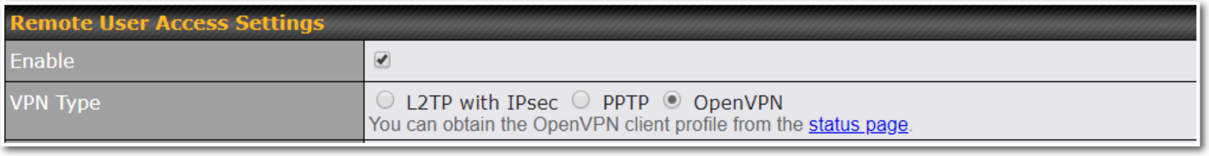
Remote User Access Settings

Enable	☑
VPN Type	● L2TP with IPsec ○ PPTP ○ OpenVPN
Preshared Key ?	☐ ☑ Hide Characters

L2TP with IPsec Remote User Access Settings	
Pre-shared Key	Enter your pre shared key in the text field. Please note that remote devices will need this preshared key to access the Balance.
Listen On	This setting is for specifying the WAN IP addresses that allow remote user access.
Disable Weak Ciphers	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.

23.2 OpenVPN

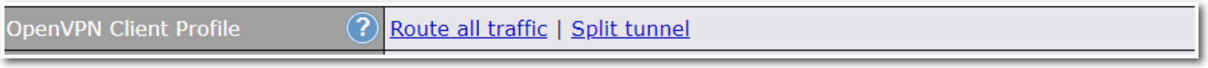


Remote User Access Settings

Enable	☑
VPN Type	○ L2TP with IPsec ○ PPTP ● OpenVPN You can obtain the OpenVPN client profile from the status page.

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.

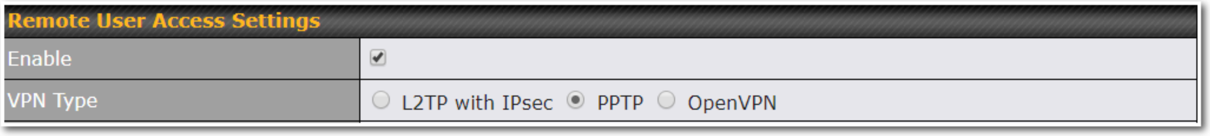


OpenVPN Client Profile | Route all traffic | Split tunnel

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.

23.3 PPTP



Remote User Access Settings

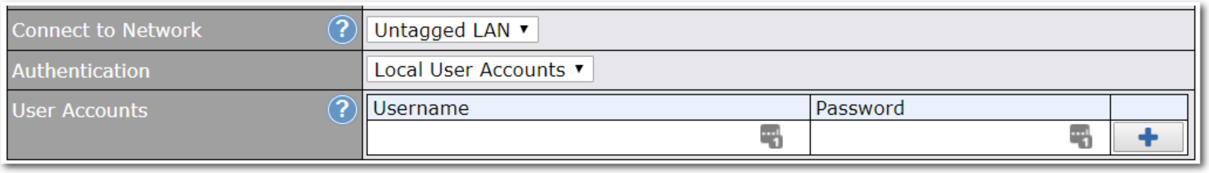
Enable	☑
VPN Type	○ L2TP with IPsec ● PPTP ○ OpenVPN

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.

23.4 Authentication Methods



Connect to Network	Untagged LAN
Authentication	Local User Accounts
User Accounts	Username / Password

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

User accounts:

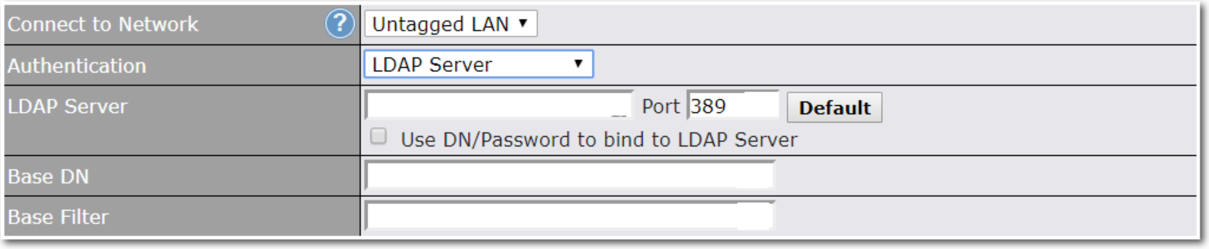
This setting allows you to define the Remote User Accounts.
Click Add to input username and password to create an account. After adding the user accounts, you can click on a username to edit the account password.

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.

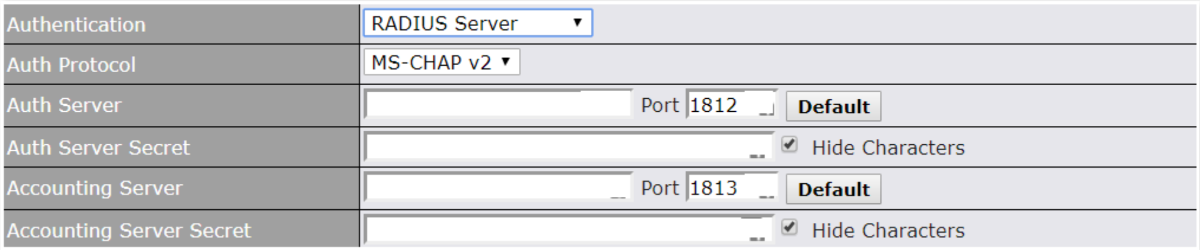
LDAP Server:



Connect to Network	Untagged LAN ▾
Authentication	LDAP Server ▾
LDAP Server	Port 389 Default ☐ Use DN/Password to bind to LDAP Server
Base DN	
Base Filter	

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

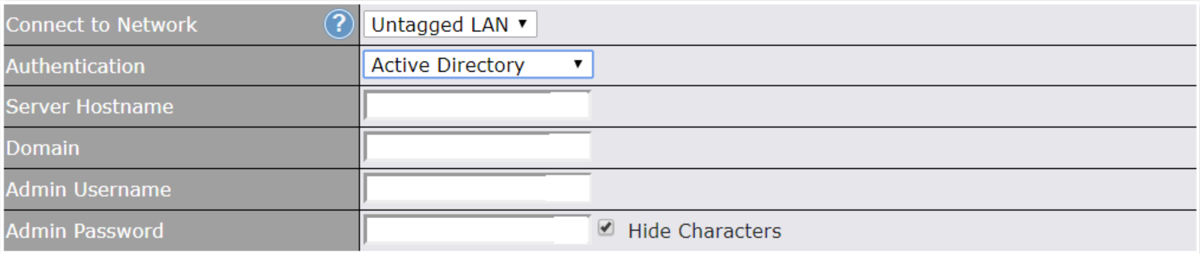
Radius Server:



Authentication	RADIUS Server ▾
Auth Protocol	MS-CHAP v2 ▾
Auth Server	Port 1812 Default
Auth Server Secret	☑ Hide Characters
Accounting Server	Port 1813 Default
Accounting Server Secret	☑ 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	
Domain	
Admin Username	
Admin Password	☑ Hide Characters

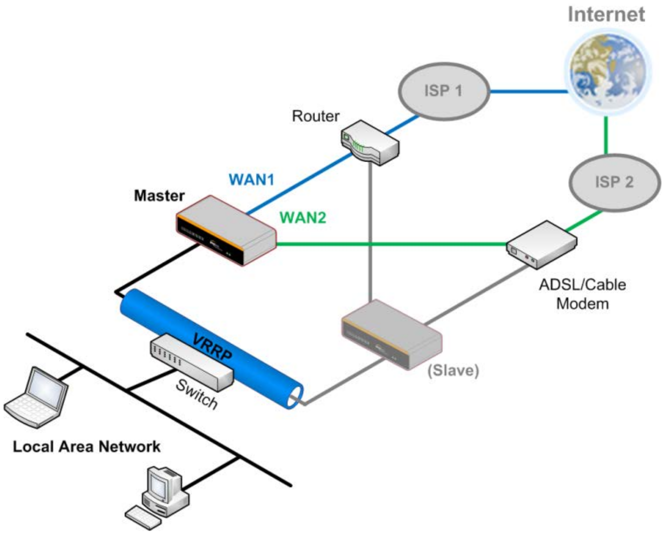
Enter the matching Active Directory details to allow for Active Directory server authentication.

24 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).

24.1 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:

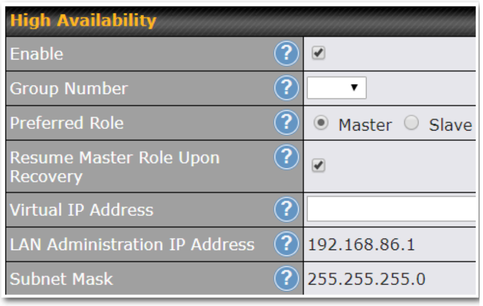
- In an HA configuration, the two Pepwave routers communicate with each other using VRRP over the LAN.
- The two Pepwave routers broadcast heartbeat signals to the LAN at a frequency of one heartbeat signal per second.
- In the event that no heartbeat signal from the master Pepwave router is received 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.

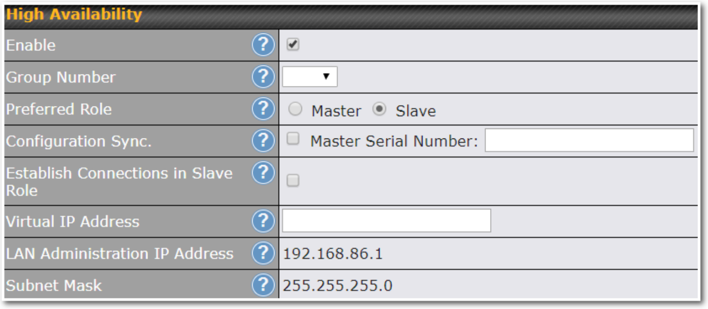
You can configure high availability at **Advanced>Misc. Settings>High Availability**.

Interface for Master Router



High Availability	
Enable	☑
Group Number	
Preferred Role	● Master ○ Slave
Resume Master Role Upon Recovery	☑
Virtual IP Address	
LAN Administration IP Address	192.168.86.1
Subnet Mask	255.255.255.0

Interface for Slave Router



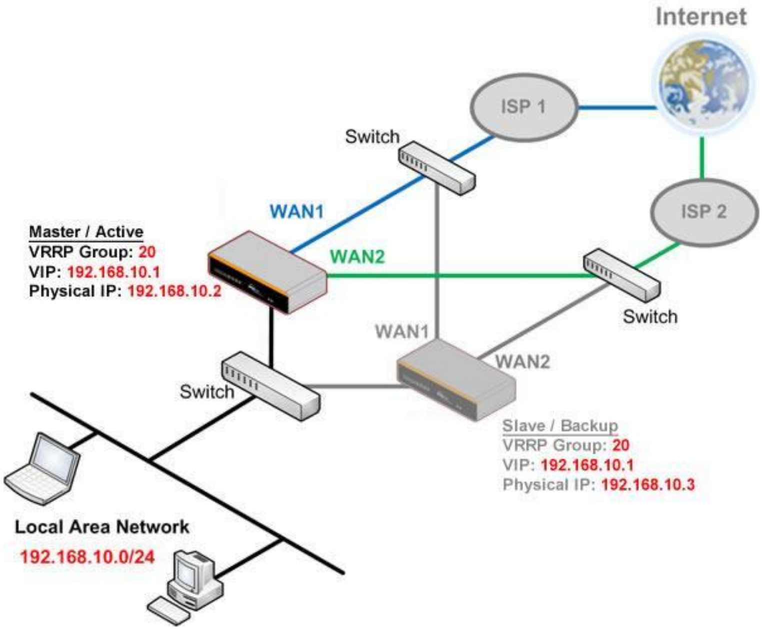
High Availability	
Enable	☑
Group Number	
Preferred Role	○ Master ● Slave
Configuration Sync.	☐ Master Serial Number:
Establish Connections in Slave Role	☐
Virtual IP Address	
LAN Administration IP Address	192.168.86.1
Subnet Mask	255.255.255.0

High Availability	
Enable	Checking this box specifies that the Pepwave router is part of a high availability configuration.
Group Number	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 **Group Number** value.
Preferred Role	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.
Resume Master Role Upon Recovery	This option is displayed when **Master** mode is selected in **Preferred Role**. If this option is enabled, once the device has recovered from an outage, it will take over and resume its **Master** role from the slave unit.
Configuration Sync.	This option is displayed when **Slave** mode is selected in **Preferred Role**. If this option is enabled and the **Master Serial Number** entered matches with the actual master unit's, the master unit will automatically transfer the configuration to this unit. Please make sure the **LAN IP Address** and the **Subnet Mask** fields are set correctly in the LAN settings page. You can refer to the **Event Log** for the configuration synchronization status.
Master Serial Number	If **Configuration Sync.** is checked, the serial number of the master unit is required here for the feature to work properly.
Virtual IP	The HA pair must share the same **Virtual IP**. The **Virtual IP** and the **LAN**

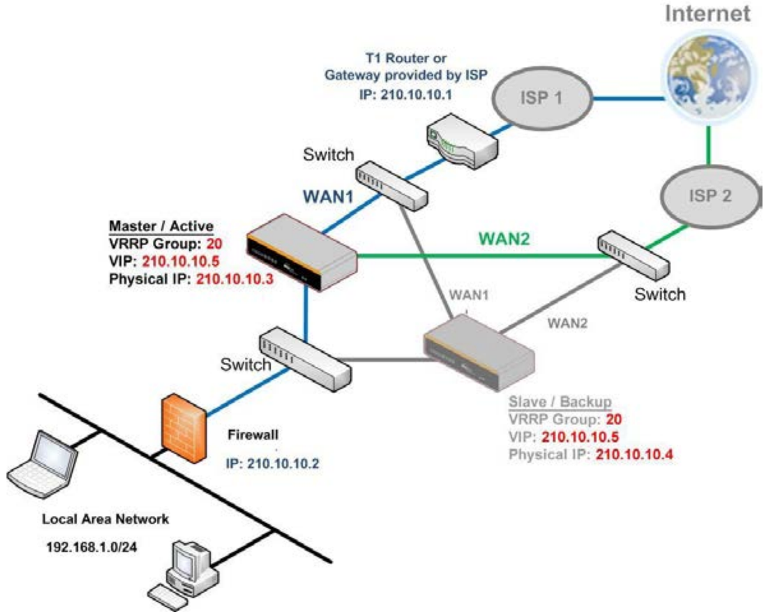
	Administration IP must be under the same network.
LAN Administration IP	This setting specifies a LAN IP address to be used for accessing administration functionality. This address should be unique within the LAN.
Subnet Mask	This setting specifies the subnet mask of the LAN.

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.

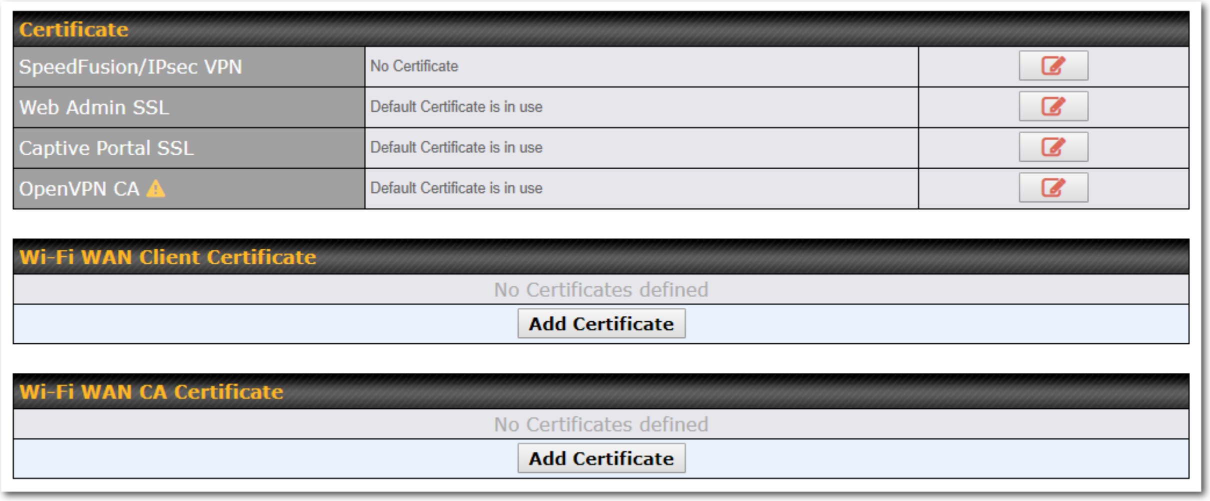

Internet
ISP 1
Switch
ISP 2
WAN1
Master / Active
VRRP Group: 20
VIP: 192.168.10.1
Physical IP: 192.168.10.2
WAN2
Switch
WAN1
WAN2
Switch
Slave / Backup
VRRP Group: 20
VIP: 192.168.10.1
Physical IP: 192.168.10.3
Local Area Network
192.168.10.0/24

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


Internet
T1 Router or
Gateway provided by ISP
IP: 210.10.10.1
ISP 1
ISP 2
Switch
WAN1
WAN2
Master / Active
VRRP Group: 20
VIP: 210.10.10.5
Physical IP: 210.10.10.3
WAN1
WAN2
Switch
Switch
Firewall
IP: 210.10.10.2
Slave / Backup
VRRP Group: 20
VIP: 210.10.10.5
Physical IP: 210.10.10.4
Local Area Network
192.168.1.0/24

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

24.2 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

Add Certificate

Wi-Fi WAN CA Certificate

No Certificates defined

Add Certificate

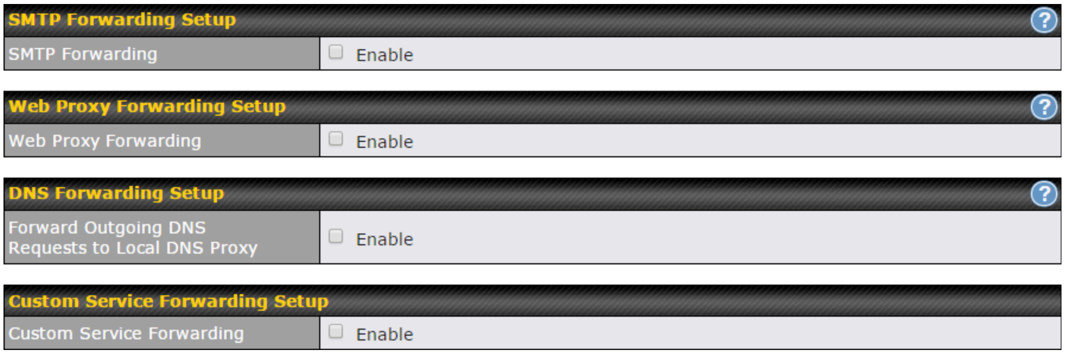
This section allows for certificates to be assigned to the local VPN, Web Admin SSL, Captive Portal SSL, OpenVPN CA, Wi-Fi WAN Client certificate and Wi-Fi WAN CA Certificate.

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/

24.3 Service Forwarding

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



SMTP Forwarding Setup

SMTP Forwarding ☐ Enable

Web Proxy Forwarding Setup

Web Proxy Forwarding ☐ Enable

DNS Forwarding Setup

Forward Outgoing DNS Requests to Local DNS Proxy ☐ Enable

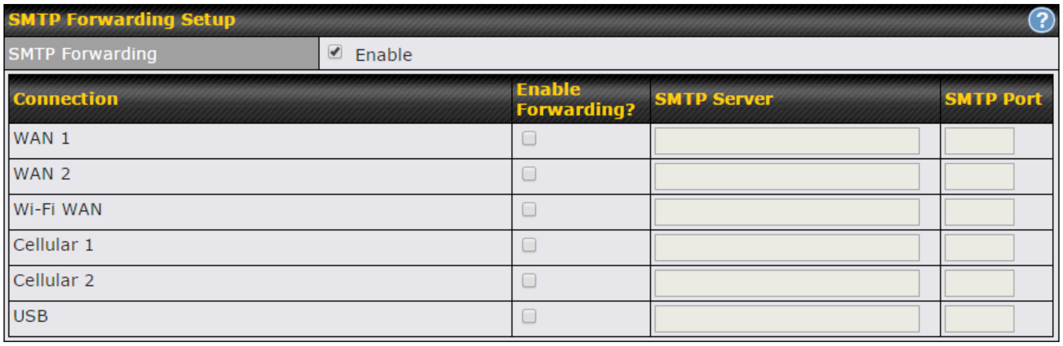
Custom Service Forwarding Setup

Custom Service Forwarding ☐ Enable

Service Forwarding	
SMTP Forwarding	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 **Enable**.
Web Proxy Forwarding	When this option is enabled, all outgoing connections destined for the proxy server specified in **Web Proxy Interception Settings** 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 **Enable**.
DNS Forwarding	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.
Custom Service Forwarding	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.

24.3.1 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	☐		
WAN 2	☐		
Wi-Fi WAN	☐		
Cellular 1	☐		
Cellular 2	☐		
USB	☐		

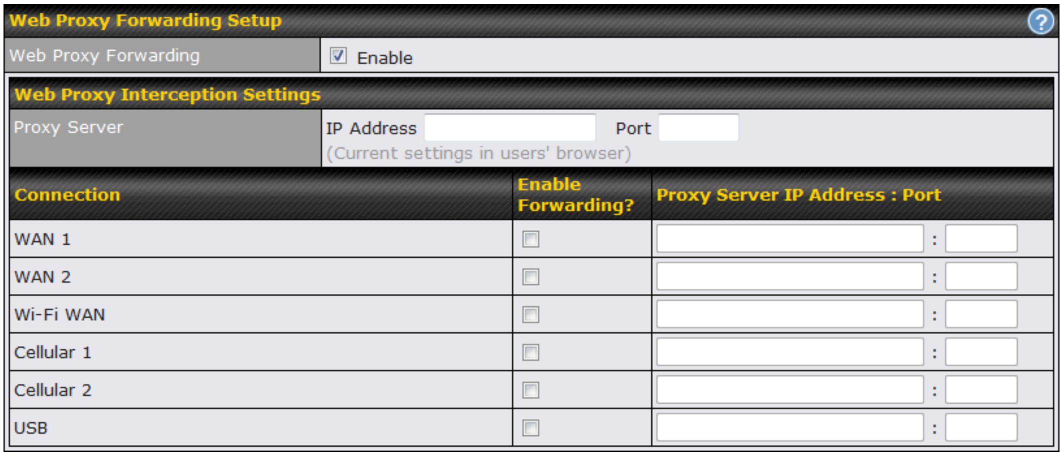
To enable the feature, select **Enable** under **SMTP Forwarding Setup**. Check **Enable Forwarding** for the WAN connection(s) that needs forwarding. Under **SMTP Server**, enter the ISP's e-mail server host name or IP address. Under **SMTP Port**, enter the TCP port number for each WAN.

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**).

24.3.2 Web Proxy Forwarding



Web Proxy Forwarding Setup

Web Proxy Forwarding	☑ Enable

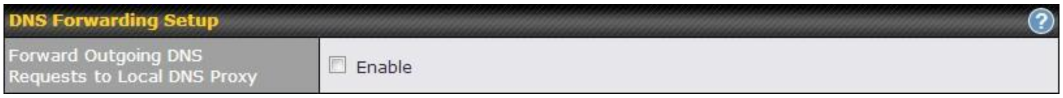
Web Proxy Interception Settings

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

Connection	Enable Forwarding?	Proxy Server IP Address : Port
WAN 1	☐	:
WAN 2	☐	:
Wi-Fi WAN	☐	:
Cellular 1	☐	:
Cellular 2	☐	:
USB	☐	:

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.

24.3.3 DNS Forwarding

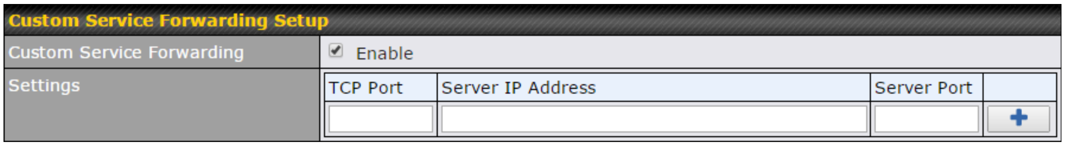


DNS Forwarding Setup

Forward Outgoing DNS Requests to Local DNS Proxy	☐ Enable

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

24.3.4 Custom Service Forwarding



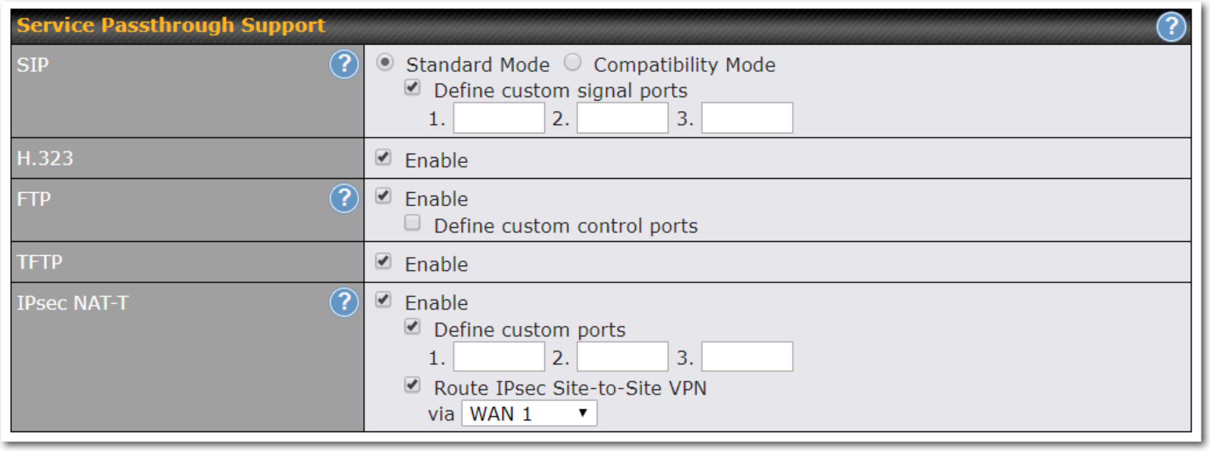
Custom Service Forwarding Setup

Custom Service Forwarding	☑ Enable
Settings	TCP Port / Server IP Address / Server Port

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.

24.4 Service Passthrough

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



Service Passthrough Support

SIP	● Standard Mode ○ Compatibility Mode ☑ Define custom signal ports 1. 2. 3.
H.323	☑ Enable
FTP	☑ Enable ☐ Define custom control ports
TFTP	☑ Enable
IPsec NAT-T	☑ Enable ☑ Define custom ports 1. 2. 3. ☑ Route IPsec Site-to-Site VPN via WAN 1

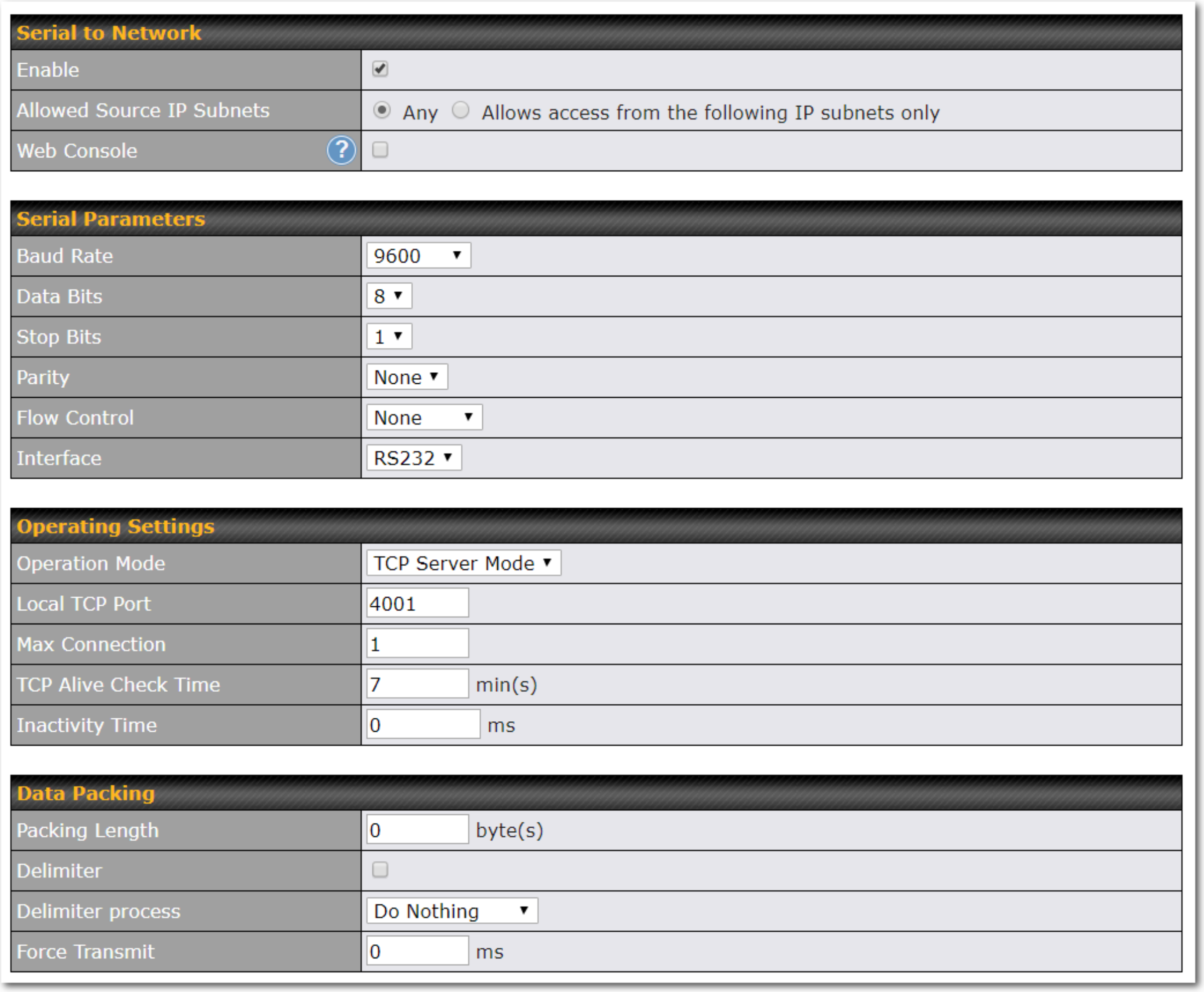
Some Internet services need to be specially handled in a multi-WAN environment. Pepwave routers can handle these services such that Internet applications do not notice being behind a multi-WAN router. Settings for service passthrough support are available here.

Service Passthrough Support	
SIP	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: **Standard Mode** and **Compatibility Mode**. If your SIP server's signal port number is non-standard, you can check the box **Define custom signal ports** and input the port numbers to the text boxes.
H.323	With this option enabled, protocols that provide audio-visual communication sessions will be defined on any packet network and pass through the Pepwave router.
FTP	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 **Define custom control ports** and enter the port numbers in the text boxes.
TFTP	The Pepwave router monitors outgoing TFTP connections and routes any incoming TFTP data packets back to the client. Select **Enable** if you want to enable TFTP passthrough support.
IPsec NAT-T	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 **Define custom ports**. If the VPN contains IPsec site-to-site VPN traffic, check **Route IPsec Site-to-Site VPN** and choose the WAN connection to route the traffic to.

24.5 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	☑
Allowed Source IP Subnets	● Any ○ Allows access from the following IP subnets only
Web Console	☐

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	☐
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	–

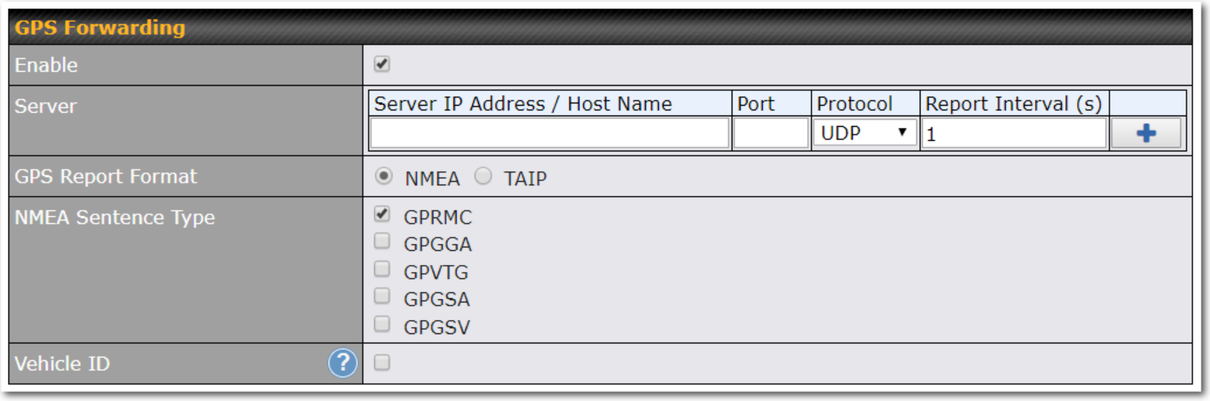
The RS232 serial interface is not an isolated RS232. External galvanic isolation may be added if required.

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.

24.6 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	☑
Server	Server IP Address / Host Name: Port: Protocol: UDP ▾ Report Interval (s): 1 +
GPS Report Format	● NMEA ○ TAIP
NMEA Sentence Type	☑ GPRMC ☐ GPGGA ☐ GPVTG ☐ GPGSA ☐ GPGSV
Vehicle ID ?	☐

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

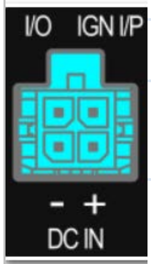
24.7 Ignition Sensing

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

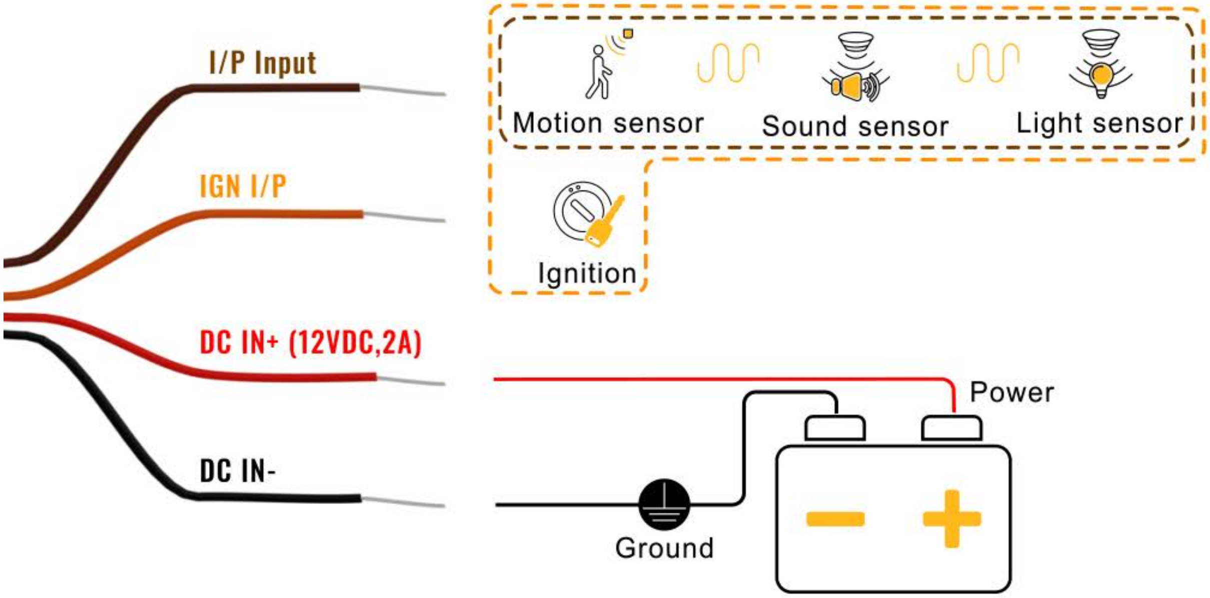
started or turned off.
The time delay setting between ignition off and power down of the router is a configurable setting, which allows the router to stay on for a period of time after the engine of a vehicle is turned off.

Ignition Sensing installation

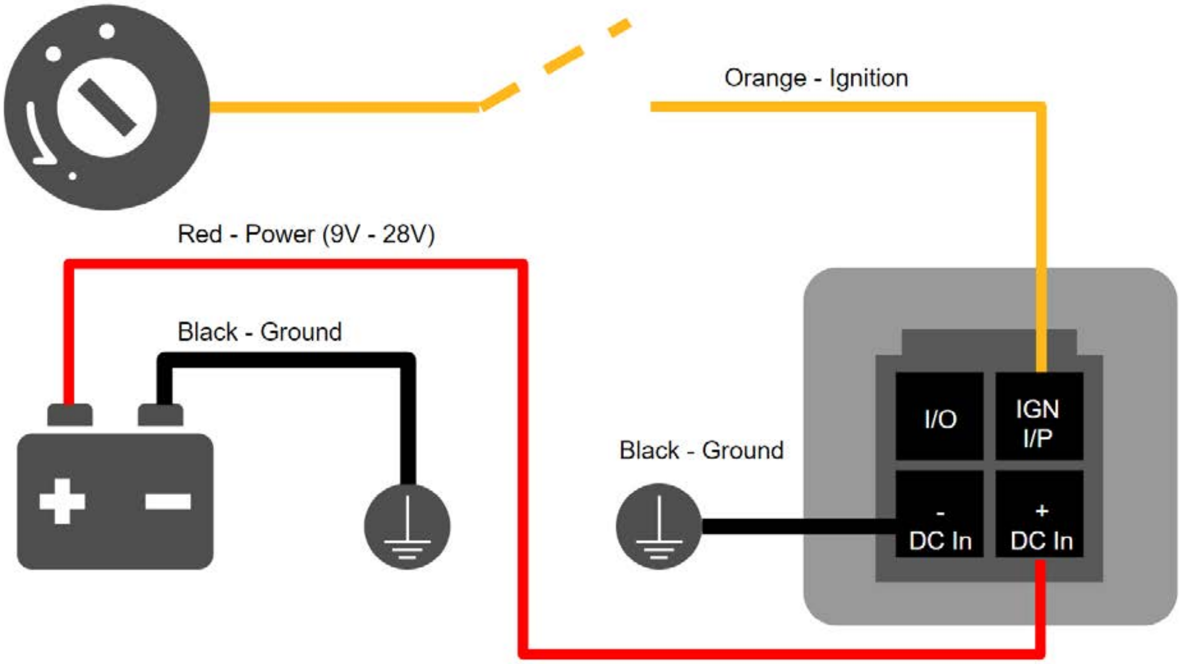
	Functoin		Colour Wire
	**I/O**	optional*	Brown
	IGN I/P	connected to positive feed on the ignition .	Orange
	DC IN -	connected to permanent negative feed (ground)	Black
	DC IN +	connected to permanent positive feed (power 12VDC, 2A)).	Red

I/O
IGN I/P
- +
DC IN

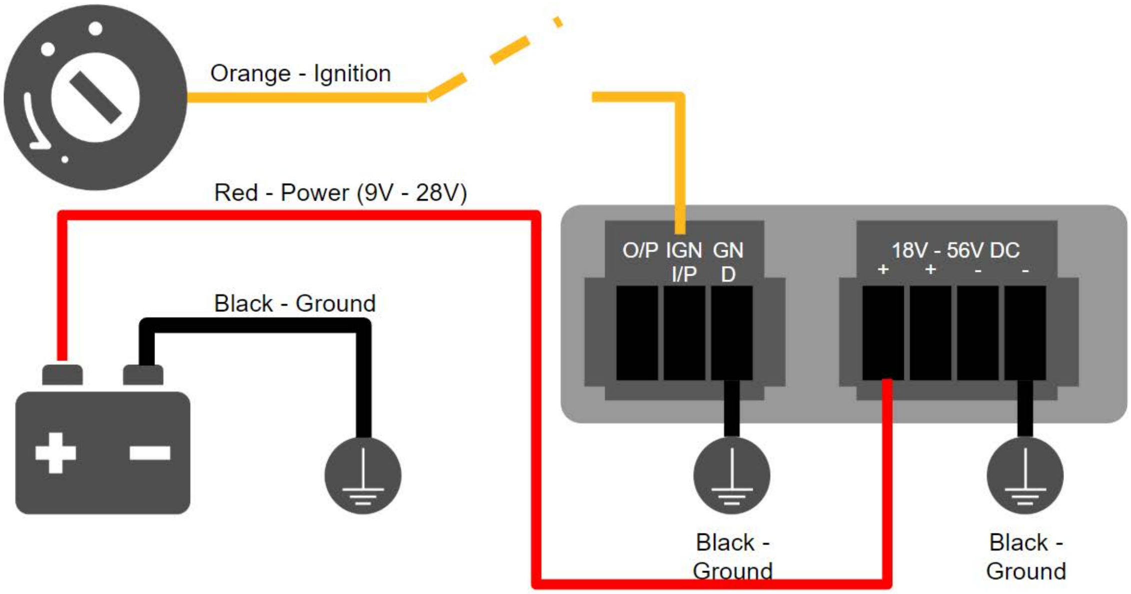
* Currently not functional; will be used for additional features in future firmware


I/P Input
IGN I/P
DC IN+ (12VDC,2A)
DC IN-
Motion sensor
Sound sensor
Light sensor
Ignition
Power
Ground

Connectivity diagram for devices with 4-pin connector


Orange - Ignition
Red - Power (9V - 28V)
Black - Ground
Black - Ground
I/O
IGN I/P
- DC In
+ DC In

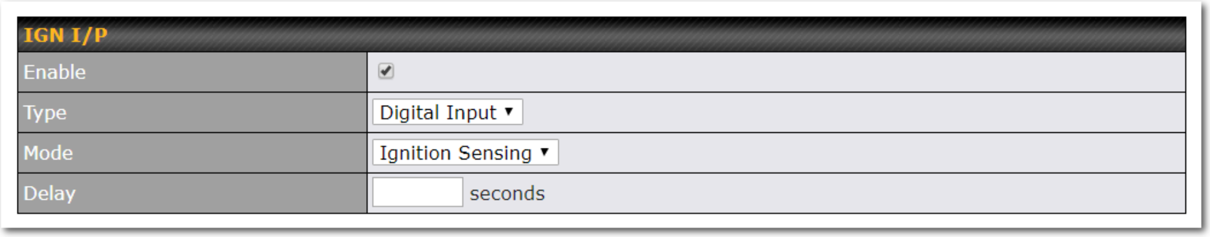
Connectivity diagram for devices with terminal block connection


Orange - Ignition
Red - Power (9V - 28V)
Black - Ground
O/P IGN I/P GND
18V - 56V DC
+ + - -
Black - Ground
Black - Ground

GPIO Menu

Note: This feature is applicable for certain models that come with a GPIO interface.

Ignition Sensing options can be found in **Advanced > GPIO.**
The configurable option for Ignition Input is **Delay;** the time in seconds that the router stays powered on after the ignition is turned off.

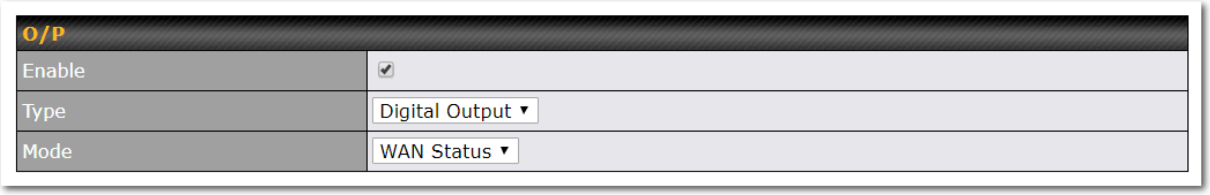


IGN I/P	
Enable	☑
Type	Digital Input ▾
Mode	Ignition Sensing ▾
Delay	seconds

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

Digital Input - the connection supports input sensing; it reads the external input and determines 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).



O/P	
Enable	☑
Type	Digital Output ▾
Mode	WAN Status ▾

Note: The Digital Output state (on/off) upon rebooting the device may vary depending on the model, eg. MAX BR1 MK2 = Persistent; MAX Transit Mini with ContentHub = Reset to default, etc.

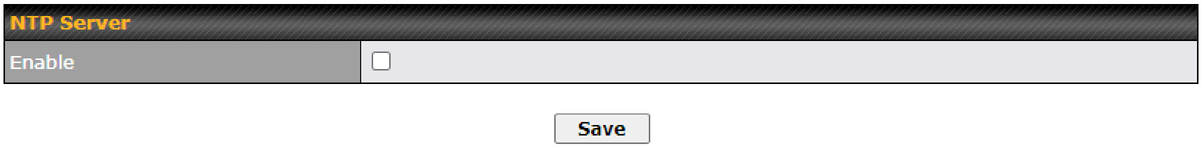
Analog Input - to be confirmed. In most cases, it should read the external input and determine the voltage level.

24.8 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.

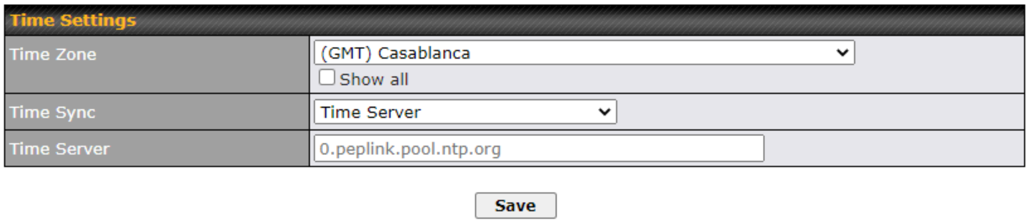
Compatible with: BR1 ENT, 700 HW3, HD2/4, Transit

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



NTP Server	
Enable	☐

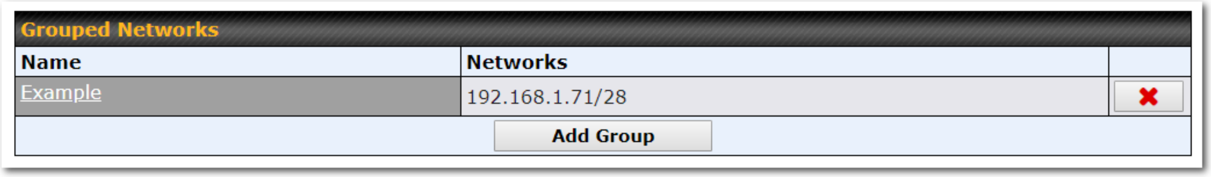
Time Settings can be found at **System>Time>Time Settings**



Time Settings	
Time Zone	(GMT) Casablanca ☐ Show all
Time Sync	Time Server
Time Server	0.peplink.pool.ntp.org

24.9 Grouped Networks

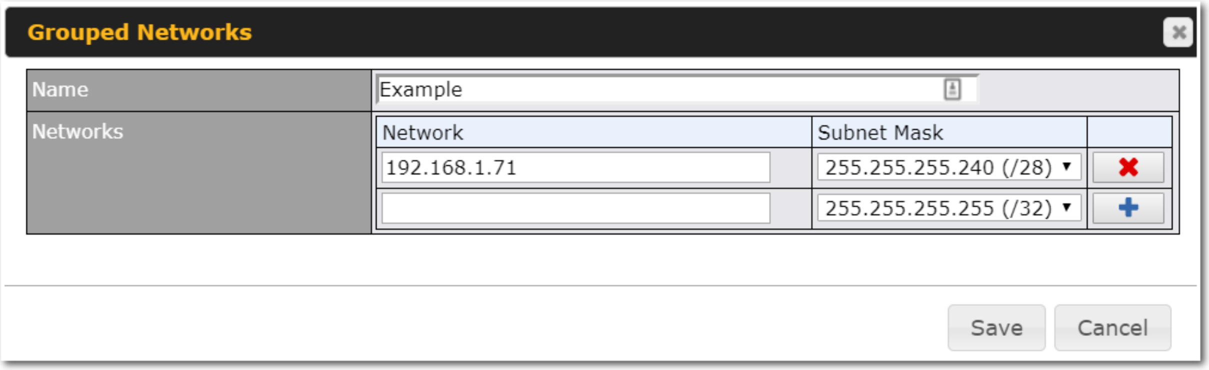
Advanced > Grouped Networks allows to configure destination networks in grouped format.



Grouped Networks

Name	Networks	
Example	192.168.1.71/28	✖

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



Grouped Networks

Name	Example
Networks	

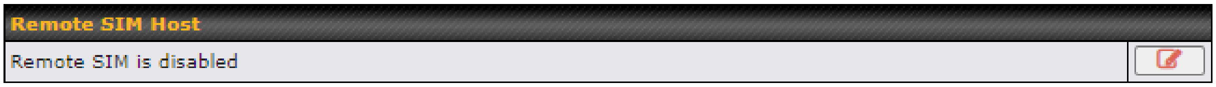
Network	Subnet Mask	
192.168.1.71	255.255.255.240 (/28)	✖
	255.255.255.255 (/32)	✚

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

24.10 Remote SIM Management

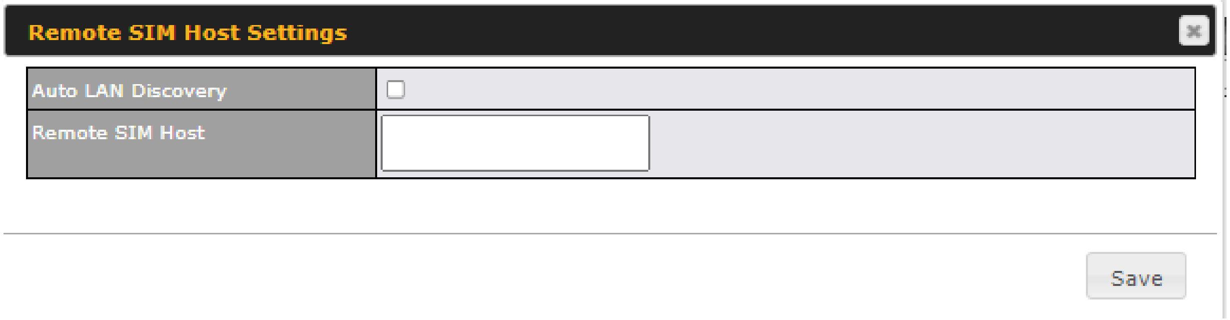
The Remote SIM management is accessible via **Advanced > Misc Settings > Remote SIM Management**. By default, this feature is disabled.

Please note that a limited number of Pepwave routers support the SIM Injector, may refer to the link: https://www.peplink.com/products/sim-injector/ or Appendix B for more details on FusionSIM Manual.


Remote SIM Host

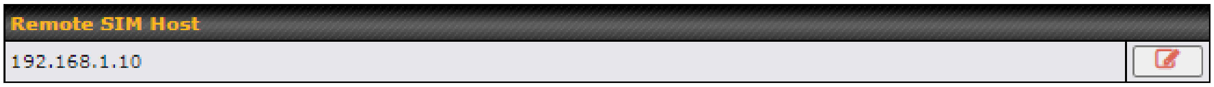
Remote SIM is disabled

Remote SIM Host Settings

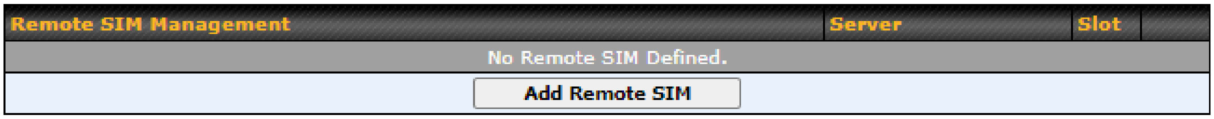

Remote SIM Host Settings

Auto LAN Discovery	☐
Remote SIM Host	

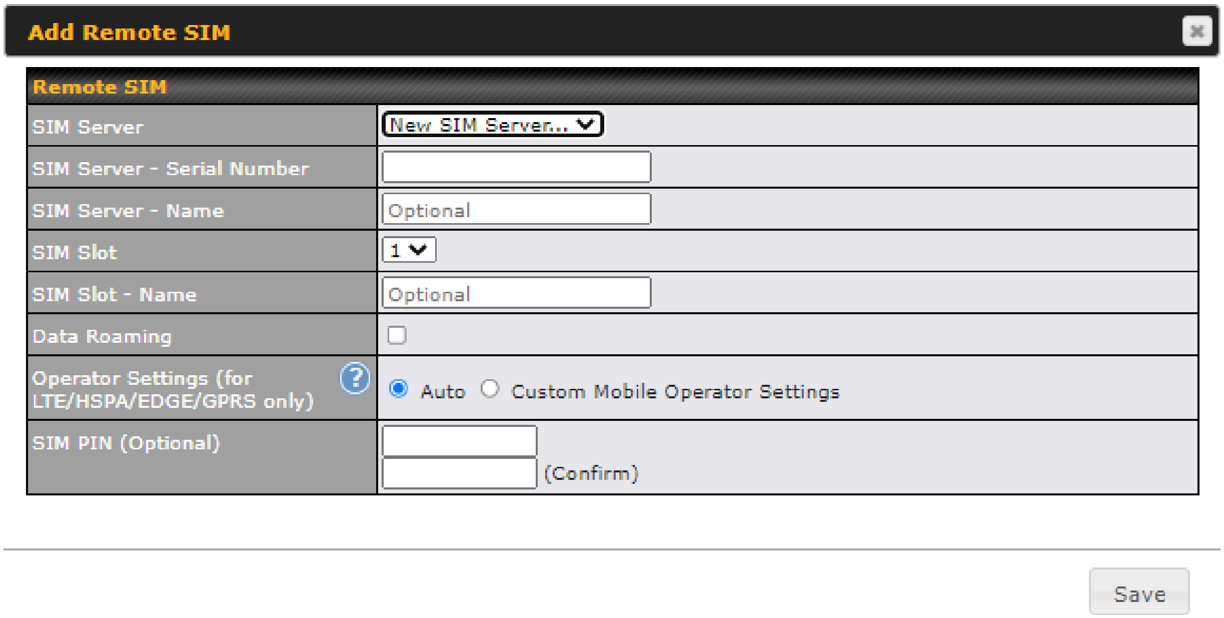
Remote SIM Host Settings	
Active LAN Discovery	Check this box to enable Auto LAN discovery of the remote SIM server..
Remote SIM Host	Enter the public IP address of the SIM Injector. If you enter IP addresses here, it is not necessary to tick the "**Auto LAN Discovery**" box above.


Remote SIM Host

192.168.1.10


Remote SIM Management	Server	Slot
No Remote SIM Defined.		

You may define the Remote SIM information by clicking the "**Add Remote SIM**". Here, you can enable **Data Roaming** and **custom APN** for your SIM cards.



Add Remote SIM

Remote SIM

SIM Server	New SIM Server...
SIM Server - Serial Number	
SIM Server - Name	Optional
SIM Slot	1
SIM Slot - Name	Optional
Data Roaming	☐
Operator Settings (for LTE/HSPA/EDGE/GPRS only)	● Auto ○ Custom Mobile Operator Settings
SIM PIN (Optional)	 (Confirm)

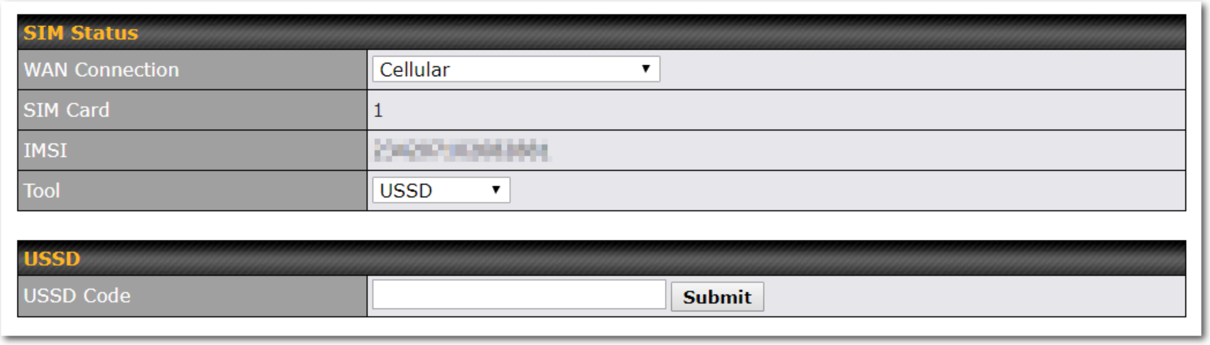
Add Remote SIM Settings	
SIM Server	Add a new SIM Server
SIM Server - Serial Number	Enter the serial number of SIM Server
SIM Server - Name	This optional field allows you define a name for the SIM Server
SIM Slot	Click the drop-down menu and choose which SIM slot you want to connect.
SIM Slot - Name	This optional field allows you define a name for the SIM slot.
Data Roaming	Enables data roaming on this particular SIM card.
Operator Settings (for LTE//HSPA/EDGE/GPRS Only)	This setting allows you to configure the APN settings of your connection. If **Auto** is selected, the mobile operator should be detected automatically. The connected device will be configured and connection will be made automatically. If there is any difficulty in making a connection, you may select **Custom** to enter your carrier’s APN, Username and Password settings manually. The correct values can be obtained from your carrier. The default and recommended setting is Auto.

24.11 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.



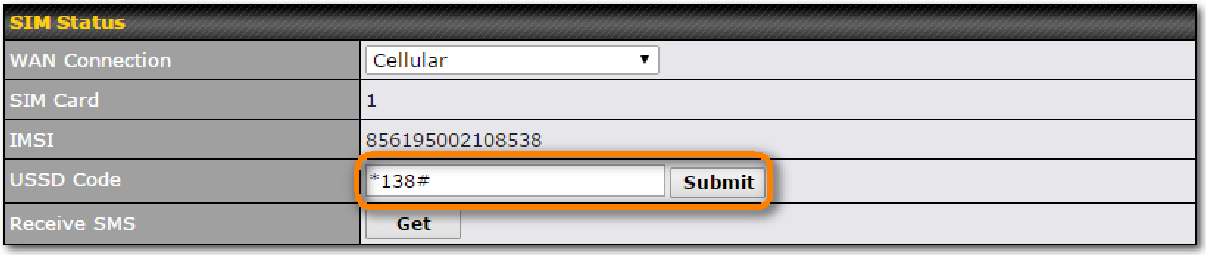
SIM Status

WAN Connection	Cellular
SIM Card	1
IMSI	[redacted]
Tool	USSD

USSD

USSD Code	Submit

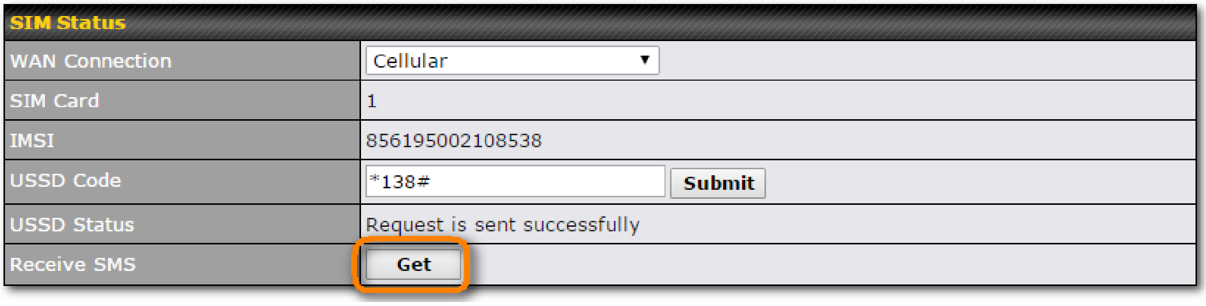
Enter your USSD code under the **USSD Code** text field and click **Submit**.



SIM Status

WAN Connection	Cellular
SIM Card	1
IMSI	856195002108538
USSD Code	*138# Submit
Receive SMS	Get

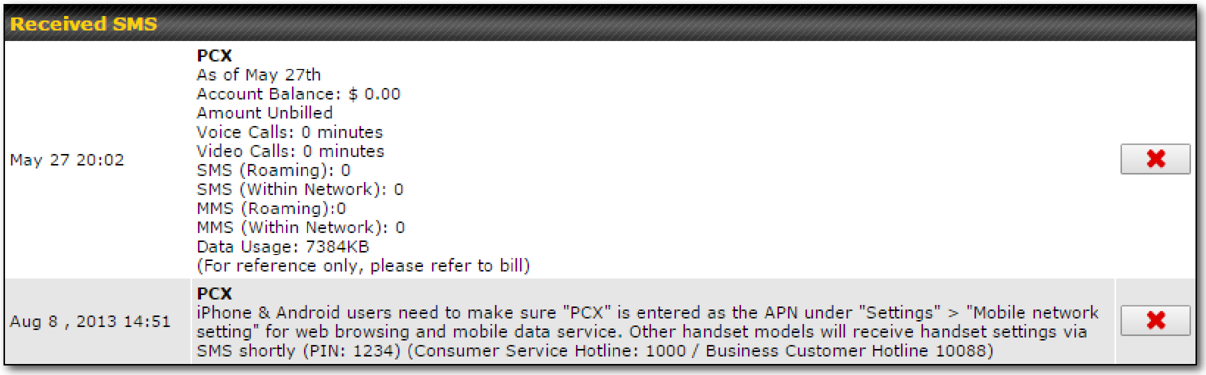
You will receive a confirmation. To check the SMS response, click **Get**.



SIM Status

WAN Connection	Cellular
SIM Card	1
IMSI	856195002108538
USSD Code	*138# Submit
USSD Status	Request is sent successfully
Receive SMS	Get

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

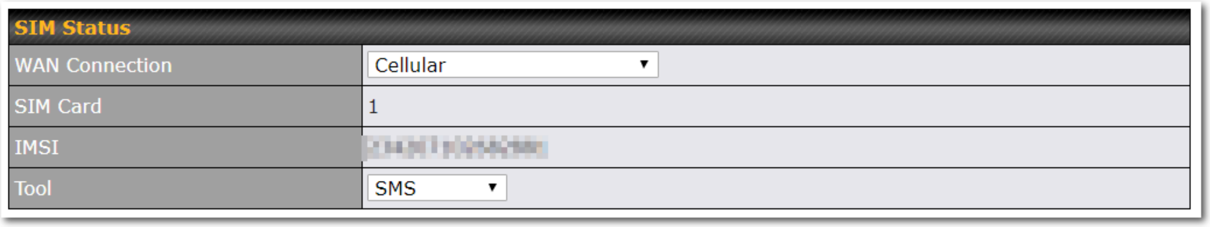


Received SMS

May 27 20:02	**PCX** 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	**PCX** 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)	✖

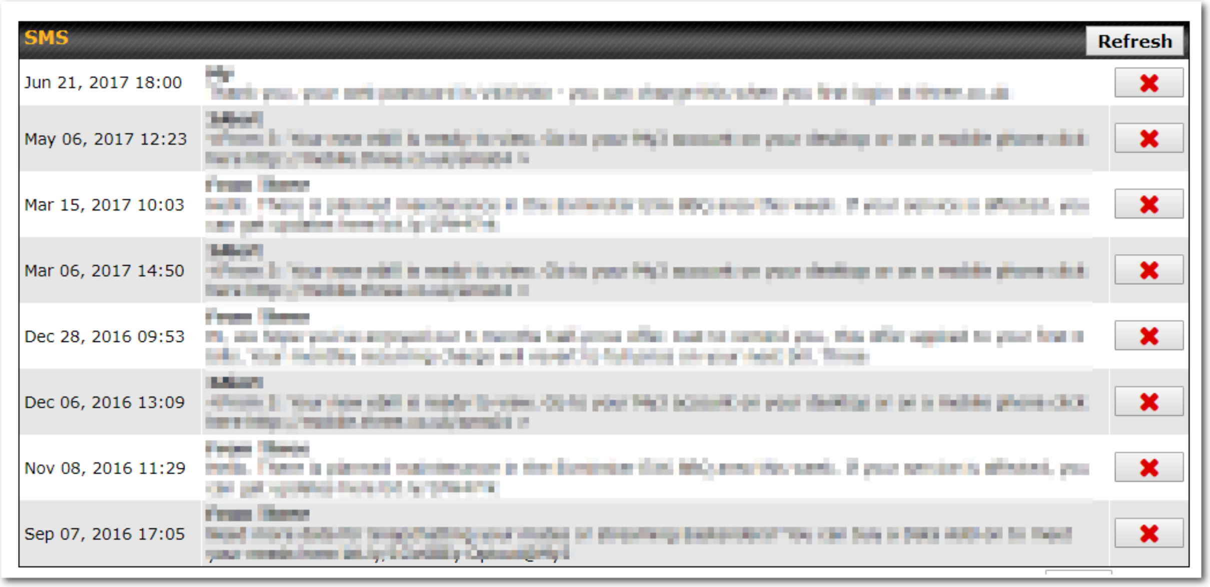
SMS

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



SIM Status

WAN Connection	Cellular ▾
SIM Card	1
IMSI	[redacted]
Tool	SMS ▾



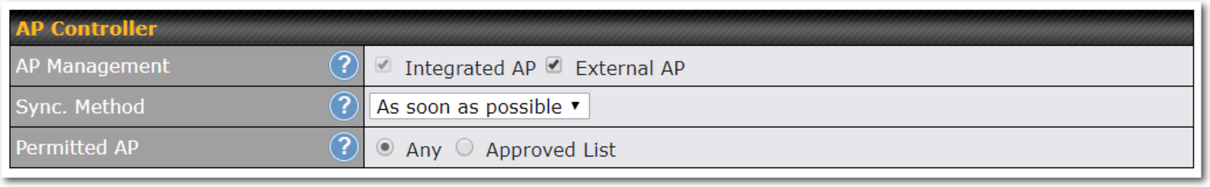
SMS Refresh

Jun 21, 2017 18:00	[redacted]	✖
May 06, 2017 12:23	[redacted]	✖
Mar 15, 2017 10:03	[redacted]	✖
Mar 06, 2017 14:50	[redacted]	✖
Dec 28, 2016 09:53	[redacted]	✖
Dec 06, 2016 13:09	[redacted]	✖
Nov 08, 2016 11:29	[redacted]	✖
Sep 07, 2016 17:05	[redacted]	✖

25 AP

25.1 AP Controller

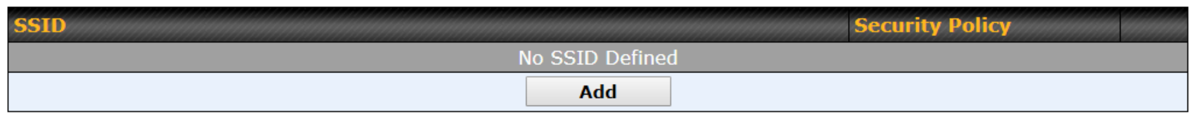
The AP controller acts as a centralized controller of Pepwave Access Points.
With this feature, users can customize and manage up to 1500 Access Points from a single Pepwave router interface.
To configure, navigate to the **AP** tab. and the following screen appears.



AP Controller	
AP Management	☑ Integrated AP ☑ External AP
Sync. Method	As soon as possible ▾
Permitted AP	● Any ○ Approved List

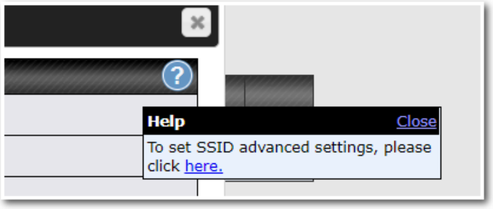
AP Controller	
AP Management	The AP controller for managing Pepwave APs can be enabled by checking this box. When this option is enabled, the AP controller will wait for management connections originating from APs over the LAN on TCP and UDP port 11753. It will also wait for captive portal connections on TCP port 443. An extended DHCP option, **CAPWAP Access Controller addresses** (field 138), will be added to the DHCP server. A local DNS record, **AP Controller**, will be added to the local DNS proxy.
Sync Method	● As soon as possible ● Progressively ● One at a time
Permitted AP	Access points to manage can be specified here. If **Any** is selected, the AP controller will manage any AP that reports to it. If **Approved List** is selected, only APs with serial numbers listed in the provided text box will be managed.

25.2 Wireless SSID



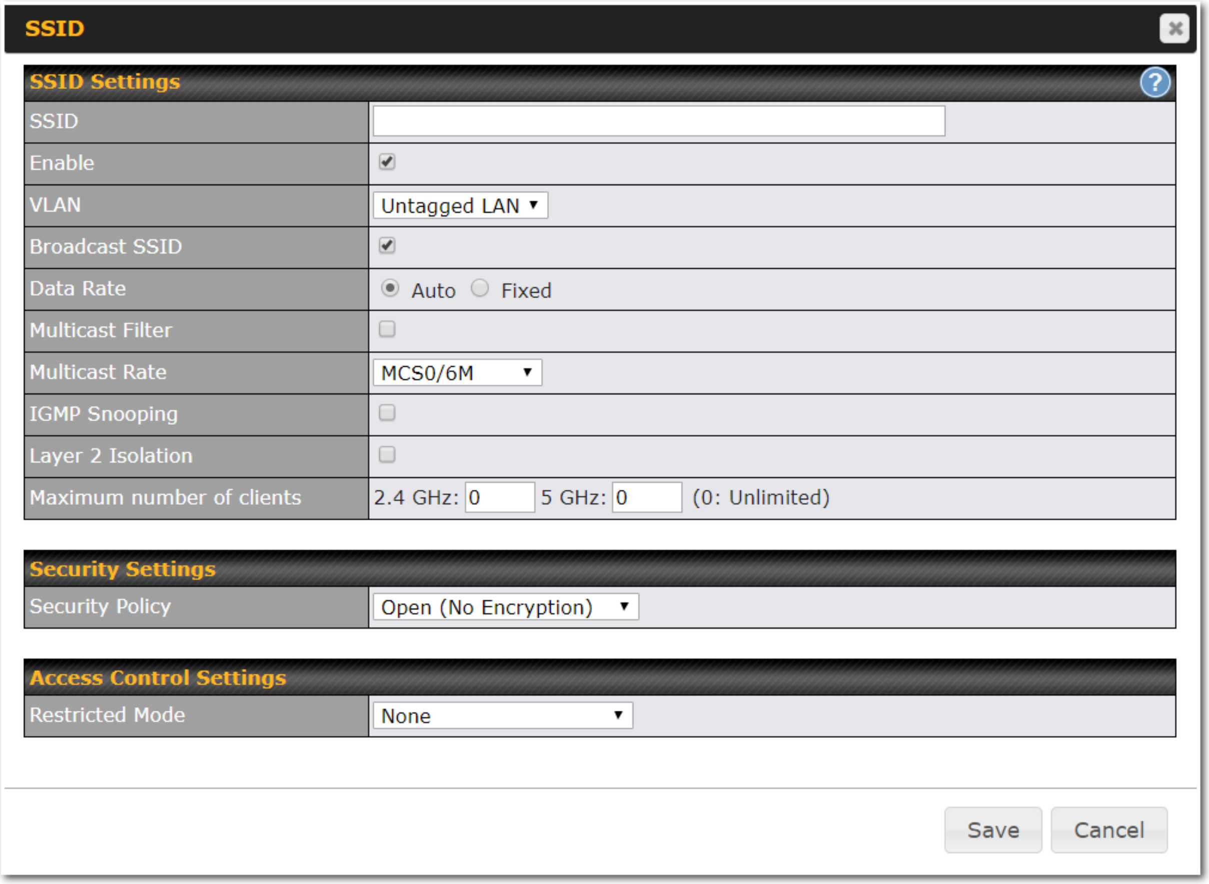
SSID	Security Policy
No SSID Defined	

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 ishows a new SSID window with Advanced Settings enabled (these are available by selecting the question mark in the top right corner).



Help Close

To set SSID advanced settings, please click here.



SSID

SSID Settings

SSID	
Enable	☑
VLAN	Untagged LAN ▾
Broadcast SSID	☑
Data Rate	● Auto ○ Fixed
Multicast Filter	☐
Multicast Rate	MCS0/6M ▾
IGMP Snooping	☐
Layer 2 Isolation	☐
Maximum number of clients	2.4 GHz: 0 5 GHz: 0 (0: Unlimited)

Security Settings

Security Policy	Open (No Encryption) ▾

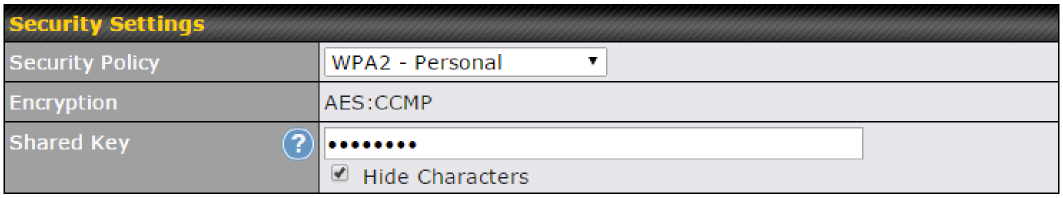
Access Control Settings

Restricted Mode	None ▾

SSID Settings	
SSID	This setting specifies the SSID of the virtual AP to be scanned by Wi-Fi clients.
Enable	Click the drop-down menu to apply a time schedule to this interface
VLAN	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 **0**, which means VLAN tagging is disabled (instead of tagged with zero).

Broadcast SSID	This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. **Broadcast SSID** is enabled by default.
Data Rate [A]	Select **Auto** to allow the Pepwave router to set the data rate automatically, or select **Fixed** and choose a rate from the displayed drop-down menu.
Multicast Filter[A]	This setting enables the filtering of multicast network traffic to the wireless SSID.
Multicast Rate[A]	This setting specifies the transmit rate to be used for sending multicast network traffic. The selected **Protocol** and **Channel Bonding** settings will affect the rate options and values available here.
IGMP Snooping [A]	To allow the Pepwave router to listen to internet group management protocol (IGMP) network traffic, select this option.
DHCP Option 82 [A]	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.
Layer 2 Isolation [A]	**Layer 2** 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.
Maximum Number of Clients	Indicate the maximum number of clients that should be able to connect to each frequency.

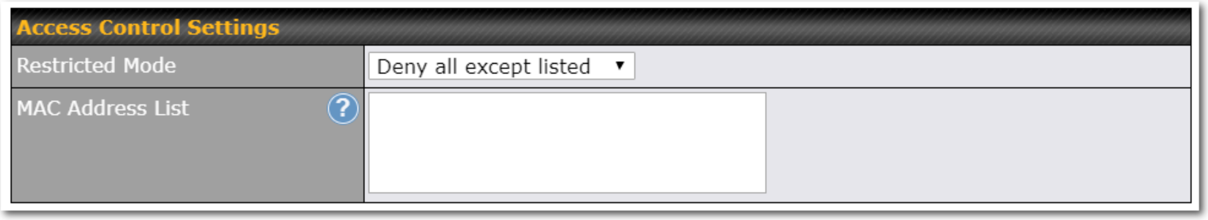
[A] - Advanced feature. Click the ? button on the top right-hand corner to activate.



Security Settings	
Security Policy	WPA2 - Personal ▾
Encryption	AES:CCMP
Shared Key ?	•••••••• ☑ Hide Characters

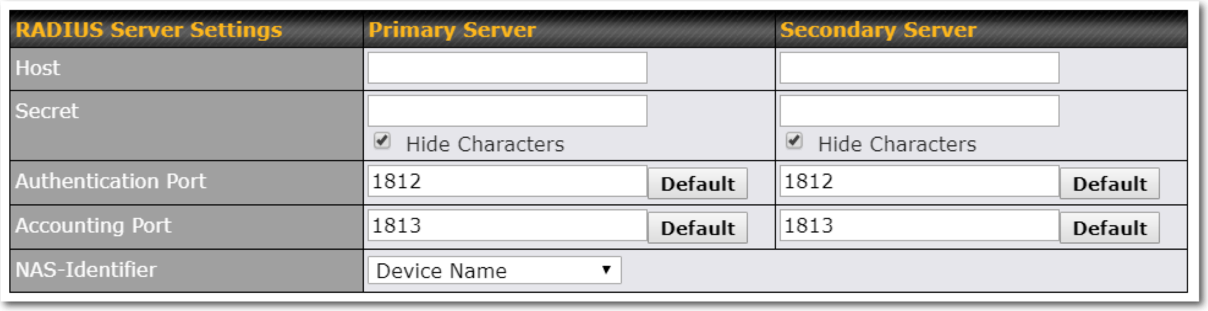
Security Settings	
Security Policy	This setting configures the wireless authentication and encryption methods. Available options : ● **Open** (No Encryption) ● **WPA3 -Personal** (AES:CCMP) ● **WPA2/WPA3 -Personal** (AES:CCMP) ● **WPA2 -Personal** (AES:CCMP) ● **WPA2 – Enterprise** ● **WPA/WPA2 - Personal** (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 ?	

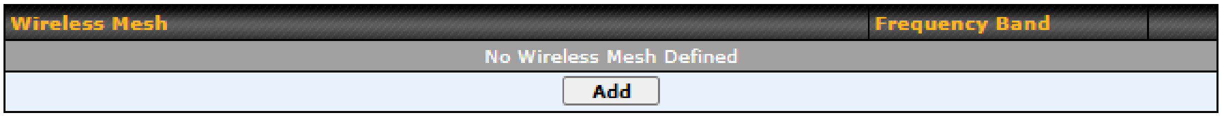
Access Control	
Restricted Mode	The settings allow the administrator to control access using MAC address filtering. Available options are **None**, **Deny all except listed**, and **Accept all except listed**
MAC Address List	Connection coming from the MAC addresses in this list will be either denied 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		
Secret	☑ Hide Characters	☑ Hide Characters
Authentication Port	1812 Default	1812 Default
Accounting Port	1813 Default	1813 Default
NAS-Identifier	Device Name ▾	

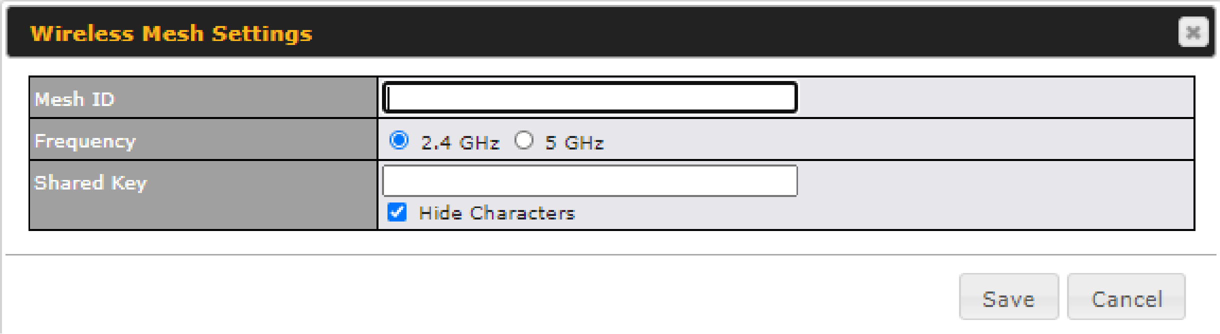
RADIUS Server Settings	
Host	Enter the IP address of the primary RADIUS server and, if applicable, the secondary RADIUS server.
Secret	Enter the RADIUS shared secret for the primary server and, if applicable, the secondary RADIUS server.
Authentication Port	In the field, enter the UDP authentication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

25.3 Wireless Mesh



Wireless Mesh Support is available on devices running 802.11ac (Wi-Fi 5) and above. Along with the AP Controller, mesh network extensions can be established, which can expand network coverage. Note that the Wireless Mesh settings need to match the Mesh ID and Shared Key of the other devices on the same selected frequency band.

To create a new Wireless Mesh profile, go to **AP** > **Wireless Mesh**, and click **Add**.



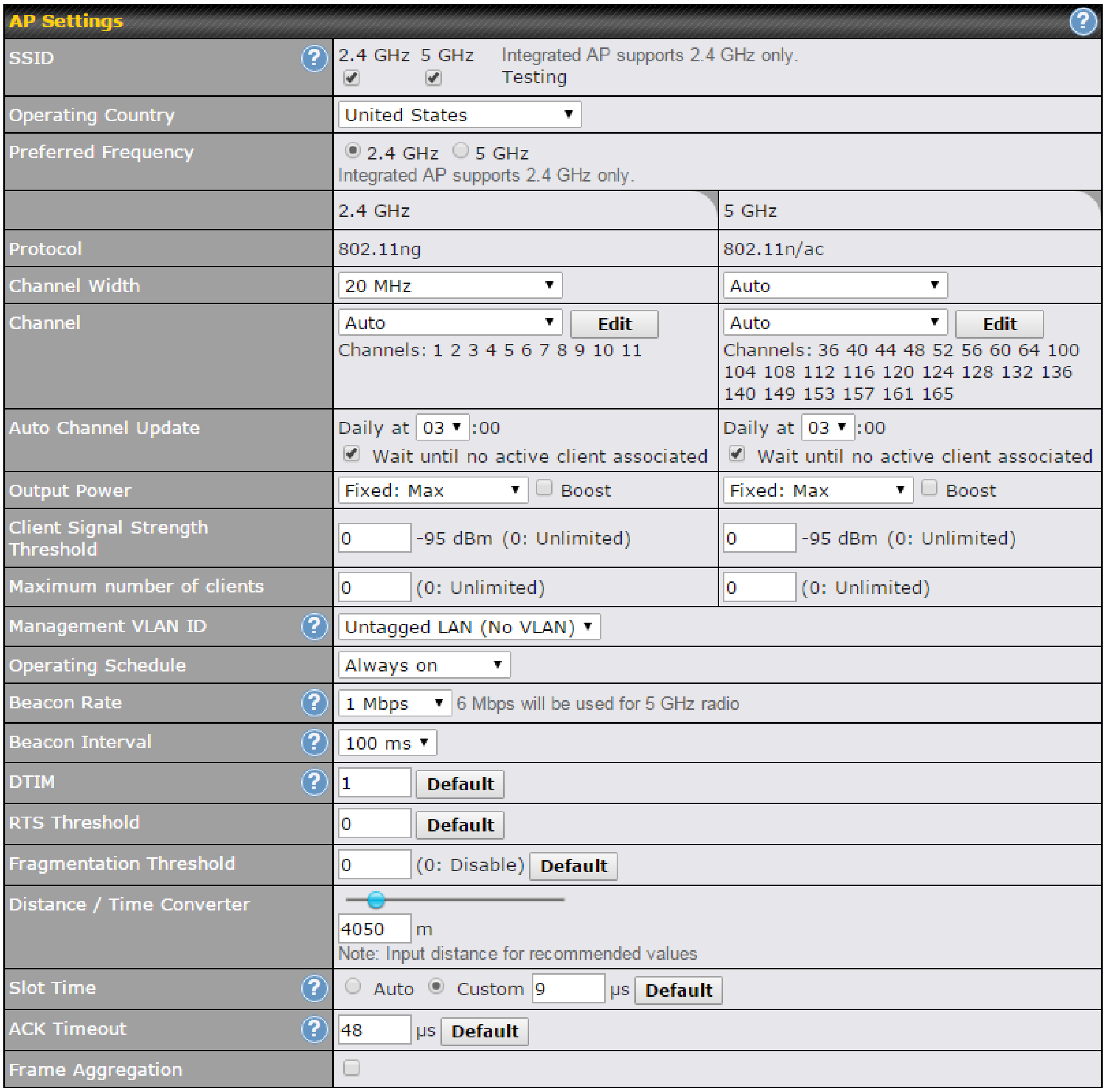
Mesh ID	
Frequency	● 2.4 GHz ○ 5 GHz
Shared Key	☑ Hide Characters

Wireless Mesh Settings	
Mesh ID	Enter a name to represent the Mesh profile.

Frequency	Select the 2.4GHz or 5GHz frequency to be used.
Shared Key	Enter the shared key in the text field. Please note that it needs to match the shared keys of the other APs in the Wireless Mesh settings. Click **Hide / Show Characters** to toggle visibility.

25.4 Settings

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



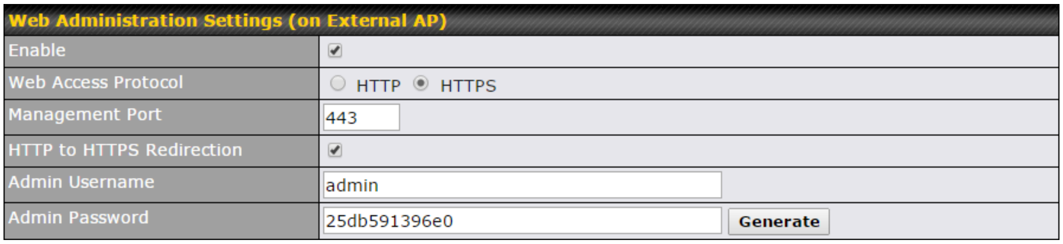
AP Settings

SSID	2.4 GHz ☑ 5 GHz ☑ Integrated AP supports 2.4 GHz only. Testing	
Operating Country	United States ▾	
Preferred Frequency	● 2.4 GHz ○ 5 GHz Integrated AP supports 2.4 GHz only.	
	2.4 GHz	5 GHz
Protocol	802.11ng	802.11n/ac
Channel Width	20 MHz ▾	Auto ▾
Channel	Auto ▾ Edit Channels: 1 2 3 4 5 6 7 8 9 10 11	Auto ▾ 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 ☑ Wait until no active client associated	Daily at 03 ▾ :00 ☑ Wait until no active client associated
Output Power	Fixed: Max ▾ ☐ Boost	Fixed: Max ▾ ☐ 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)
Management VLAN ID	Untagged LAN (No VLAN) ▾	
Operating Schedule	Always on ▾	
Beacon Rate	1 Mbps ▾ 6 Mbps will be used for 5 GHz radio	
Beacon Interval	100 ms ▾	
DTIM	1 Default	
RTS Threshold	0 Default	
Fragmentation Threshold	0 (0: Disable) Default	
Distance / Time Converter	4050 m Note: Input distance for recommended values	
Slot Time	○ Auto ● Custom 9 μs Default	
ACK Timeout	48 μs Default	
Frame Aggregation	☐	

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 Pepwave MAX 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 should follow. ● 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). ● If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW). Note: Users are required to choose an option suitable to local laws and regulations. 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.
Preferred Frequency	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.
Protocol	This section displays the 2.4 GHz protocols your APs are using.
Channel Width	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.
Channel	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 **Auto** is set, the system will perform channel scanning based on the scheduled time set and choose the most suitable channel automatically.
Auto Channel Update	Indicate the time of day at which update automatic channel selection.
Output Power^{A}	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 **Dynamic** settings are selected, the AP will adjust its power level based on its surrounding APs in order to maximize performance. The **Dynamic: Auto** setting will set the AP to do this automatically. Otherwise, the **Dynamic: Manual** setting will set the AP to dynamically adjust only if instructed to do so. If you have set **Dynamic:Manual**, you can go to **AP>Toolbox>Auto Power Adj.** to give your AP further instructions.

	If you click the **Boost** 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.
Client Signal Strength Threshold[A]	This field determines that maximum signal strength each individual client will receive. The measurement unit is megawatts.
Max number of Clients[A]	This field determines the maximum clients that can be connected to APs under this profile.
Management VLAN ID	This field specifies the VLAN ID to tag to management traffic, such as AP to AP controller communication traffic. The value is **0** 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.
Operating Schedule	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.
Beacon Rate[A]	This drop-down menu provides the option to send beacons in different transmit bit rates. The bit rates are **1Mbps**, **2Mbps**, **5.5Mbps**, **6Mbps**, and **11Mbps**.
Beacon Interval[A]	This drop-down menu provides the option to set the time between each beacon send. Available options are **100ms**, **250ms**, and **500ms**.
DTIM[A]	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.
RTS Threshold[A]	This field provides the option to set the minimum packet size for the unit to send an RTS using the RTS/CTS handshake. Setting **0** disables this feature.
Fragmentation Threshold[A]	Determines the maximum size (in bytes) that each packet fragment will be broken down into. Set 0 to disable fragmentation.
Distance/Time Converter[A]	Select the distance you want your Wi-Fi to cover in order to adjust the below parameters. Default values are recommended.
Slot Time[A]	This field provides the option to modify the unit wait time before it transmits. The default value is **9μs.**
ACK Timeout[A]	This field provides the option to set the wait time to receive acknowledgement packet before doing retransmission. The default value is **48μs.**
Frame Aggregation[A]	With this feature enabled, throughput will be increased by sending two or more data frames in a single transmission.
Frame Length	This field is only available when **Frame Aggregation** is enabled. It specifies the frame length for frame aggregation. By default, it is set to **50000**.

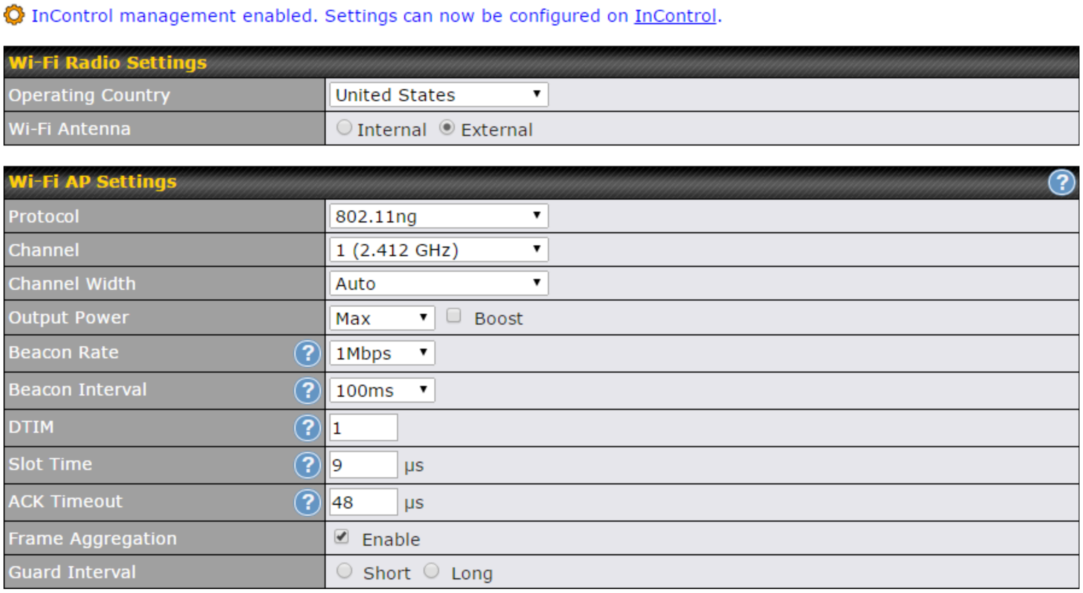
[A] - Advanced feature. Click the ? button on the top right-hand corner to activate.



Web Administration Settings (on External AP)	
Enable	☑
Web Access Protocol	○ HTTP ● HTTPS
Management Port	443
HTTP to HTTPS Redirection	☑
Admin Username	admin
Admin Password	25db591396e0 Generate

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

Wi-Fi AP Settings	
Protocol	802.11ng
Channel	1 (2.412 GHz)
Channel Width	Auto
Output Power	Max ☐ Boost
Beacon Rate	1Mbps
Beacon Interval	100ms
DTIM	1
Slot Time	9 µs
ACK Timeout	48 µs
Frame Aggregation	☑ Enable
Guard Interval	○ Short ○ 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.

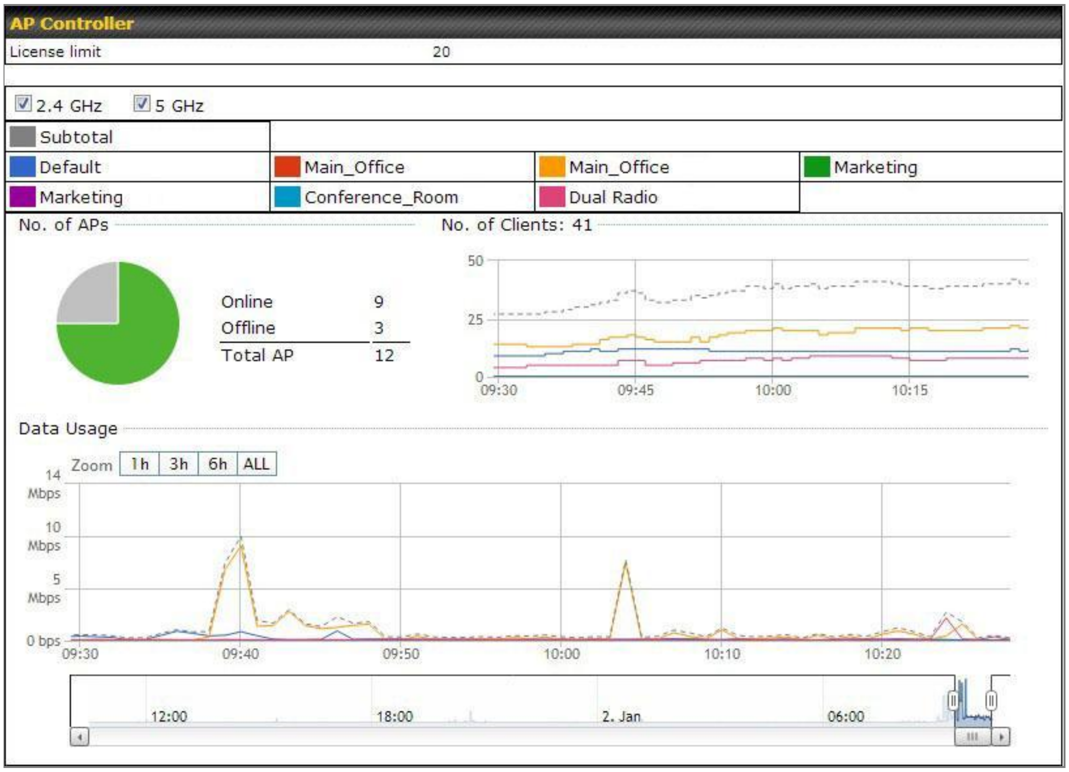
Beacon Rate[A]	This option is for setting the transmit bit rate for sending a beacon. By default, **1Mbps** is selected.
Beacon Interval[A]	This option is for setting the time interval between each beacon. By default, **100ms** is selected.
DTIM[A]	This field allows you to set the frequency for the beacon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

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

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

License limit	20

☑ 2.4 GHz ☑ 5 GHz

⬛ Subtotal			
🟦 Default	🟥 Main_Office	🟧 Main_Office	🟩 Marketing
🟪 Marketing	🟦 Conference_Room	🟥 Dual Radio	

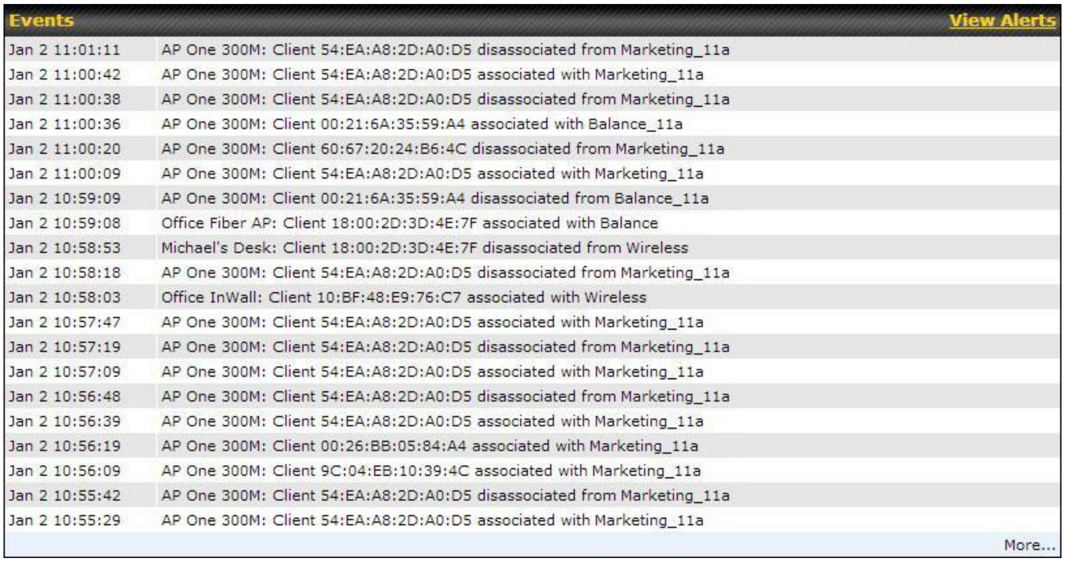
No. of APs

Online	9
Offline	3
Total AP	12

No. of Clients: 41

AP Controller	
License Limit	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.
Frequency	Underneath, there are two check boxes labeled **2.4 Ghz** and **5 Ghz**. 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.
SSID	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.
No. of APs	This pie chart and table indicates how many APs are online and how many are offline.
No.of Clients	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.
Data Usage	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 **Zoom** to select the time scale you wish to view. In addition, you could use the sliders at the bottom to further refine your timescale.

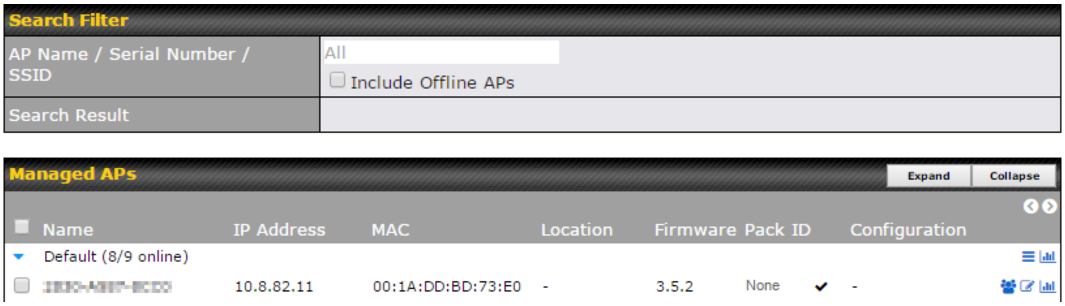


```
Jan 2 11:01:11   AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a
Jan 2 11:00:42   AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a
Jan 2 11:00:38   AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a
Jan 2 11:00:36   AP One 300M: Client 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
```

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 ☐ Include Offline APs
Search Result	

Managed APs

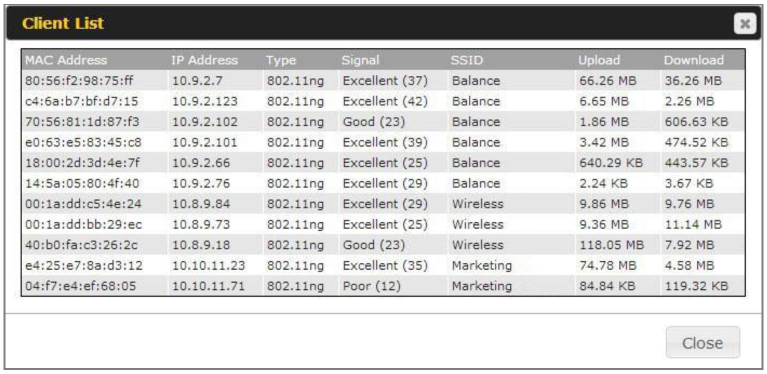
☐	Name	IP Address	MAC	Location	Firmware	Pack ID		Configuration
▾	Default (8/9 online)							
☐	[redacted]	10.8.82.11	00:1A:DD:BD:73:E0	-	3.5.2	None	✓	-

<table>
<tr><th colspan="2">Usage</th></tr>
<tr><td>AP Name/Serial Number</td><td>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.</td></tr>
<tr><td>Online Status</td><td>This button toggles whether your search will include offline devices.</td></tr>
<tr><td>Managed Wireless Devices</td><td>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.

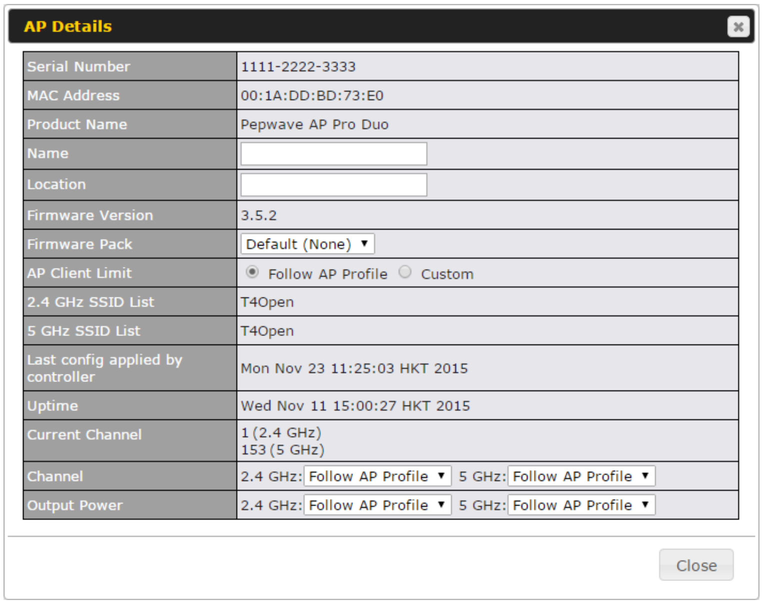
You could also expand and collapse all groups by using the Expand Collapse buttons.

On the right of the table, you will see the following icons: 👥 ✎ 📊 .

Click the 👥 icon to see a usage table for each client:


Client List
<table>
<tr><th>MAC Address</th><th>IP Address</th><th>Type</th><th>Signal</th><th>SSID</th><th>Upload</th><th>Download</th></tr>
<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></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></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></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></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></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></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></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></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></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></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></tr>
</table>

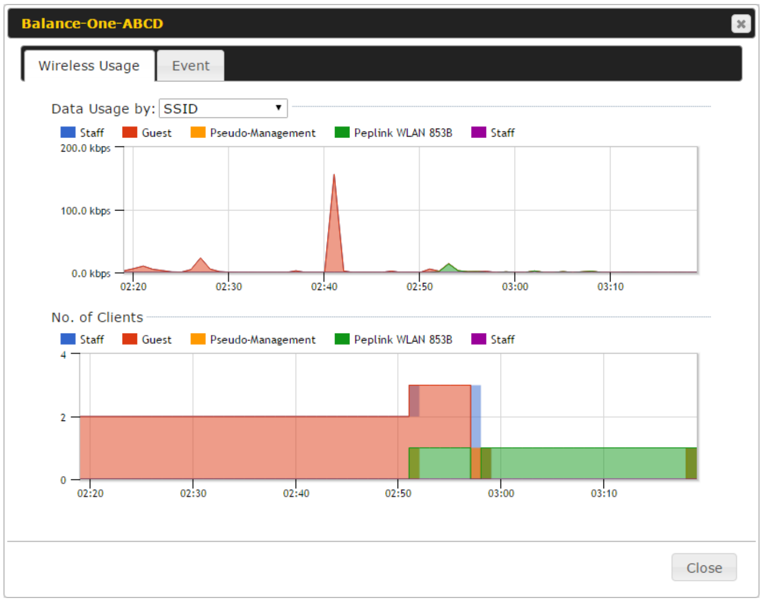
Click the ✎ icon to configure each client</td></tr>
</table>


AP Details
Close

Serial Number	1111-2222-3333
MAC Address	00:1A:DD:BD:73:E0
Product Name	Pepwave AP Pro Duo
Name	
Location	
Firmware Version	3.5.2
Firmware Pack	Default (None) ▾
AP Client Limit	● Follow AP Profile ○ 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 ▾

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.

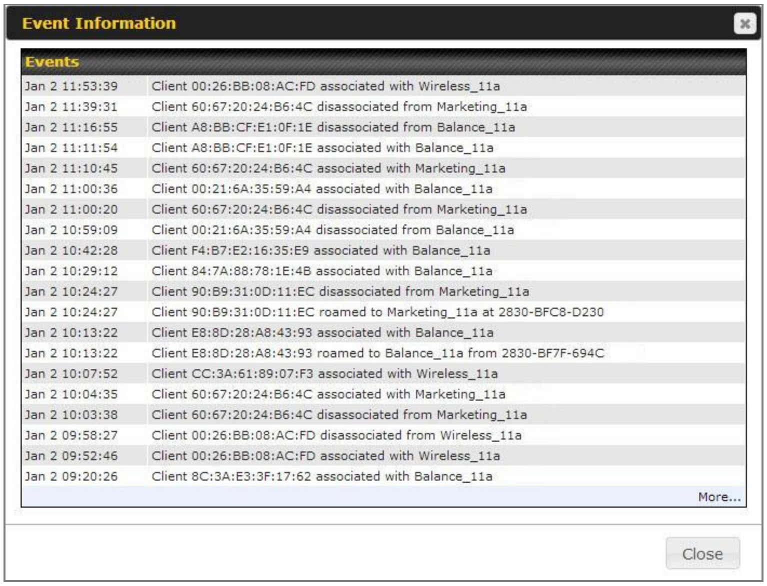
Click the 📊 icon to see a graph displaying usage:


Balance-One-ABCD
Wireless Usage
Event
Staff
Guest
Pseudo-Management
Peplink WLAN 853B
Staff
200.0 kbps
100.0 kbps
0.0 kbps
02:20
02:30
02:40
02:50
03:00
03:10
No. of Clients
Staff
Guest
Pseudo-Management
Peplink WLAN 853B
Staff
4
2
0
02:20
02:30
02:40
02:50
03:00
03:10
Close

Data Usage by: SSID ▾

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:



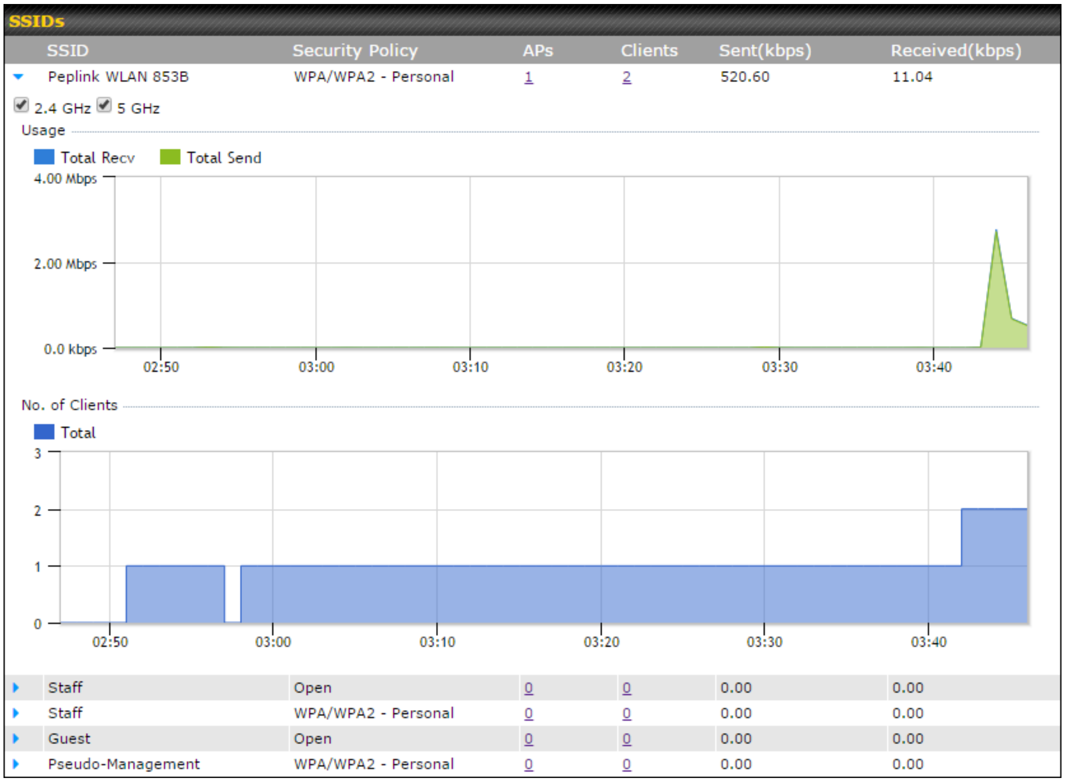
Events

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...

26.3 Wireless SSID

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



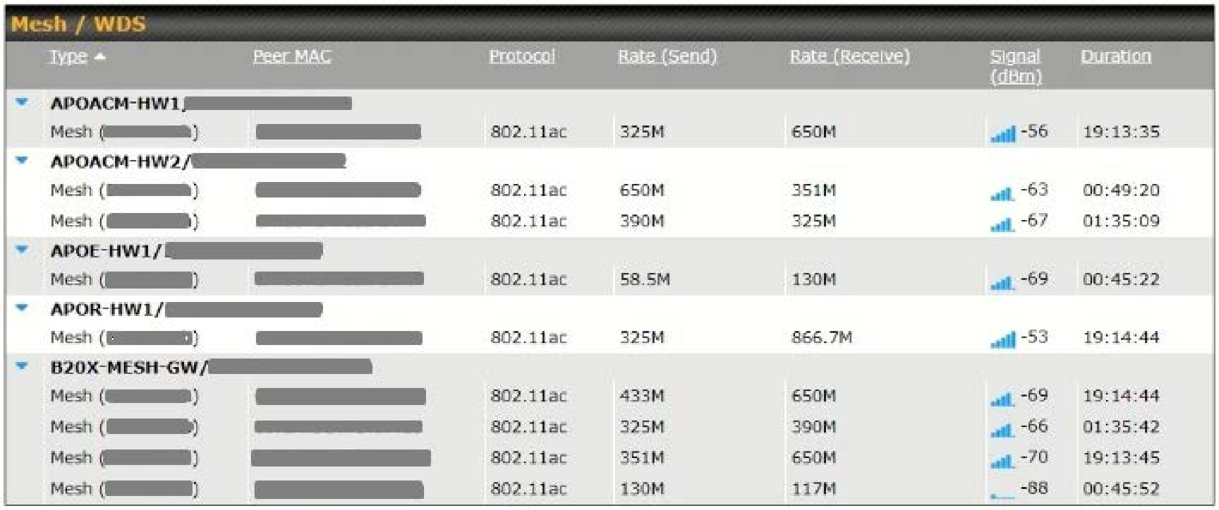
SSIDs

SSID	Security Policy	APs	Clients	Sent(kbps)	Received(kbps)
Peplink WLAN 853B	WPA/WPA2 - Personal	1	2	520.60	11.04
Staff	Open	0	0	0.00	0.00
Staff	WPA/WPA2 - Personal	0	0	0.00	0.00
Guest	Open	0	0	0.00	0.00
Pseudo-Management	WPA/WPA2 - Personal	0	0	0.00	0.00

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

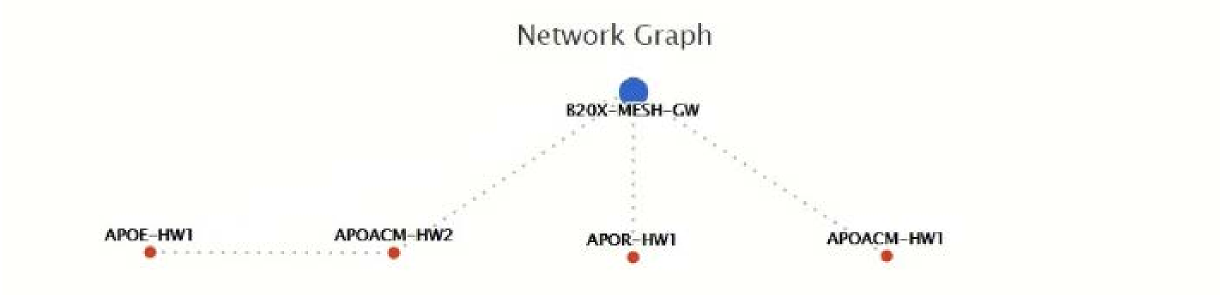
26.4 Mesh / WDS

Mesh / WDS allows you to monitor the status of your wireless distribution system (WDS) or Mesh, and track activity by MAC address by navigating to **AP > Controller Status > Mesh / WDS**. This table shows the detailed information of each AP, including protocol, transmit rate (sent / received), signal strength, and duration.



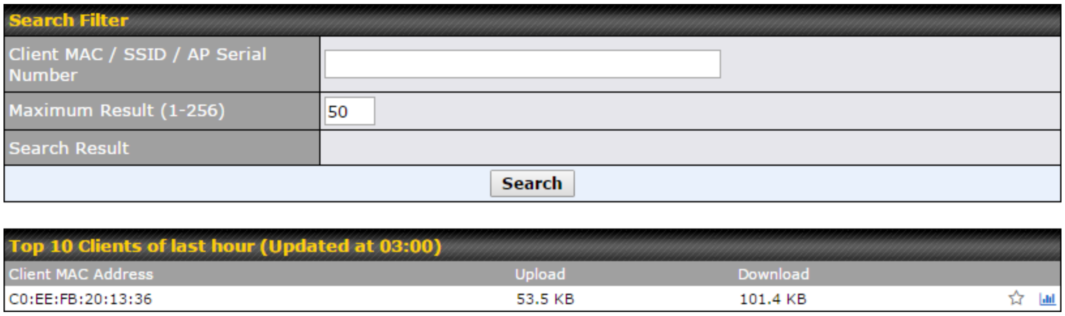
Mesh / WDS

Type ▲	Peer MAC	Protocol	Rate (Send)	Rate (Receive)	Signal (dBm)	Duration
APOACM-HW1/[redacted]						
Mesh ([redacted])	[redacted]	802.11ac	325M	650M	-56	19:13:35
APOACM-HW2/[redacted]						
Mesh ([redacted])	[redacted]	802.11ac	650M	351M	-63	00:49:20
Mesh ([redacted])	[redacted]	802.11ac	390M	325M	-67	01:35:09
APOE-HW1/[redacted]						
Mesh ([redacted])	[redacted]	802.11ac	58.5M	130M	-69	00:45:22
APOR-HW1/[redacted]						
Mesh ([redacted])	[redacted]	802.11ac	325M	866.7M	-53	19:14:44
B20X-MESH-GW/[redacted]						
Mesh ([redacted])	[redacted]	802.11ac	433M	650M	-69	19:14:44
Mesh ([redacted])	[redacted]	802.11ac	325M	390M	-66	01:35:42
Mesh ([redacted])	[redacted]	802.11ac	351M	650M	-70	19:13:45
Mesh ([redacted])	[redacted]	802.11ac	130M	117M	-88	00:45:52



26.5 Wireless Client

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



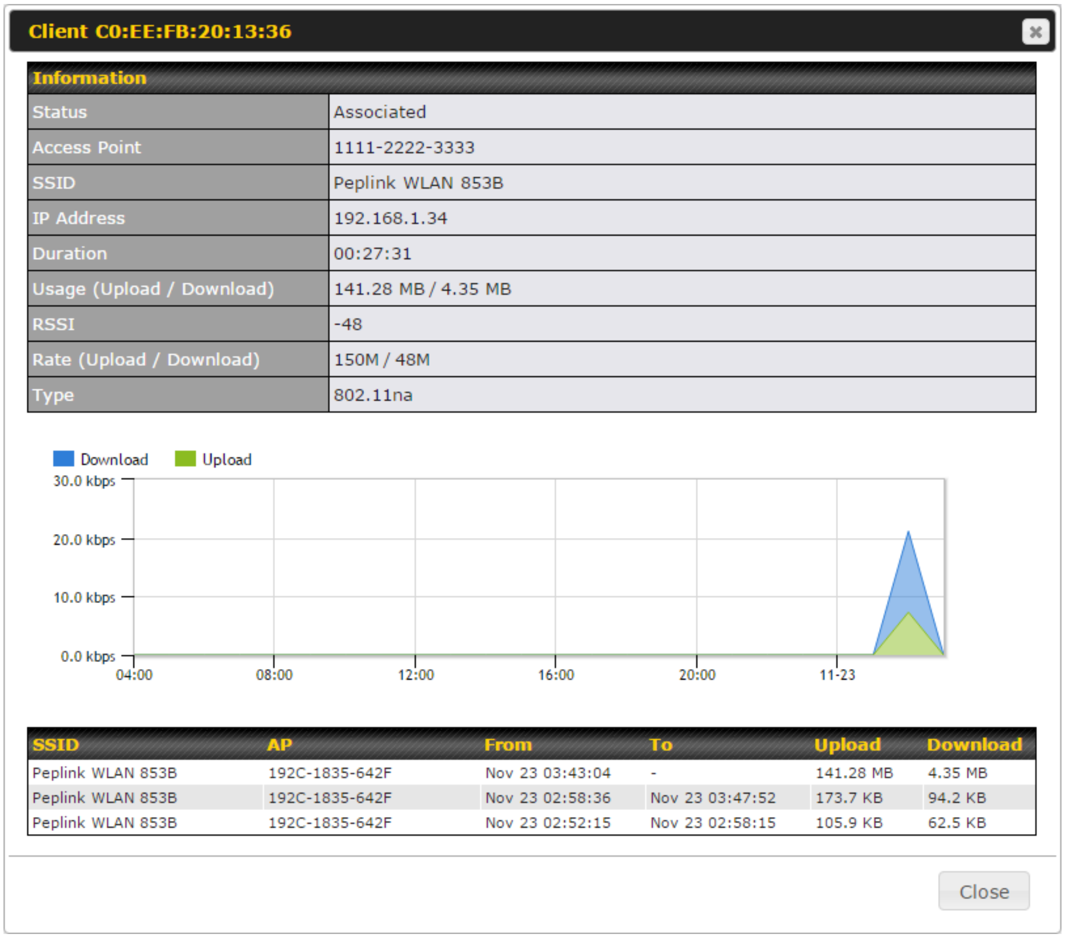
Search Filter

Client MAC / SSID / AP Serial Number	
Maximum Result (1-256)	50
Search Result	

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:



Client C0:EE:FB:20:13:36

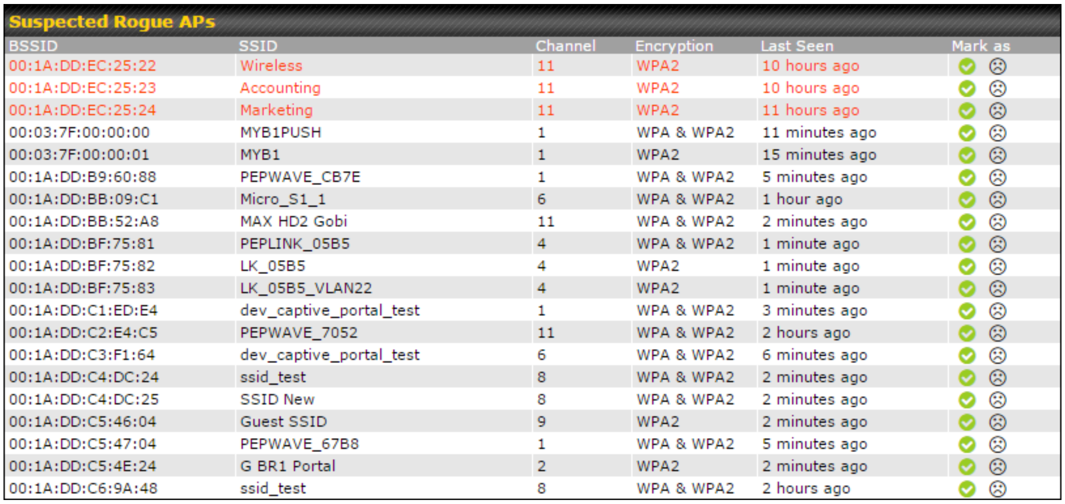
Information	
Status	Associated
Access Point	1111-2222-3333
SSID	Peplink WLAN 853B
IP Address	192.168.1.34
Duration	00:27:31
Usage (Upload / Download)	141.28 MB / 4.35 MB
RSSI	-48
Rate (Upload / Download)	150M / 48M
Type	802.11na

🟦 Download
🟩 Upload
30.0 kbps
20.0 kbps
10.0 kbps
0.0 kbps
04:00
08:00
12:00
16:00
20:00
11-23

SSID	AP	From	To	Upload	Download
Peplink WLAN 853B	192C-1835-642F	Nov 23 03:43:04	-	141.28 MB	4.35 MB
Peplink WLAN 853B	192C-1835-642F	Nov 23 02:58:36	Nov 23 03:47:52	173.7 KB	94.2 KB
Peplink WLAN 853B	192C-1835-642F	Nov 23 02:52:15	Nov 23 02:58:15	105.9 KB	62.5 KB

26.6 Nearby Device

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



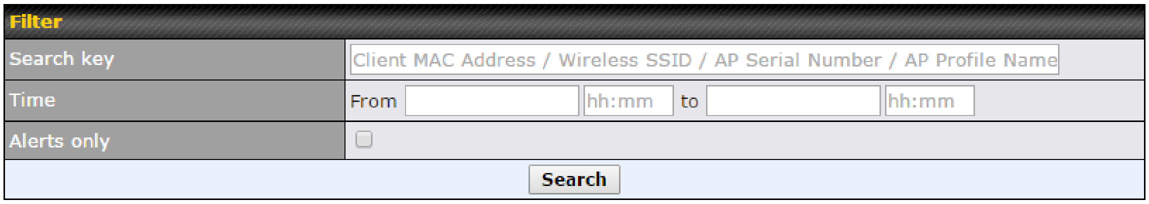
Suspected Rogue APs

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.

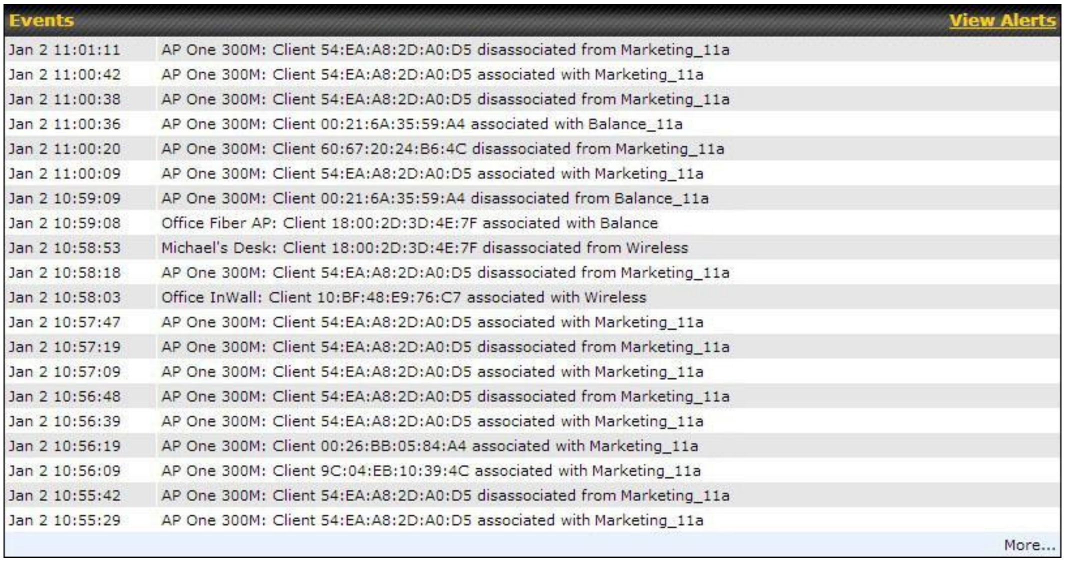
26.7 Event Log

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



Filter

Search key	Client MAC Address / Wireless SSID / AP Serial Number / AP Profile Name
Time	From hh:mm to hh:mm
Alerts only	☐

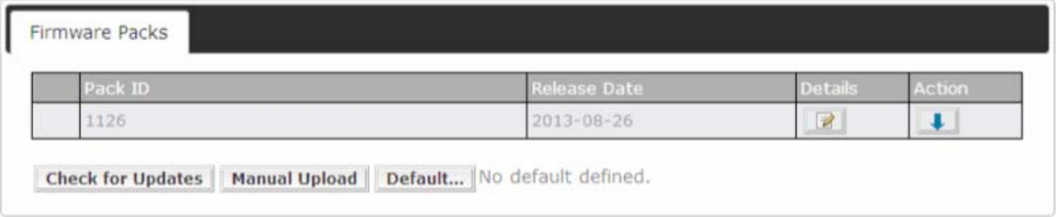


```
Jan 2 11:01:11   AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a
Jan 2 11:00:42   AP One 300M: Client 54:EA:A8:2D:A0:D5 associated with Marketing_11a
Jan 2 11:00:38   AP One 300M: Client 54:EA:A8:2D:A0:D5 disassociated from Marketing_11a
Jan 2 11:00:36   AP One 300M: Client 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
```

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**.



	Pack ID	Release Date	Details	Action
	1126	2013-08-26	📝	⬇

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

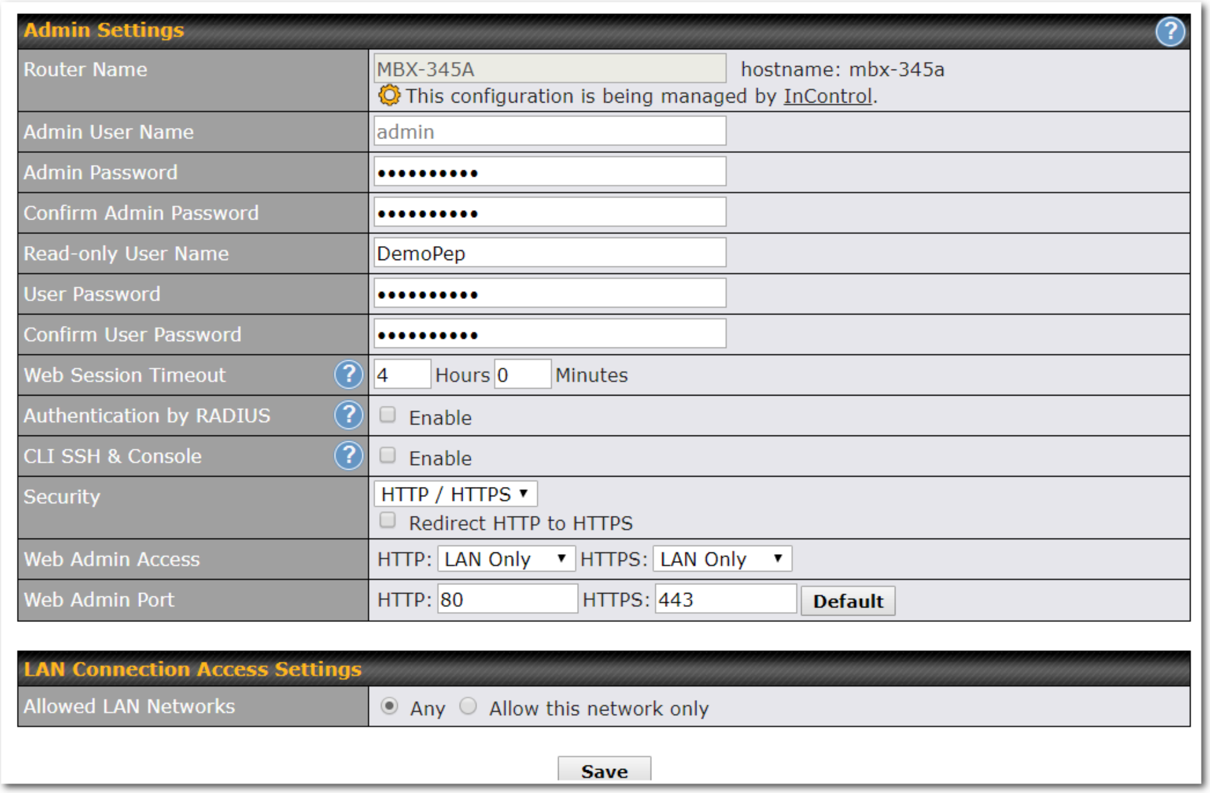
28.1 Admin Security

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**.

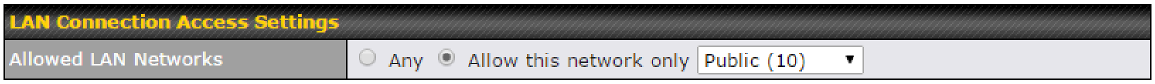


Admin Settings	
Router Name	MBX-345A hostname: mbx-345a This configuration is being managed by InControl.
Admin User Name	admin
Admin Password	••••••••••
Confirm Admin Password	••••••••••
Read-only User Name	DemoPep
User Password	••••••••••
Confirm User Password	••••••••••
Web Session Timeout	4 Hours 0 Minutes
Authentication by RADIUS	☐ Enable
CLI SSH & Console	☐ Enable
Security	HTTP / HTTPS ☐ 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	● Any ○ Allow this network only

Admin Settings	
Router Name	This field allows you to define a name for this Pepwave router. By default, **Router Name** is set as **MAX_XXXX**, where *XXXX* refers to the last 4 digits of the unit's serial number.
Admin User Name	**Admin User Name** is set as *admin* by default, but can be changed, if desired.
Admin Password	This field allows you to specify a new administrator password.
Confirm Admin Password	This field allows you to verify and confirm the new administrator password.
Read-only User Name	**Read-only User Name** is set as *user* by default, but can be changed, if desired.
User Password	This field allows you to specify a new user password. Once the user password is set, the read-only user feature will be enabled.
Confirm User Password	This field allows you to verify and confirm the new user password.

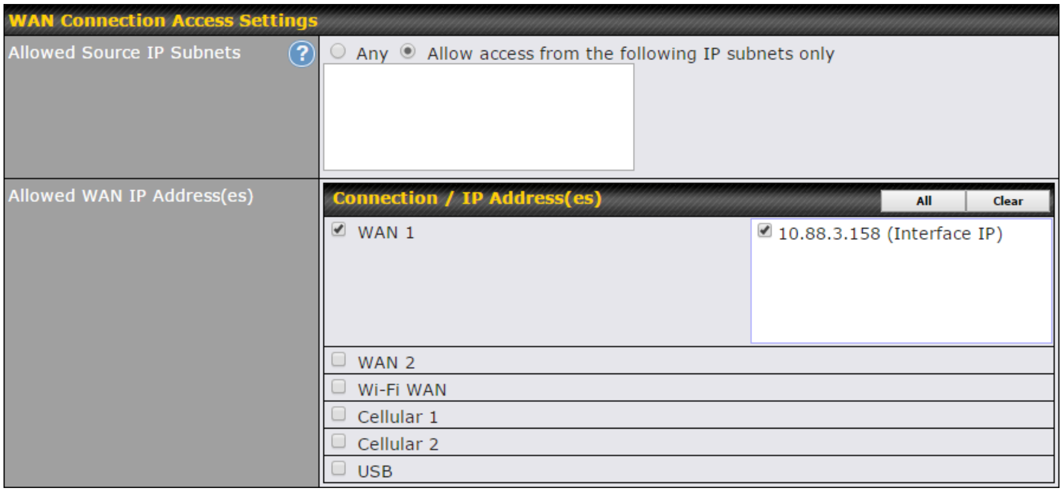
Web Session Timeout	This field specifies the number of hours and minutes that a web session can remain idle before the Pepwave router terminates its access to the web admin interface. By default, it is set to **4 hours**.
Authentication by RADIUS	With this box is checked, the web admin will authenticate 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.
Auth Protocol	This specifies the authentication protocol used. Available options are **MS-CHAP v2** and **PAP**.
Auth Server	This specifies the access address and port of the external RADIUS server.
Auth Server Secret	This field is for entering the secret key for accessing the RADIUS server.
Auth Timeout	This option specifies the time value for authentication timeout.
Accounting Server	This specifies the access address and port of the external accounting server.
Accounting Server Secret	This field is for entering the secret key for accessing the accounting server.
Network Connection	This option is for specifying the network connection to be used for authentication. Users can choose from LAN, WAN, and VPN connections.
CLI SSH	The CLI (command line interface) can be accessed via SSH. This field enables CLI support. For additional information regarding CLI, please refer to **Section 30.5.**
CLI SSH Port	This field determines the port on which clients can access CLI SSH.
CLI SSH Access	This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only.
Security	This option is for specifying the protocol(s) through which the web admin interface can be accessed: ● HTTP ● HTTPS ● HTTP/HTTPS
Web Admin Port	This field is for specifying the port number on which the web admin interface can be accessed.
Web Admin	This option is for specifying the network interfaces through which the web admin

Access	interface can be accessed: - LAN only - LAN/WAN If LAN/WAN is chosen, the **WAN Connection Access Settings** form will be displayed.



LAN Connection Access Settings	
Allowed LAN Networks	○ Any ● Allow this network only Public (10) ▾

LAN Connection Access Settings	
Allowed LAN Networks	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
☑ WAN 1	☑ 10.88.3.158 (Interface IP)
☐ WAN 2	
☐ Wi-Fi WAN	
☐ Cellular 1	
☐ Cellular 2	
☐ USB	

WAN Connection Access Settings	
Allowed Source IP Subnets	This field allows you to restrict web admin access only from defined IP subnets. - **Any** - Allow web admin accesses to be from anywhere, without IP address restriction. - **Allow access from the following IP subnets only** - Restrict web admin access only from the defined IP subnets. When this is chosen, a text input area will be displayed beneath: The allowed IP subnet addresses should be entered into this text area. Each IP subnet must be in form of *w.x.y.z/m*, where *w.x.y.z* is an IP address (e.g., *192.168.0.0*), and *m* is the subnet mask in CIDR format, which is between 0 and 32 inclusively (For example, *192.168.0.0/24*). To define multiple subnets, separate each IP subnet one in a line. For example:

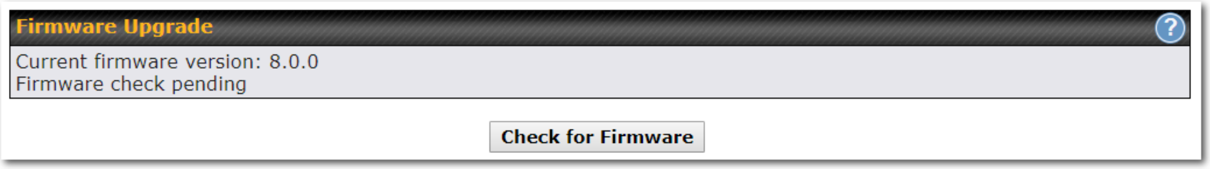
	- 192.168.0.0/24 - 10.8.0.0/16
Allowed WAN IP Address(es)	This is to choose which WAN IP address(es) the web server should listen on.

28.2 Firmware

Web admin interface : automatically check for updates

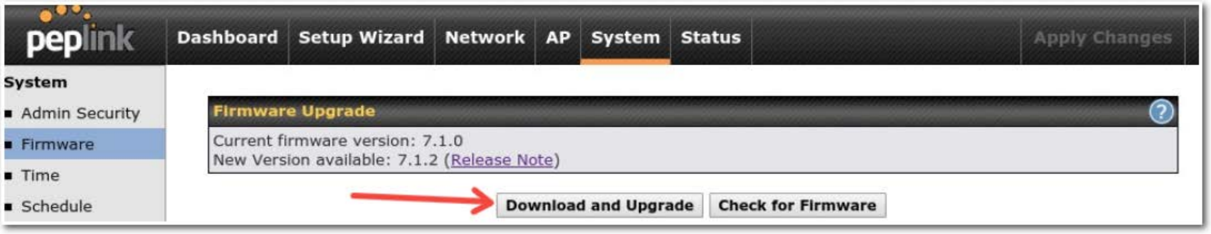
Upgrading firmware can be done in one of three ways.
Using the router's interface to automatically check for an update, using the router's interface to manually upgrade the firmware, or using InControl2 to push an upgrade to a router.

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


Firmware Upgrade
Check for Firmware

Current firmware version: 8.0.0
Firmware check pending

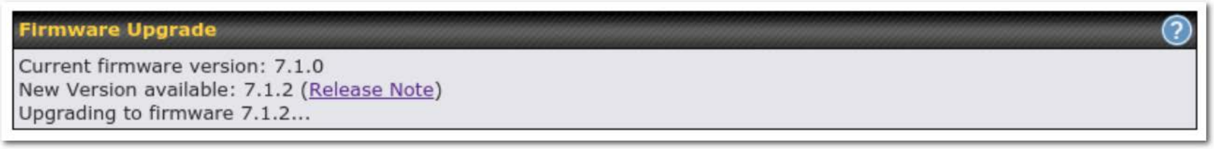
If an update is found the buttons will change to allow you to **Download and Update** the firmware.


peplink
Dashboard
Setup Wizard
Network
AP
System
Status
Apply Changes
System
Admin Security
Firmware
Time
Schedule
Firmware Upgrade
Download and Upgrade
Check for Firmware

Current firmware version: 7.1.0
New Version available: 7.1.2 (Release Note)

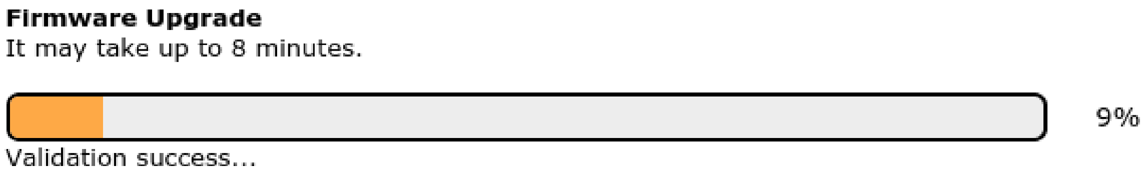
Click on the **Download and Upgrade** button. A prompt will be displayed advising to download the Current Active Configuration. Please click on the underlined download text. After downloading the current config click the **Ok** button to start the upgrade process.

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


Firmware Upgrade

Current firmware version: 7.1.0
New Version available: 7.1.2 (Release Note)
Upgrading to firmware 7.1.2...

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.

9%

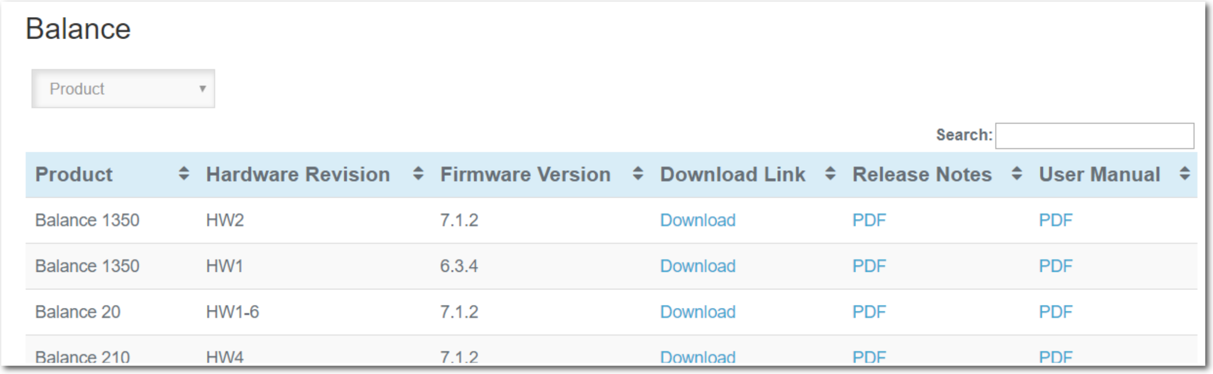
Validation success...

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

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/Pepwave 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.



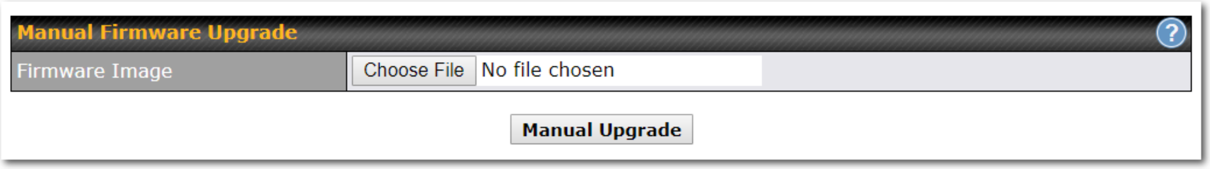
Balance

Product	Hardware Revision	Firmware Version	Download Link	Release Notes	User Manual
Balance 1350	HW2	7.1.2	Download	PDF	PDF
Balance 1350	HW1	6.3.4	Download	PDF	PDF
Balance 20	HW1-6	7.1.2	Download	PDF	PDF
Balance 210	HW4	7.1.2	Download	PDF	PDF

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.

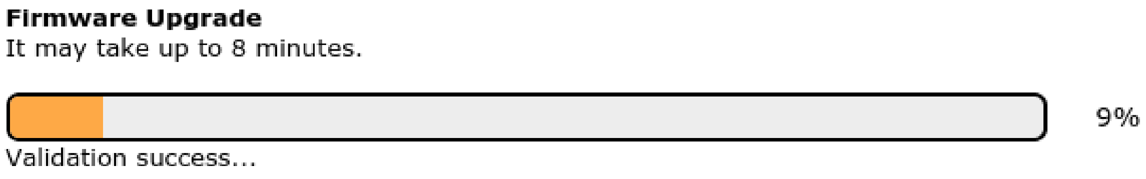
Click on the Manual Upgrade button to start the upgrade process.



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.

9%

Validation success...

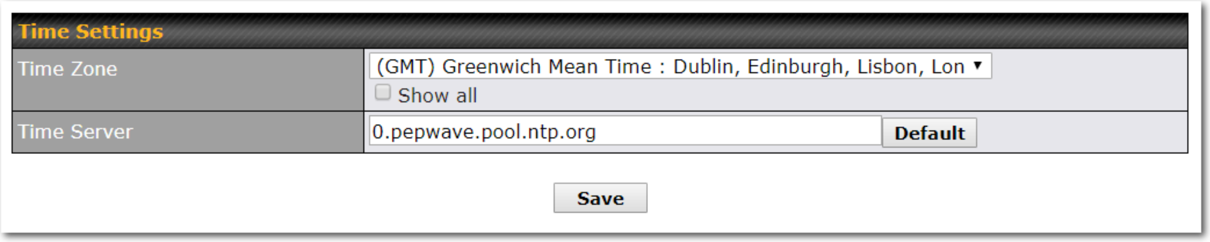
***Upgrading the firmware will cause the router to reboot.**

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**.



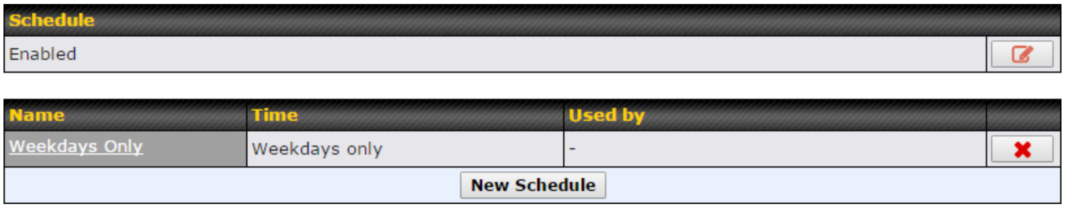
Time Settings

Time Zone	(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, Lon ▾ ☐ Show all
Time Server	0.pepwave.pool.ntp.org

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

28.4 Schedule

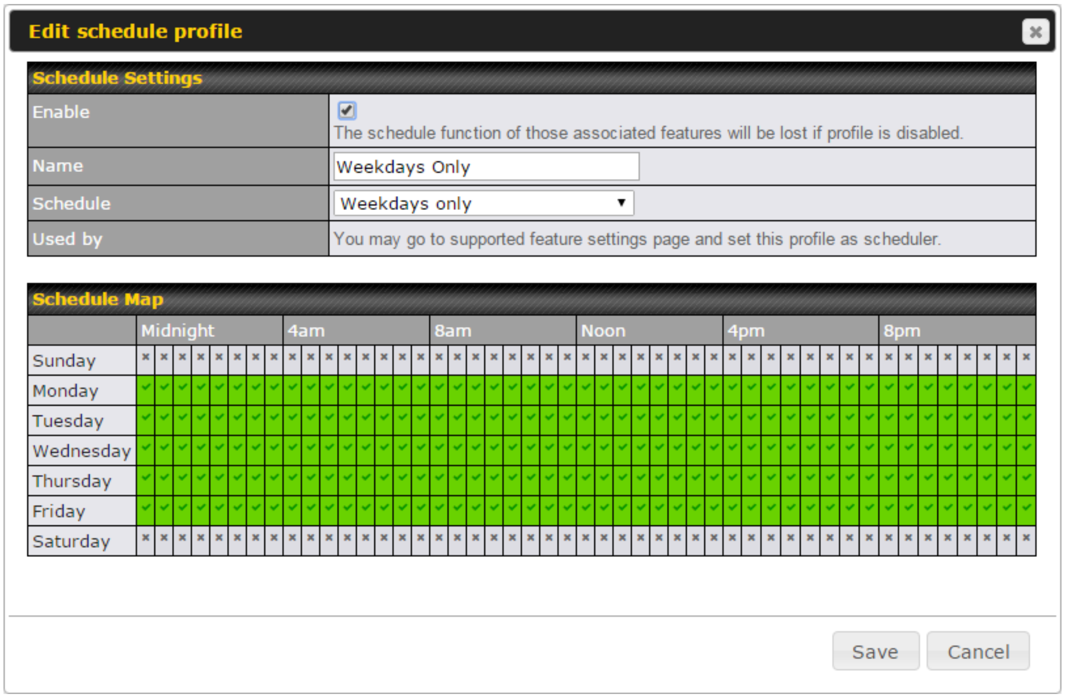
Enable and disable different functions (such as WAN connections, outbound policy, and firewalls at different times, based on a user-scheduled configuration profile. The settings for this are located at **System > Schedule**



Schedule	
Enabled	

Name	Time	Used by
Weekdays Only	Weekdays only	-

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



Edit schedule profile

Schedule Settings	
Enable	☑ The schedule function of those associated features will be lost if profile is disabled.
Name	Weekdays Only
Schedule	Weekdays only
Used by	You may go to supported feature settings page and set this profile as scheduler.

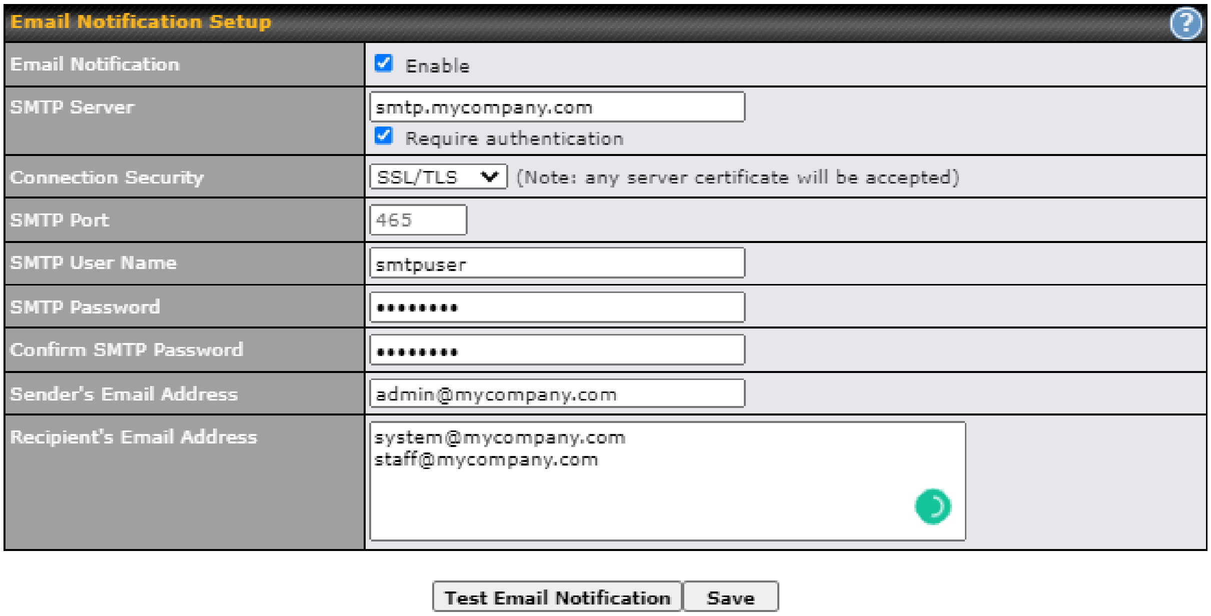
Schedule Map

	Midnight								4am								8am								Noon								4pm								8pm							
Sunday	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
Monday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Tuesday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Wednesday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Thursday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Friday	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Saturday	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×

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**.

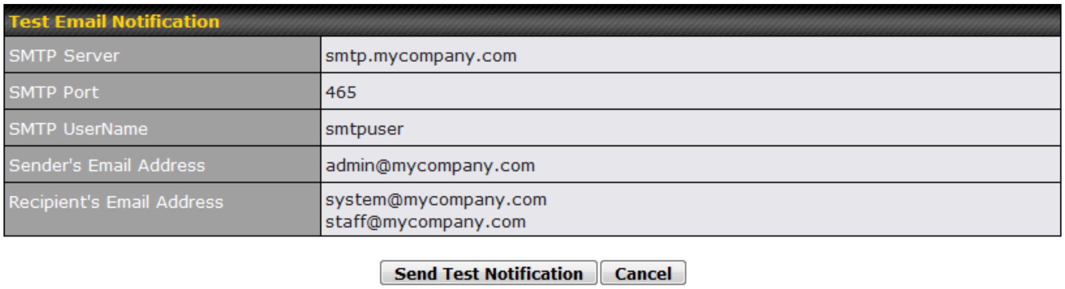


Email Notification Setup	
Email Notification	☑ Enable
SMTP Server	smtp.mycompany.com ☑ Require authentication
Connection Security	SSL/TLS (Note: any server certificate will be accepted)
SMTP Port	465
SMTP User Name	smtpuser
SMTP Password	••••••••
Confirm SMTP Password	••••••••
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

Email Notification Settings	
Email Notification	This setting specifies whether or not to enable email notification. If **Enable** is checked, the Pepwave router will send email messages to system administrators when the WAN status changes or when new firmware is available. If **Enable** is not checked, email notification is disabled and the Pepwave router will not send email messages.
SMTP Server	This setting specifies the SMTP server to be used for sending email. If the server requires authentication, check **Require authentication**.
Connection Security	This setting specifies via a drop-down menu one of the following valid Connection Security: ● None ● STARTTLS ● SSL/TLS
SMTP Port	This field is for specifying the SMTP port number. By default, this is set to **25**. If Connection Security is selected "**STARTTLS**", the default port number will be set to **587**. If Connection Security is selected "**SSL/TLS**", the default port number will be set to **465**. You may customize the port number by editing this field.

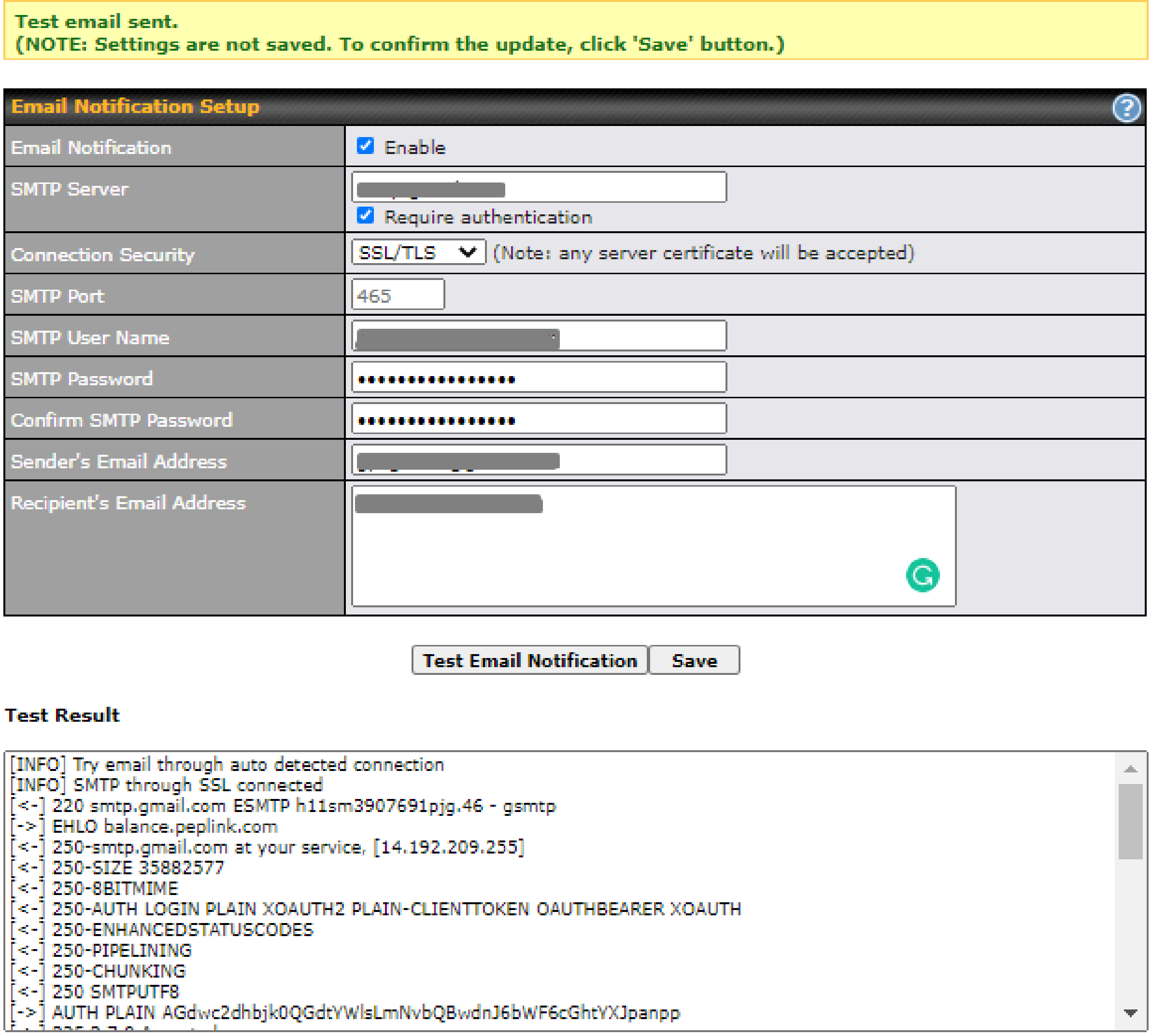
SMTP User Name / Password	This setting specifies the SMTP username and password while sending email. These options are shown only if **Require authentication** is checked in the **SMTP Server** setting.
Confirm SMTP Password	This field allows you to verify and confirm the new administrator password.
Sender's Email Address	This setting specifies the email address the Pepwave router will use to send reports.
Recipient's Email Address	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.
(NOTE: Settings are not saved. To confirm the update, click 'Save' button.)

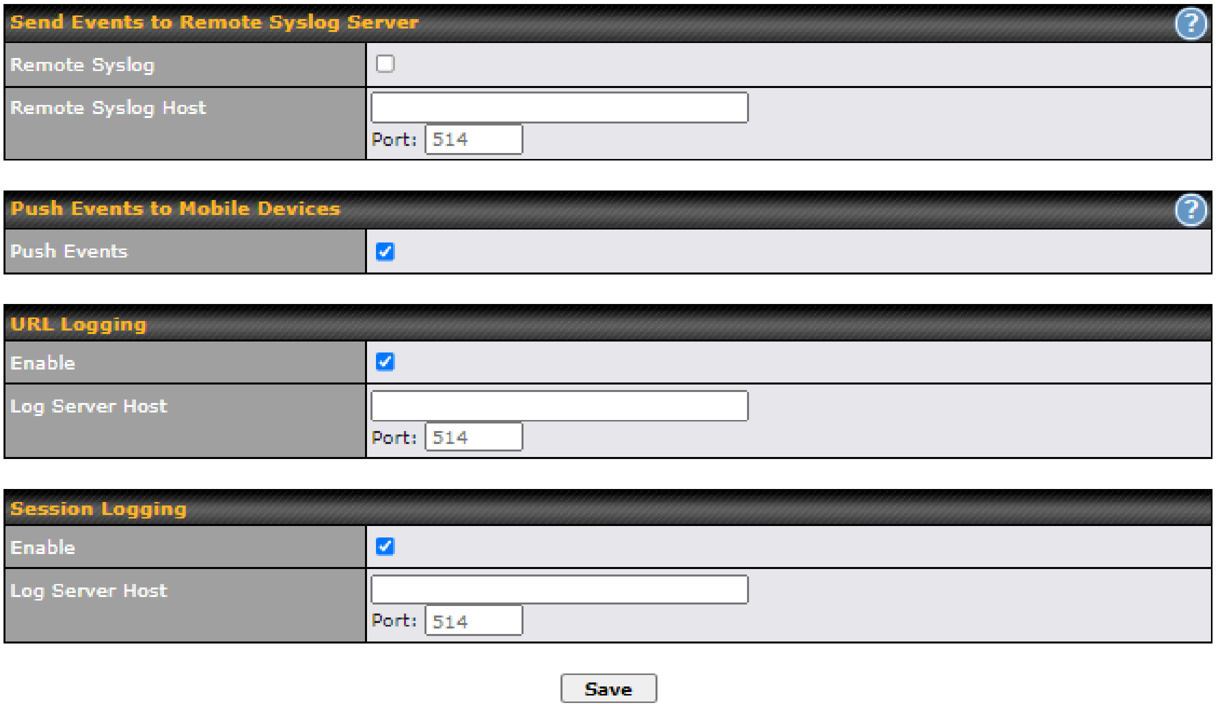
Email Notification Setup	
Email Notification	☑ Enable
SMTP Server	[redacted] ☑ Require authentication
Connection Security	SSL/TLS (Note: any server certificate will be accepted)
SMTP Port	465
SMTP User Name	[redacted]
SMTP Password	••••••••••••••••
Confirm SMTP Password	••••••••••••••••
Sender's Email Address	[redacted]
Recipient's Email Address	[redacted]

Test Result

```
[INFO] Try email through auto detected connection
[INFO] SMTP through SSL connected
[<-] 220 smtp.gmail.com ESMTP h11sm3907691pjg.46 - gsmtp
[->] EHLO balance.peplink.com
[<-] 250-smtp.gmail.com at your service, [14.192.209.255]
[<-] 250-SIZE 35882577
[<-] 250-8BITMIME
[<-] 250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN OAUTHBEARER XOAUTH
[<-] 250-ENHANCEDSTATUSCODES
[<-] 250-PIPELINING
[<-] 250-CHUNKING
[<-] 250 SMTPUTF8
[->] AUTH PLAIN AGdwc2dhbjk0QGdtYWlsLmNvbQBwdnJ6bWF6cGhtYXJpanpp
```

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	☐
Remote Syslog Host	Port: 514

Push Events to Mobile Devices	
Push Events	☑

URL Logging	
Enable	☑
Log Server Host	Port: 514

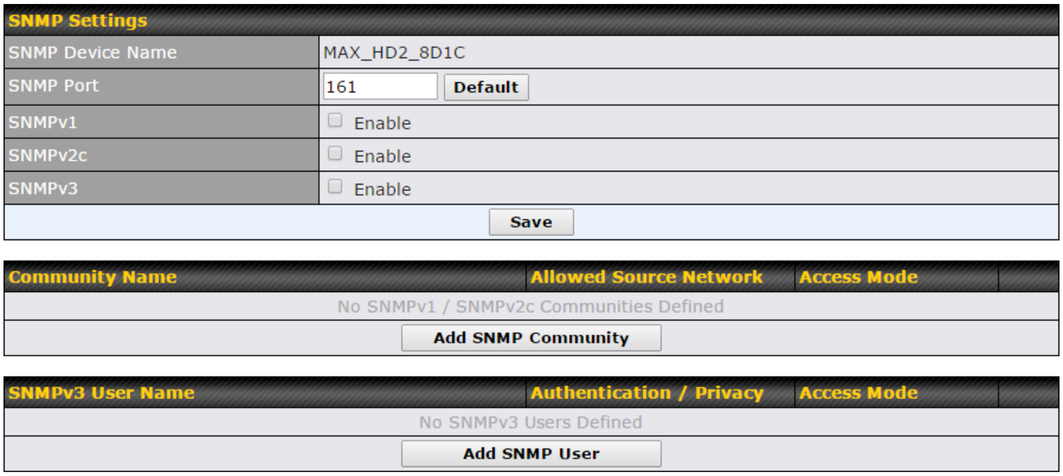
Session Logging	
Enable	☑
Log Server Host	Port: 514

Event Log Settings	
Remote Syslog	This setting specifies whether or not to log events at the specified remote syslog server.
Remote Syslog Host	This setting specifies the IP address or hostname of the remote syslog server.
Push Events	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.
URL Logging	This setting is to enable event logging at the specified log server.
URL Logging Host	This setting specifies the IP address or hostname of the URL log server.
Session Logging	This setting is to enable event logging at the specified log server.

Session Logging Host	This setting specifies the IP address or hostname of the Session log server.
	For more information on the Router Utility, go to: www.peplink.com/products/router-utility

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

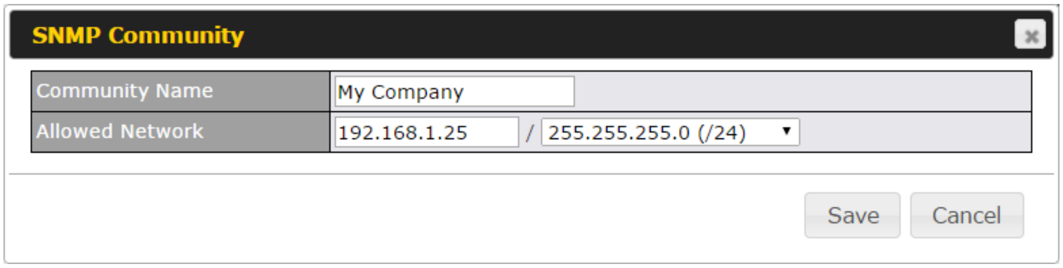
SNMP Device Name	MAX_HD2_8D1C
SNMP Port	161 Default
SNMPv1	☐ Enable
SNMPv2c	☐ Enable
SNMPv3	☐ Enable

Community Name	Allowed Source Network	Access Mode
No SNMPv1 / SNMPv2c Communities Defined		

SNMPv3 User Name	Authentication / Privacy	Access Mode
No SNMPv3 Users Defined		

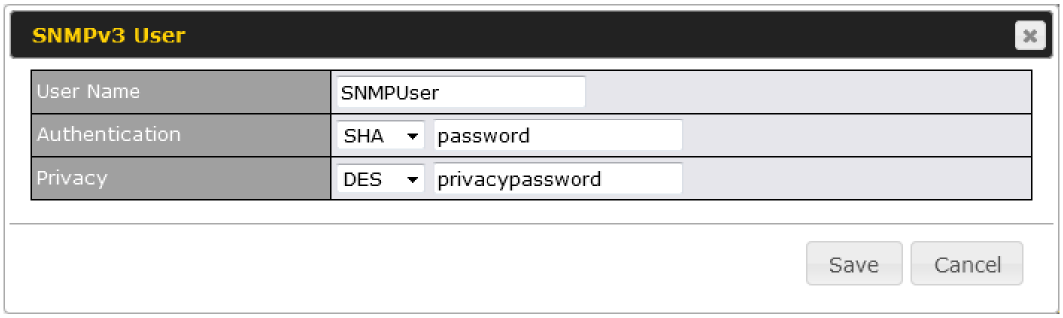
SNMP Settings	
SNMP Device Name	This field shows the router name defined at **System>Admin Security**.
SNMP Port	This option specifies the port which SNMP will use. The default port is **161**.
SNMPv1	This option allows you to enable SNMP version 1.
SNMPv2	This option allows you to enable SNMP version 2.
SNMPv3	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:



SNMP Community

Community Name	My Company
Allowed Network	192.168.1.25 / 255.255.255.0 (/24)



SNMPv3 User

User Name	SNMPUser
Authentication	SHA password
Privacy	DES privacypassword

SNMP Community Settings	
Community Name	This setting specifies the SNMP community name.
Allowed Source Subnet Address	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	
User Name	This setting specifies a user name to be used in SNMPv3.
Authentication Protocol	This setting specifies via a drop-down menu one of the following valid authentication protocols: • NONE • MD5 • SHA When MD5 or SHA is selected, an entry field will appear for the password.
Privacy Protocol	This setting specifies via a drop-down menu one of the following valid privacy protocols: • NONE • DES

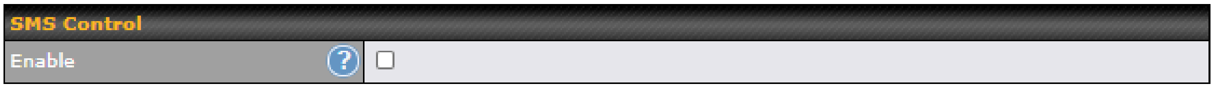
When DES is selected, an entry field will appear for the password.

28.8 SMS Control

SMS Control allows the user to control the device using SMS even if the modem does not have a data connection. The settings for configuring the SMS Control can be found at **System>SMS Control**.

Supported Models

- **Balance/MAX**: *-LTE-E, *-LTEA-W, *-LTEA-P, *-LTE-MX
- **EPX**: *-LW*, *-LP*



SMS Control

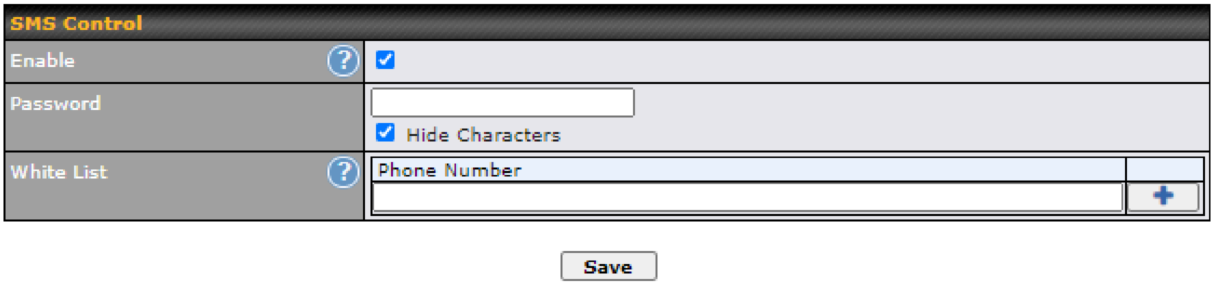
Enable ☐

When this box is checked, the device will be allowed to take actions according to received commands via SMS.

Make sure your mobile plan supports SMS, and note that some plans may incur additional charges for this.

SMS Control can reboot devices and configure cellular settings over signalling channels, even if the modem does not have a data connection.

For details of supported SMS command sets, please refer to our knowledge base.



SMS Control

Enable ☑

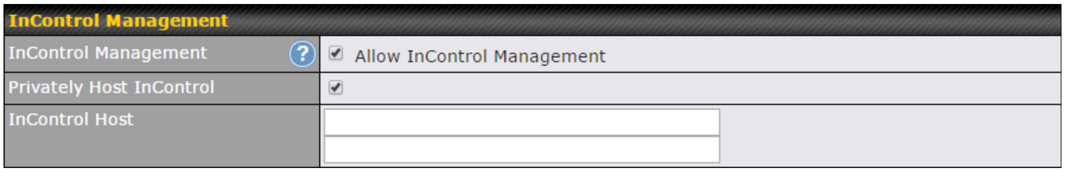
Password

☑ Hide Characters

White List

SMS Control Settings	
Enable	Click the checkbox to enable the SMS Control.
Password	This setting sets the password for authentication - maximum of 32 characters, which cannot include semicolon (;).
White List	Optionally, you can add phone number(s) to the whitelist. Only matching phone numbers are allowed to issue SMS commands. Phone numbers must be in the E.164 International Phone Numbers format.

28.9 InControl



InControl Management	
InControl Management	☑ Allow InControl Management
Privately Host InControl	☑
InControl Host	

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.

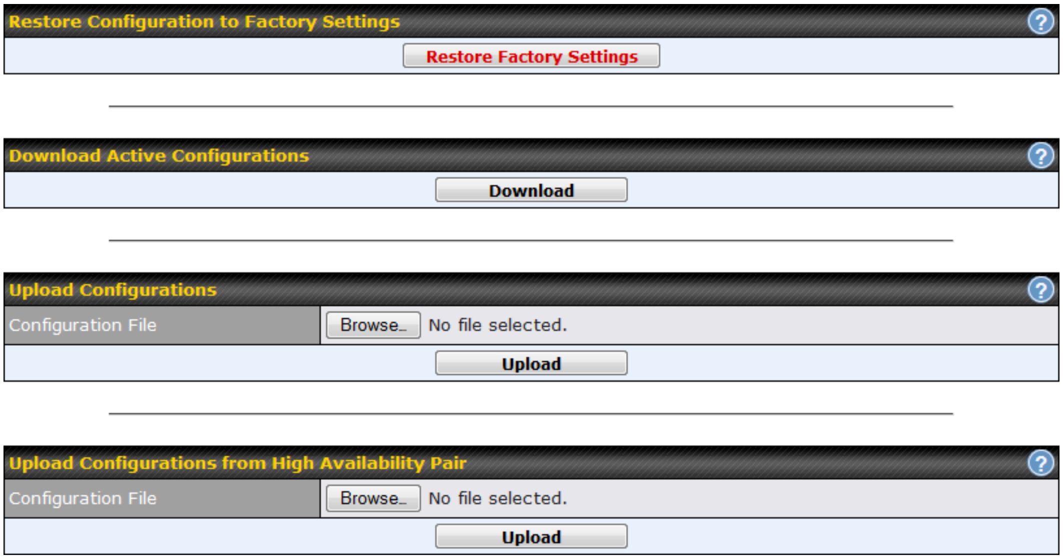
When this check box is checked, the device's status information will be sent to the Peplink InControl system. This device's usage data and configuration will be sent to the system if you enable the features in the system.

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.

28.10 Configuration

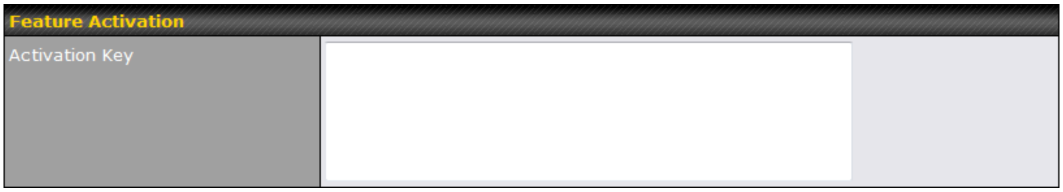
Backing up Pepwave router settings immediately after successful completion of initial setup is strongly recommended. The functionality to download and upload Pepwave router settings is found at **System>Configuration**. Note that available options vary by model.


Restore Configuration to Factory Settings
Restore Factory Settings
Download Active Configurations
Download
Upload Configurations
Configuration File
Browse...
No file selected.
Upload
Upload Configurations from High Availability Pair
Configuration File
Browse...
No file selected.
Upload

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

28.11 Feature Add-ons

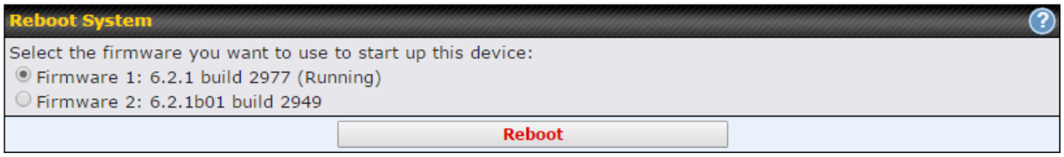
Some Pepwave routers have features that can be activated upon purchase. Once the purchase is complete, you will receive an activation key. Enter the key in the **Activation Key** field, click **Activate**, and then click **Apply Changes**.



28.12 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.



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

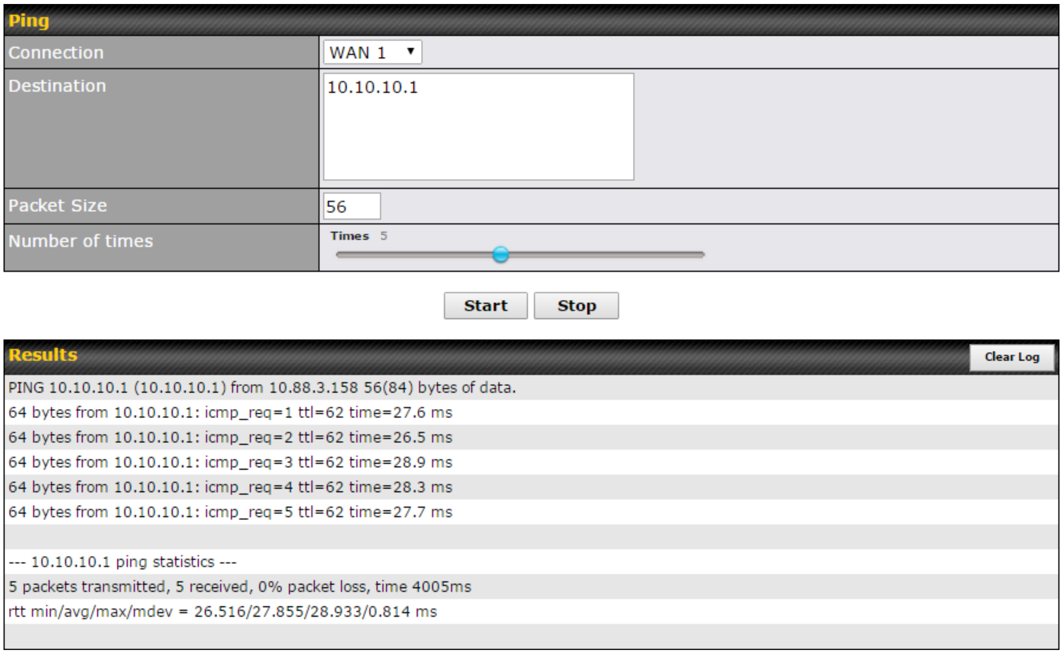
● Firmware 1: 6.2.1 build 2977 (Running)

○ Firmware 2: 6.2.1b01 build 2949

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:



Connection	WAN 1
Destination	10.10.10.1
Packet Size	56
Number of times	Times 5

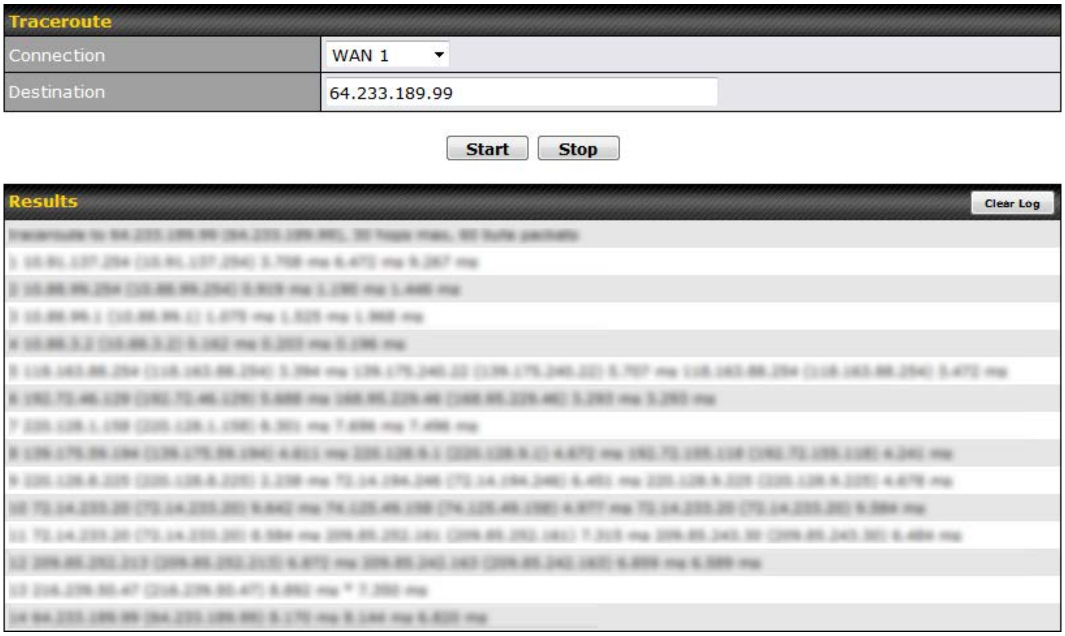
```
PING 10.10.10.1 (10.10.10.1) from 10.88.3.158 56(84) bytes of data.
64 bytes from 10.10.10.1: icmp_req=1 ttl=62 time=27.6 ms
64 bytes from 10.10.10.1: icmp_req=2 ttl=62 time=26.5 ms
64 bytes from 10.10.10.1: icmp_req=3 ttl=62 time=28.9 ms
64 bytes from 10.10.10.1: icmp_req=4 ttl=62 time=28.3 ms
64 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^{TM} connection. The traceroute test utility is located at **System>Tools>Traceroute**.



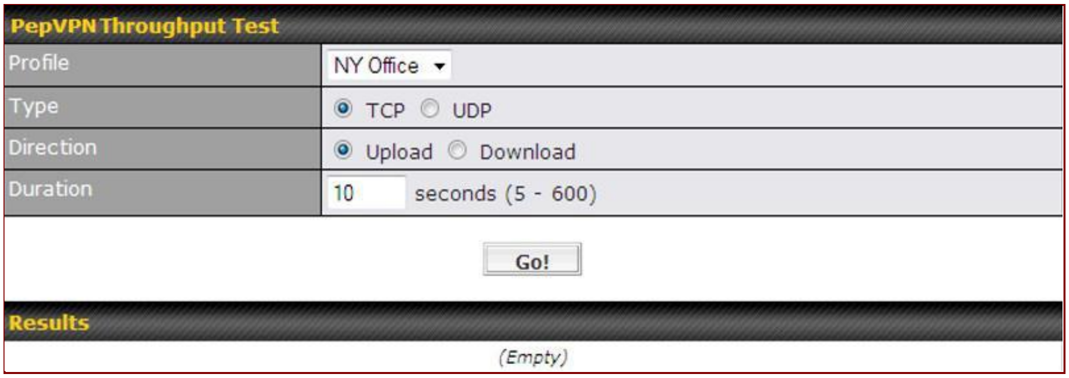
Connection	WAN 1
Destination	64.233.189.99

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

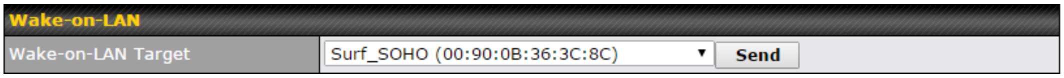
Profile	NY Office
Type	● TCP ○ UDP
Direction	● Upload ○ Download
Duration	10 seconds (5 - 600)

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**



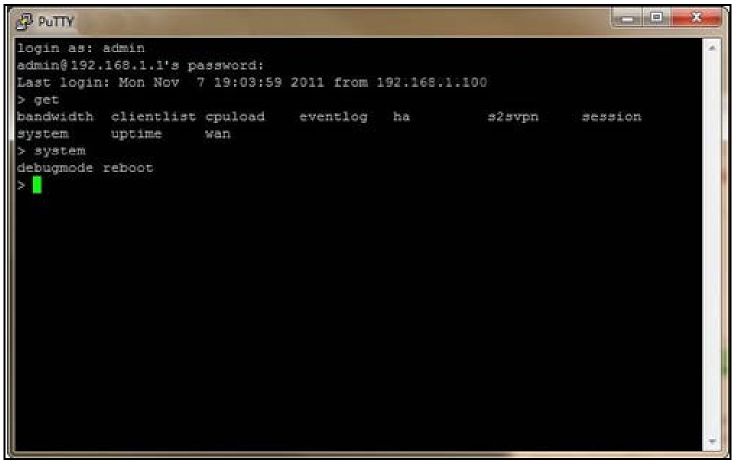
Wake-on-LAN

Wake-on-LAN Target	Surf_SOHO (00:90:0B:36:3C:8C)

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.

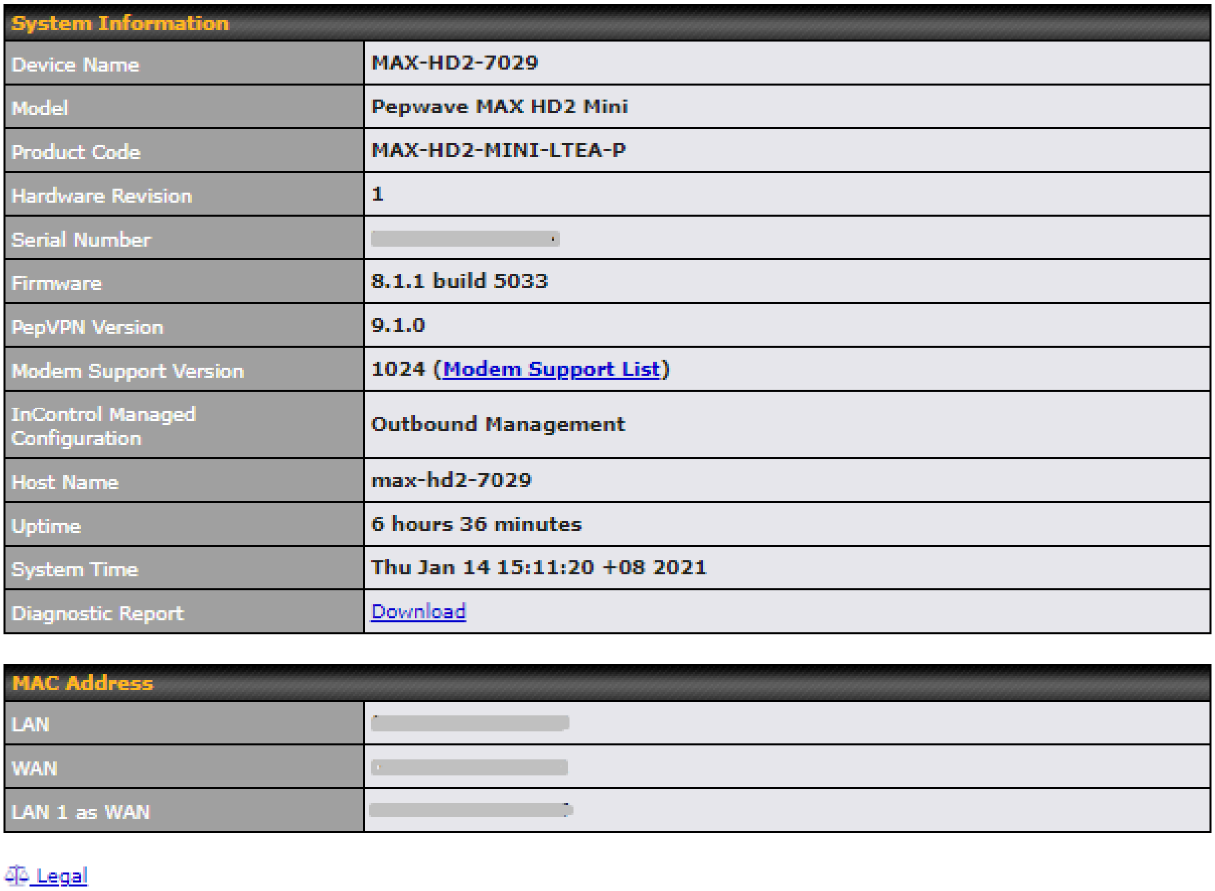


```
login as: admin
admin@192.168.1.1's password:
Last login: Mon Nov  7 19:03:59 2011 from 192.168.1.100
> get
bandwidth  clientlist cpuload    eventlog   ha          s2svpn     session
system     uptime     wan
> system
debugmode reboot
> 
```

30 Status

30.1 Device

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



System Information	
Device Name	MAX-HD2-7029
Model	Pepwave MAX HD2 Mini
Product Code	MAX-HD2-MINI-LTEA-P
Hardware Revision	1
Serial Number	[redacted]
Firmware	8.1.1 build 5033
PepVPN Version	9.1.0
Modem Support Version	1024 (Modem Support List)
InControl Managed Configuration	Outbound Management
Host Name	max-hd2-7029
Uptime	6 hours 36 minutes
System Time	Thu Jan 14 15:11:20 +08 2021
Diagnostic Report	Download

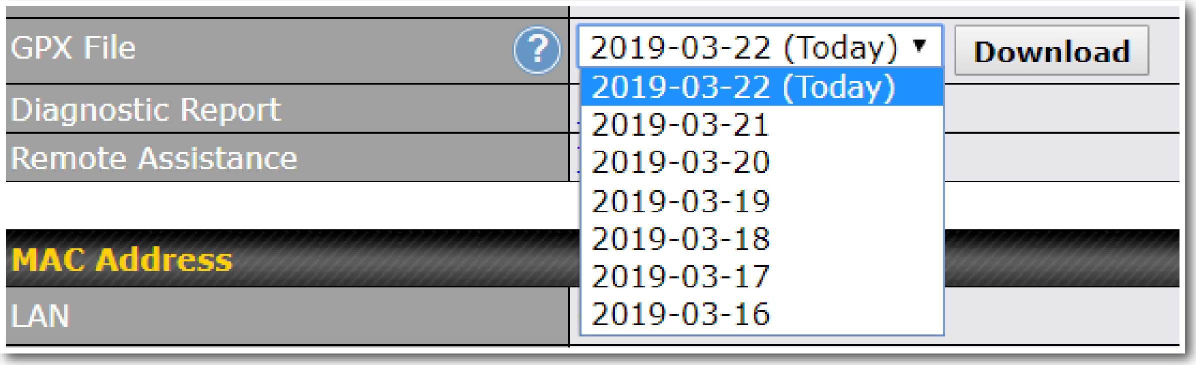
MAC Address	
LAN	[redacted]
WAN	[redacted]
LAN 1 as WAN	[redacted]

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

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

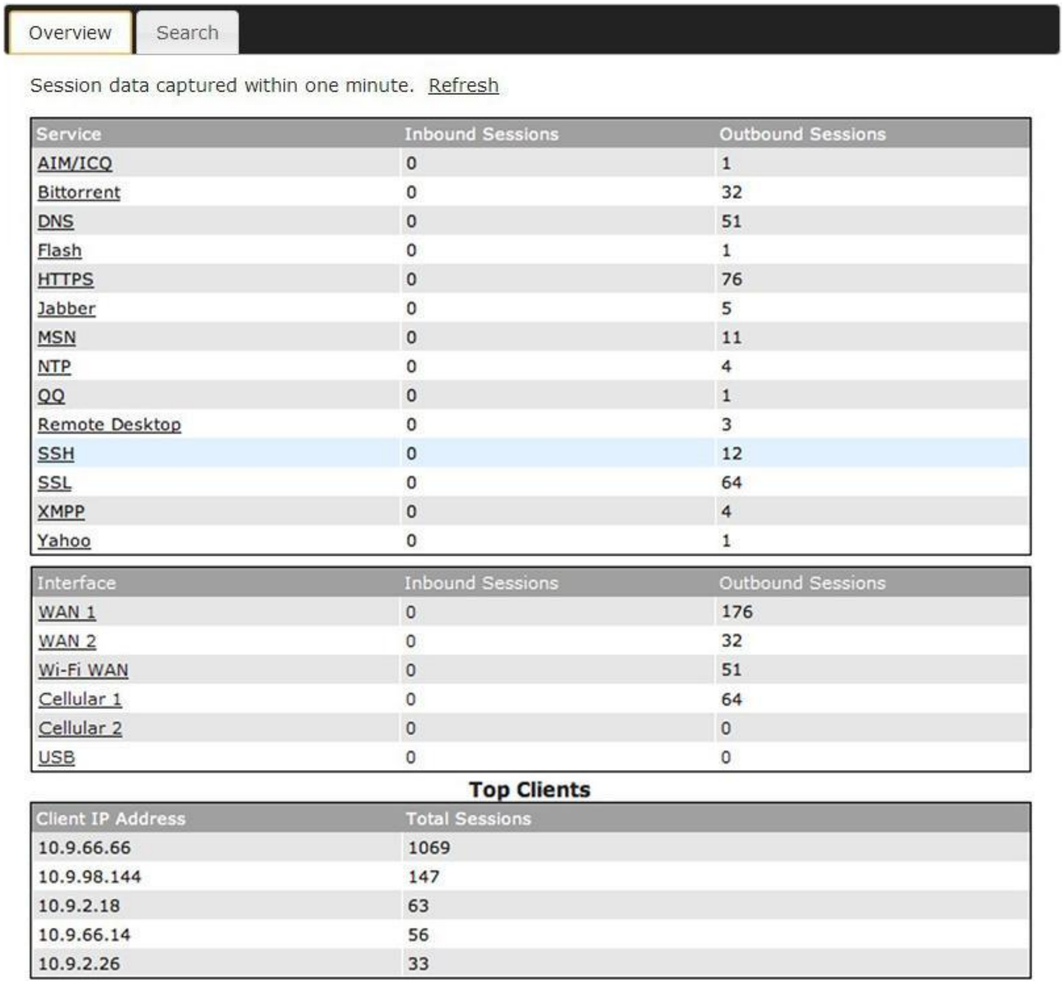

GPX File
?
2019-03-22 (Today) ▾
Download
2019-03-22 (Today)
2019-03-21
2019-03-20
2019-03-19
2019-03-18
2019-03-17
2019-03-16
Diagnostic Report
Remote Assistance
MAC Address
LAN

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.**



Session data captured within one minute. Refresh

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

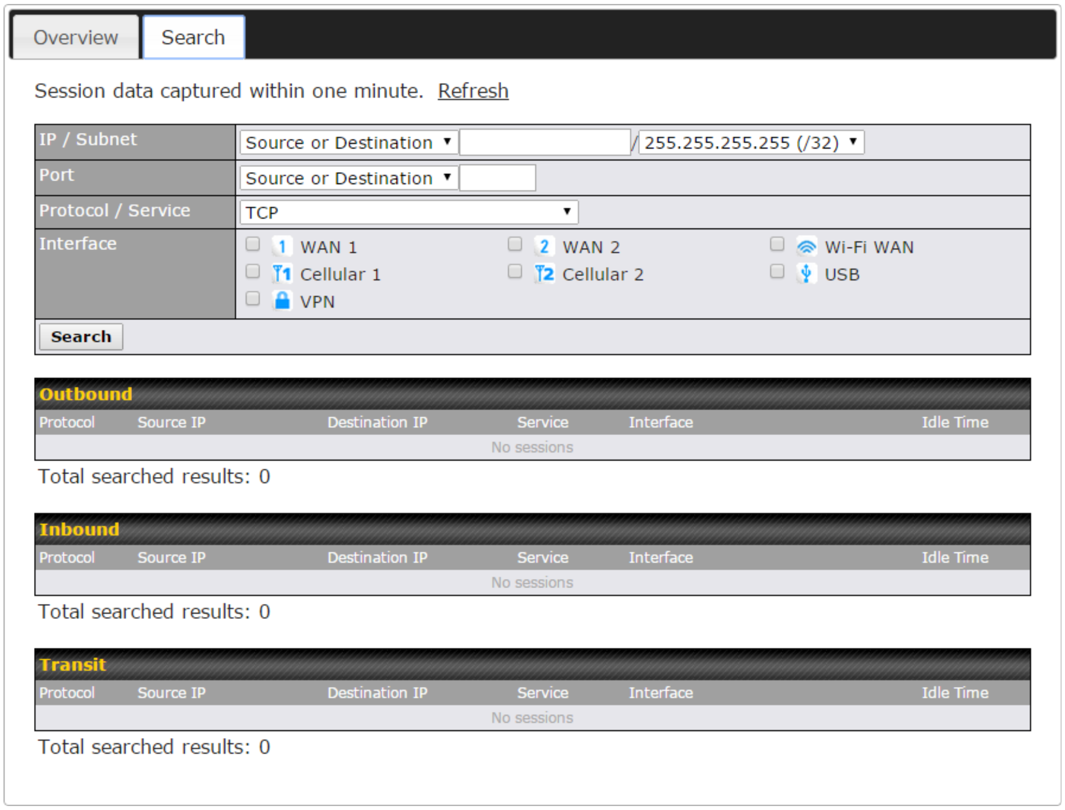
Interface	Inbound Sessions	Outbound Sessions
WAN 1	0	176
WAN 2	0	32
Wi-Fi WAN	0	51
Cellular 1	0	64
Cellular 2	0	0
USB	0	0

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**.



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	☐ 1 WAN 1 ☐ 2 WAN 2 ☐ Wi-Fi WAN ☐ Cellular 1 ☐ Cellular 2 ☐ USB ☐ VPN

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					

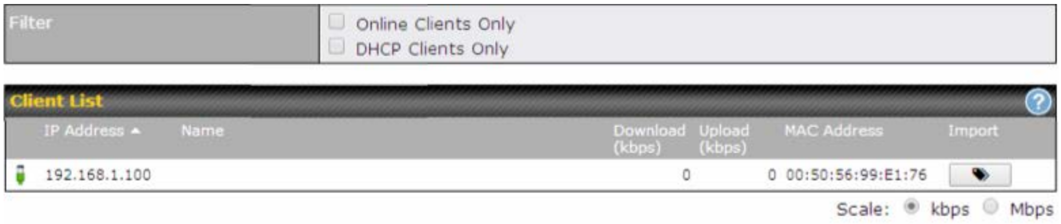
Total searched results: 0

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

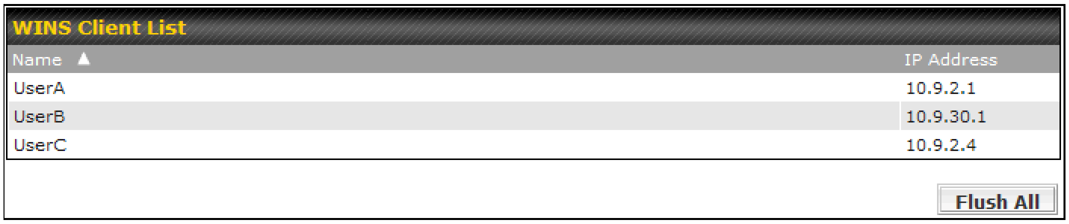
	IP Address ▲	Name	Download (kbps)	Upload (kbps)	MAC Address	Import
	192.168.1.100		0	0	00:50:56:99:E1:76	🏷

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

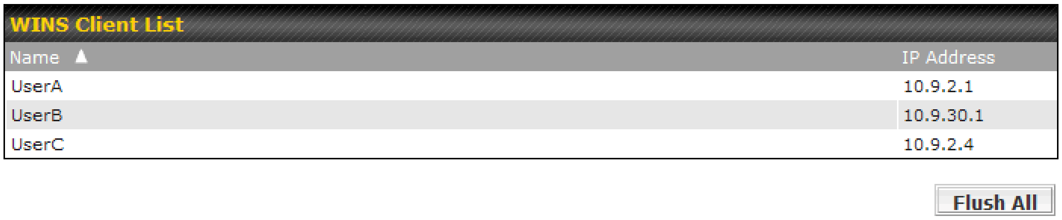
The WINS client list table is located at **Status>WINS Client**.



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.

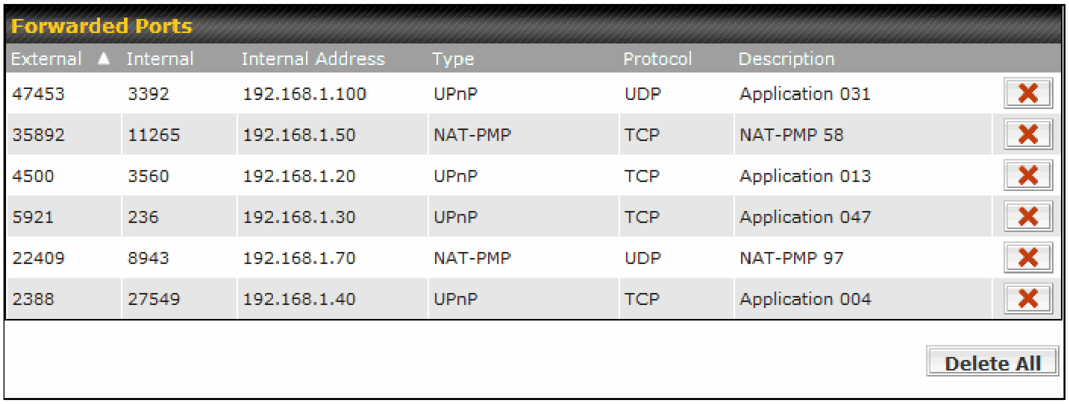


WINS Client List

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	☒

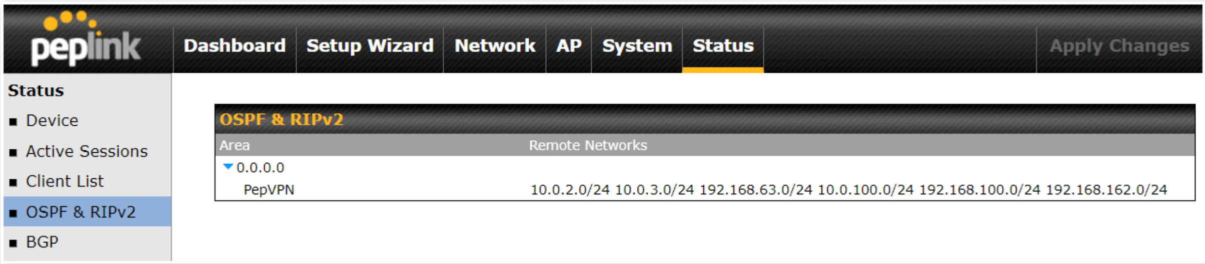
Click ☒ to delete a single UPnP / NAT-PMP record in its corresponding row. To delete all records, click **Delete All** on the right-hand side below the table.

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



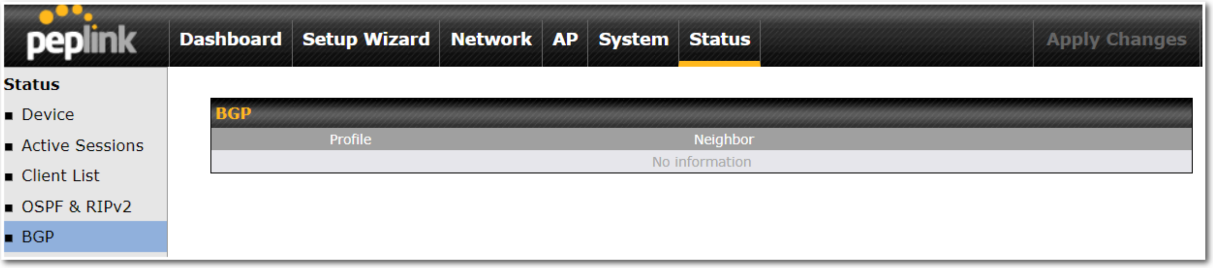
peplink
Dashboard
Setup Wizard
Network
AP
System
Status
Apply Changes
Status
Device
Active Sessions
Client List
OSPF & RIPv2
BGP

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

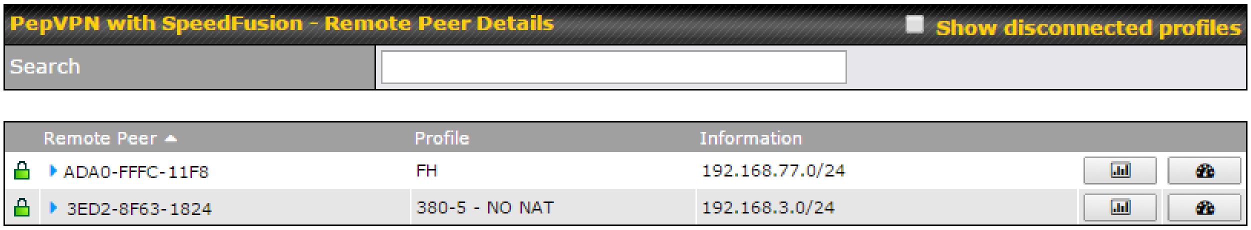

peplink
Dashboard
Setup Wizard
Network
AP
System
Status
Apply Changes
Status
Device
Active Sessions
Client List
OSPF & RIPv2
BGP

BGP

Profile	Neighbor
No information	

30.9 SpeedFusion Status

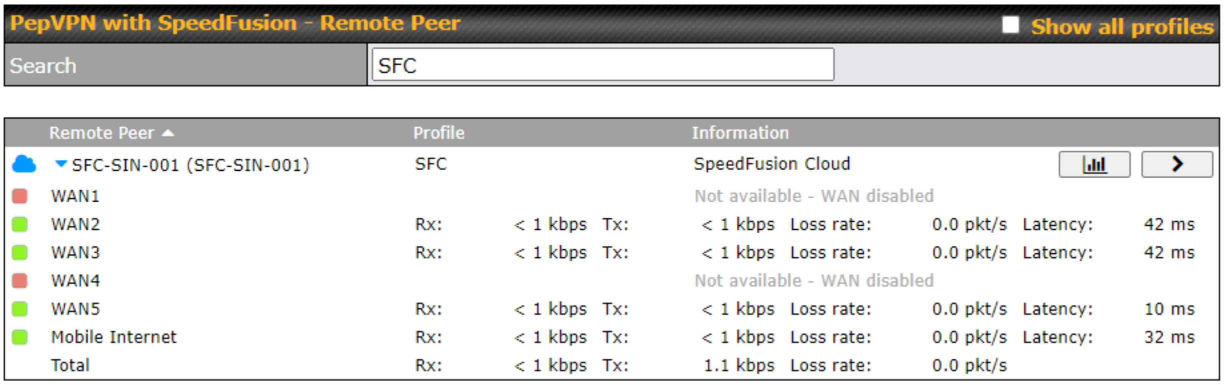
Current SpeedFusion^{TM} status information is located at **Status>SpeedFusion^{TM}**.
Details about SpeedFusion^{TM} connection peers appears as below:


PepVPN with SpeedFusion - Remote Peer Details ☐ Show disconnected profiles

Search

	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

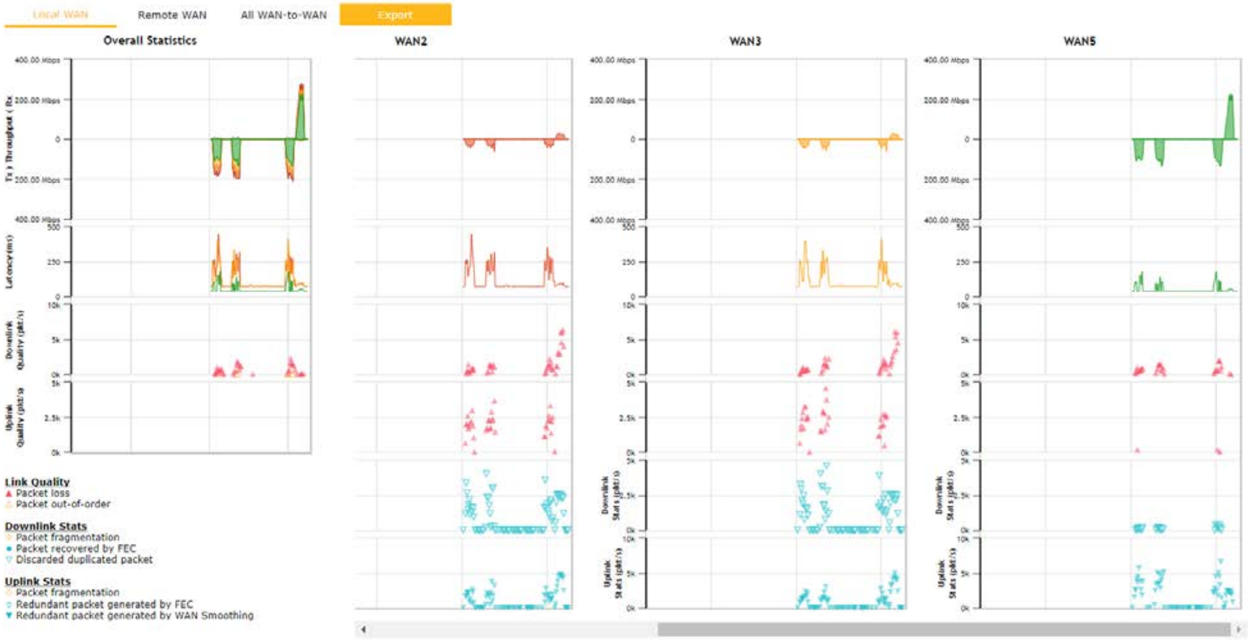
Click on the corresponding peer name to explore the WAN connection(s) status and subnet information of each VPN peer.


PepVPN with SpeedFusion - Remote Peer ☐ Show all profiles

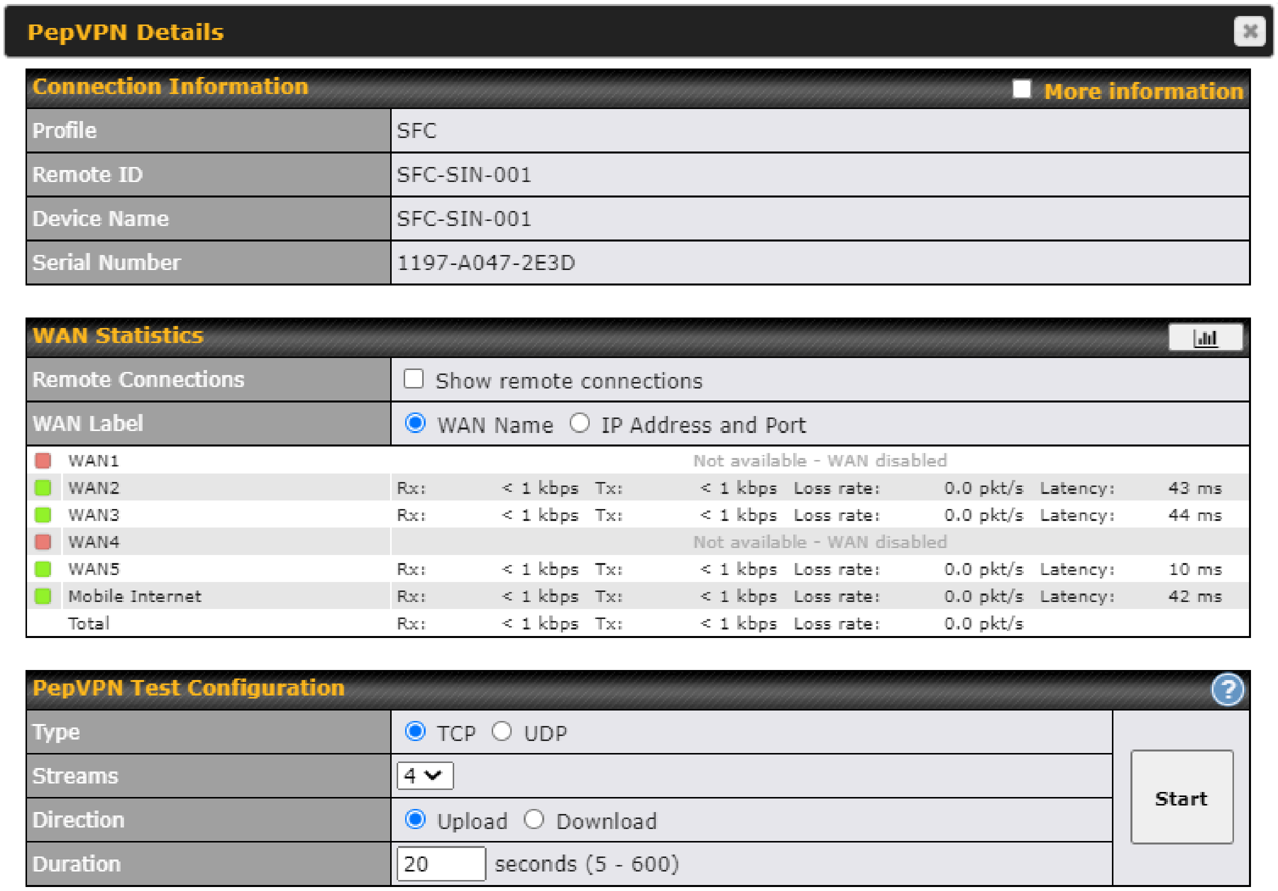
Search: SFC

	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.


Local WAN
Remote WAN
All WAN-to-WAN
Export
Overall Statistics
WAN2
WAN3
WAN5
Tx) Throughput (Rx
400.00 Mbps
200.00 Mbps
0
200.00 Mbps
400.00 Mbps
Latency (ms)
500
250
0
Downlink Quality (pkt/s)
10k
5k
0k
Uplink Quality (pkt/s)
5k
2.5k
0k
Downlink Stats (pkt/s)
Uplink Stats (pkt/s)
Link Quality
▲ Packet loss
△ Packet out-of-order
Downlink Stats
▽ Packet fragmentation
● Packet recovered by FEC
▽ Discarded duplicated packet
Uplink Stats
△ Packet fragmentation
◇ Redundant packet generated by FEC
▼ Redundant packet generated by WAN Smoothing

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

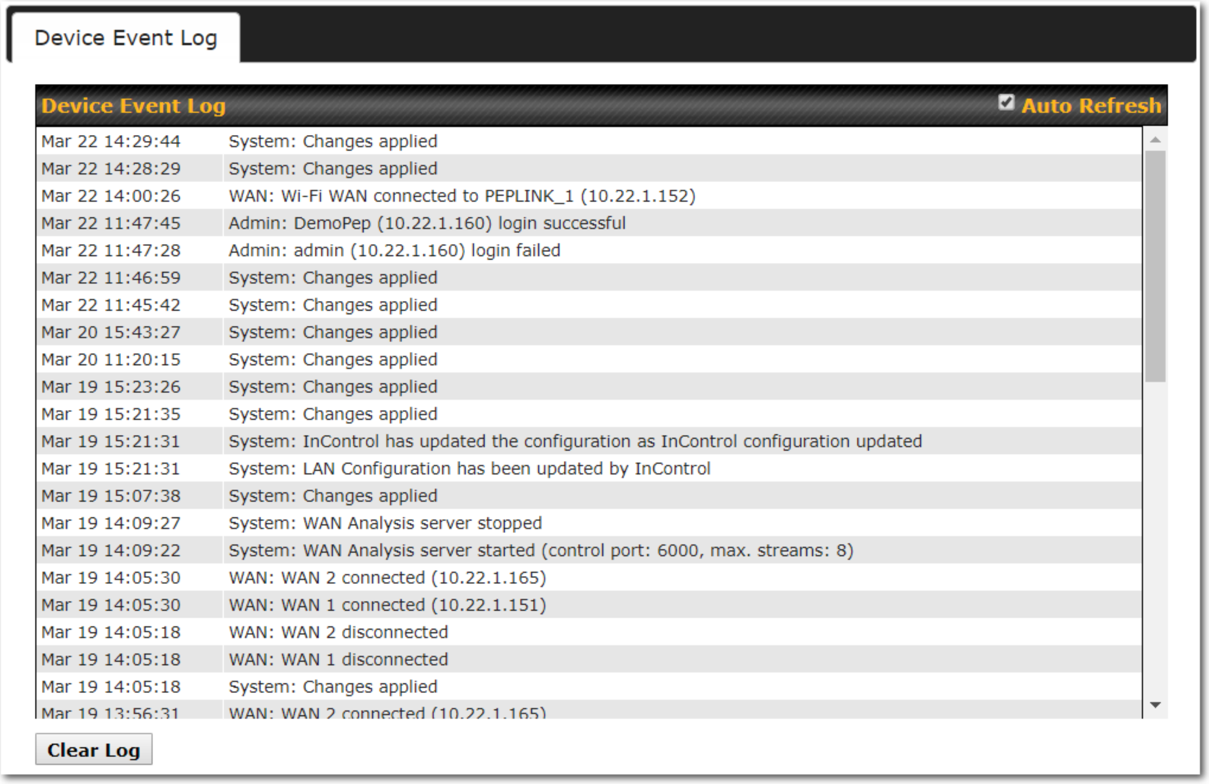
Type	● TCP ○ UDP
Streams	4
Direction	● Upload ○ Download
Duration	20 seconds (5 - 600)

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

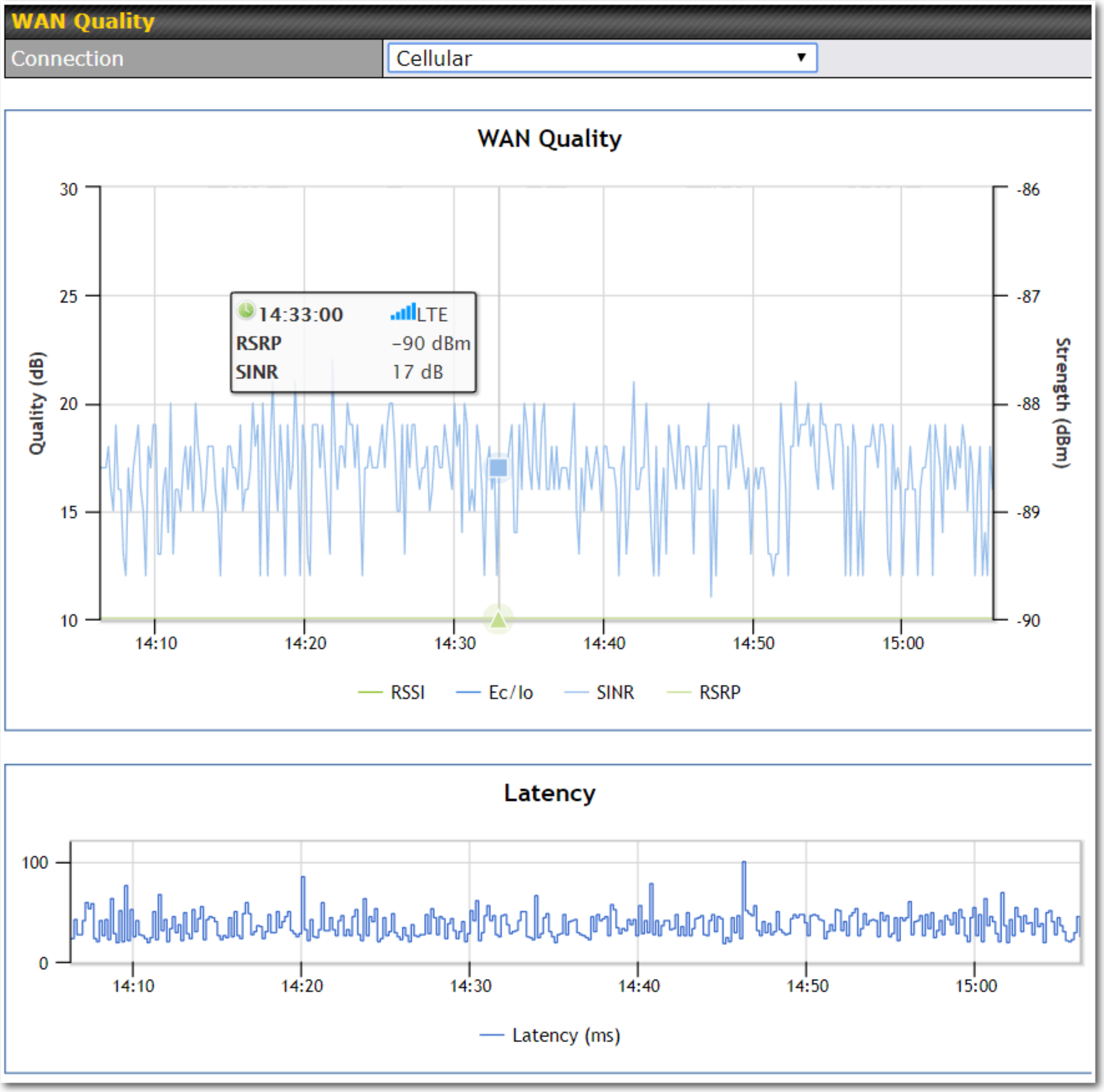
Event log information is located at **Status>Event Log**.



```
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)
```

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


WAN Quality
Connection
Cellular
WAN Quality
14:33:00
LTE
RSRP
-90 dBm
SINR
17 dB
Quality (dB)
Strength (dBm)
30
25
20
15
10
-86
-87
-88
-89
-90
14:10
14:20
14:30
14:40
14:50
15:00
RSSI
Ec/Io
SINR
RSRP
Latency
100
0
14:10
14:20
14:30
14:40
14:50
15:00
Latency (ms)

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

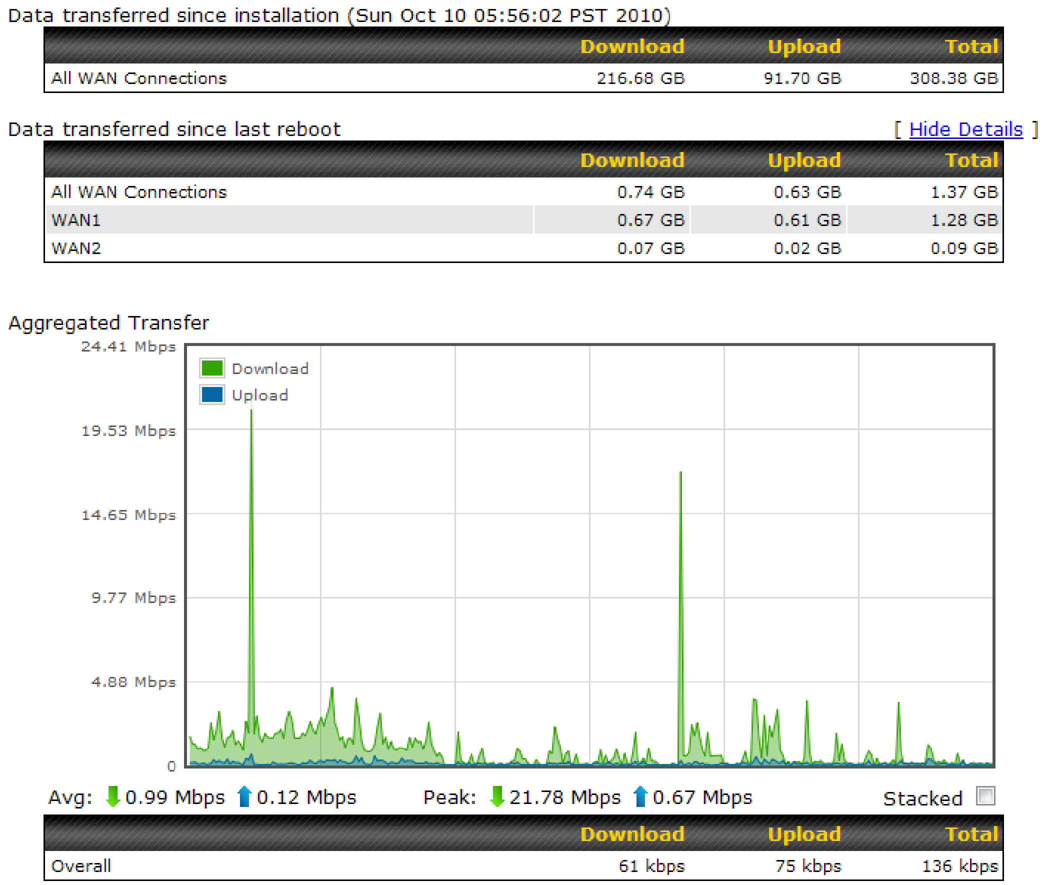
For cellular connections it shows signal strength, quality, throughput and latency for the past hour.

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.



Data transferred since installation (Sun Oct 10 05:56:02 PST 2010)

	Download	Upload	Total
All WAN Connections	216.68 GB	91.70 GB	308.38 GB

Data transferred since last reboot [Hide Details]

	Download	Upload	Total
All WAN Connections	0.74 GB	0.63 GB	1.37 GB
WAN1	0.67 GB	0.61 GB	1.28 GB
WAN2	0.07 GB	0.02 GB	0.09 GB

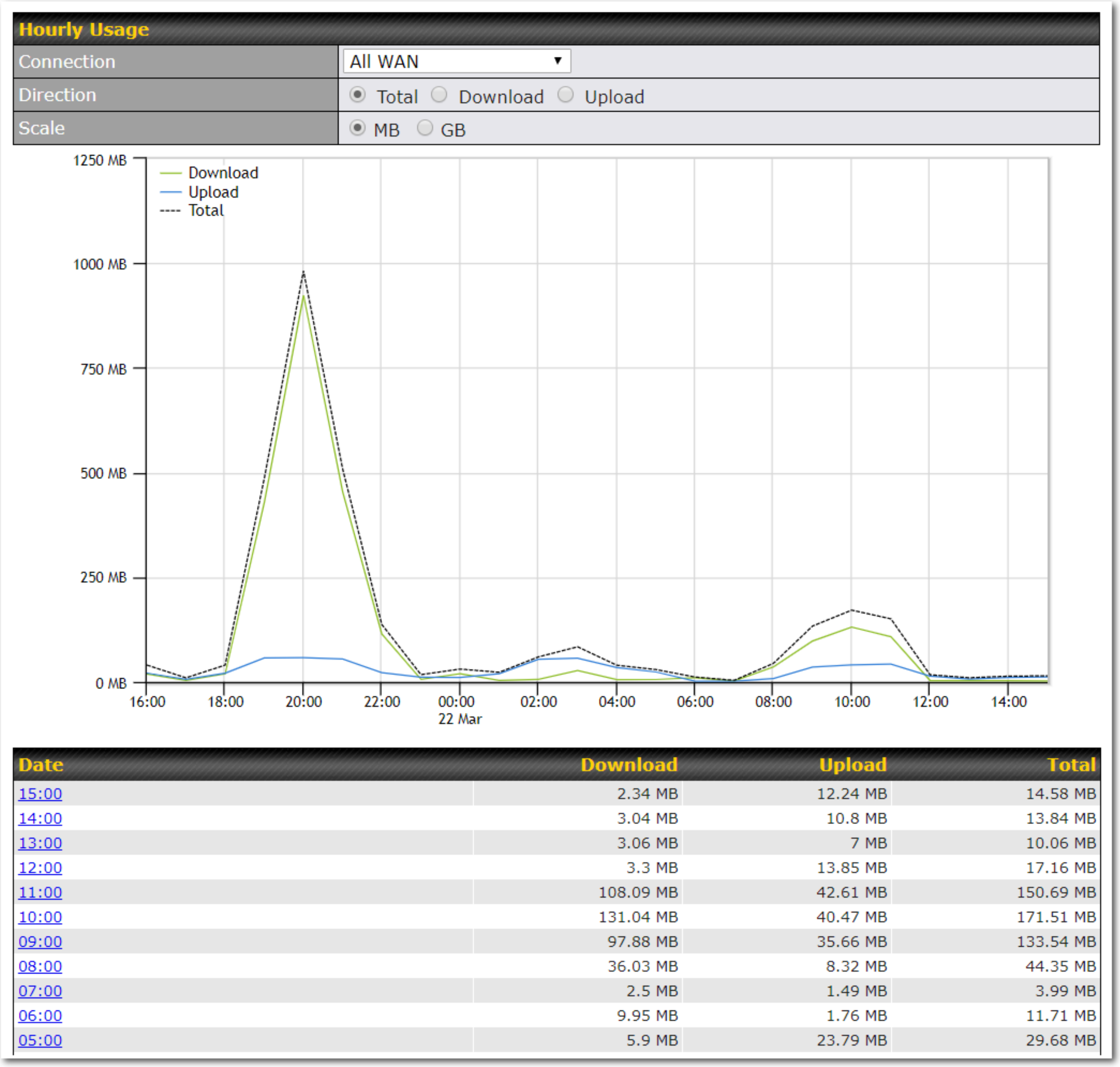
Aggregated Transfer

Avg: ⬇0.99 Mbps ⬆0.12 Mbps Peak: ⬇21.78 Mbps ⬆0.67 Mbps Stacked ☐

	Download	Upload	Total
Overall	61 kbps	75 kbps	136 kbps

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.



Hourly Usage

Connection	All WAN ▼
Direction	● Total ○ Download ○ Upload
Scale	● MB ○ GB

1250 MB
1000 MB
750 MB
500 MB
250 MB
0 MB
Download
Upload
Total
16:00
18:00
20:00
22:00
00:00
22 Mar
02:00
04:00
06:00
08:00
10:00
12:00
14:00

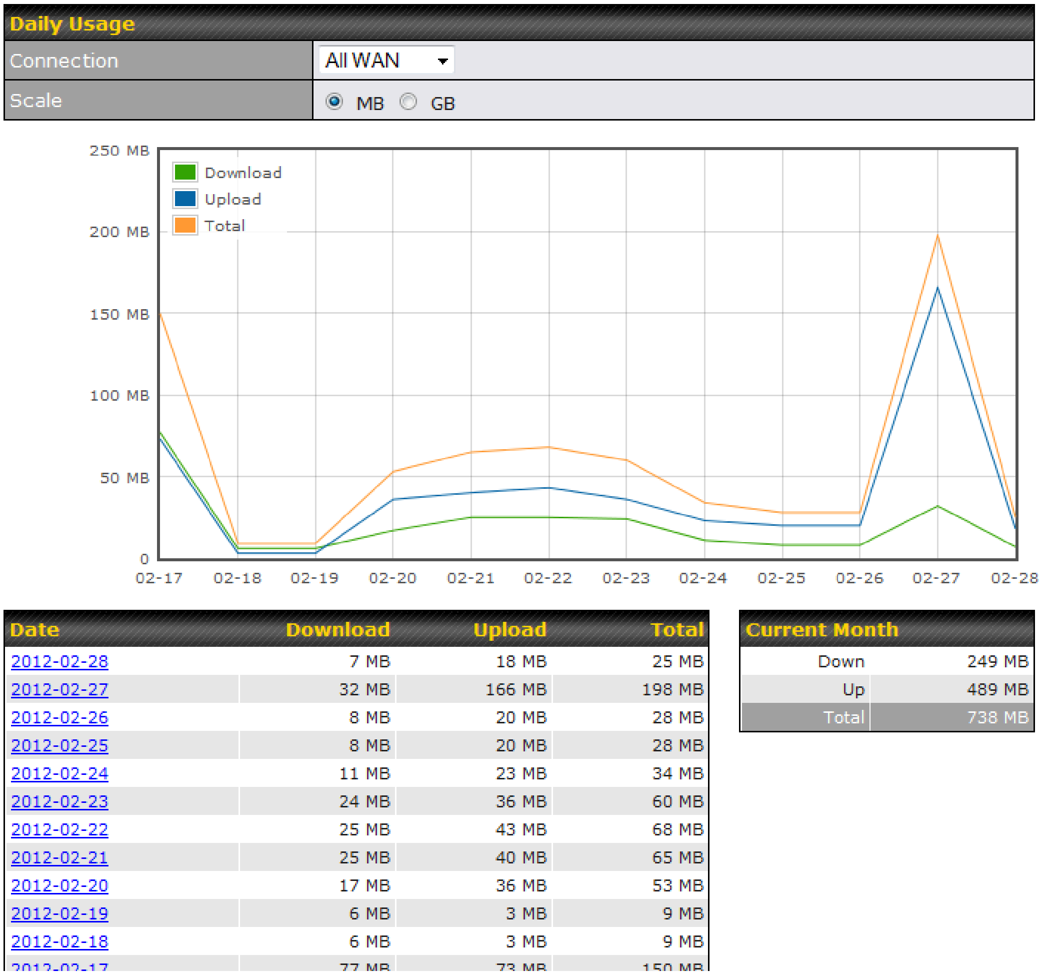
Date	Download	Upload	Total
15:00	2.34 MB	12.24 MB	14.58 MB
14:00	3.04 MB	10.8 MB	13.84 MB
13:00	3.06 MB	7 MB	10.06 MB
12:00	3.3 MB	13.85 MB	17.16 MB
11:00	108.09 MB	42.61 MB	150.69 MB
10:00	131.04 MB	40.47 MB	171.51 MB
09:00	97.88 MB	35.66 MB	133.54 MB
08:00	36.03 MB	8.32 MB	44.35 MB
07:00	2.5 MB	1.49 MB	3.99 MB
06:00	9.95 MB	1.76 MB	11.71 MB
05:00	5.9 MB	23.79 MB	29.68 MB

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**).



Daily Usage

Connection	All WAN
Scale	● MB ○ GB

Date	Download	Upload	Total
2012-02-28	7 MB	18 MB	25 MB
2012-02-27	32 MB	166 MB	198 MB
2012-02-26	8 MB	20 MB	28 MB
2012-02-25	8 MB	20 MB	28 MB
2012-02-24	11 MB	23 MB	34 MB
2012-02-23	24 MB	36 MB	60 MB
2012-02-22	25 MB	43 MB	68 MB
2012-02-21	25 MB	40 MB	65 MB
2012-02-20	17 MB	36 MB	53 MB
2012-02-19	6 MB	3 MB	9 MB
2012-02-18	6 MB	3 MB	9 MB
2012-02-17	77 MB	73 MB	150 MB

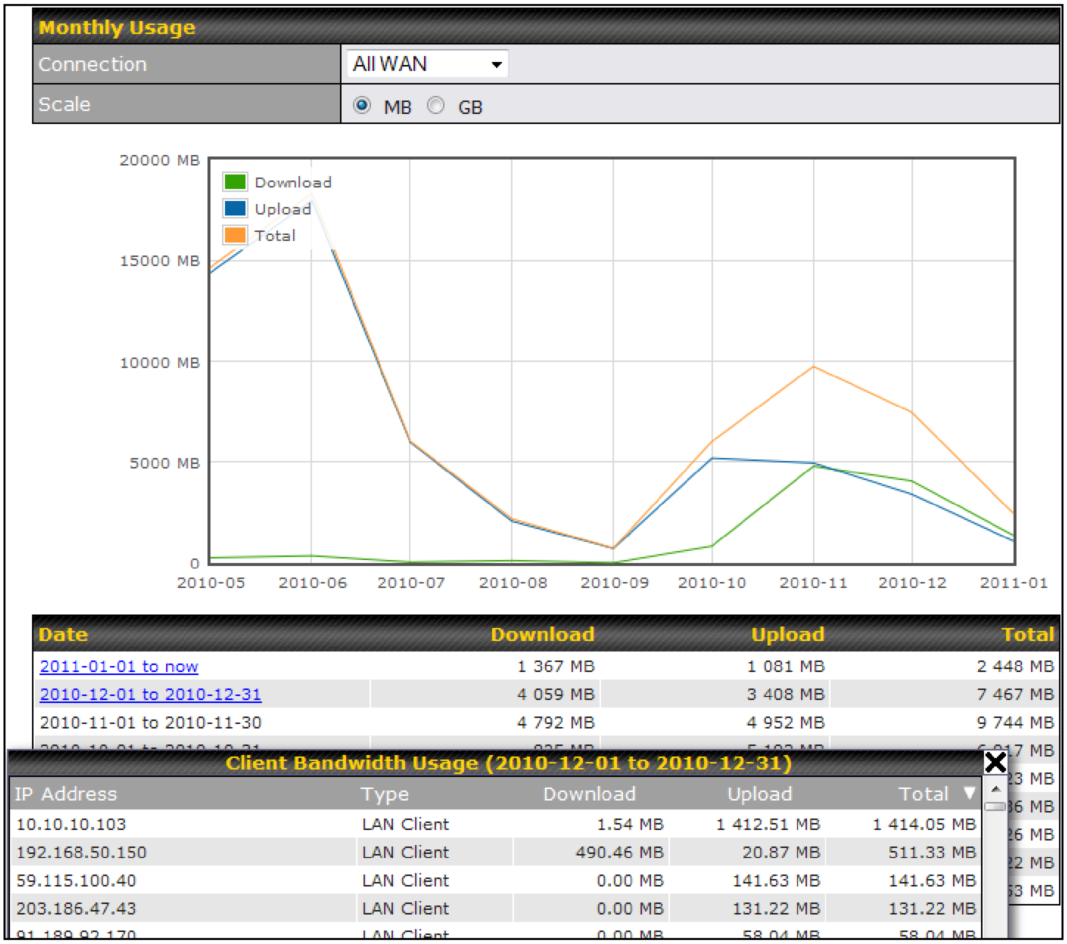
Current Month	
Down	249 MB
Up	489 MB
Total	738 MB

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**).


20000 MB
15000 MB
10000 MB
5000 MB
0
Download
Upload
Total
2010-05
2010-06
2010-07
2010-08
2010-09
2010-10
2010-11
2010-12
2011-01

Monthly Usage

Connection: All WAN

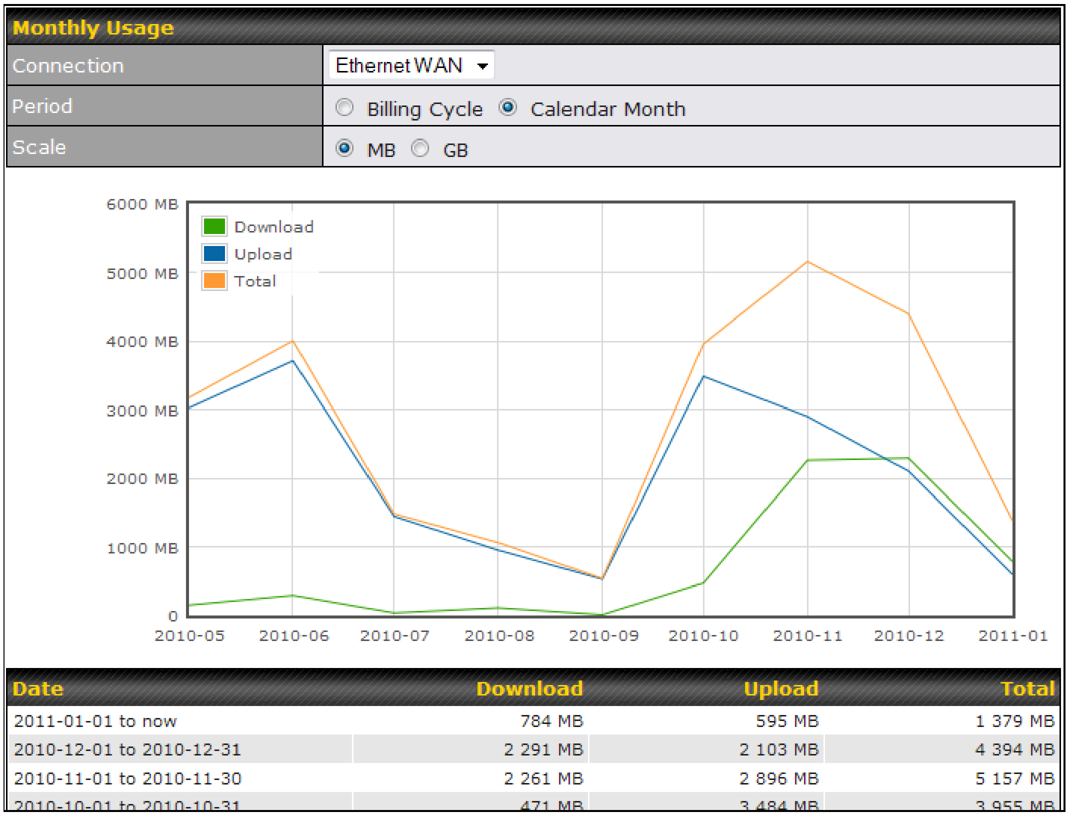
Scale: ● MB ○ GB

Date	Download	Upload	Total
2011-01-01 to now	1 367 MB	1 081 MB	2 448 MB
2010-12-01 to 2010-12-31	4 059 MB	3 408 MB	7 467 MB
2010-11-01 to 2010-11-30	4 792 MB	4 952 MB	9 744 MB

Client Bandwidth Usage (2010-12-01 to 2010-12-31)

IP Address	Type	Download	Upload	Total ▼
10.10.10.103	LAN Client	1.54 MB	1 412.51 MB	1 414.05 MB
192.168.50.150	LAN Client	490.46 MB	20.87 MB	511.33 MB
59.115.100.40	LAN Client	0.00 MB	141.63 MB	141.63 MB
203.186.47.43	LAN Client	0.00 MB	131.22 MB	131.22 MB

All WAN Monthly Bandwidth Usage



Monthly Usage

Connection	Ethernet WAN
Period	○ Billing Cycle ● Calendar Month
Scale	● MB ○ GB

🟩 Download
🟦 Upload
🟧 Total
6000 MB
5000 MB
4000 MB
3000 MB
2000 MB
1000 MB
0
2010-05
2010-06
2010-07
2010-08
2010-09
2010-10
2010-11
2010-12
2011-01

Date	Download	Upload	Total
2011-01-01 to now	784 MB	595 MB	1 379 MB
2010-12-01 to 2010-12-31	2 291 MB	2 103 MB	4 394 MB
2010-11-01 to 2010-11-30	2 261 MB	2 896 MB	5 157 MB
2010-10-01 to 2010-10-31	471 MB	3 484 MB	3 955 MB

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.

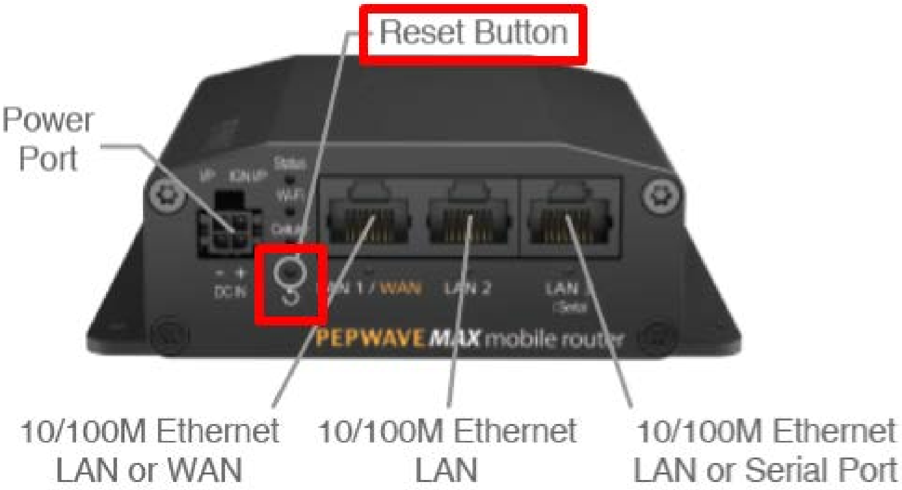
Note: There is a dual function to the reset button.

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.


Reset Button
Power Port
10/100M Ethernet LAN or WAN
10/100M Ethernet LAN
10/100M Ethernet LAN or Serial Port
PEPWAVE MAX mobile router

Appendix B: FusionSIM Manual

Peplink has developed a unique technology called FusionSIM, which allows SIM cards to remotely link to a cellular router. This can be done via cloud or within the same physical network. There are a few key scenarios to fit certain applications.

The purpose of this manual is to provide an introduction on where to start and how to set up for the most common scenarios and uses.

Requirements

1. A Cellular router that supports FusionSIM technology
2. SIM Injector
3. SIM card

Notes:

- Always check for the latest Firmware version for both the cellular router and the SIM Injector. You can also check for the latest Firmware version on the device's WEB configuration page.
- A list of products that support FusionSIM can be found on the SIM Injector WEB page. Please check under the section **Supported models**.

SIM Injector reset and login details

How to reset a SIM Injector:

- Hold the reset button for 5-10 seconds. Once the LED status light turns RED, the reset button can be released. SIM Injector will reboot and start with the factory default settings.

The default WEB login settings:

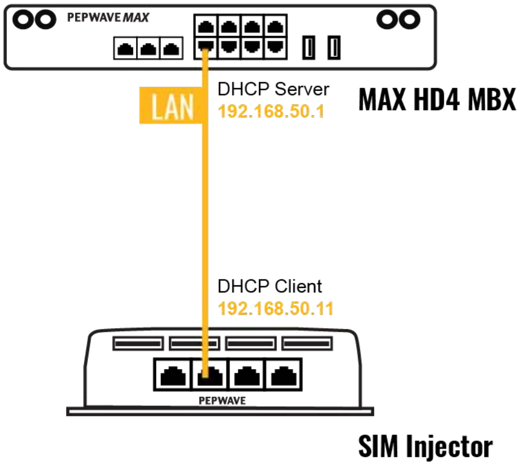
- **User**: admin
- **Password**: admin
- IP address: the device only has a DHCP client and no fallback IP address. Therefore, it is advised to check every time what IP address is assigned to the SIM Injector.

Notes:

- The SIM Injector can be monitored via InControl 2. Configuration is not supported.

Scenario 1: SIM Injector in LAN of Cellular Router

Setup topology



This is the most basic scenario in which the SIM Injector is connected directly to the cellular router's LAN port via an ethernet cable. This allows for the cellular router to be positioned for the best possible signal. Meanwhile, the SIM cards can be conveniently located in other locations such as the office, passenger area, or the bridge of a ship. The SIM Injector allows for easily swapping SIM cards without needing to access a cellular router.

IMPORTANT: Cellular WAN will not fallback to the local SIM if it is configured to use the SIM Injector.

Configuring the SIM Injector

1. Connect the SIM Injector to the LAN port of the cellular router.
2. Insert SIM cards into the SIM Injector. The SIM cards will be automatically detected.

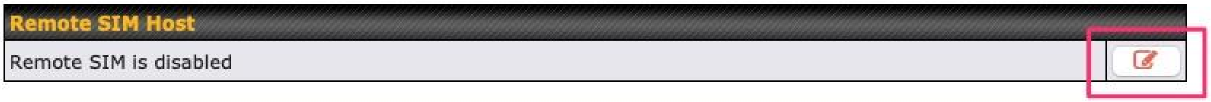
IMPORTANT: SIM cards inserted into SIM Injector must not have a PIN code.

Note 1: The SIM Injector gets its IP address via DHCP and doesn't have a static IP address. To find it's address, please check the DHCP lease on the cellular router.

Configuring the Cellular Router

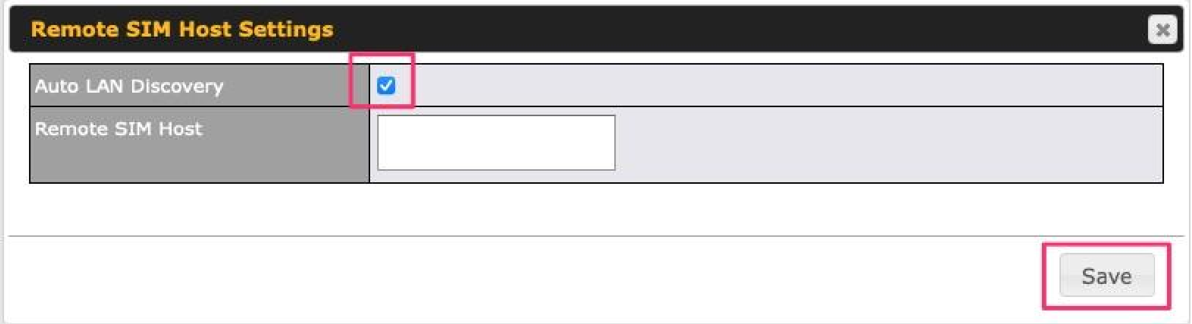
Step 1. Enable the SIM Injector communication protocol.

1a. If you are using a Balance cellular router, go to the **Network** tab (top navigation bar).
1b. If you are using a MAX cellular router, go to the **Advanced** tab (top navigation bar).
2. Under **Misc. settings** (left navigation bar) find **Remote SIM Management**.
3. In **Remote SIM Management**, click on the edit icon next to **Remote SIM is Disabled**.


Remote SIM Host

Remote SIM is disabled

4. Check the **Auto LAN discovery** checkbox and click **Save** and **Apply Changes**.

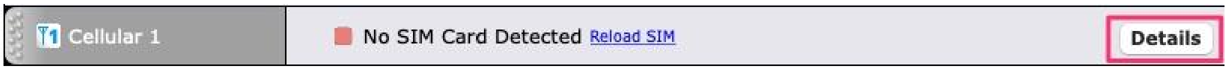

Remote SIM Host Settings

Auto LAN Discovery	☑
Remote SIM Host	

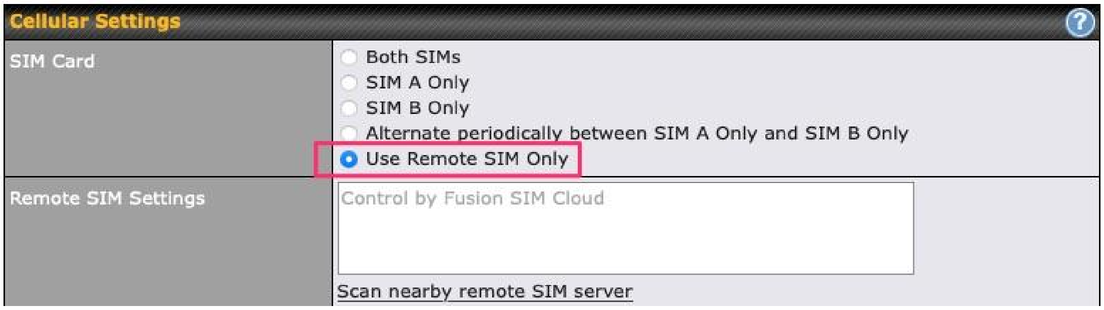
5. Click **Save** and then **Apply Changes**.

Step 2. Enable RemoteSIM for the selected Cellular interface.

1. Go to **Network** (top navigation bar), then **WAN** (left navigation bar) and click **Details** for a selected cellular WAN. This will open the WAN Connection Settings page.


Cellular 1 — 🟥 No SIM Card Detected Reload SIM

2. Scroll down to **Cellular settings**.
3. In the **SIM Card** section, select **Use Remote SIM Only**.

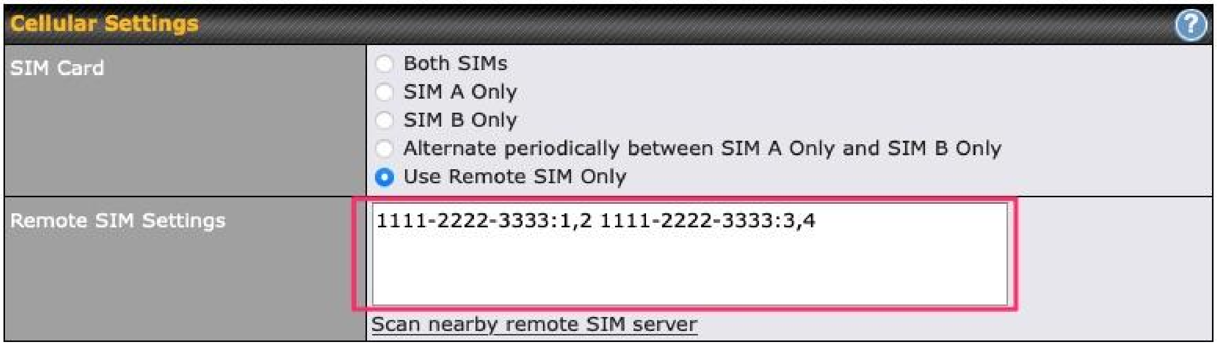

Cellular Settings

SIM Card	○ Both SIMs ○ SIM A Only ○ SIM B Only ○ Alternate periodically between SIM A Only and SIM B Only ● Use Remote SIM Only
Remote SIM Settings	Control by Fusion SIM Cloud Scan nearby remote SIM server

4. Enter configuration settings in **Remote SIM Settings** section. Click on **Scan nearby remote SIM server** to show the serial number(s) of the connected SIM Injector(s). Available configuration options for cellular interface are shown below:

A. Defining SIM Injector(s)
   - Format: <S/N>
   - Example 1: 1111-2222-3333
   - Example 2: 1111-2222-3333 4444-5555-6666

B. Defining SIM Injector(s) SIM slot(s):
   - Format: <S/N:slot number>
   - Example 1: 1111-2222-3333:7,5 (the Cellular Interface will use SIM in slot 7, then 5)
   - Example 2: 1111-2222-3333:1,2 1111-2222-3333:3,4 (the cellular Interface will use SIM in slot 1, then in 2 from the first SIM Injector, and then it will use 3 and 4 from the second SIM Injector).


Cellular Settings

SIM Card	○ Both SIMs ○ SIM A Only ○ SIM B Only ○ Alternate periodically between SIM A Only and SIM B Only ● Use Remote SIM Only
Remote SIM Settings	1111-2222-3333:1,2 1111-2222-3333:3,4 Scan nearby remote SIM server

Note: It is recommended to use different SIM slots for each cellular interface.

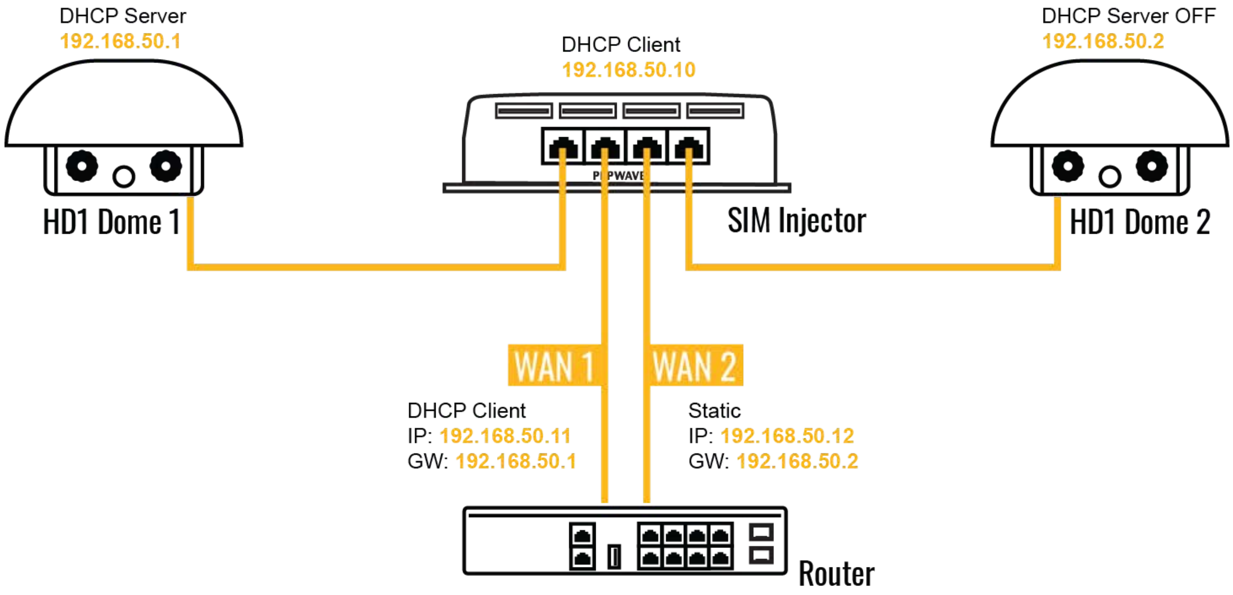
5. Click **Save** and **Apply Changes**.

Step 3. (Optional) Custom SIM cards settings.

1a. For a Balance router, go to the **Network** (Top tab).
1b. For a MAX router, go to the **Advanced** (Top tab).
2. Under **Misc. settings** (Left-side tab) find **Remote SIM Management**.
3. Click on the **Add Remote SIM** button, fill in all the required info and click **Save**. This section allows defining custom requirements for a SIM card located in a certain SIM slot:
   - Enable/Disable roaming (by default roaming is disabled).
   - Add Custom mobile operator settings (APN, user name, password).
4. Repeat configuration for all SIM cards which need custom settings.
5. Click **Apply Changes** to take effect.

Scenario 2: SIM Injector in WAN of main Router and multiple Cellular Routers

Setup topology


DHCP Server
192.168.50.1
HD1 Dome 1
DHCP Client
192.168.50.10
PEPWAVE
SIM Injector
DHCP Server OFF
192.168.50.2
HD1 Dome 2
WAN 1
WAN 2
DHCP Client
IP: 192.168.50.11
GW: 192.168.50.1
Static
IP: 192.168.50.12
GW: 192.168.50.2
Router

In this scenario, each HD Dome creates a WAN connection to the main router. A single SIM Injector is used to provide SIM cards for each HD Dome. The HD Dome can be replaced with any Peplink cellular router supporting RemoteSIM technology.

This scenario requires the completion of the configuration steps shown in Scenario 1 in addition to the configuration steps explained below.

Additional configurations for Cellular Routers

Step 1. Disable the DHCP server.

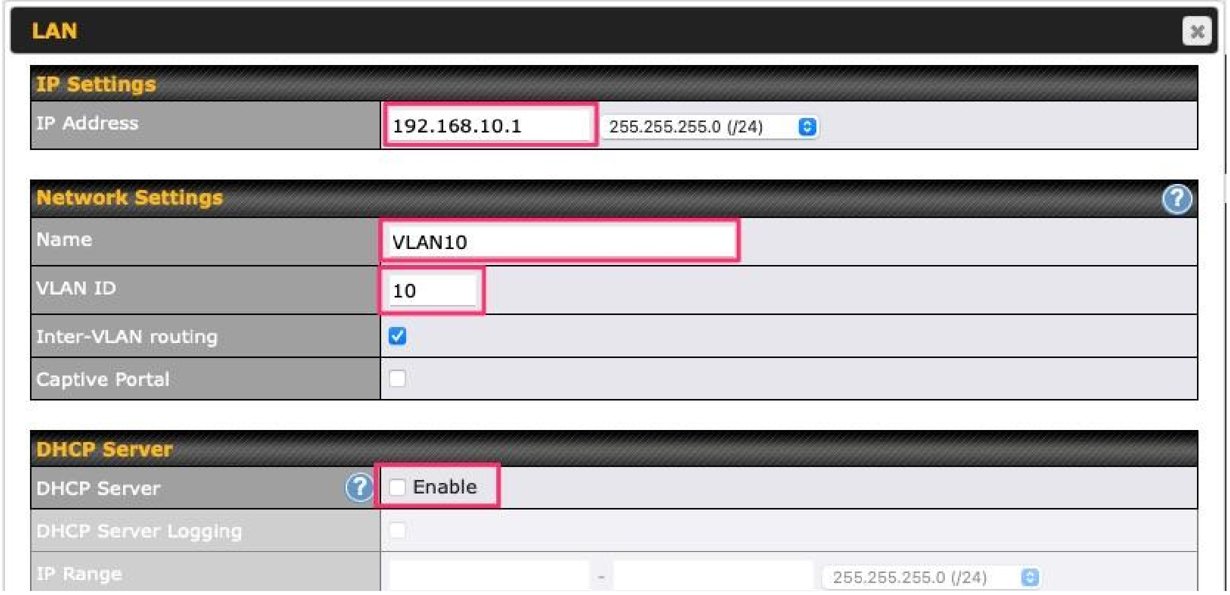
- HD Dome 1 should act as a DHCP server.
- HD Dome 2 should be configured to have a static IP address with DHCP disabled.
- Both routers should be in the same subnet (e.g. 192.168.50.1 and 192.168.50.2).

1. Go to **Network** (Top tab), then **Network Settings** (Left-side tab), and click on **Untagged LAN**. This will open up the LAN settings page.
2. Change the IP address to 192.168.50.2.
3. In the **DHCP Server** section, uncheck the checkbox to disable DHCP Server.
4. Click **Save** and **Apply Changes**.

Step 2. Ethernet port configuration

The Ethernet port must be set to **ACCESS** mode for each HD Dome. To do this, dummy VLANs need to be created first.

1. Go to **Network** (Top tab), then **Network Settings** (Left-side tab), and click on **New LAN**. This will open the settings page to create a dummy VLAN.
2. The image below shows the values that need to be changed to create a new VLAN:



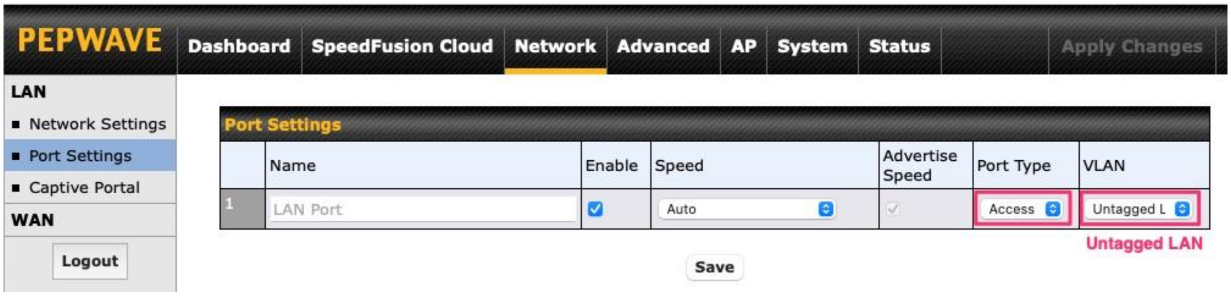
IP Settings	
IP Address	192.168.10.1 255.255.255.0 (/24)

Network Settings	
Name	VLAN10
VLAN ID	10
Inter-VLAN routing	☑
Captive Portal	☐

DHCP Server	
DHCP Server	☐ Enable
DHCP Server Logging	☐
IP Range	- 255.255.255.0 (/24)

Note: set different IP addresses for each HD dome (e.g. 192.168.10.1 and 192.168.10.2).

3. Click Save and **Apply Changes**.
4. Go to **Network** (Top tab), then **Port Settings** (Left-side tab).
5. Set the Port Type to **Access** and set VLAN to **Untagged LAN** (see picture below).


PEPWAVE
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
Apply Changes
LAN
Network Settings
Port Settings
Captive Portal
WAN
Logout
Save
Untagged LAN

Port Settings

	Name	Enable	Speed	Advertise Speed	Port Type	VLAN
1	LAN Port	☑	Auto	✓	Access	Untagged L

6. Click **Save** and **Apply Changes**.

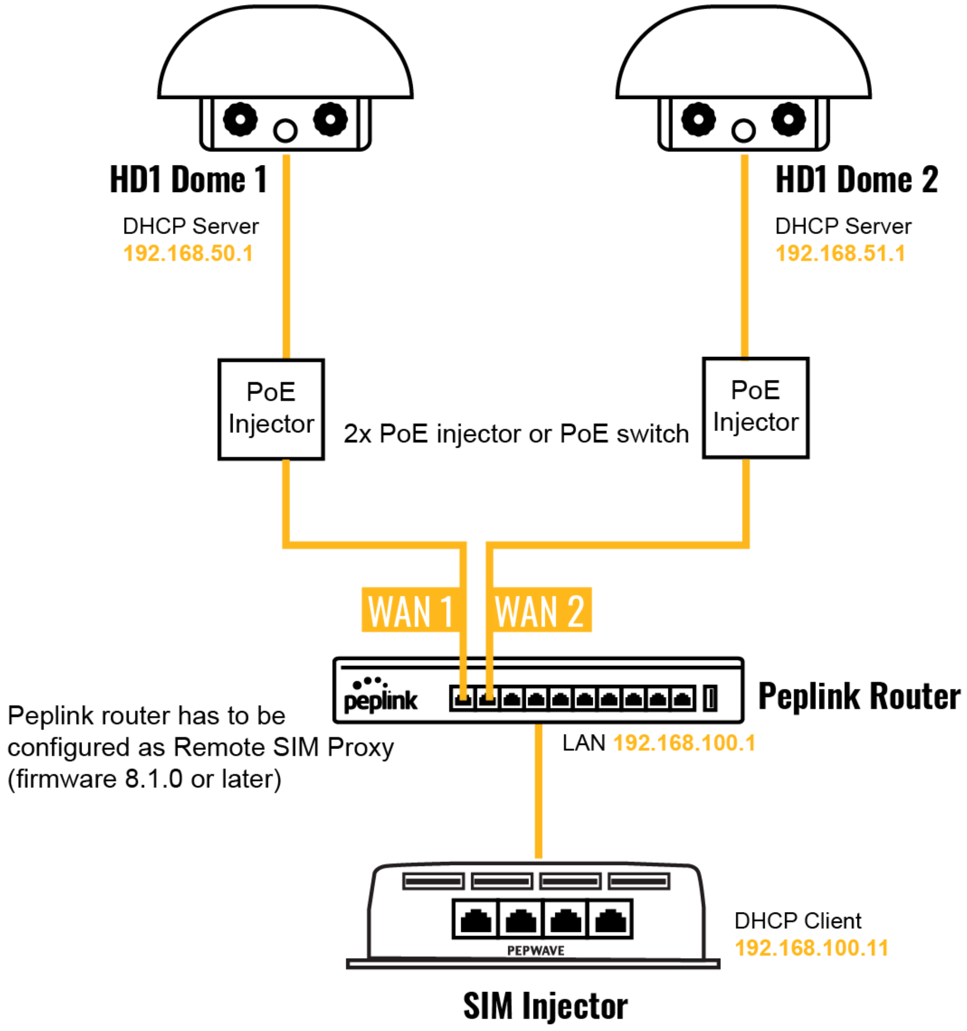
Configuration requirements for the main Router

Requirements for the main router are:

- Configure **WAN 1** as a DHCP client.
- **WAN 1** will automatically get the Gateway IP address from HD Dome 1.
- Configure **WAN 2** as a Static IP and set it to 192.168.50.12.
- Configure **WAN 2** Gateway to 192.168.50.2. Same as the HD Dome 2’s IP address.

Scenario 3: SIM Injector in LAN of main Router and multiple Cellular Routers

Setup topology


HD1 Dome 1
DHCP Server
192.168.50.1
HD1 Dome 2
DHCP Server
192.168.51.1
PoE Injector
2x PoE injector or PoE switch
PoE Injector
WAN 1
WAN 2
peplink
Peplink Router
Peplink router has to be configured as Remote SIM Proxy (firmware 8.1.0 or later)
LAN 192.168.100.1
PEPWAVE
DHCP Client
192.168.100.11
SIM Injector

In this scenario, SIMs are provided to the HD Domes via the main router. In this example, the **Remote SIM Proxy** functionality needs to be enabled on the main router.

Notes:

- HD Dome can be replaced with any other cellular router that supports RemoteSIM.
- It is recommended to use Peplink Balance series or X series routers as the main router.

This scenario requires the completion of the configuration steps for the cellular router and the SIM Injector as in Scenario 1. The configuration for the main router is explained below.

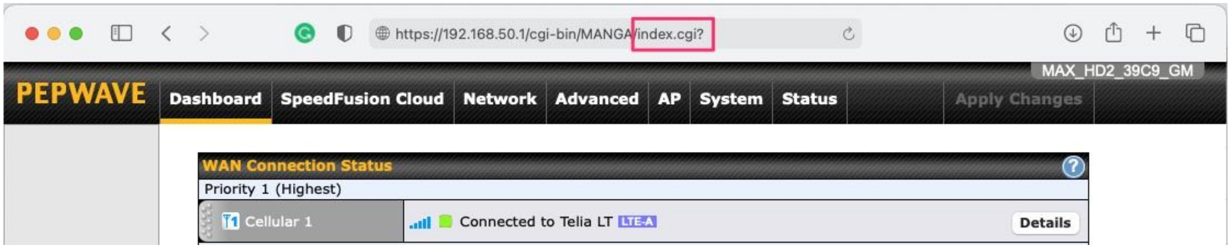
Main Router configuration

IMPORTANT: Main router LAN side and Cellular Routers must be configured using different subnets, e.g. 192.168.**50**.1/24 and 192.168.**100**.1/24.

Note: please make sure the Peplink router is running Firmware 8.1.0 or above.

1. Open the main router WEB interface and change:
From <IP address>/cgi-bin/MANGA/**index.cgi** to <IP address>/cgi-bin/MANGA/**support.cgi**.

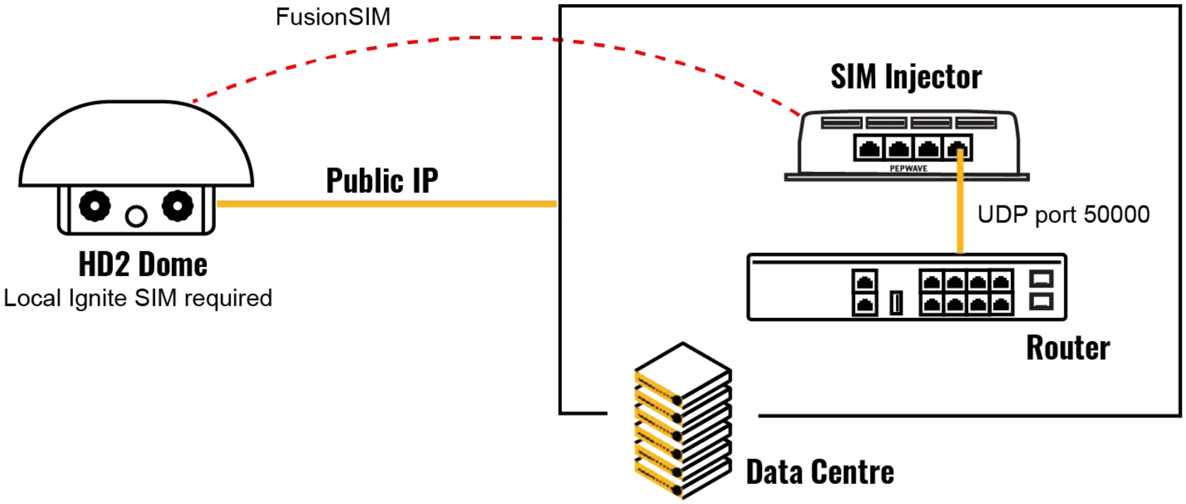
This will open the support.cgi page.


https://192.168.50.1/cgi-bin/MANGA/index.cgi?
MAX_HD2_39C9_GM
PEPWAVE
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
Apply Changes
WAN Connection Status
Priority 1 (Highest)
Cellular 1
Connected to Telia LT LTE-A
Details

2. Scroll down to find **Remote SIM Proxy** and click on **[click to configure]** that is located next to it.
3. Check the **Enable** checkbox.
4. Click on **Save**.
5. Go back to the index.cgi page and click on **Apply Changes**.

Scenario 4: SIM Injector in a remote location

Setup topology



Requirements for installing a SIM Injector in a remote location:

- Cellular router communicates with the SIM Injector via UDP port 50000. Therefore this port must be reachable via public IP over the Internet.
- The one way latency between the cellular router and the SIM Injector should be **up to 250 ms.** A higher latency may lead to stability issues.
- The cellular router must have Internet connection to connect to the SIM Injector. It can be another Internet connection via Ethernet or Fiber if possible, or a secondary cellular interface with a local SIM (Ignite SIM).
- Due to its high latency, it is not recommended to use satellite WAN for connecting to a SIM Injector in remote locations.

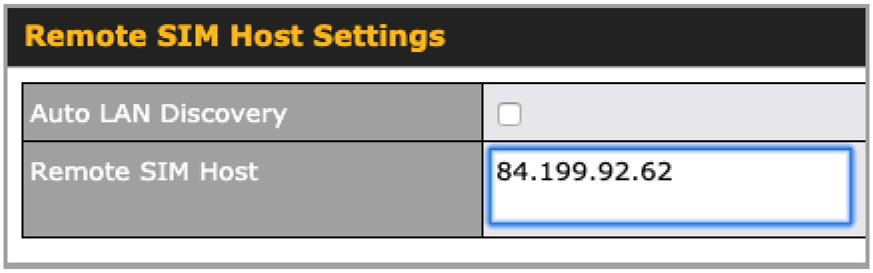
SIM Injector configuration is the same as in Scenario 1.

Cellular Router configuration

Step 1. Enable the SIM Injector communication protocol.

1a. For a Balance cellular router, go to the **Network** (Top tab).
1b. For a MAX cellular router, go to the **Advanced** (Top tab).

2. Under **Misc. settings** (Left-side tab), find **Remote SIM Management**.
3. In **Remote SIM Management**, click on the edit icon next to **Remote SIM is Disabled.**
4. Enter the public IP of the SIM Injector and click **Save** and **Apply Changes**.



Remote SIM Host Settings

Auto LAN Discovery	☐
Remote SIM Host	84.199.92.62

Notes:

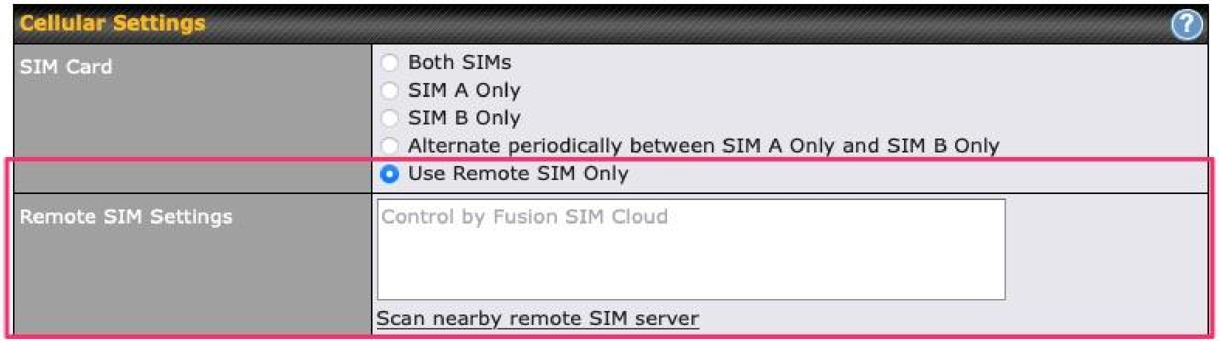
- **Do NOT check Auto LAN Discovery.**
- **Do NOT add a SIM Injector serial number to the Remote SIM Host field.**

Step 2. RemoteSIM and custom SIM card settings configurations are the same as in Scenario 1.

How to check if a Pepwave Cellular Router supports Remote SIM

1. Go to **Network** (Top tab), then **WAN** (Left-side tab), and click **Details** on any cellular WAN. This will open the WAN Connection Settings page.
2. Scroll down to **Cellular settings**.

If you can see the **Remote SIM Settings** section, then the cellular router supports Remote SIMs.

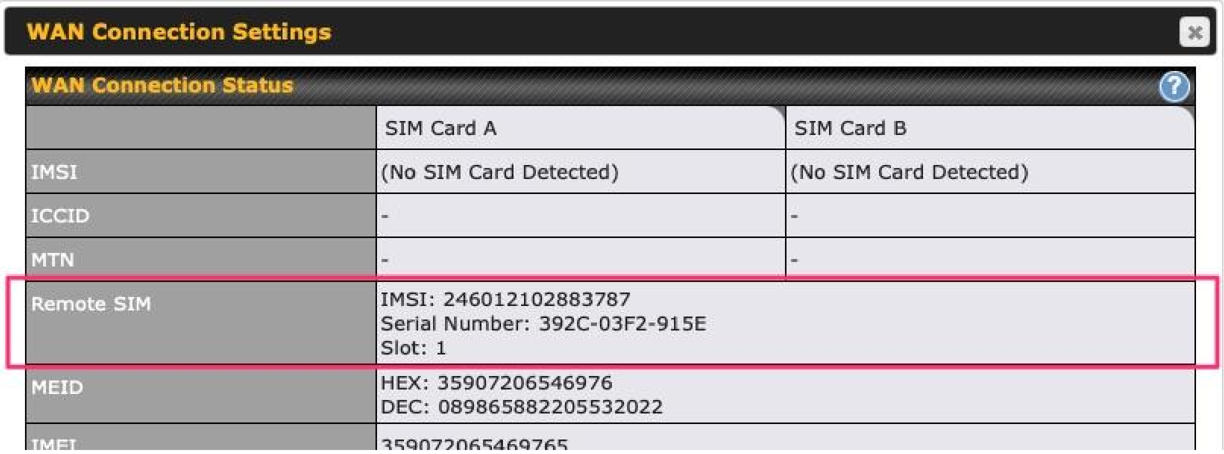


Cellular Settings

SIM Card	○ Both SIMs ○ SIM A Only ○ SIM B Only ○ Alternate periodically between SIM A Only and SIM B Only ● Use Remote SIM Only
Remote SIM Settings	Control by Fusion SIM Cloud Scan nearby remote SIM server

Monitor the status of the Remote SIM

1. Go to **Network** (Top tab), then **WAN** (Left-side tab), and click **Details** on the cellular WAN which was configured to use RemoteSIM.
2. Check the **WAN Connection Status** section. Within the cell WAN details, there is a section for **Remote SIM** (SIM card IMSI, SIM Injector serial number and SIM slot).



WAN Connection Settings

WAN Connection Status

	SIM Card A	SIM Card B
IMSI	(No SIM Card Detected)	(No SIM Card Detected)
ICCID	-	-
MTN	-	-
Remote SIM	IMSI: 246012102883787 Serial Number: 392C-03F2-915E Slot: 1	
MEID	HEX: 35907206546976 DEC: 089865882205532022	
IMEI	359072065469765	

Appendix C: Overview of ports used by Peplink SD-WAN routers and other Peplink services

Default Port Number	Usage	Service	Inbound/Outbound	Default Status
UDP 5246	Data flow	InControl	Outbound	Enabled
TCP 443	HTTPS service	InControl	Outbound	Enabled
TCP 5246	Optional, used when TCP 443 is not responding	InControl	Outbound	Enabled
TCP 5246	Remote Web Admin	InControl Virtual Appliance	Outbound	Enabled
TCP 4500	VPN Data (TCP Mode)	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
TCP 32015	VPN handshake	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
UDP 4500	VPN Data	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
UDP 32015º	VPN Data (alternative)	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
TCP/UDP 4500+N-1^	VPN Sub-Tunnels Data	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
UDP 32015+N-1^	VPN Sub-Tunnels Data (alternative)	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
UDP 4500	VPN Data	IPsec	Inbound / Outbound*	Disabled
UDP 500	VPN initiation	IPsec	Inbound / Outbound*	Disabled
UDP 500	L2TP	Remote User Access	Inbound	Disabled
UDP 1701	L2TP	Remote User Access	Inbound	Disabled
UDP 4500	L2TP	Remote User Access	Inbound	Disabled
UDP 1194	OpenVPN	Remote User Access	Inbound	Disabled
IP 47	PPTP (GRE)	Remote User Access	Inbound	Disabled
TCP 2222	Remote Assistance Direct connection	Peplink Troubleshooting Assistance	Outbound	Enabled
TCP 80	HTTP traffic	Web Admin	Inbound	Enabled

		Interface access		
TCP 443	HTTPS traffic	Web Admin Interface access (secure)	Inbound	Enabled
TCP 8822	SSH	SSH	Inbound	Disabled
UDP 161	SNMP Get	SNMP monitoring	Inbound	Disabled
UDP 162	SNMP Trap	SNMP monitoring	Outbound	Disabled
TCP, UDP 1812	Radius Authentication	Radius	Outbound	Disabled
TCP, UDP 1813	Radius Accounting	Radius	Outbound	Disabled
UDP 123	Network Time Protocol	NTP	Inbound Outbound	Disabled Enabled
TCP 60660	Real-time location data in NMEA format	GPS	Outbound	Disabled

Disclaimer:

- By default, only TCP 32015 and UDP 4500 are needed for PepVPN / SpeedFusion.
- Inbound / Outbound* - Inbound = For Server mode; Outbound = For Client mode
- UDP 32015º - If IPsec VPN or L2TP/IPsec RUA is enabled, the UDP 4500 is occupied, so PepVPN / SpeedFusion will automatically switch to UPD 32015 as VPN data port .
- UDP 32015+N-1^ / TCP/UDP 4500+N-1^ - When using Sub-Tunnels, multiple ports are in use (1 for each Sub-Tunnel profile).
- The default UDP data ports used when using (N number of Sub-Tunnel profiles) are: 4500…4500+N-1, or (when port 4500 is in use by IPsec or L2TP/IPsec) 32015… 32015+N-1".

Appendix D: 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.

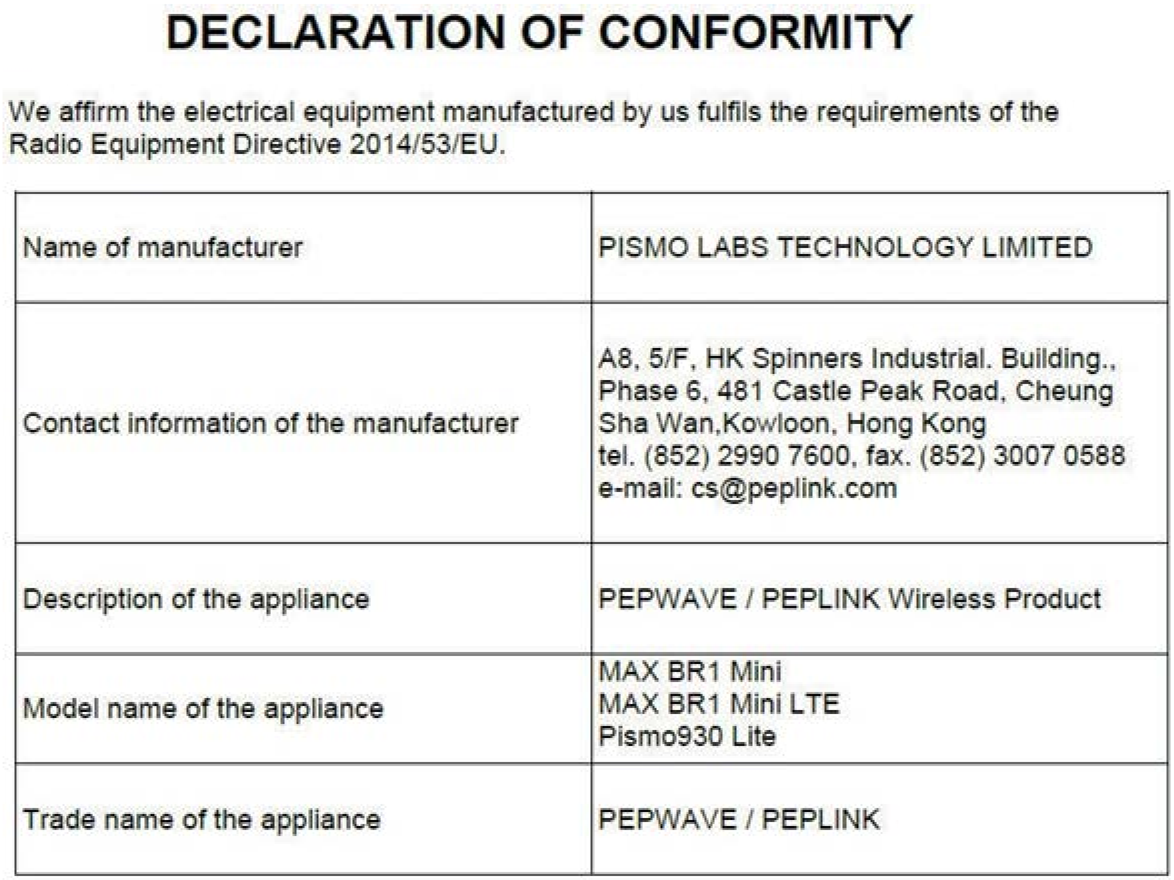
FCC Caution Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. IEEE 802.11b or 802.11g operation of this product in the U.S.A. is firmware-limited to channels 1 through 11.

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.

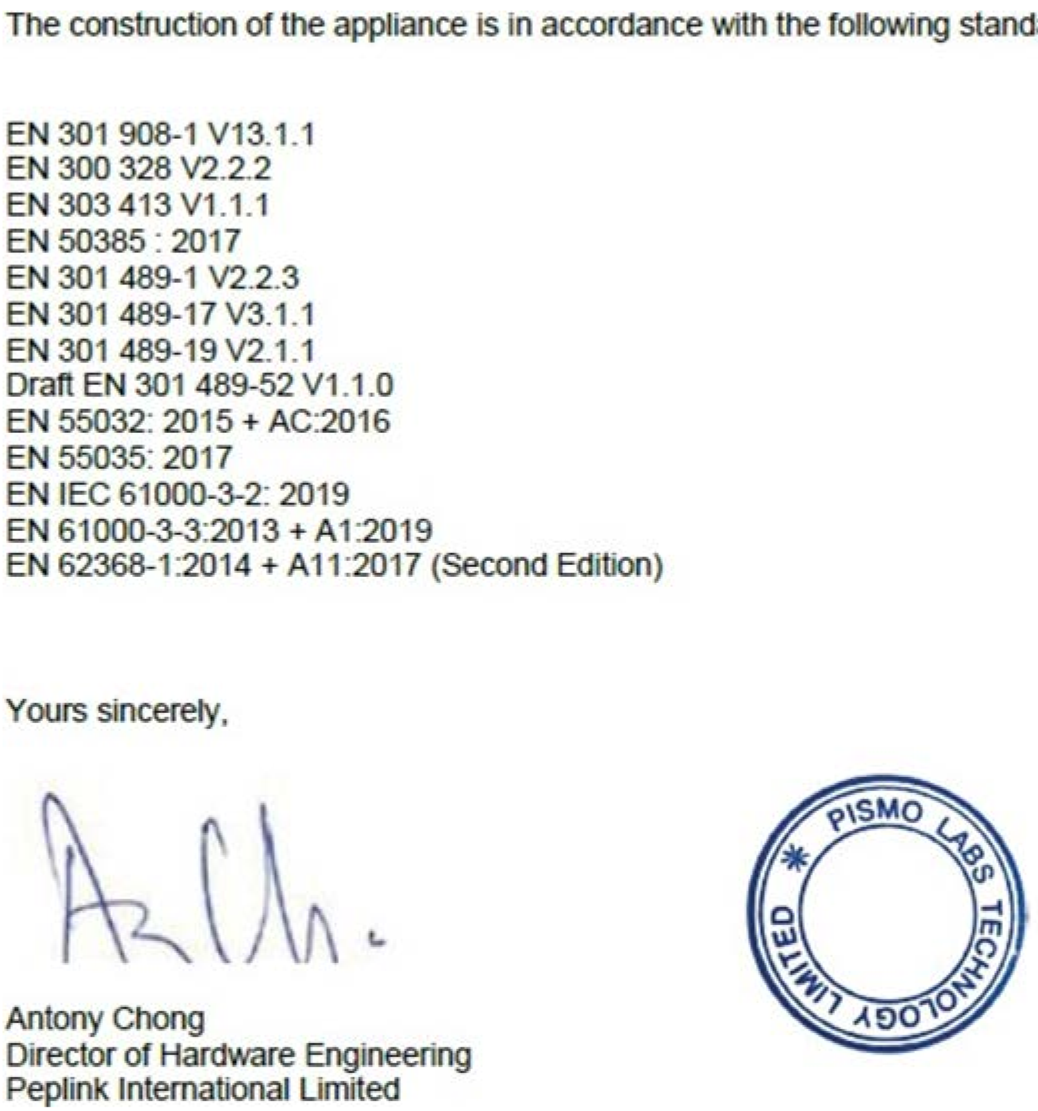
CE Statement for Pepwave Routers (MAX BR1 Mini for EC25-E)



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



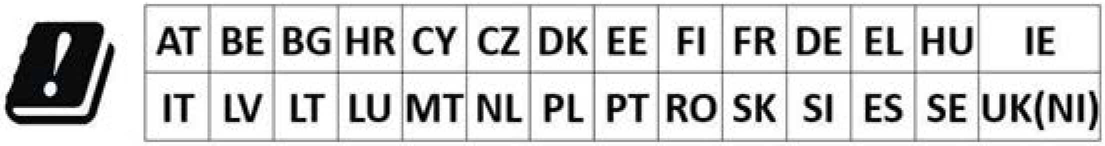
The construction of the appliance is in accordance with the following standards:

EN 301 908-1 V13.1.1
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
EN 301 489-19 V2.1.1
Draft EN 301 489-52 V1.1.0
EN 55032: 2015 + AC:2016
EN 55035: 2017
EN IEC 61000-3-2: 2019
EN 61000-3-3:2013 + A1:2019
EN 62368-1:2014 + A11:2017 (Second Edition)

Yours sincerely,

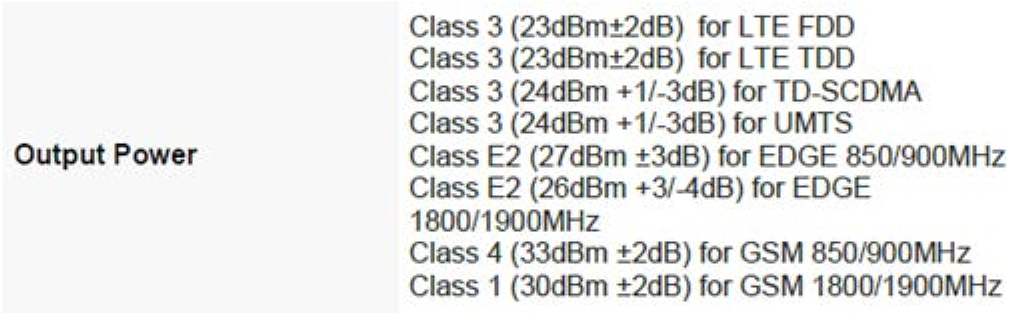
PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



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

2.4GHz (2412 – 2472 MHz) : 16.38 dBm
WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

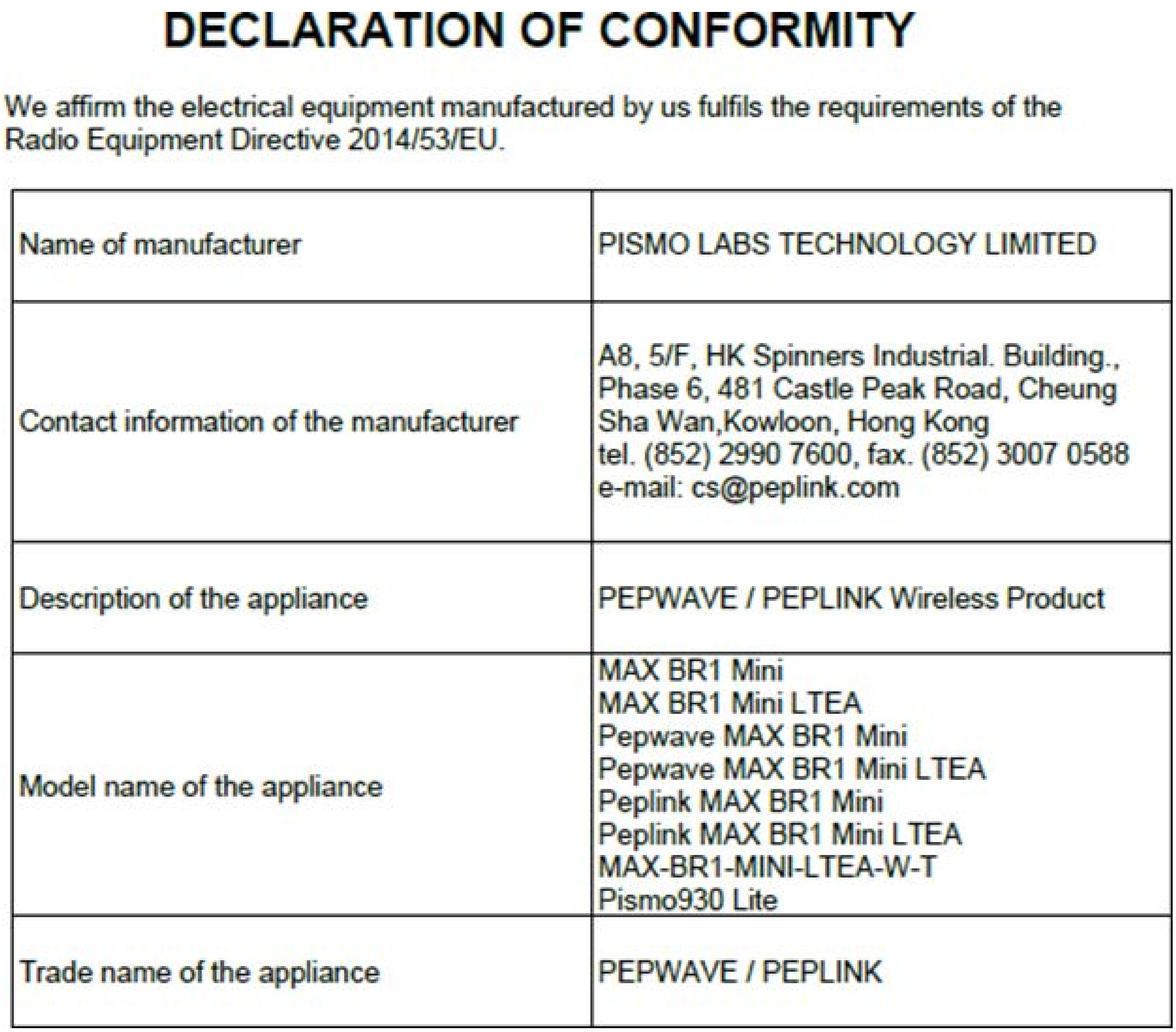


Output Power	Class 3 (23dBm±2dB) for LTE FDD Class 3 (23dBm±2dB) for LTE TDD Class 3 (24dBm +1/-3dB) for TD-SCDMA Class 3 (24dBm +1/-3dB) for UMTS Class E2 (27dBm ±3dB) for EDGE 850/900MHz Class E2 (26dBm +3/-4dB) for EDGE 1800/1900MHz Class 4 (33dBm ±2dB) for GSM 850/900MHz Class 1 (30dBm ±2dB) for GSM 1800/1900MHz

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/

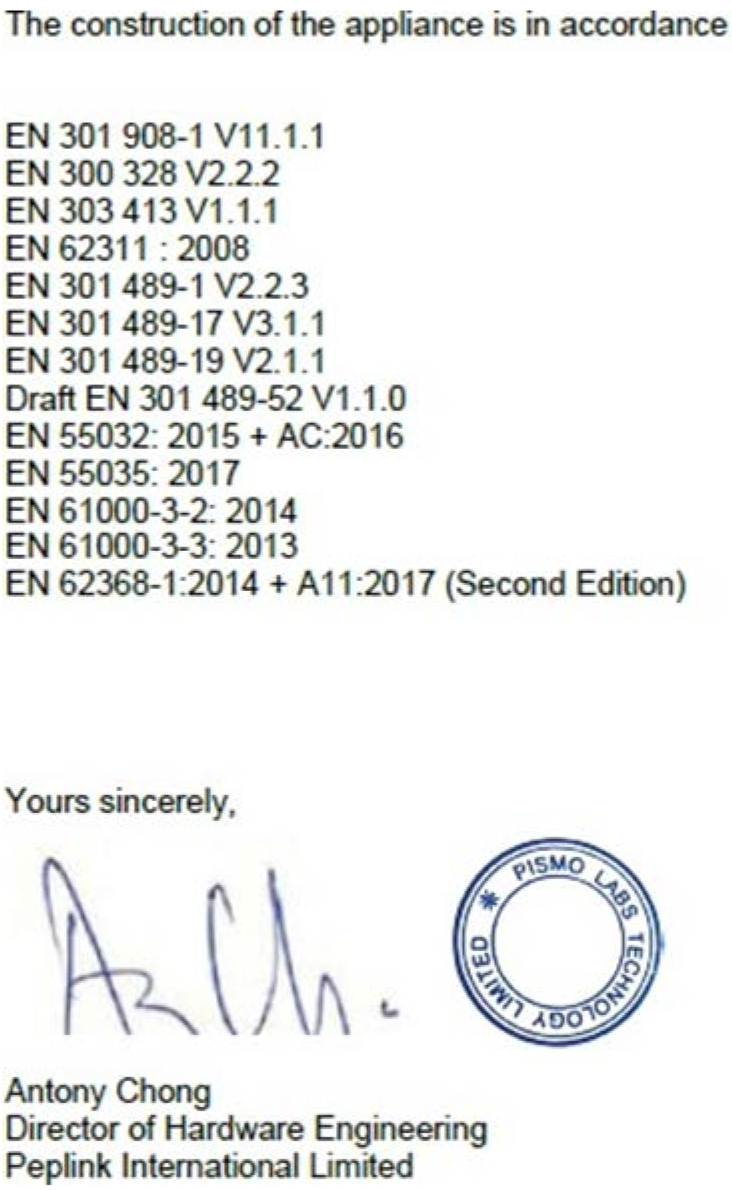
CE Statement for Pepwave Routers (MAX BR1 Mini for MC7455)



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 LTEA Pepwave MAX BR1 Mini Pepwave MAX BR1 Mini LTEA Peplink MAX BR1 Mini Peplink MAX BR1 Mini LTEA MAX-BR1-MINI-LTEA-W-T Pismo930 Lite
Trade name of the appliance	PEPWAVE / PEPLINK



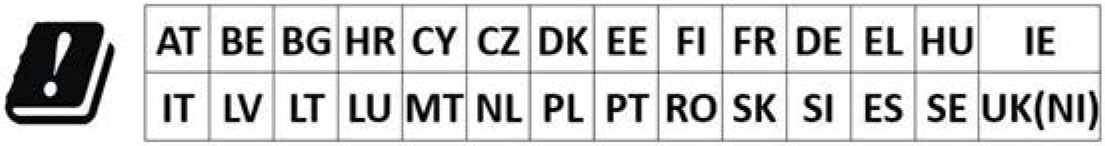
The construction of the appliance is in accordance with the following standards:

EN 301 908-1 V11.1.1
EN 300 328 V2.2.2
EN 303 413 V1.1.1
EN 62311 : 2008
EN 301 489-1 V2.2.3
EN 301 489-17 V3.1.1
EN 301 489-19 V2.1.1
Draft EN 301 489-52 V1.1.0
EN 55032: 2015 + AC:2016
EN 55035: 2017
EN 61000-3-2: 2014
EN 61000-3-3: 2013
EN 62368-1:2014 + A11:2017 (Second Edition)

Yours sincerely,

PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



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

2.4GHz (2412 – 2472 MHz) : 16.38 dBm

WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

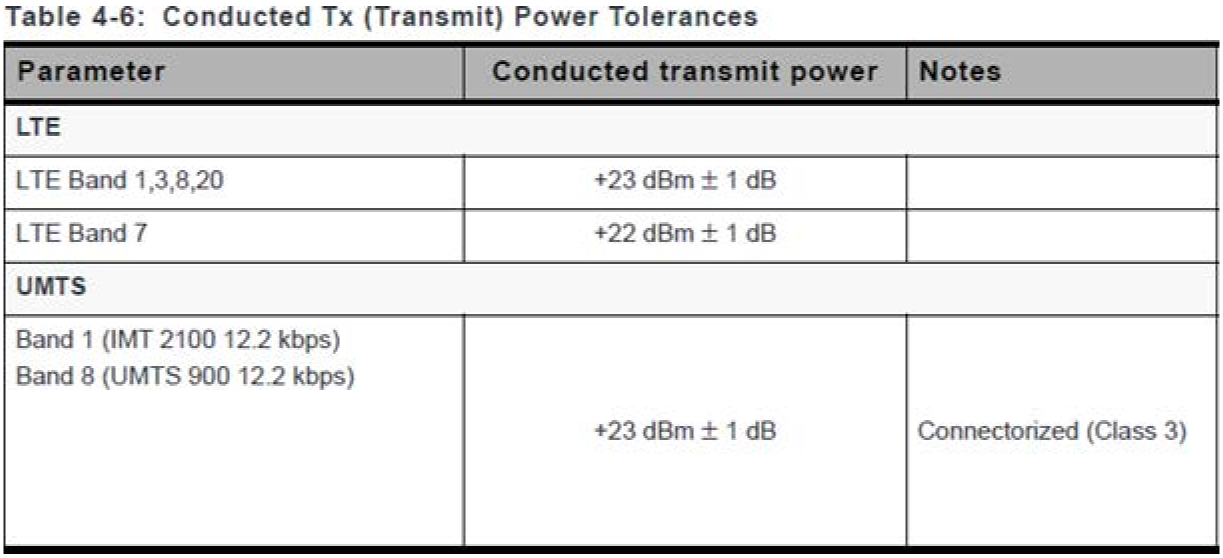


Table 4-6: Conducted Tx (Transmit) Power Tolerances

Parameter	Conducted transmit power	Notes
LTE		
LTE Band 1,3,8,20	+23 dBm ± 1 dB	
LTE Band 7	+22 dBm ± 1 dB	
UMTS		
Band 1 (IMT 2100 12.2 kbps) Band 8 (UMTS 900 12.2 kbps)	+23 dBm ± 1 dB	Connectorized (Class 3)

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

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Le présent produit est conforme aux spécifications techniques applicables d'Innovation, Sciences et Développement économique Canada.

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

Cet équipement est conforme avec l'exposition aux radiations ISED définies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à une distance minimum de 20 cm entre le radiateur et votre corps.

FCC & IC Requirements for Operation in the United States and Canada (for MAX BR1 Mini)

FCC ID : U8G-P1930LITER6

FCC 15.21: The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

RF exposure warning: This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

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.

IC Warning:

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions

1. This device may not cause interference.
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Le present appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence.

L'exploitation est autorisee aux deux conditions suivantes

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioelect rique subi, meme si le brouillage est susceptible d'en compromettre le fonctionnement.

Informations concernant l'exposition aux frequences radio (RF)

Cet equipement est conforme avec l'exposition aux radiations IC definies pour un environnement noncontrole.

Cet equipement doit etre installe et utilise a une distance minimum de 20 cm entre le radiateuret votre corps.

Cet emetteur ne doit pas etre co-localisees ou operant en conjonction avec une autreantenne ou transmetteur.

Les utilisateurs finaux et les installateurs doivent etre informes des instructions d'installation de l'antenne et des conditions de fonctionnement de l'emetteur afin de satisfaire a la conformite d'exposition RF.

This radio transmitter IC 20682-P1930LITER6 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.

Le present emetteur radio 20682-P1930LITER6 a ete approuve par Innovation, Sciences et Developpement economique Canada pour fonctionner avec les types d'antenne enumeres ci dessous et ayant un gain admissible maximal. Les types d'antenne non inclus dans cette liste, et dont le gain est superieur au gain maximal indique pour tout type figurant sur la liste, sont strictement interdits pour l'exploitation de l'emetteur.

antenna type Omni-directional

antenna gain 5.33

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.

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

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 24cm between the radiator & your body.

Industry Canada Statement (For MAX BR1 MK2)

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Le présent produit est conforme aux spécifications techniques applicables d'Innovation, Sciences et Développement économique Canada.

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada’s licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference.

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le present appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisee aux deux conditions suivantes:

(1) l'appareil ne doit pas produire de brouillage, et
(2) l'utilisateur de l'appareil doit accepter tout brouillage radioelectrique subi, meme si le brouillage est susceptible d'en

(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) For devices with detachable antenna(s), 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
The high-power radars are allocated as primary users (i.e. priority users) of the band 5725-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

(i) Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé 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 avec antenne(s) amovible(s) utilisant la bande 5725-5850 MHz doit se conformer à la limitation P.I.R.E spécifiée pour l'exploitation point à point et non point à point, selon le cas.

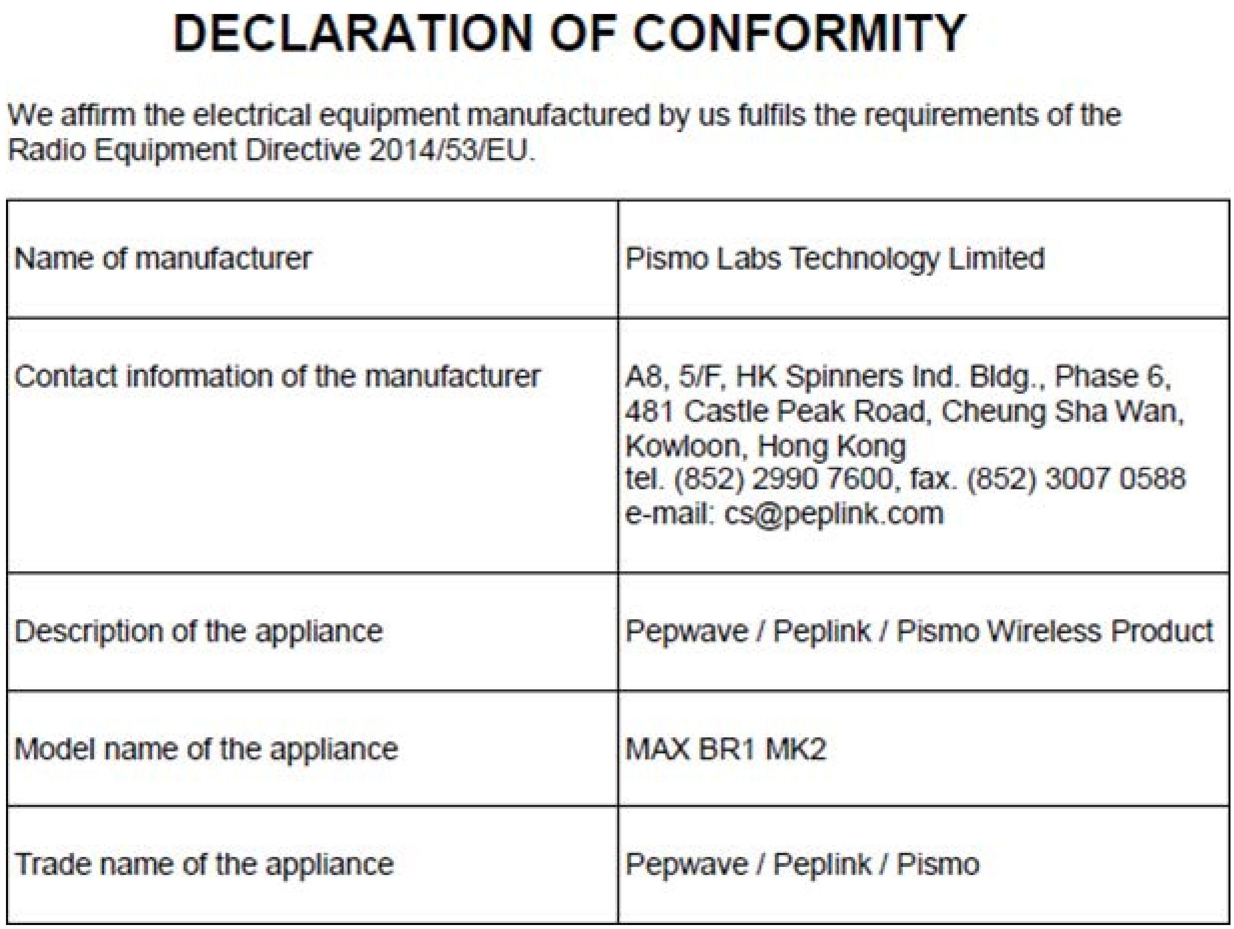
En outre, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bande 5725-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Radiation Exposure Statement

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

Cet équipement est conforme avec l'exposition aux radiations ISED définies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à une distance minimum de 20 cm entre le radiateur et votre corps.

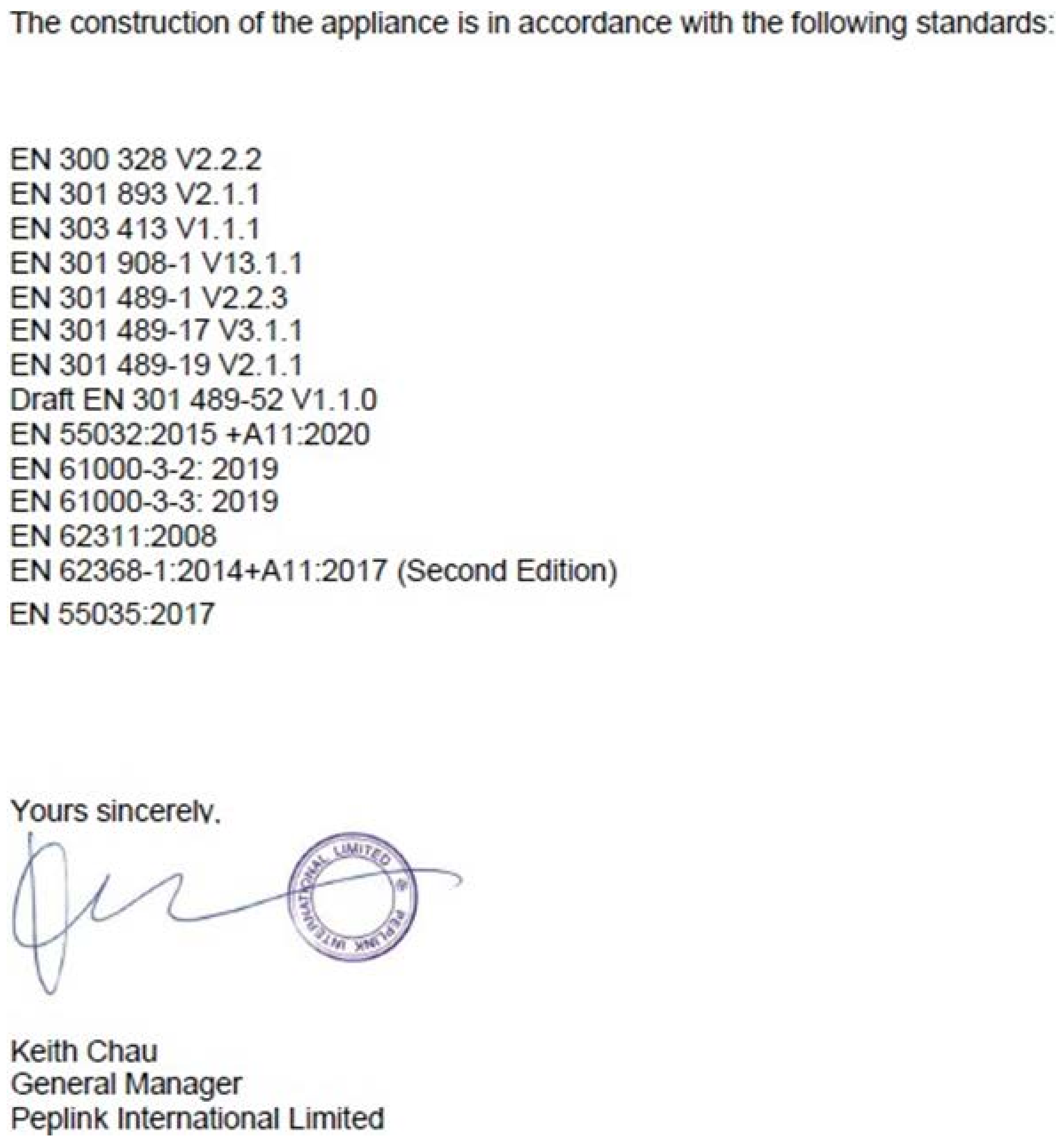
CE Statement for Pepwave Routers (MAX BR1 MK2)



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

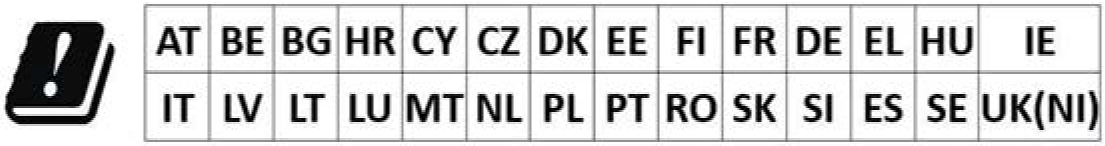


The construction of the appliance is in accordance with the following standards:

EN 300 328 V2.2.2
EN 301 893 V2.1.1
EN 303 413 V1.1.1
EN 301 908-1 V13.1.1
EN 301 489-1 V2.2.3
EN 301 489-17 V3.1.1
EN 301 489-19 V2.1.1
Draft EN 301 489-52 V1.1.0
EN 55032:2015 +A11:2020
EN 61000-3-2: 2019
EN 61000-3-3: 2019
EN 62311:2008
EN 62368-1:2014+A11:2017 (Second Edition)
EN 55035:2017

Yours sincerely,

Keith Chau
General Manager
Peplink International Limited



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

2.4GHz (2412 – 2472 MHz) : 19.95 dBm

5GHz (5150 - 5250 MHz) : 22.73 dBm

WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

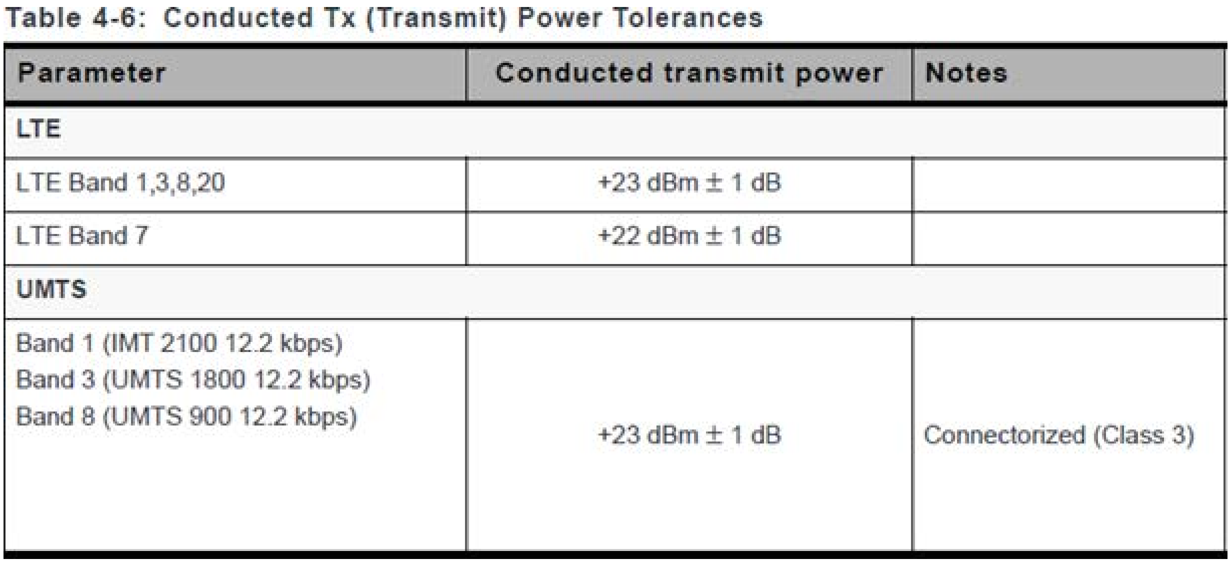


Table 4-6: Conducted Tx (Transmit) Power Tolerances

Parameter	Conducted transmit power	Notes
LTE		
LTE Band 1,3,8,20	+23 dBm ± 1 dB	
LTE Band 7	+22 dBm ± 1 dB	
UMTS		
Band 1 (IMT 2100 12.2 kbps) Band 3 (UMTS 1800 12.2 kbps) Band 8 (UMTS 900 12.2 kbps)	+23 dBm ± 1 dB	Connectorized (Class 3)

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.

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.

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

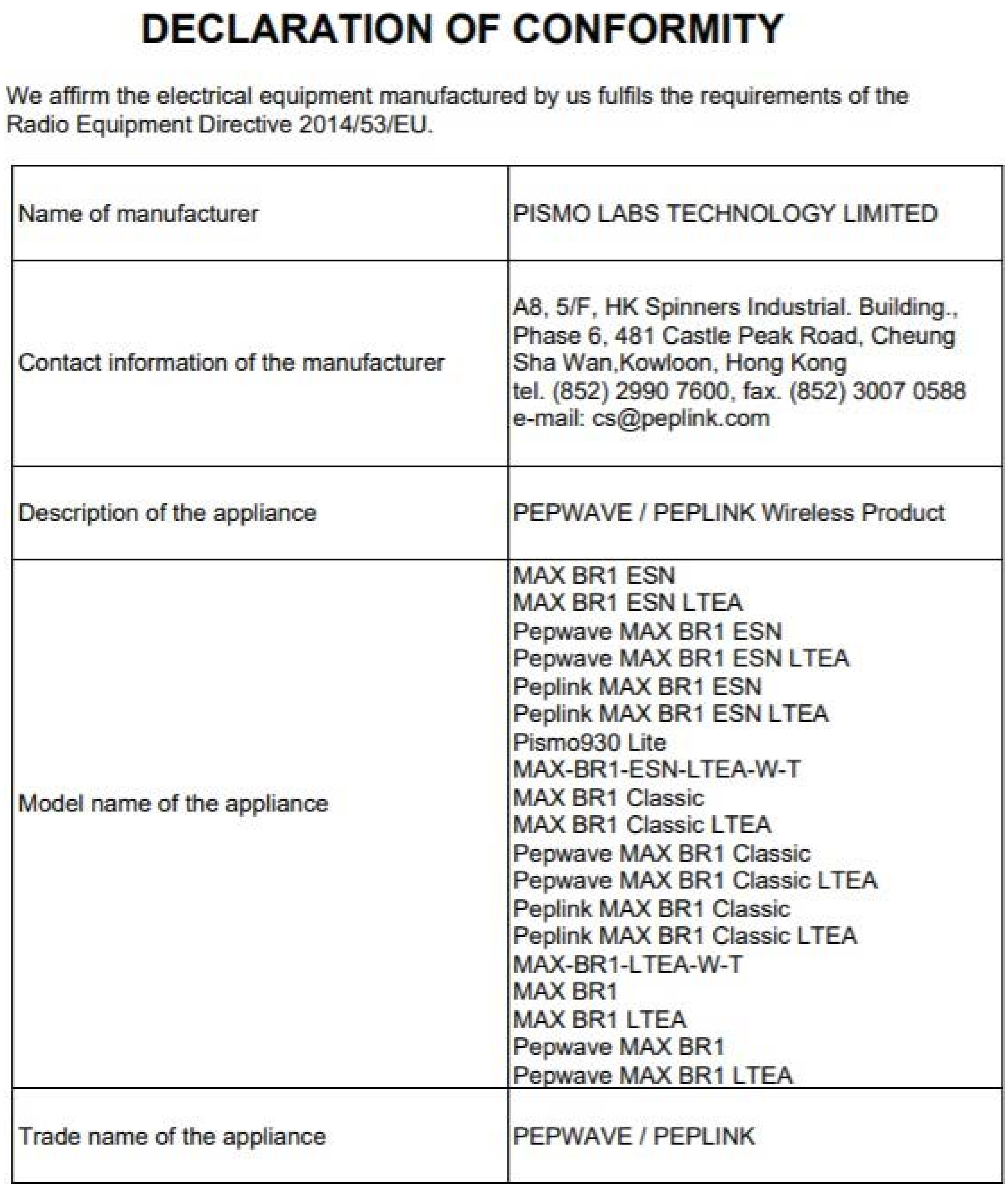
This device complies with the ISED radiation exposure limit set forth for an uncontrolled environment. This device should be installed and operated with minimum distance 20cm between the radiator & your body.

Cet équipement est conforme avec l'exposition aux radiations ISED définies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à une distance minimum de 20 cm entre le radiateur et votre corps.

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Le présent produit est conforme aux spécifications techniques applicables d'Innovation, Sciences et Développement économique Canada.

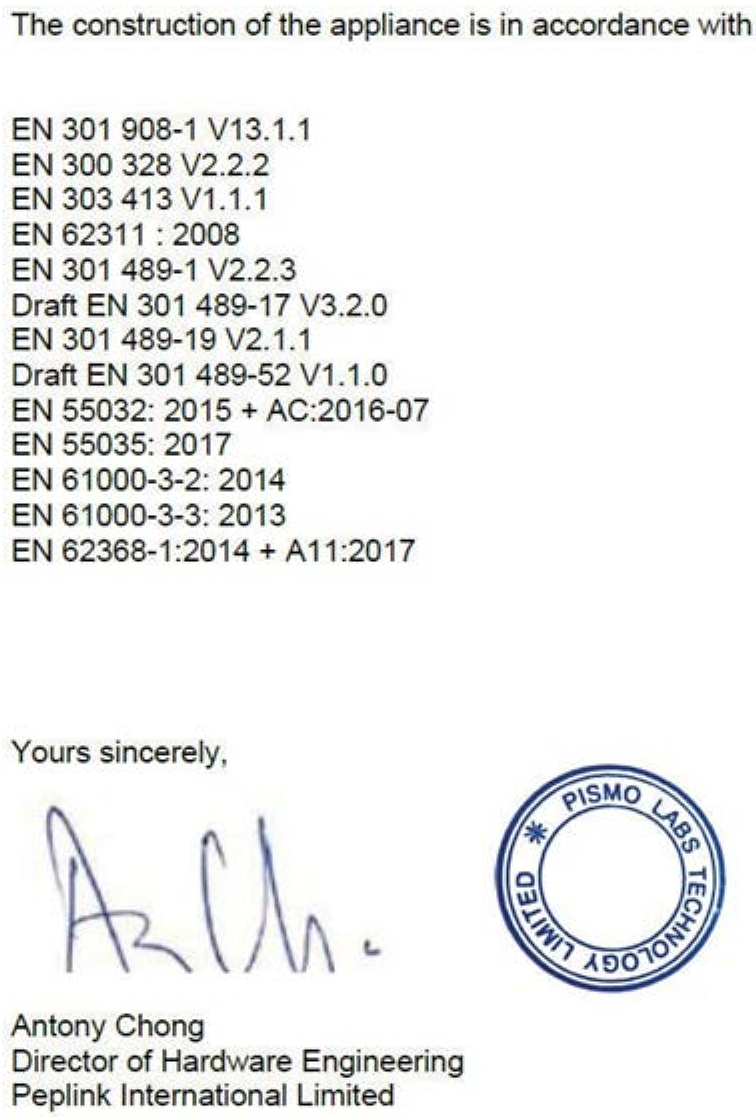
CE Statement for Pepwave Routers (MAX BR1 Classic for MC7455)



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



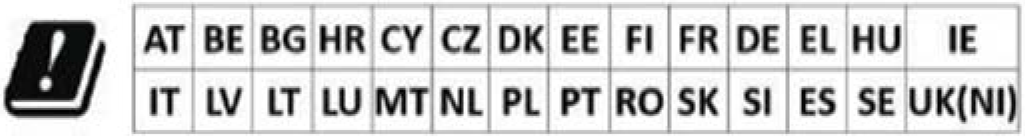
The construction of the appliance is in accordance with the following standards:

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,

PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



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

2.4GHz (2412 – 2472 MHz) : 19.78 dBm

WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

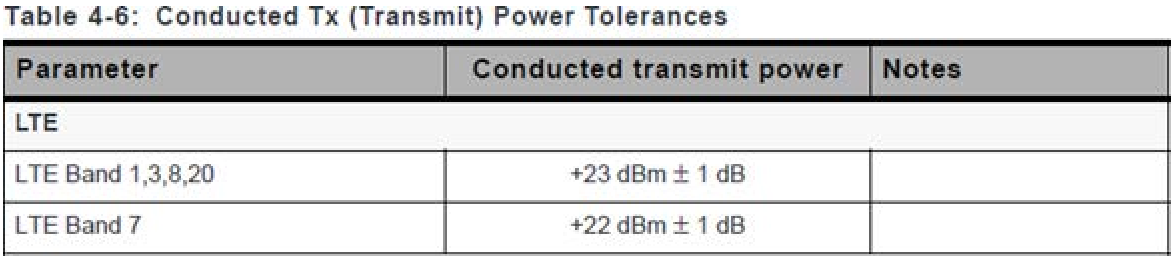


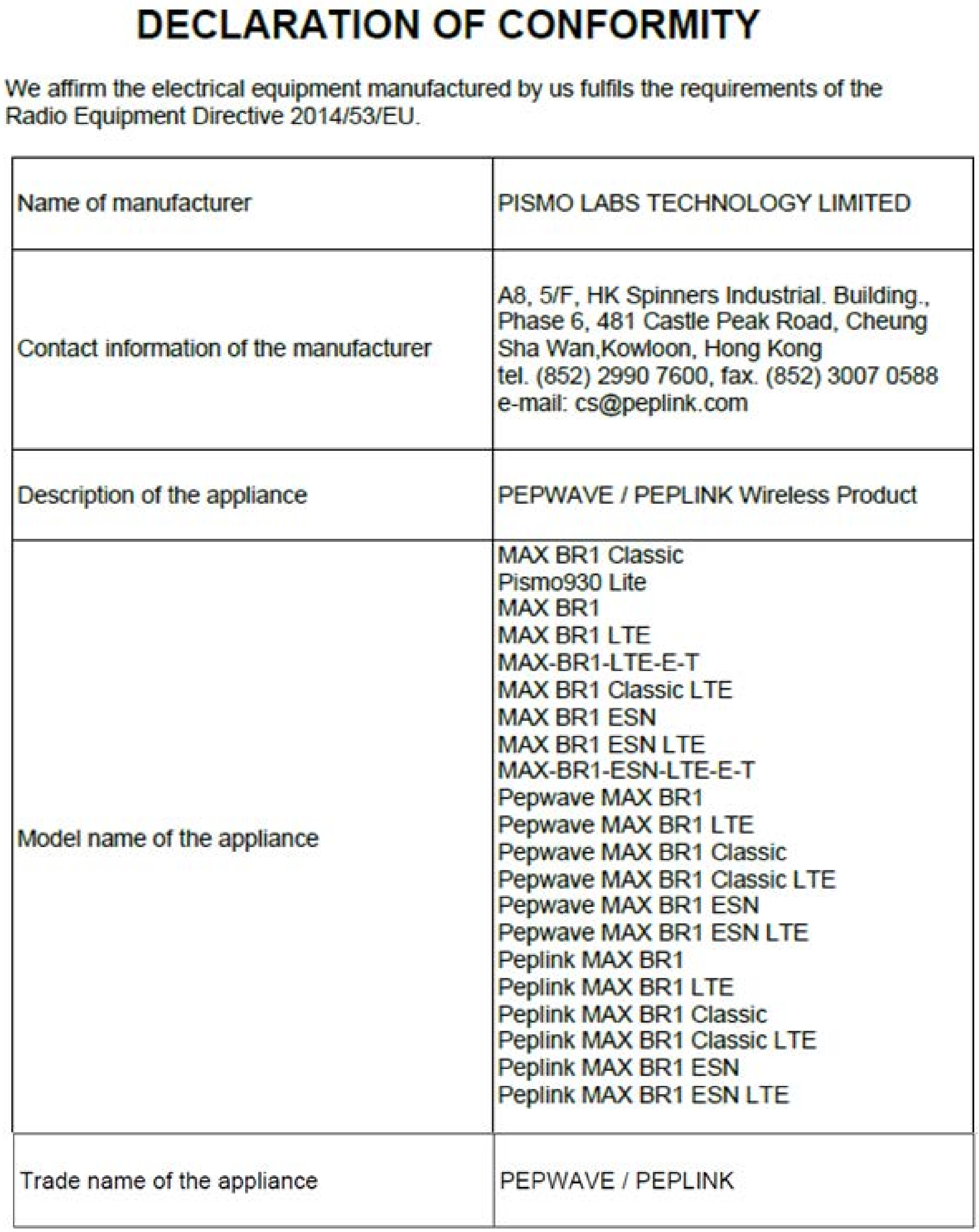
Table 4-6: Conducted Tx (Transmit) Power Tolerances

Parameter	Conducted transmit power	Notes
LTE		
LTE Band 1,3,8,20	+23 dBm ± 1 dB	
LTE Band 7	+22 dBm ± 1 dB	

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/

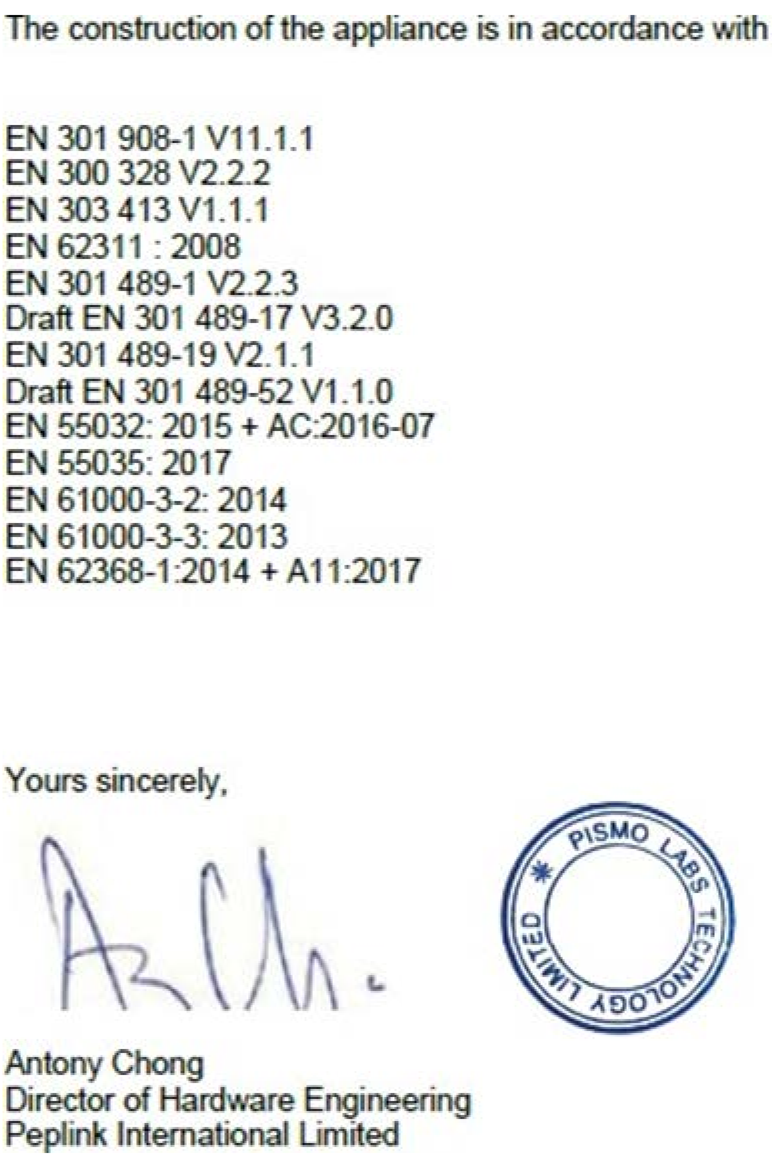
CE Statement for Pepwave Routers (MAX BR1 Classic for EC25-E)



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 Classic Pismo930 Lite MAX BR1 MAX BR1 LTE MAX-BR1-LTE-E-T MAX BR1 Classic LTE MAX BR1 ESN MAX BR1 ESN LTE MAX-BR1-ESN-LTE-E-T Pepwave MAX BR1 Pepwave MAX BR1 LTE Pepwave MAX BR1 Classic Pepwave MAX BR1 Classic LTE Pepwave MAX BR1 ESN Pepwave MAX BR1 ESN LTE Peplink MAX BR1 Peplink MAX BR1 LTE Peplink MAX BR1 Classic Peplink MAX BR1 Classic LTE Peplink MAX BR1 ESN Peplink MAX BR1 ESN LTE
Trade name of the appliance	PEPWAVE / PEPLINK



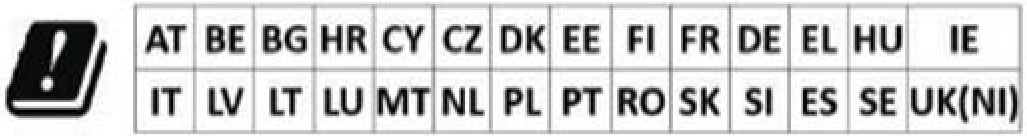
The construction of the appliance is in accordance with the following standards:

EN 301 908-1 V11.1.1
EN 300 328 V2.2.2
EN 303 413 V1.1.1
EN 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,

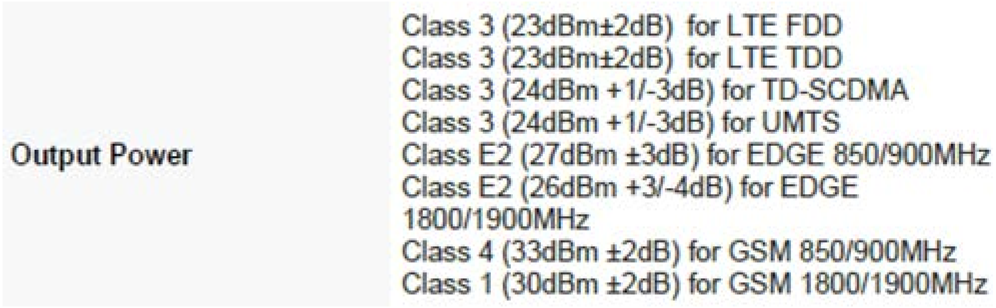
PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



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

2.4GHz (2412 – 2472 MHz) : 19.78 dBm
WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)



Output Power	Class 3 (23dBm±2dB) for LTE FDD Class 3 (23dBm±2dB) for LTE TDD Class 3 (24dBm +1/-3dB) for TD-SCDMA Class 3 (24dBm +1/-3dB) for UMTS Class E2 (27dBm ±3dB) for EDGE 850/900MHz Class E2 (26dBm +3/-4dB) for EDGE 1800/1900MHz Class 4 (33dBm ±2dB) for GSM 850/900MHz Class 1 (30dBm ±2dB) for GSM 1800/1900MHz

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, MAX HD2 MBX, MAX HD4 MBX 5G, MAX HD2 MBX 5G

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.

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 For MAX HD4 MBX

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

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Le présent produit est conforme aux spécifications techniques applicables d'Innovation, Sciences et Développement économique Canada.

(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) For devices with detachable antenna(s), 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

The high-power radars are allocated as primary users (i.e. priority users) of the band 5725-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

(i) Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé 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 avec antenne(s) amovible(s) utilisant la bande 5725-5850 MHz doit se conformer à la limitation P.I.R.E spécifiée pour l’exploitation point à point et non point à point, selon le cas.

En outre, 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 bande 5725-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

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.

Declaration d'exposition aux radiations Cet equipement est conforme aux limites d'exposition aux rayonnements IC etablies pour un environnement non controle. Cet equipement doit etre installe et utilise avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

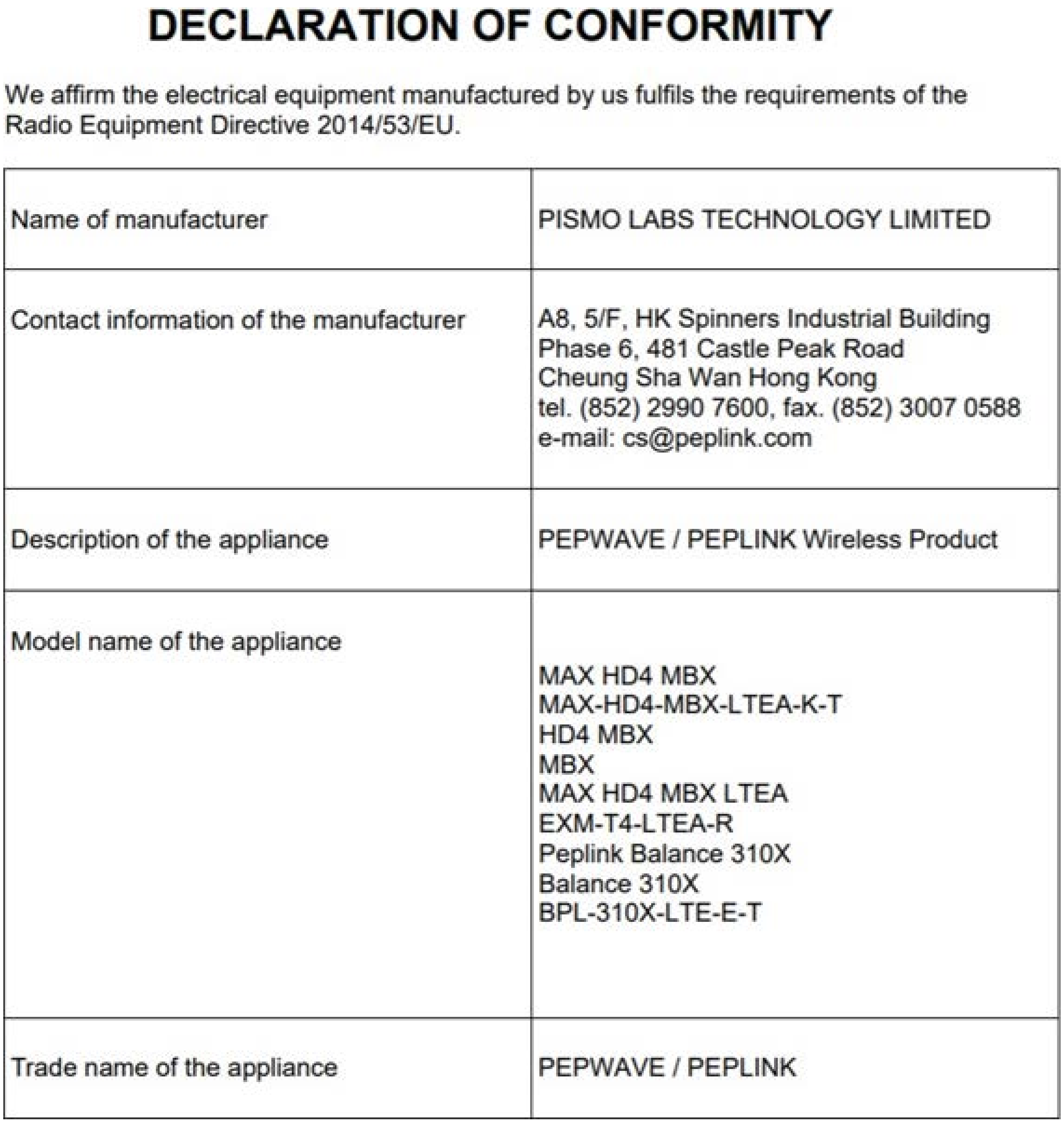
This radio transmitter 20682-P1MBX has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for 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

Battery Caution Statement (MAX HD4 MBX, MAX HD2 MBX, MAX HD4 MBX 5G, MAX HD2 MBX 5G)

Risk of explosion if the battery is replaced by an incorrect type.

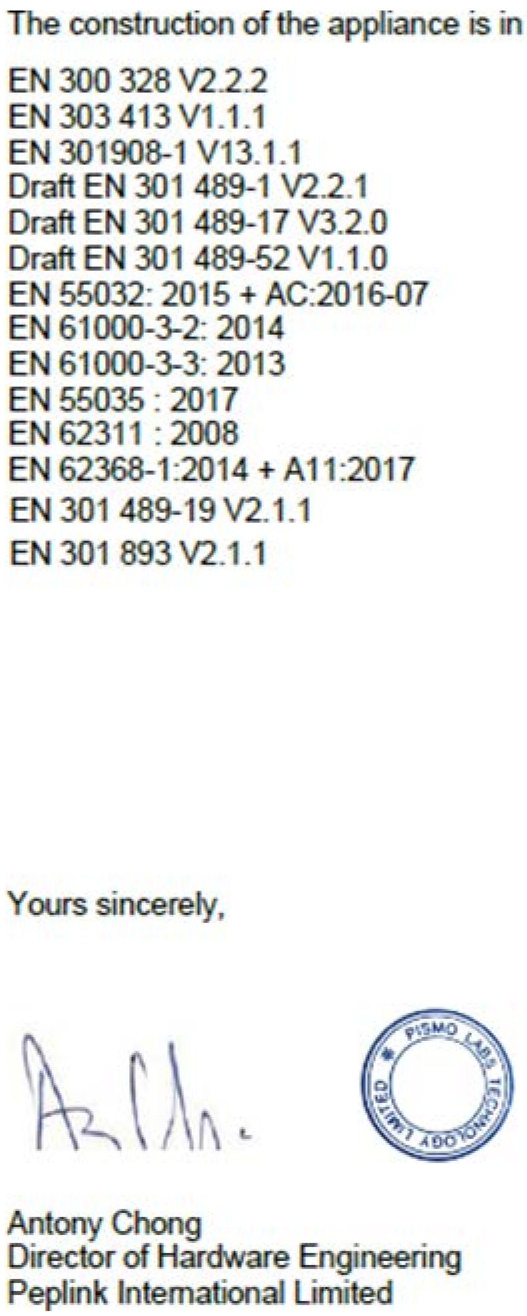
CE Statement for Pepwave Routers (MAX HD4 MBX For EM7565)



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



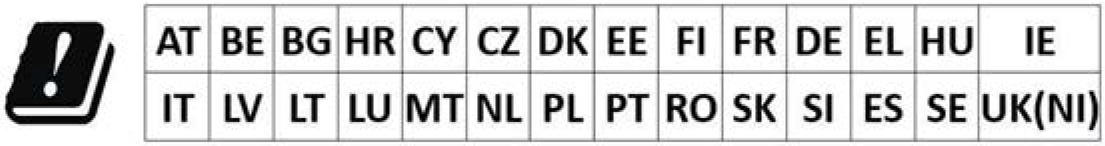
The construction of the appliance is in accordance with the following standards:

EN 300 328 V2.2.2
EN 303 413 V1.1.1
EN 301908-1 V13.1.1
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 62311 : 2008
EN 62368-1:2014 + A11:2017
EN 301 489-19 V2.1.1
EN 301 893 V2.1.1

Yours sincerely,

PISMO LABS TECHNOLOGY LIMITED

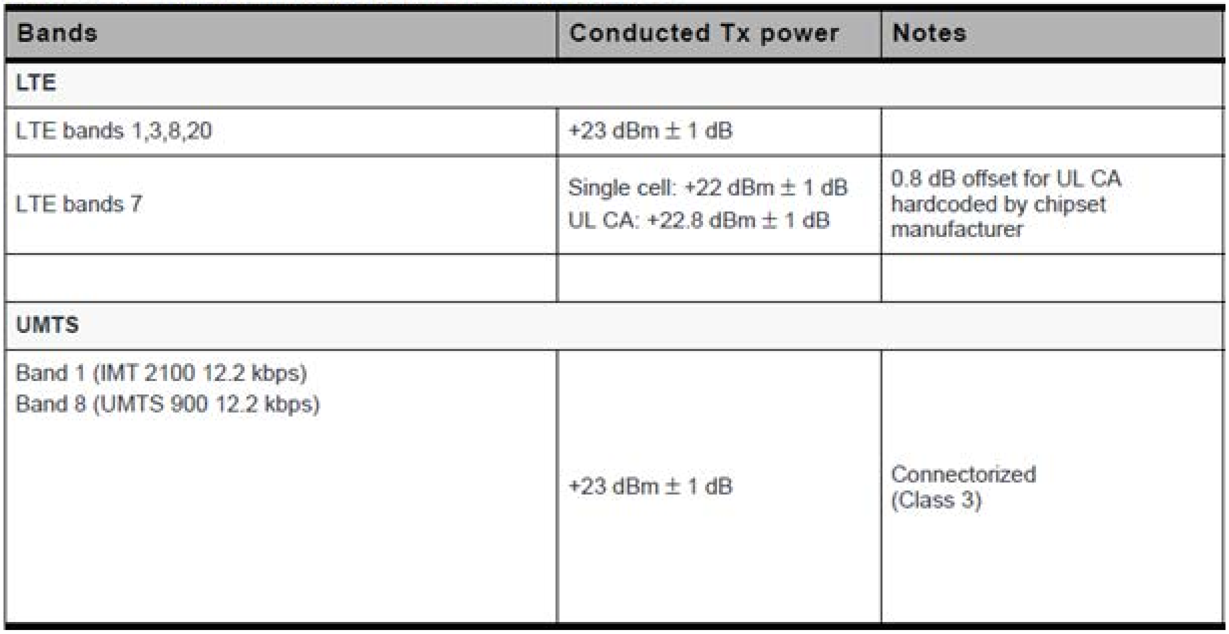
Antony Chong
Director of Hardware Engineering
Peplink International Limited



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

2.4GHz (2412 – 2472 MHz) : 19.6 dBm
5GHz (5150 - 5250 MHz) : 19.4 dBm
WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

Table 3-6: Conducted Tx (Transmit) Power Tolerances

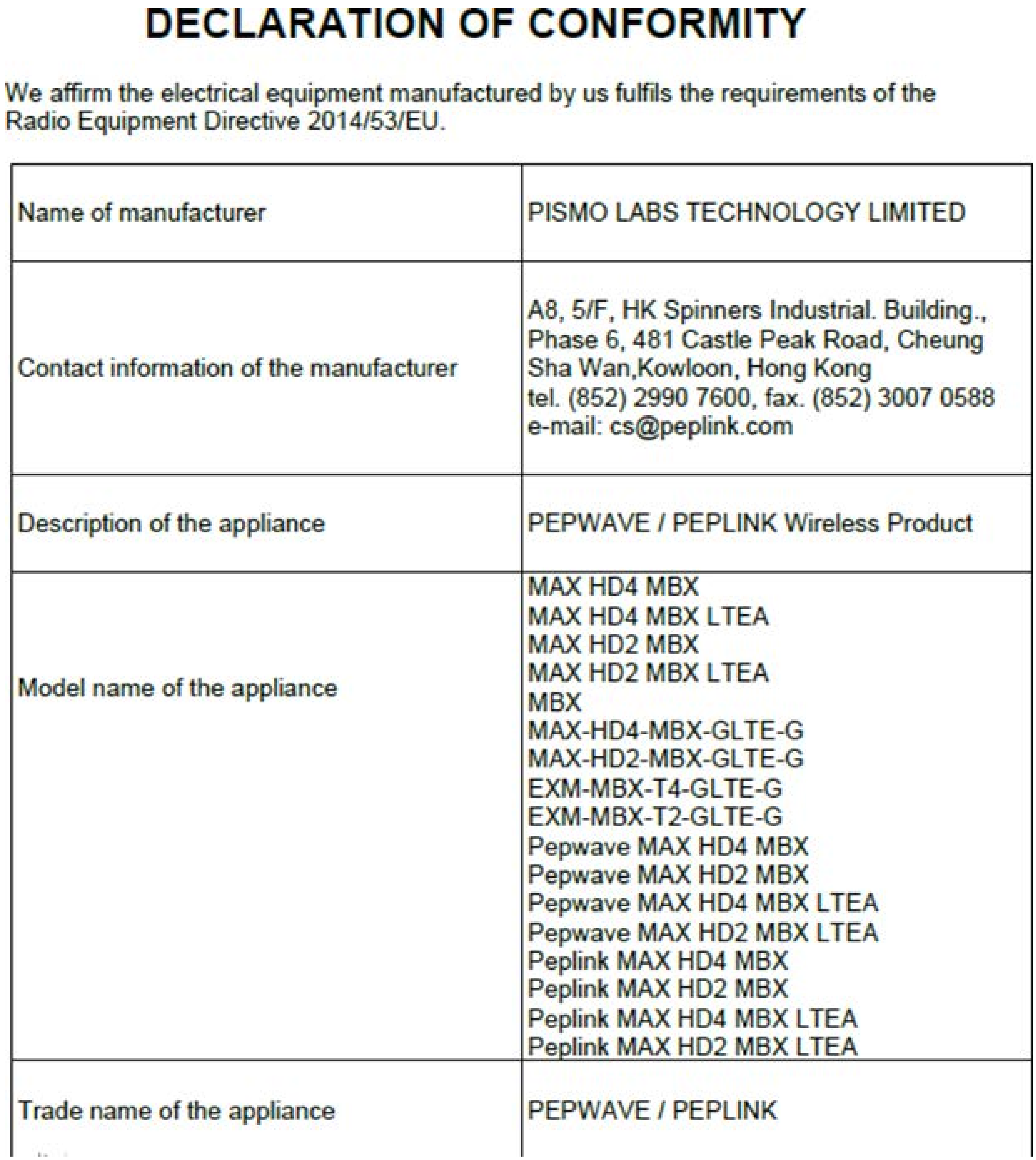


Bands	Conducted Tx power	Notes
LTE		
LTE bands 1,3,8,20	+23 dBm ± 1 dB	
LTE bands 7	Single cell: +22 dBm ± 1 dB UL CA: +22.8 dBm ± 1 dB	0.8 dB offset for UL CA hardcoded by chipset manufacturer
UMTS		
Band 1 (IMT 2100 12.2 kbps) Band 8 (UMTS 900 12.2 kbps)	+23 dBm ± 1 dB	Connectorized (Class 3)

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/

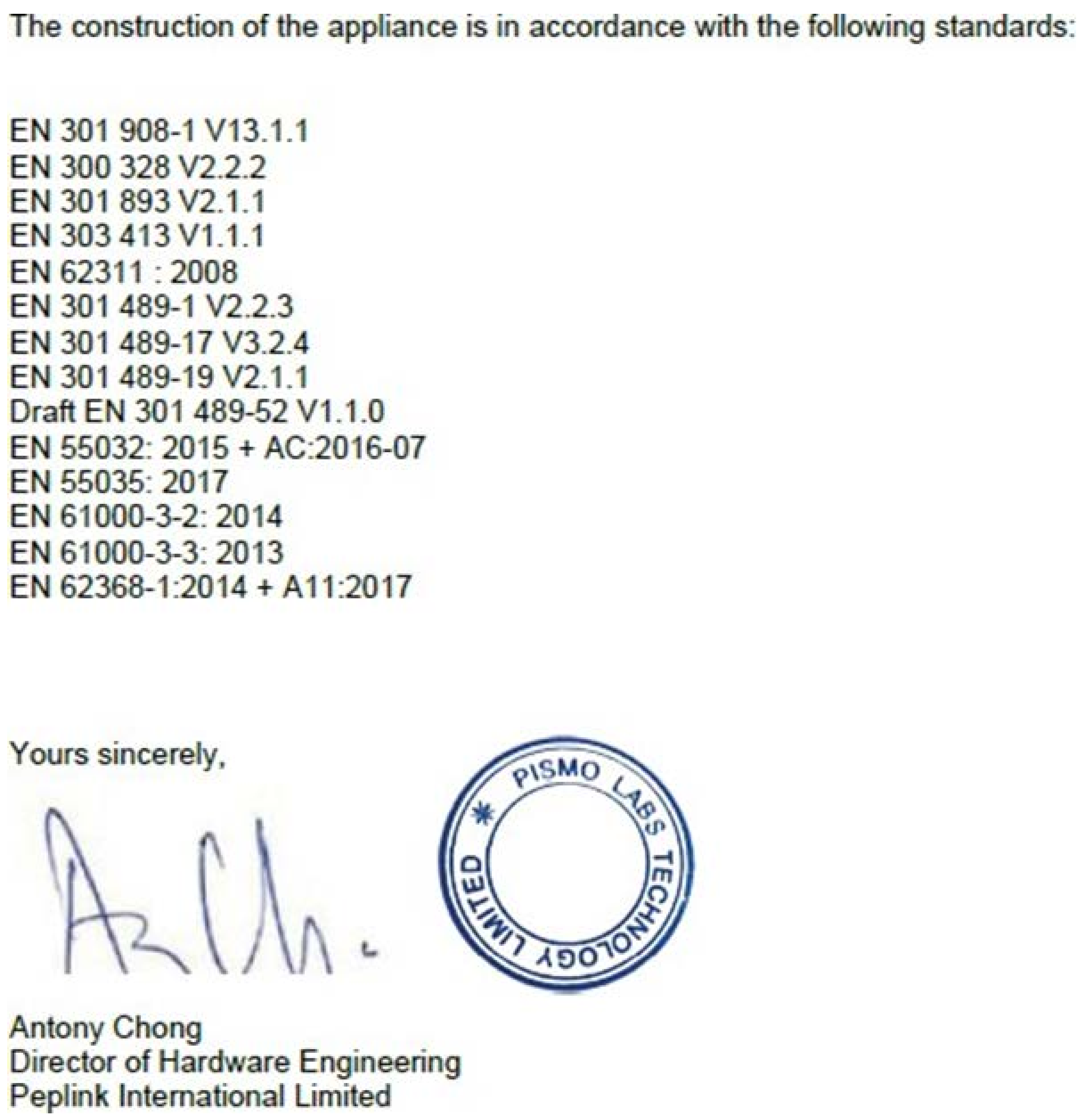
CE Statement for Pepwave Routers (MAX HD2 MBX / MAX HD4 MBX For LM960A18)



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 HD4 MBX MAX HD4 MBX LTEA MAX HD2 MBX MAX HD2 MBX LTEA MBX MAX-HD4-MBX-GLTE-G MAX-HD2-MBX-GLTE-G EXM-MBX-T4-GLTE-G EXM-MBX-T2-GLTE-G Pepwave MAX HD4 MBX Pepwave MAX HD2 MBX Pepwave MAX HD4 MBX LTEA Pepwave MAX HD2 MBX LTEA Peplink MAX HD4 MBX Peplink MAX HD2 MBX Peplink MAX HD4 MBX LTEA Peplink MAX HD2 MBX LTEA
Trade name of the appliance	PEPWAVE / PEPLINK



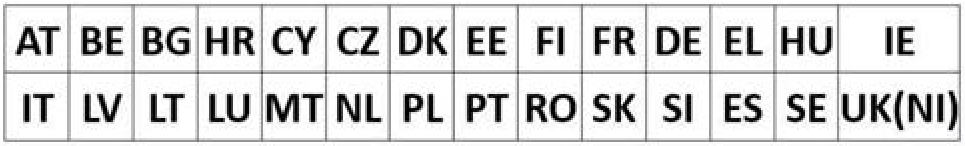
The construction of the appliance is in accordance with the following standards:

EN 301 908-1 V13.1.1
EN 300 328 V2.2.2
EN 301 893 V2.1.1
EN 303 413 V1.1.1
EN 62311 : 2008
EN 301 489-1 V2.2.3
EN 301 489-17 V3.2.4
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,

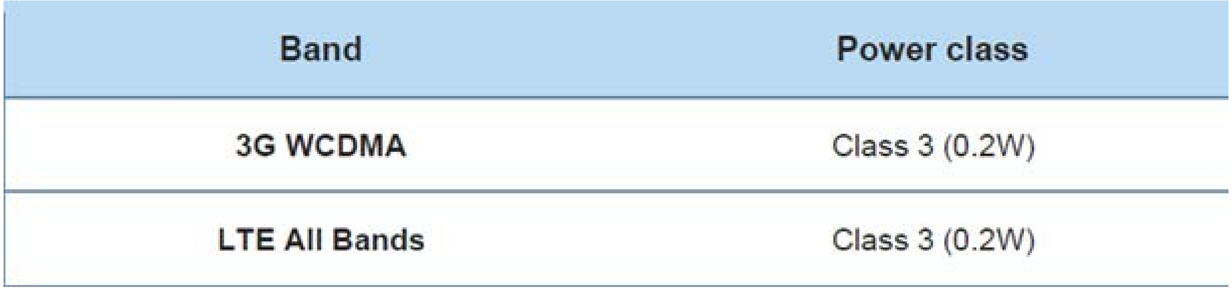
PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



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

2.4GHz (2412 – 2472 MHz) : 19.6 dBm
5GHz (5150 - 5250 MHz) : 19.4 dBm
WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

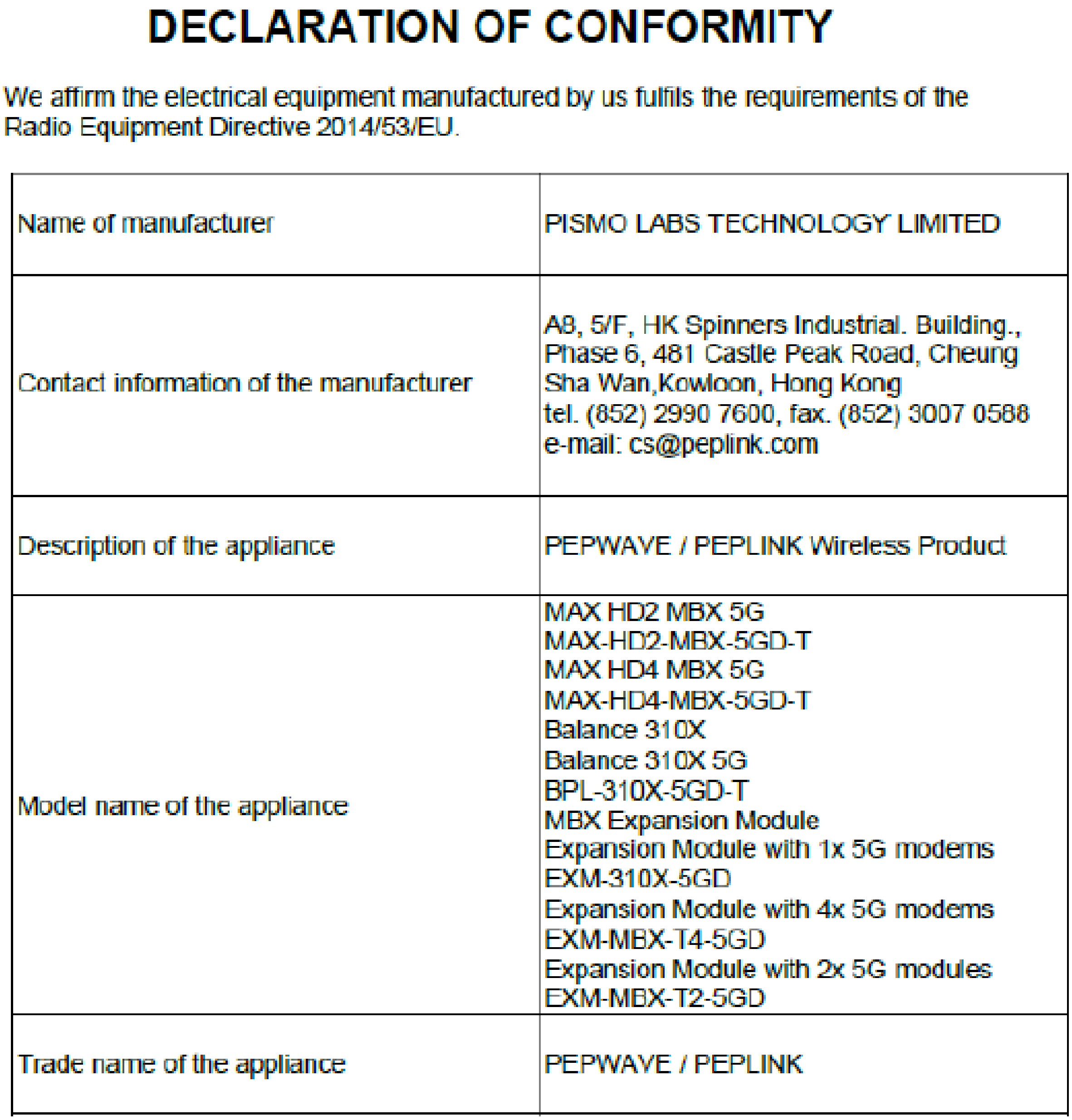


Band	Power class
3G WCDMA	Class 3 (0.2W)
LTE All Bands	Class 3 (0.2W)

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/

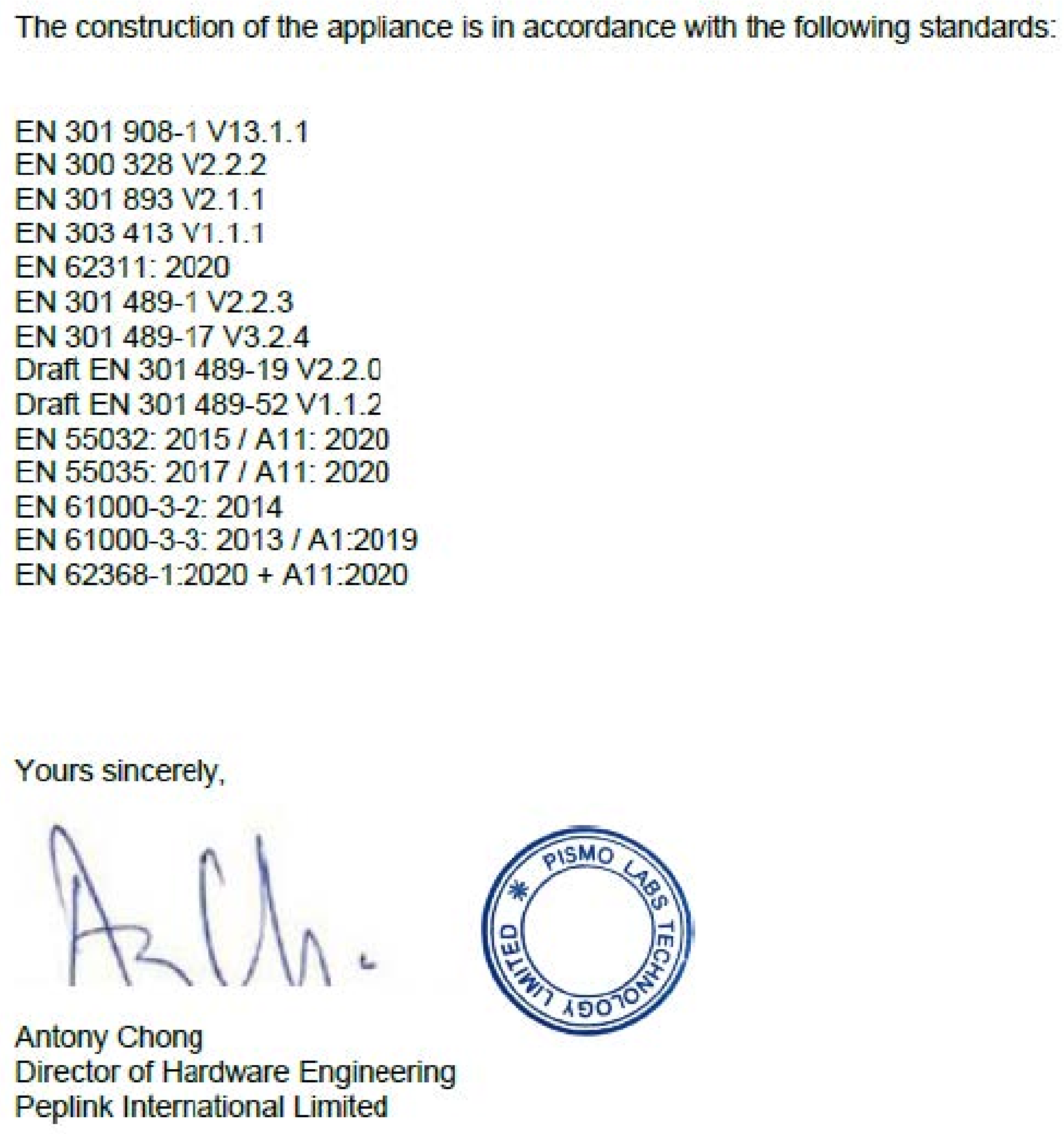
CE Statement for Pepwave Routers (MAX HD2 MBX 5G / MAX HD4 MBX 5G For MV31-W)



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 MBX 5G MAX-HD2-MBX-5GD-T MAX HD4 MBX 5G MAX-HD4-MBX-5GD-T Balance 310X Balance 310X 5G BPL-310X-5GD-T MBX Expansion Module Expansion Module with 1x 5G modems EXM-310X-5GD Expansion Module with 4x 5G modems EXM-MBX-T4-5GD Expansion Module with 2x 5G modules EXM-MBX-T2-5GD
Trade name of the appliance	PEPWAVE / PEPLINK



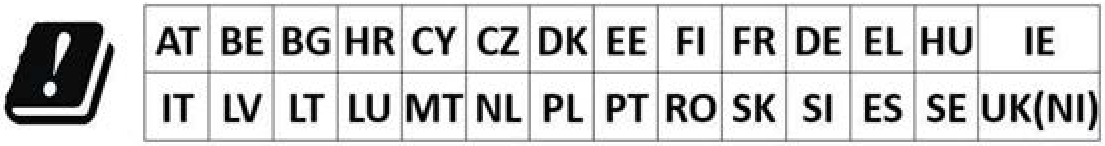
The construction of the appliance is in accordance with the following standards:

EN 301 908-1 V13.1.1
EN 300 328 V2.2.2
EN 301 893 V2.1.1
EN 303 413 V1.1.1
EN 62311: 2020
EN 301 489-1 V2.2.3
EN 301 489-17 V3.2.4
Draft EN 301 489-19 V2.2.0
Draft EN 301 489-52 V1.1.2
EN 55032: 2015 / A11: 2020
EN 55035: 2017 / A11: 2020
EN 61000-3-2: 2014
EN 61000-3-3: 2013 / A1:2019
EN 62368-1:2020 + A11:2020

Yours sincerely,

PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited

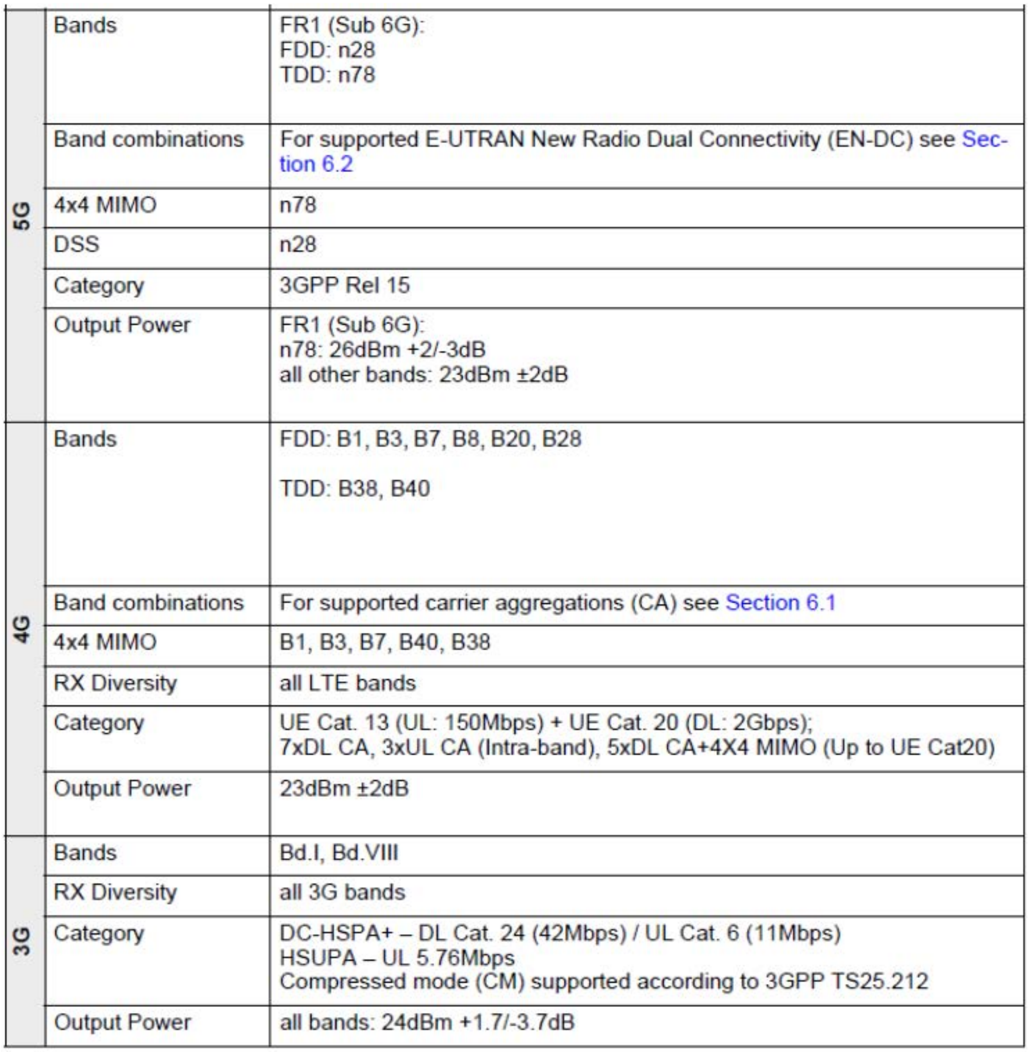


AT	BE	BG	HR	CY	CZ	DK	EE	FI	FR	DE	EL	HU	IE
IT	LV	LT	LU	MT	NL	PL	PT	RO	SK	SI	ES	SE	UK(NI)

2.4GHz (2412 – 2472 MHz) : 19.6 dBm

5GHz (5150 - 5250 MHz) : 19.4 dBm

WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)



5G	Bands	FR1 (Sub 6G): FDD: n28 TDD: n78
	Band combinations	For supported E-UTRAN New Radio Dual Connectivity (EN-DC) see Section 6.2
	4x4 MIMO	n78
	DSS	n28
	Category	3GPP Rel 15
	Output Power	FR1 (Sub 6G): n78: 26dBm +2/-3dB all other bands: 23dBm ±2dB
4G	Bands	FDD: B1, B3, B7, B8, B20, B28 TDD: B38, B40
	Band combinations	For supported carrier aggregations (CA) see Section 6.1
	4x4 MIMO	B1, B3, B7, B40, B38
	RX Diversity	all LTE bands
	Category	UE Cat. 13 (UL: 150Mbps) + UE Cat. 20 (DL: 2Gbps); 7xDL CA, 3xUL CA (Intra-band), 5xDL CA+4X4 MIMO (Up to UE Cat20)
	Output Power	23dBm ±2dB
3G	Bands	Bd.I, Bd.VIII
	RX Diversity	all 3G bands
	Category	DC-HSPA+ – DL Cat. 24 (42Mbps) / UL Cat. 6 (11Mbps) HSUPA – UL 5.76Mbps Compressed mode (CM) supported according to 3GPP TS25.212
	Output Power	all bands: 24dBm +1.7/-3.7dB

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.

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

Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 50 centimeters between the radiator and your body.

Industry Canada Statement (MAX HD2)

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Le présent produit est conforme aux spécifications techniques applicables d'Innovation, Sciences et Développement économique Canada.

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada’s licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference.

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le present appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisee aux deux conditions suivantes:

(1) l’appareil ne doit pas produire de brouillage, et

(2) l’utilisateur de l’appareil doit accepter tout brouillage radioelectrique subi, meme si le brouillage est susceptible d’en

(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) For devices with detachable antenna(s), 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

The high-power radars are allocated as primary users (i.e. priority users) of the band 5725-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

(i) Le dispositif fonctionnant dans la bande 5150-5250 MHz est réservé 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 avec antenne(s) amovible(s) utilisant la bande 5725-5850 MHz doit se conformer à la limitation P.I.R.E spécifiée pour l'exploitation point à point et non point à point, selon le cas.

En outre, 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 bande 5725-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

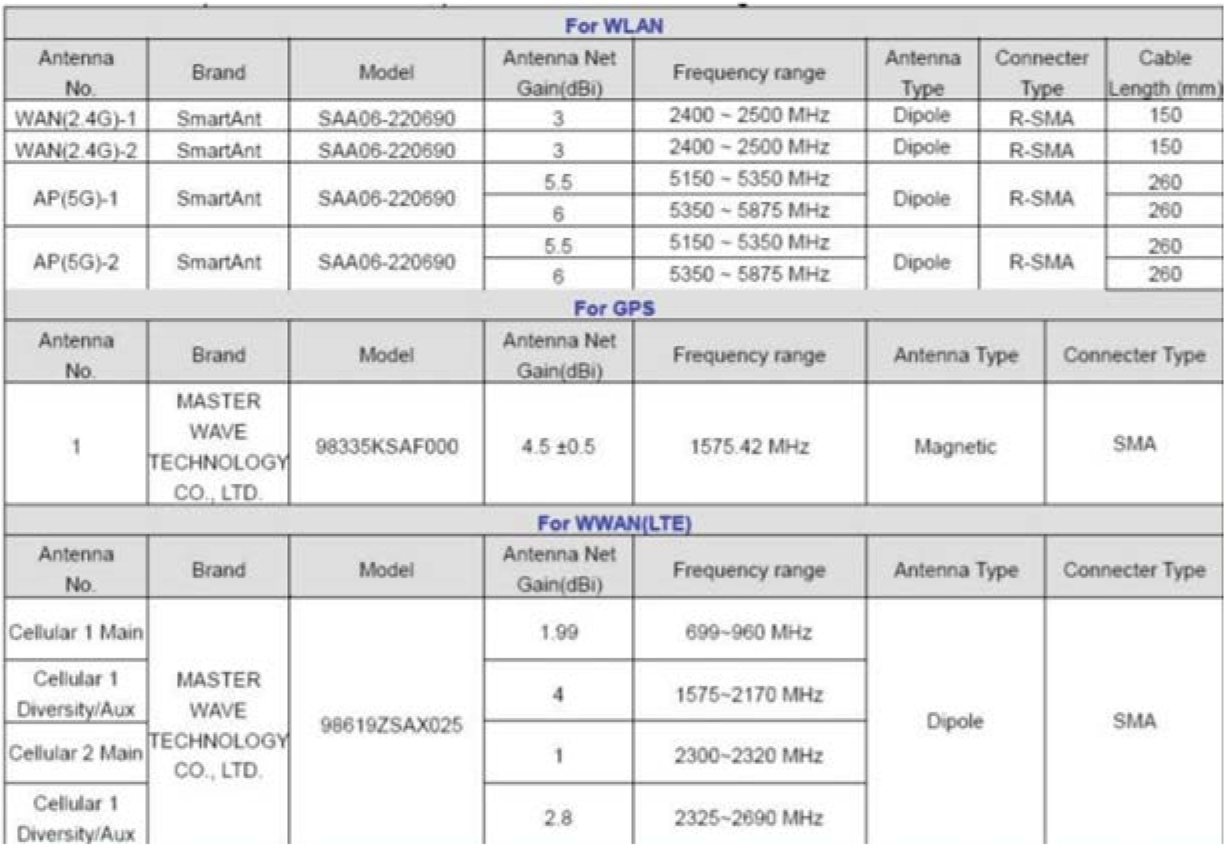
Radiation Exposure Statement

This device complies with the ISED radiation exposure limit set forth for an uncontrolled environment. This device should be installed and operated with minimum distance 37cm between the radiator & your body. 70 cm minimum distance for the device operate with plug-in USB cellular device which has maximum of 7W(ERP) output power.

Cet équipement est conforme avec l'exposition aux radiations ISED définies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à une distance minimum de 37 cm entre le radiateur et votre corps. Distance minimale de 70 cm pour que l'appareil fonctionne avec un appareil cellulaire USB enfichable qui a une puissance de sortie maximale de 7 W (ERP).

Battery Caution Statement

Risk of explosion if the battery is replaced by an incorrect type.



For WLAN

Antenna No.	Brand	Model	Antenna Net Gain(dBi)	Frequency range	Antenna Type	Connecter 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

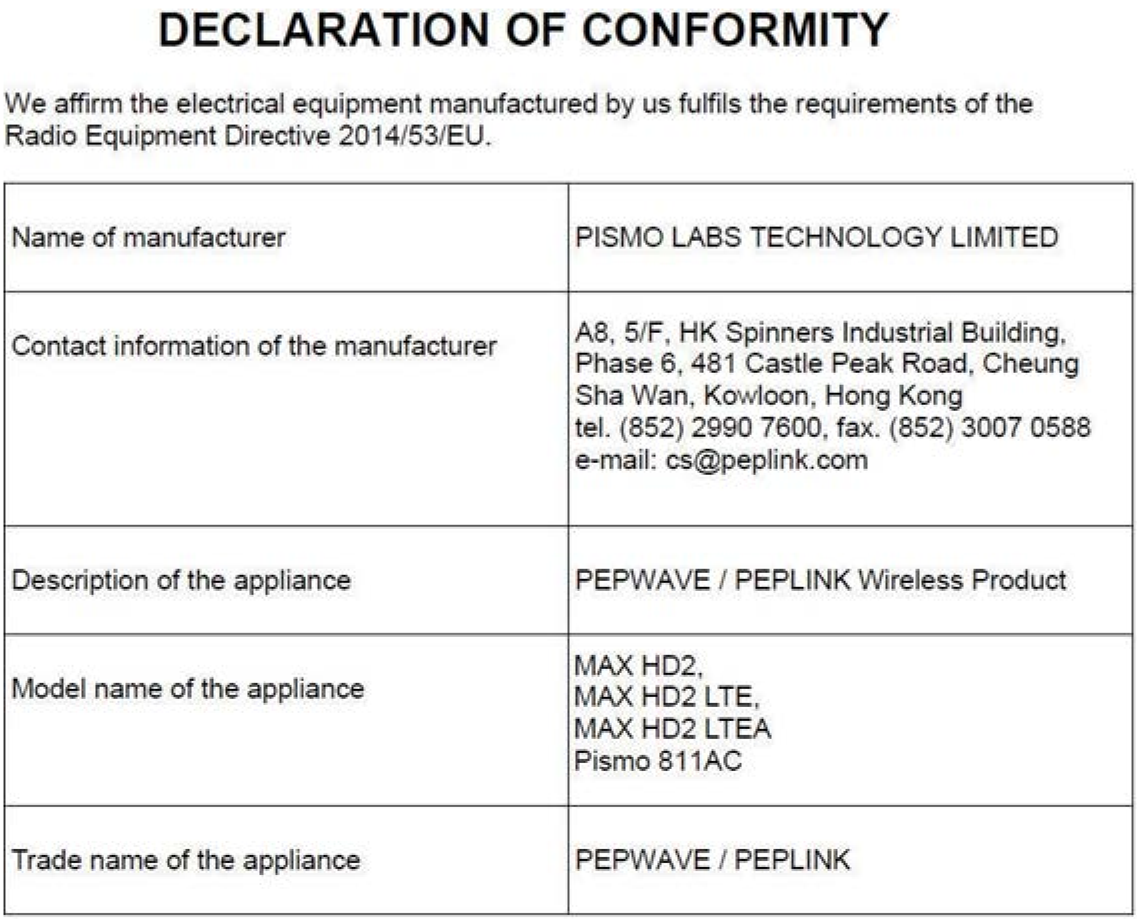
For GPS

Antenna No.	Brand	Model	Antenna Net Gain(dBi)	Frequency range	Antenna Type	Connecter 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	Connecter 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		

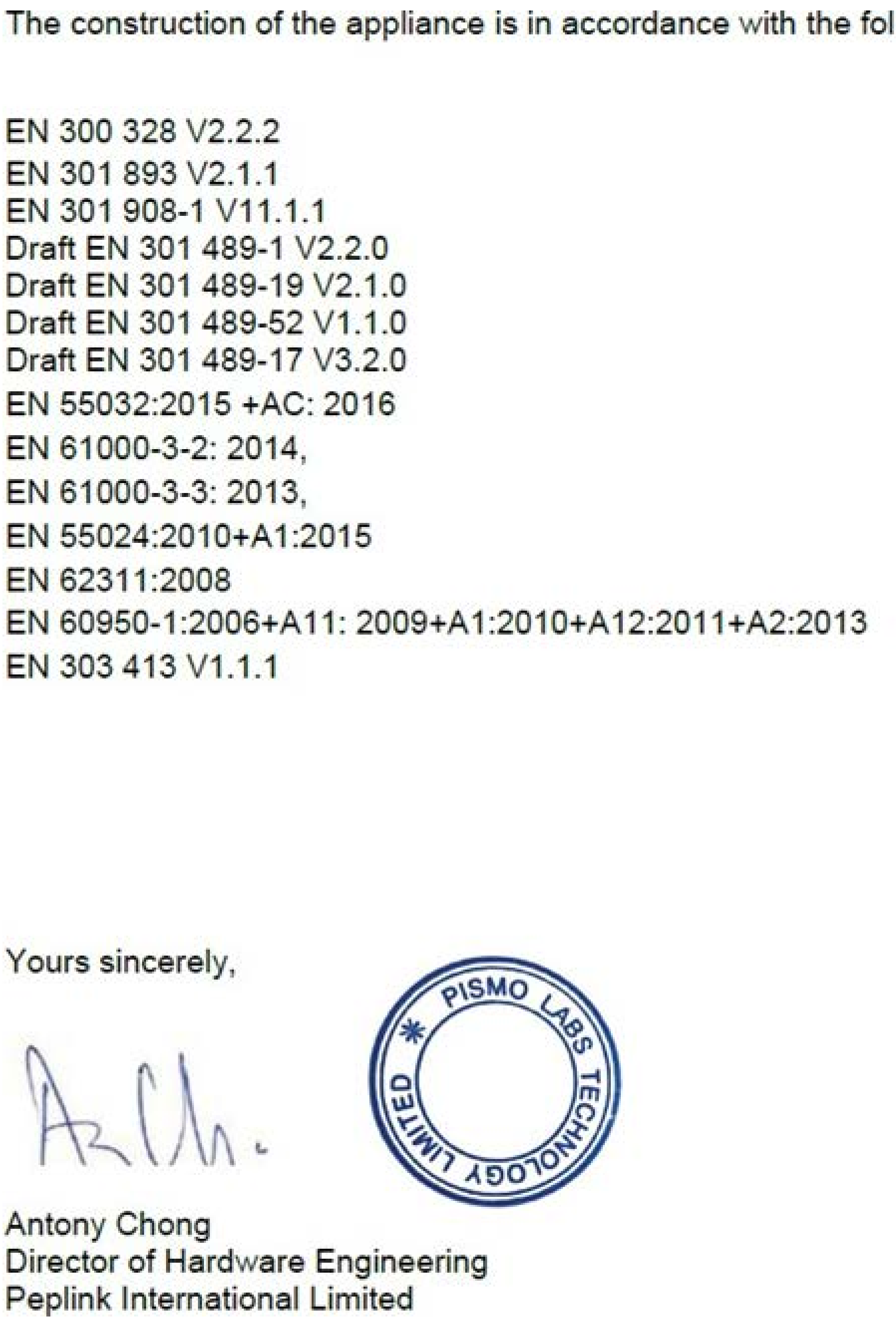
CE Statement for Pepwave Routers (MAX HD2 For MC7455)



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



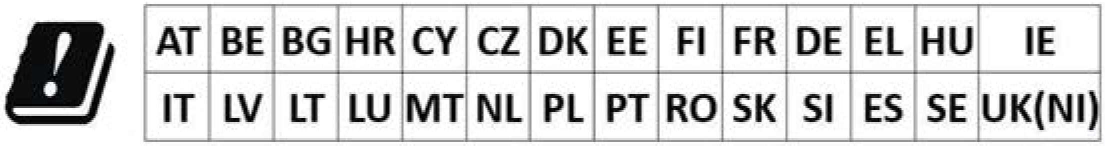
The construction of the appliance is in accordance with the following standards:

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,

PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



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

2.4GHz (2412 – 2472 MHz) : 19.90 dBm

5GHz (5150 - 5250 MHz) : 22.88 dBm

WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

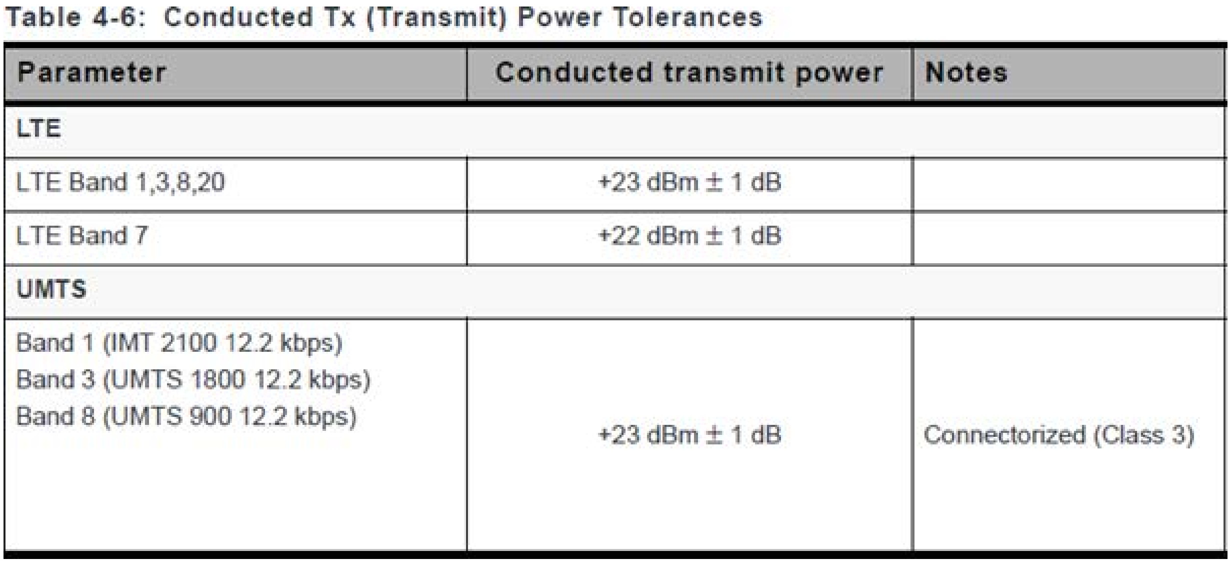


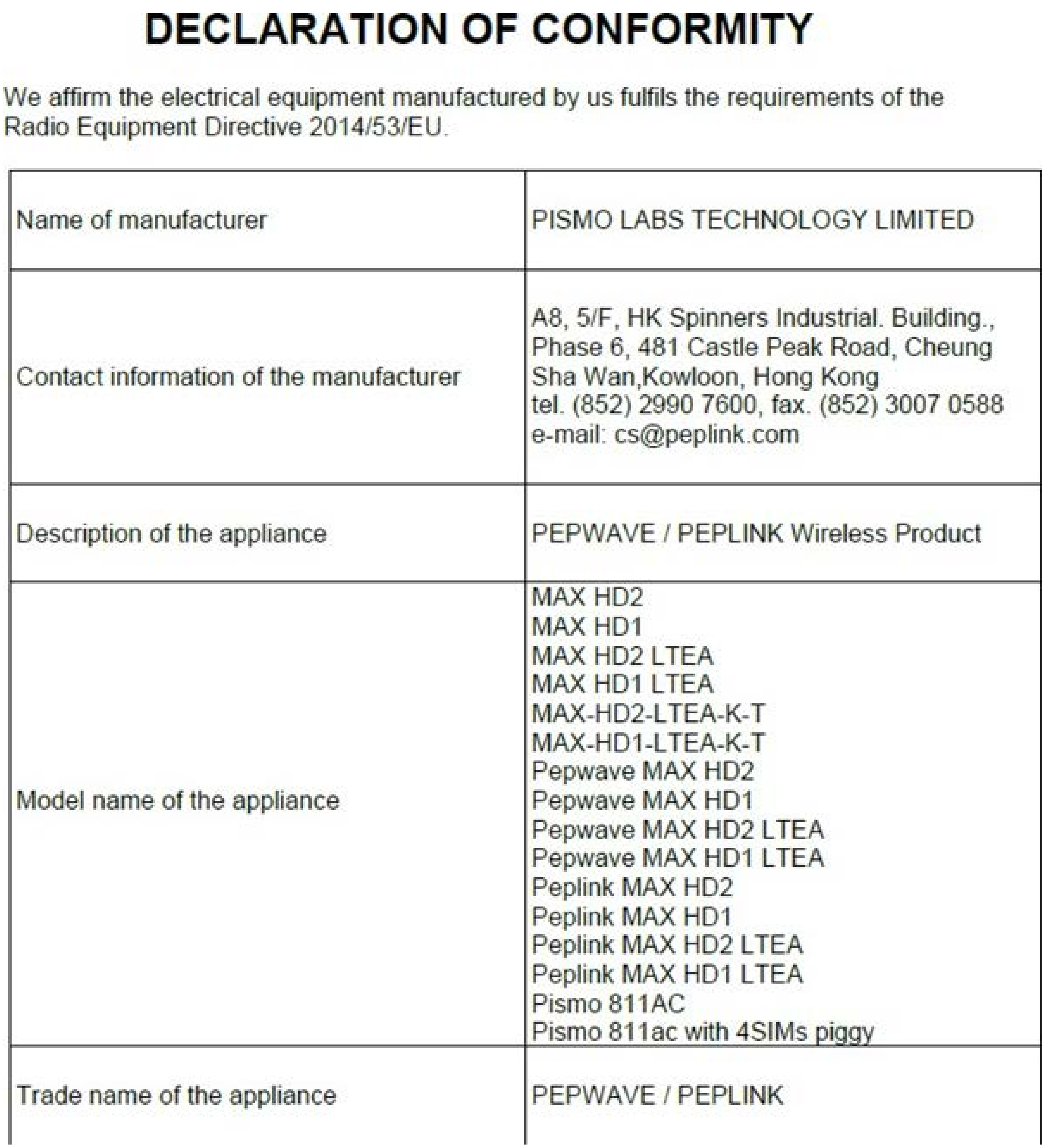
Table 4-6: Conducted Tx (Transmit) Power Tolerances

Parameter	Conducted transmit power	Notes
LTE		
LTE Band 1,3,8,20	+23 dBm ± 1 dB	
LTE Band 7	+22 dBm ± 1 dB	
UMTS		
Band 1 (IMT 2100 12.2 kbps) Band 3 (UMTS 1800 12.2 kbps) Band 8 (UMTS 900 12.2 kbps)	+23 dBm ± 1 dB	Connectorized (Class 3)

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/

CE Statement for Pepwave Routers (MAX HD2 For MC7565)



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 HD1 MAX HD2 LTEA MAX HD1 LTEA MAX-HD2-LTEA-K-T MAX-HD1-LTEA-K-T Pepwave MAX HD2 Pepwave MAX HD1 Pepwave MAX HD2 LTEA Pepwave MAX HD1 LTEA Peplink MAX HD2 Peplink MAX HD1 Peplink MAX HD2 LTEA Peplink MAX HD1 LTEA Pismo 811AC Pismo 811ac with 4SIMs piggy
Trade name of the appliance	PEPWAVE / PEPLINK

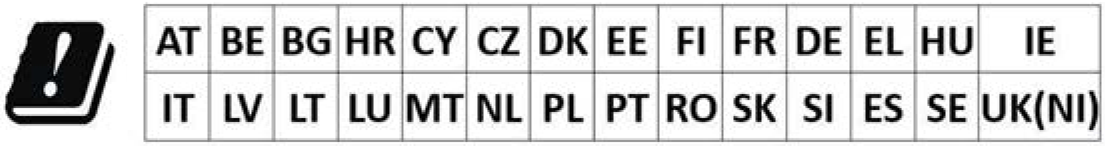
The construction of the appliance is in accordance with the following standards:

EN 301 908-1 V11.1.1
EN 300 328 V2.2.2
EN 301 893 V2.1.1
EN 303 413 V1.1.1
EN 62311 : 2008
EN 301 489-1 V2.2.3
EN 301 489-17 V3.1.1
EN 301 489-19 V2.1.1
Draft EN 301 489-52 V1.1.0
EN 55032: 2015 + AC:2016
EN 55035: 2017
EN 61000-3-2: 2014
EN 61000-3-3: 2013
EN 62368-1:2014 + A11:2017 (Second Edition)

Yours sincerely,

PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



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

2.4GHz (2412 – 2472 MHz) : 19.86 dBm
5GHz (5150 - 5250 MHz) : 22.68 dBm
WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

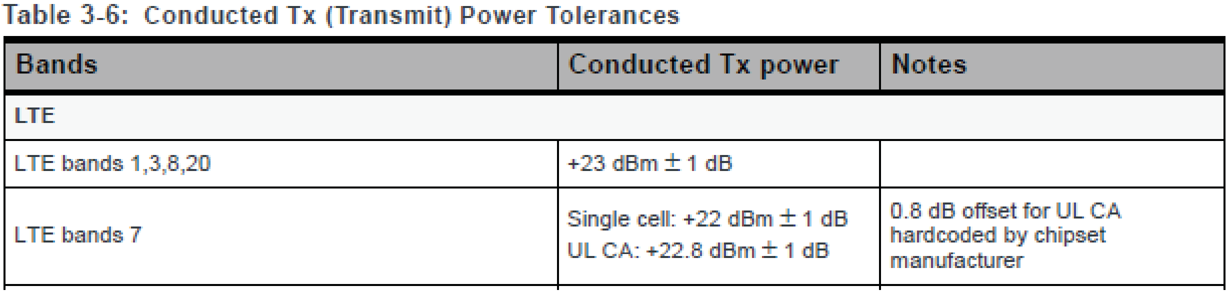


Table 3-6: Conducted Tx (Transmit) Power Tolerances

Bands	Conducted Tx power	Notes
LTE		
LTE bands 1,3,8,20	+23 dBm ± 1 dB	
LTE bands 7	Single cell: +22 dBm ± 1 dB UL CA: +22.8 dBm ± 1 dB	0.8 dB offset for UL CA hardcoded by chipset manufacturer

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/

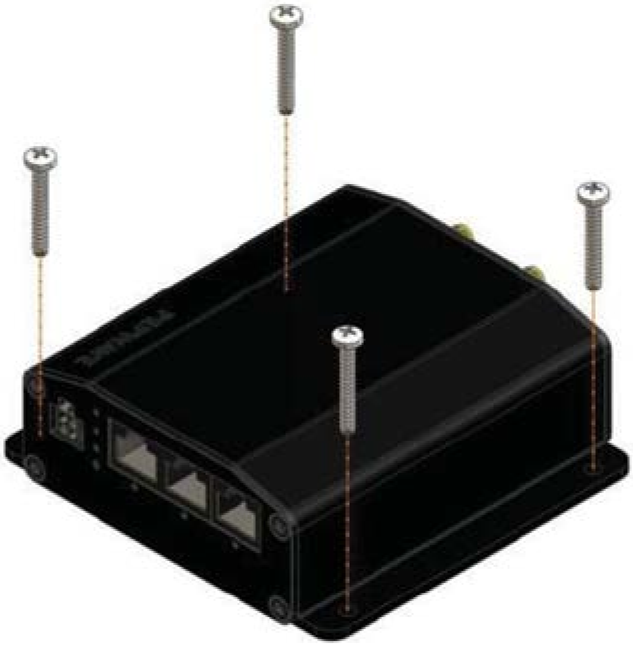
(For MAX BR1 Classic CB IEC 62368-1)

Mounting the Unit

Wall Mount

The Pepwave MAX BR1 Classic 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 Classic requires four screws for wall mounting.



Output of the external power source shall complied with ES1 and ES2 requirements, output rating 10-30 Vdc, minimum 12W (DC Jack or POE injector), with minimum ambient temperature 65 ℃, altitude = 5000m , and evaluated in accordance to UL/EN/IEC 60950-1 and / or UL/EN/IEC 62368-1

Ensure to connect the power cord of power adapter to a socket-outlet with earthing

FCC Requirements for Operation in the United States

Federal Communications Commission (FCC) Compliance Notice:

For MAX BR1 Pro 5G

FCC 15.21

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

RF exposure warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 23 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

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.

Industry Canada Statement (MAX BR1 Pro 5G)

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions

1. This device may not cause interference.

2. This device must accept any interference, including interference that may cause undesired operation of the device.

Le present appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisee aux deux conditions suivantes

1. l'appareil ne doit pas produire de brouillage, et

2. l'utilisateur de l'appareil doit accepter tout brouillage radioelectrique subi, meme si le brouillage est susceptible d'en

compromettre le fonctionnement.Informations concernant l'exposition aux frequences radio (RF)

Cet equipement est conforme avec l'exposition aux radiations IC definies pour un environnement noncontrole.

Cet equipement doit etre installe et utilise a une distance minimum de 23 cm entre le radiateuret votre corps.

Cet emetteur ne doit pas etre co-localisees ou operant en conjonction avec une autreantenne ou transmetteur.

Les utilisateurs finaux et les installateurs doivent etre informes des instructions d'installation de l'antenne et des

conditions de fonctionnement de l'emetteur afin de satisfaire a la conformite d'exposition RF.

This radio transmitter IC 20682-P1AX02 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 type Omni-directional

antenna gain for 2.4GHz 2.44 dBi

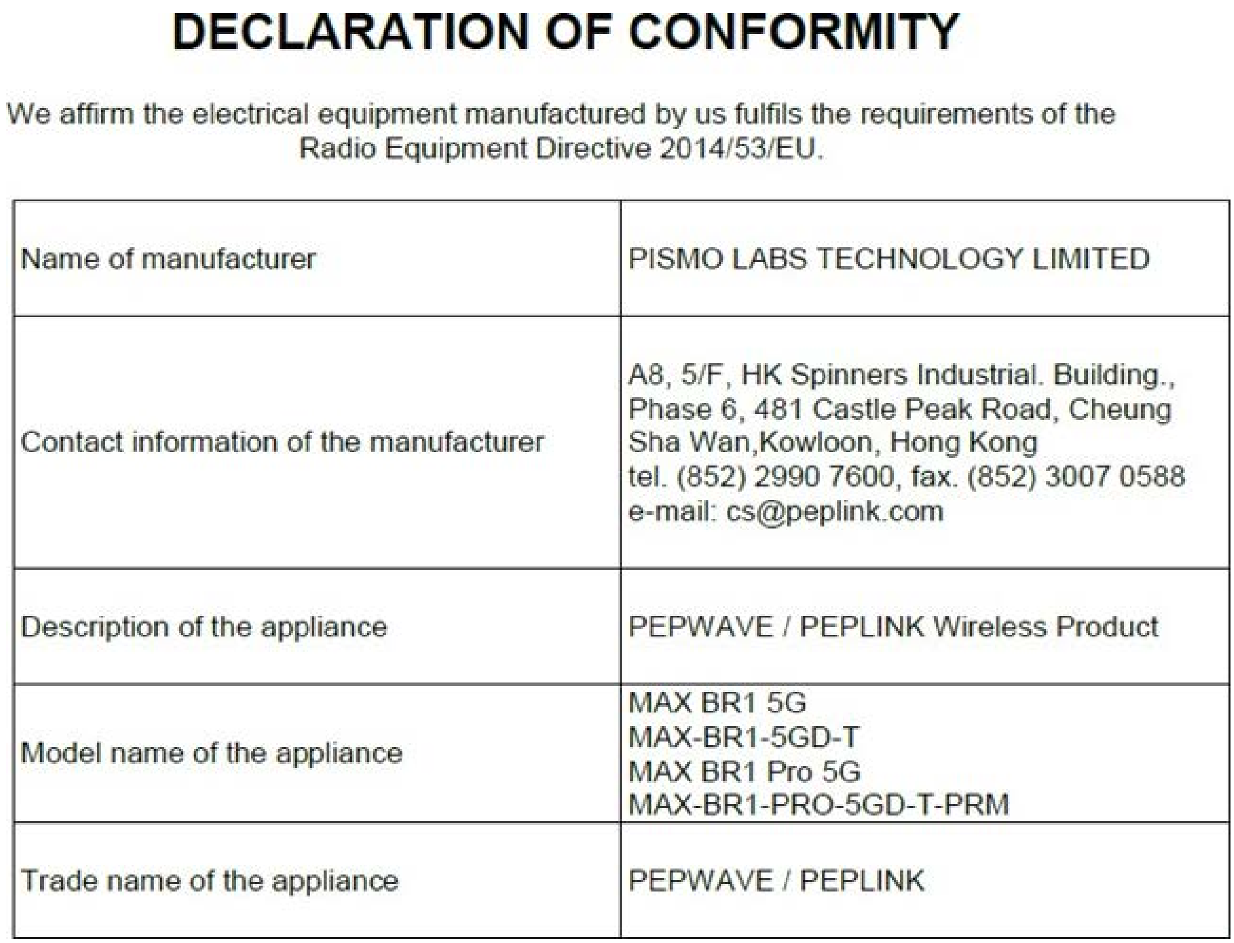
antenna gain for 5GHz (5150 ~ 5250 MHz) 4.10 dBi

antenna gain for 5GHz (5725 ~ 5850 MHz) 4.73 dBi

Battery Caution Statement

Risk of explosion if the battery is replaced by an incorrect type.

CE Statement for Pepwave Routers (MAX BR1 Pro 5G)



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 5G MAX-BR1-5GD-T MAX BR1 Pro 5G MAX-BR1-PRO-5GD-T-PRM
Trade name of the appliance	PEPWAVE / PEPLINK

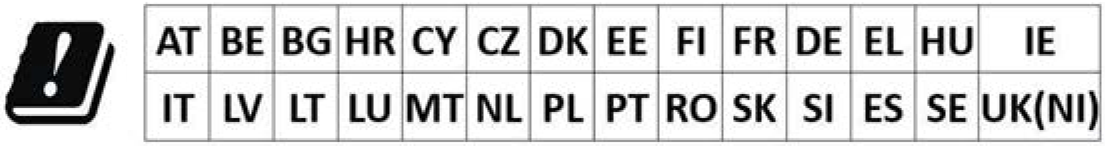
The construction of the appliance is in accordance with the following standards:

EN 301 908-1 V13.1.1
EN 300 328 V2.2.2
EN 301 893 V2.1.1
EN 303 413 V1.1.1
EN 62311 : 2020
EN 301 489-1 V2.2.3
EN 301 489-17 V3.2.4
Draft EN 301 489-19 V2.2.0
Draft EN 301 489-52 V1.1.2
EN 55032: 2015 / A11:2020
EN 55035: 2017
EN 61000-3-2: 2014
EN 61000-3-3: 2013 / A1:2019
EN 62368-1:2020+A11:2020

Yours sincerely,

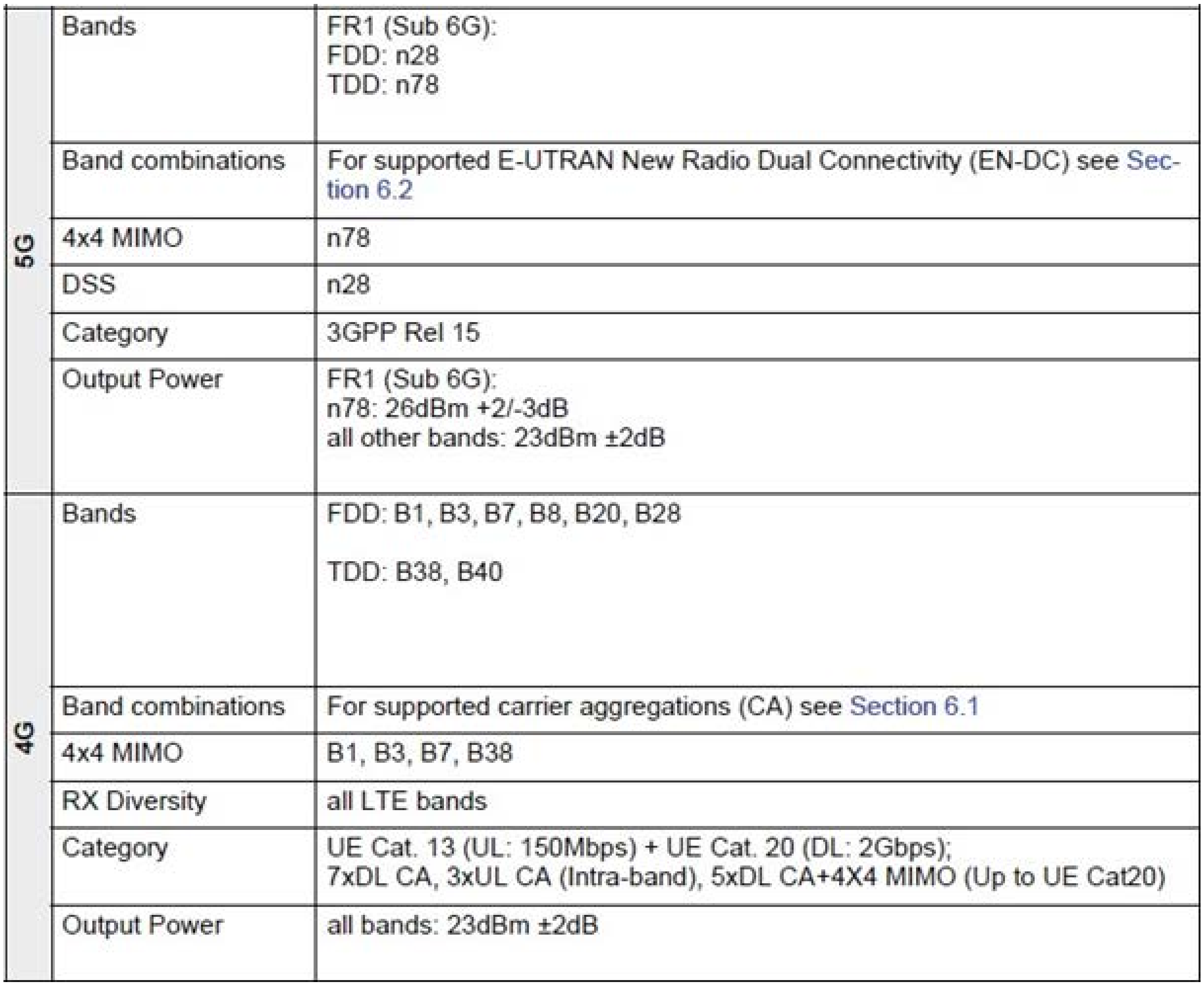
PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



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

2.4GHz (2412 – 2472 MHz) : 19.74 dBm
5GHz (5150 - 5250 MHz) : 22.66 dBm
WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)



5G	Bands	FR1 (Sub 6G): FDD: n28 TDD: n78
	Band combinations	For supported E-UTRAN New Radio Dual Connectivity (EN-DC) see Section 6.2
	4x4 MIMO	n78
	DSS	n28
	Category	3GPP Rel 15
	Output Power	FR1 (Sub 6G): n78: 26dBm +2/-3dB all other bands: 23dBm ±2dB
4G	Bands	FDD: B1, B3, B7, B8, B20, B28 TDD: B38, B40
	Band combinations	For supported carrier aggregations (CA) see Section 6.1
	4x4 MIMO	B1, B3, B7, B38
	RX Diversity	all LTE bands
	Category	UE Cat. 13 (UL: 150Mbps) + UE Cat. 20 (DL: 2Gbps); 7xDL CA, 3xUL CA (Intra-band), 5xDL CA+4X4 MIMO (Up to UE Cat20)
	Output Power	all bands: 23dBm ±2dB

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 Mini Core

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.

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

Radiation Exposure Statement

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

Industry Canada Statement (MAX BR1 Mini Core)

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Le present produit est conforme aux specifications techniques applicables a l'innovation, Science et Developpement economique Canada.

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada’s licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference.
(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le present appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisee aux deux conditions suivantes:

(1) l’appareil ne doit pas produire de brouillage, et
(2) l’utilisateur de l’appareil doit accepter tout brouillage radioelectrique subi, meme si le brouillage est susceptible d’en

Radiation Exposure Statement

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

Cet équipement est conforme avec l'exposition aux radiations ISED définies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à une distance minimum de 20 cm entre le radiateur et votre corps.

FCC Requirements for Operation in the United States

Federal Communications Commission (FCC) Compliance Notice:

For MAX 700

Federal Communication Commission Interference Statement

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 it is not installed and used in accordance with the instruction manual, it 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.

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 22 centimeters between the radiator and your body.

For MAX HD2 IP67, MAX HD2 Mini, MAX HD2 Dome, MAX HD4 IP67, MAX BR1 ENT, MAX BR1 M2M, SpeedFusion Engine

Federal Communication Commission Interference Statement

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 it is not installed and used in accordance with the instruction manual, it 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.

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Radiation Exposure Statement

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

Industry Canada Statement (MAX HD2 IP67, MAX HD2 Mini, MAX HD2 Dome, MAX HD4 IP67, MAX BR1 ENT, MAX BR1 M2M, SpeedFusion Engine)

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Le present produit est conforme aux specifications techniques applicables d'Innovation, Sciences et Developpement economique Canada.

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada’s licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference.
(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le present appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisee aux deux conditions suivantes:

(1) l’appareil ne doit pas produire de brouillage, et
(2) l’utilisateur de l’appareil doit accepter tout brouillage radioelectrique subi, meme si le brouillage est susceptible d’en

Radiation Exposure Statement

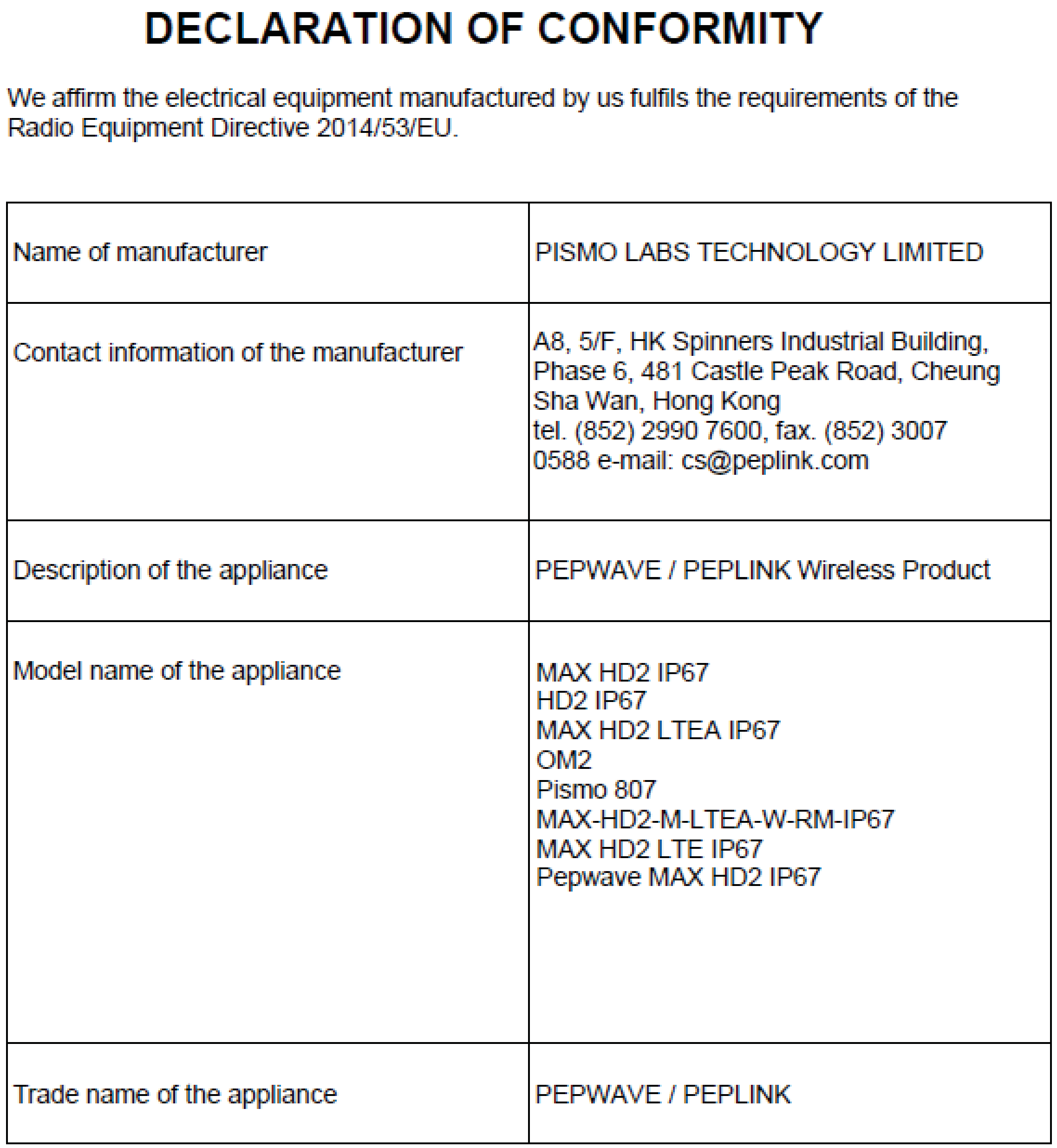
This device complies with the ISED radiation exposure limit set forth for an uncontrolled environment. This device should be installed and operated with minimum distance 20cm between the radiator & your body.

Cet équipement est conforme avec l'exposition aux radiations ISED définies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à une distance minimum de 20 cm entre le radiateur et votre corps.

Battery Caution Statement (MAX HD2 IP67, MAX HD1 Dome, MAX HD2 Dome, MAX HD4 IP67)

Risk of explosion if the battery is replaced by an incorrect type.

CE Statement for Pepwave Routers (MAX HD2 IP67)



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 HD2 IP67 HD2 IP67 MAX HD2 LTEA IP67 OM2 Pismo 807 MAX-HD2-M-LTEA-W-RM-IP67 MAX HD2 LTE IP67 Pepwave MAX HD2 IP67
Trade name of the appliance	PEPWAVE / PEPLINK

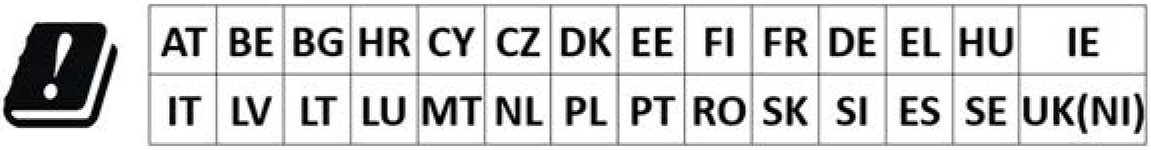
The construction of the appliance is in accordance with the following standards:

EN 301 908-1 V11.1.1
EN 303 413 V1.1.1
Draft ETSI EN 301 489-1 V2.2.0
Draft ETSI EN 301 489-52 V1.1.0
ETSI EN 301 489-19 V2.1.1
EN 55032: 2015 + AC:2016
EN 61000-3-2: 2014
EN 61000-3-3: 2013
EN 55035 : 2017
EN 62311 : 2008
EN 62368-1:2014+A11:2017

Yours sincerely,

PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



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

WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

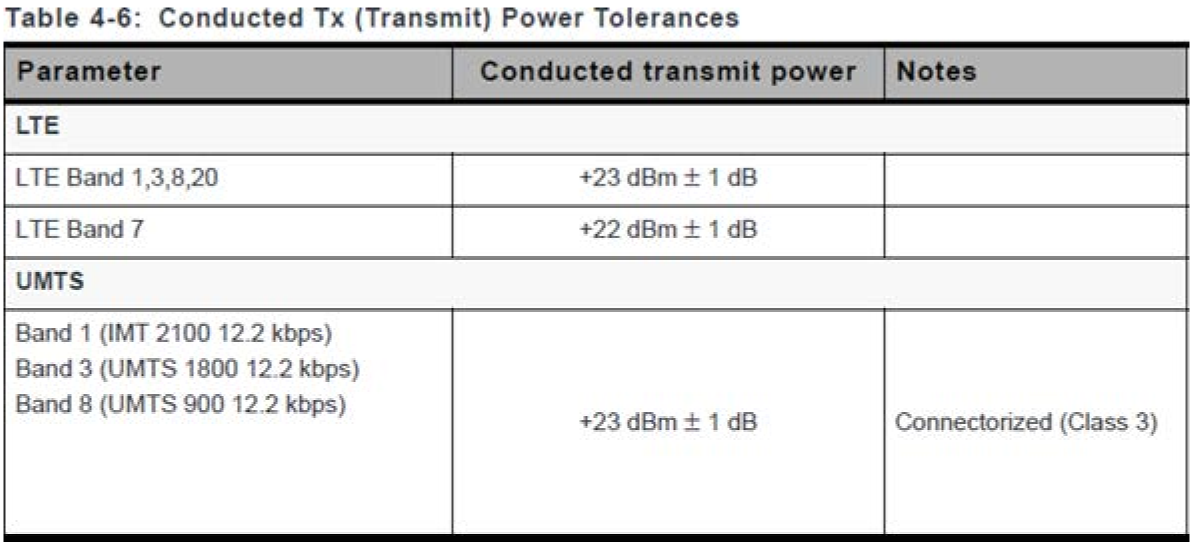


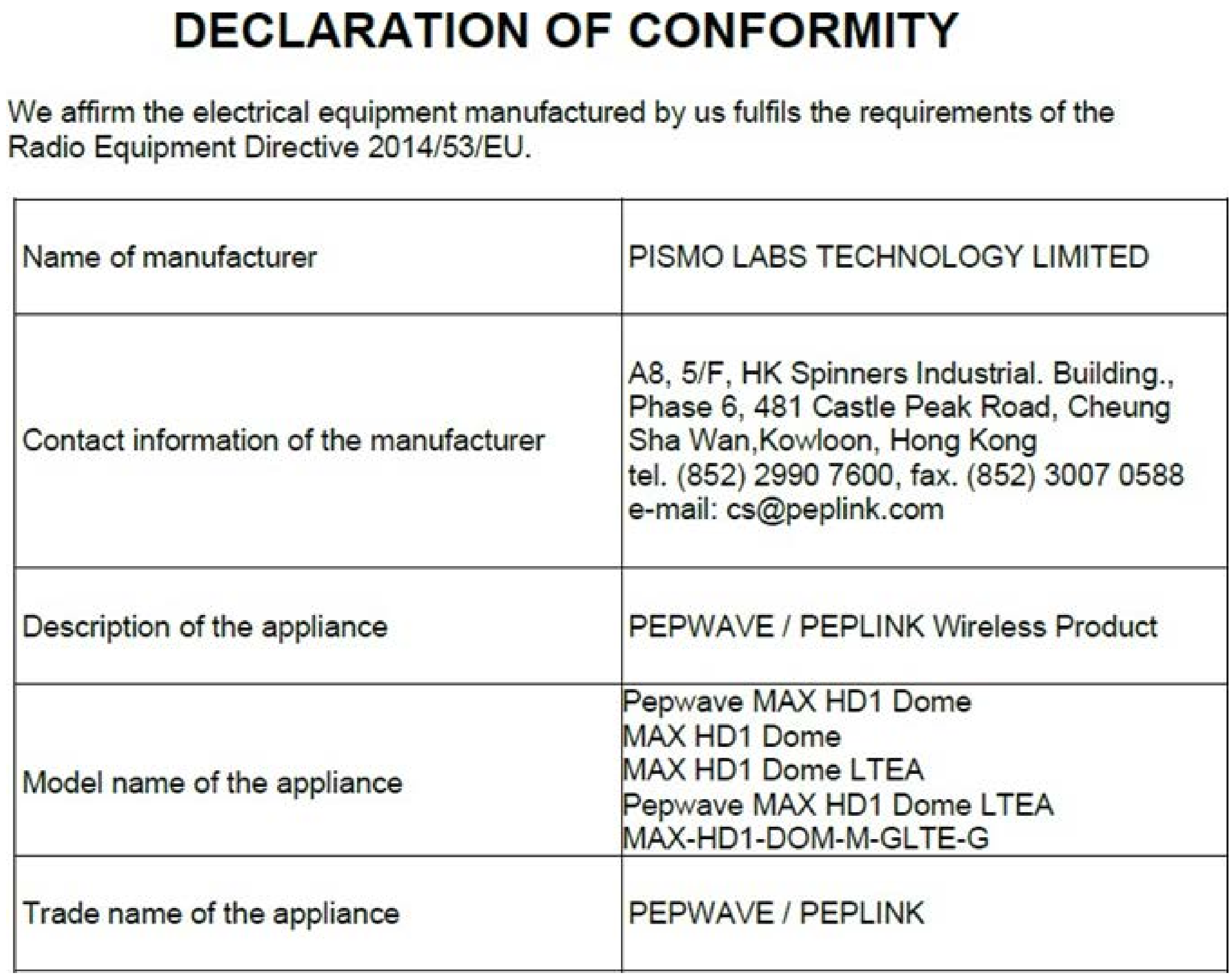
Table 4-6: Conducted Tx (Transmit) Power Tolerances

Parameter	Conducted transmit power	Notes
LTE		
LTE Band 1,3,8,20	+23 dBm ± 1 dB	
LTE Band 7	+22 dBm ± 1 dB	
UMTS		
Band 1 (IMT 2100 12.2 kbps) Band 3 (UMTS 1800 12.2 kbps) Band 8 (UMTS 900 12.2 kbps)	+23 dBm ± 1 dB	Connectorized (Class 3)

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/

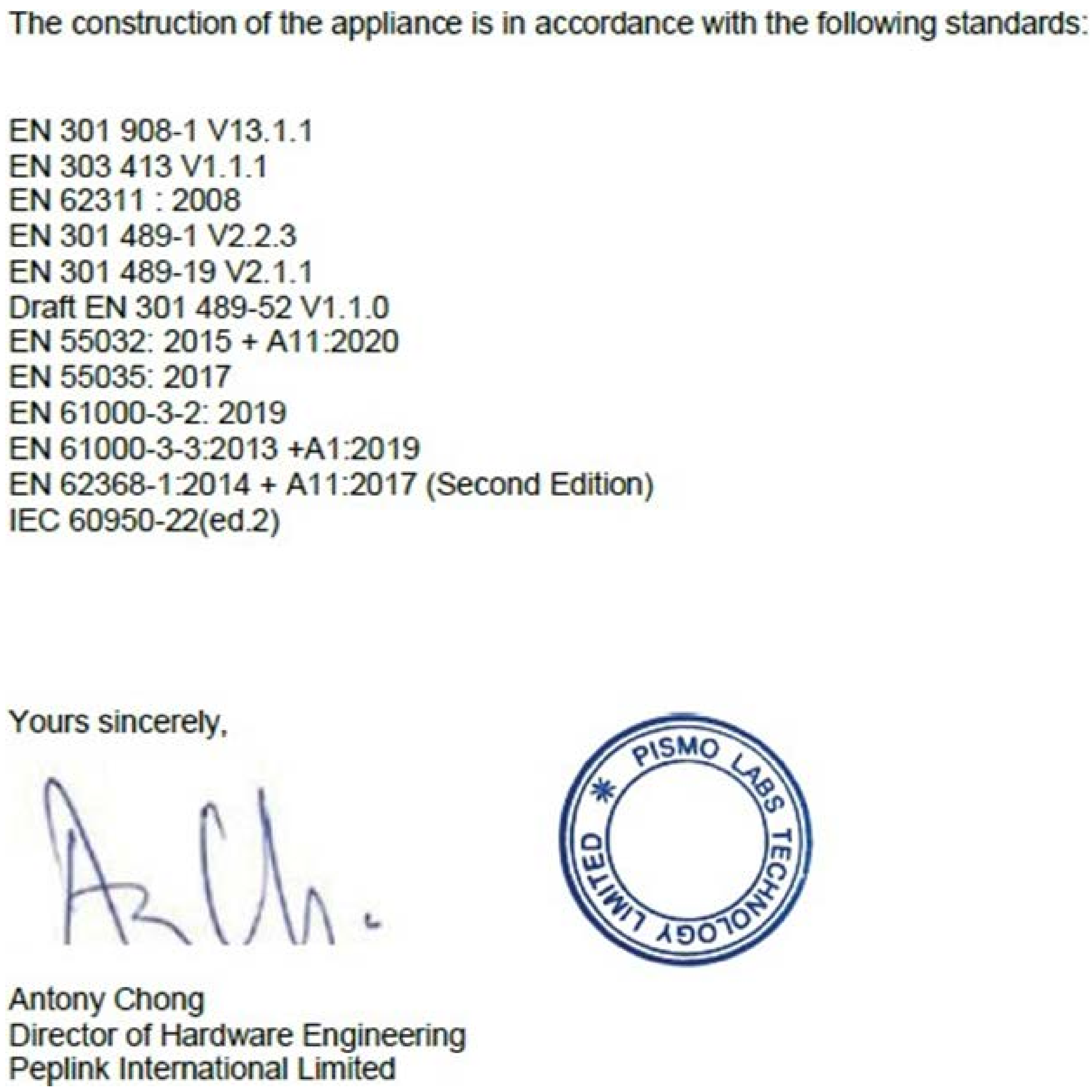
CE Statement for Pepwave Routers (MAX HD1 Dome)



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	Pepwave MAX HD1 Dome MAX HD1 Dome MAX HD1 Dome LTEA Pepwave MAX HD1 Dome LTEA MAX-HD1-DOM-M-GLTE-G
Trade name of the appliance	PEPWAVE / PEPLINK



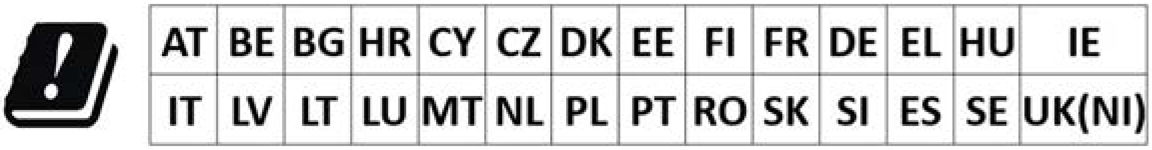
The construction of the appliance is in accordance with the following standards:

EN 301 908-1 V13.1.1
EN 303 413 V1.1.1
EN 62311 : 2008
EN 301 489-1 V2.2.3
EN 301 489-19 V2.1.1
Draft EN 301 489-52 V1.1.0
EN 55032: 2015 + A11:2020
EN 55035: 2017
EN 61000-3-2: 2019
EN 61000-3-3:2013 +A1:2019
EN 62368-1:2014 + A11:2017 (Second Edition)
IEC 60950-22(ed.2)

Yours sincerely,

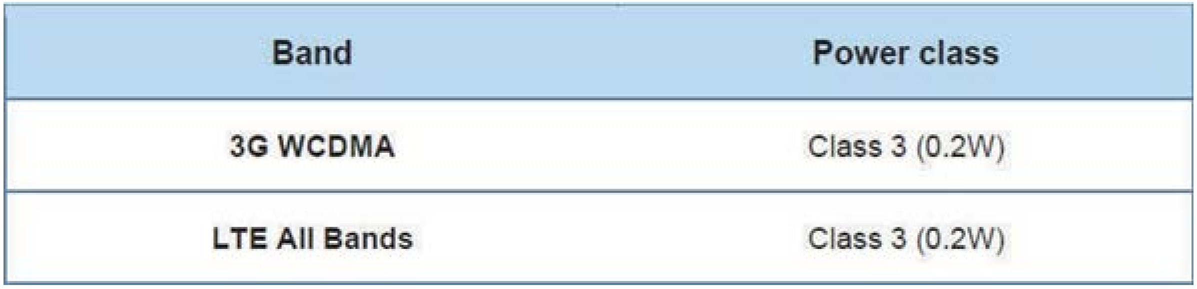
PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



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

WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

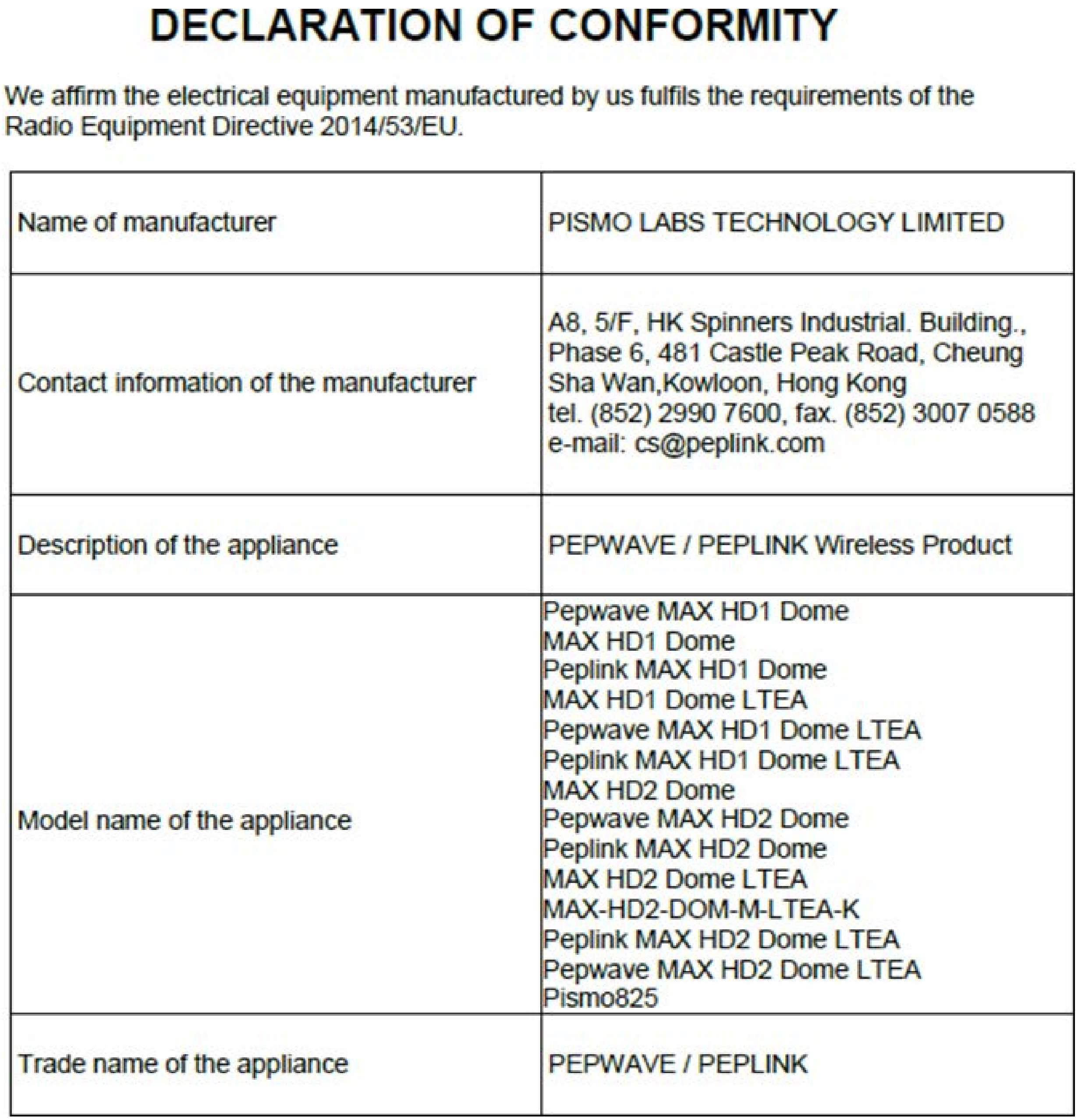


Band	Power class
3G WCDMA	Class 3 (0.2W)
LTE All Bands	Class 3 (0.2W)

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/

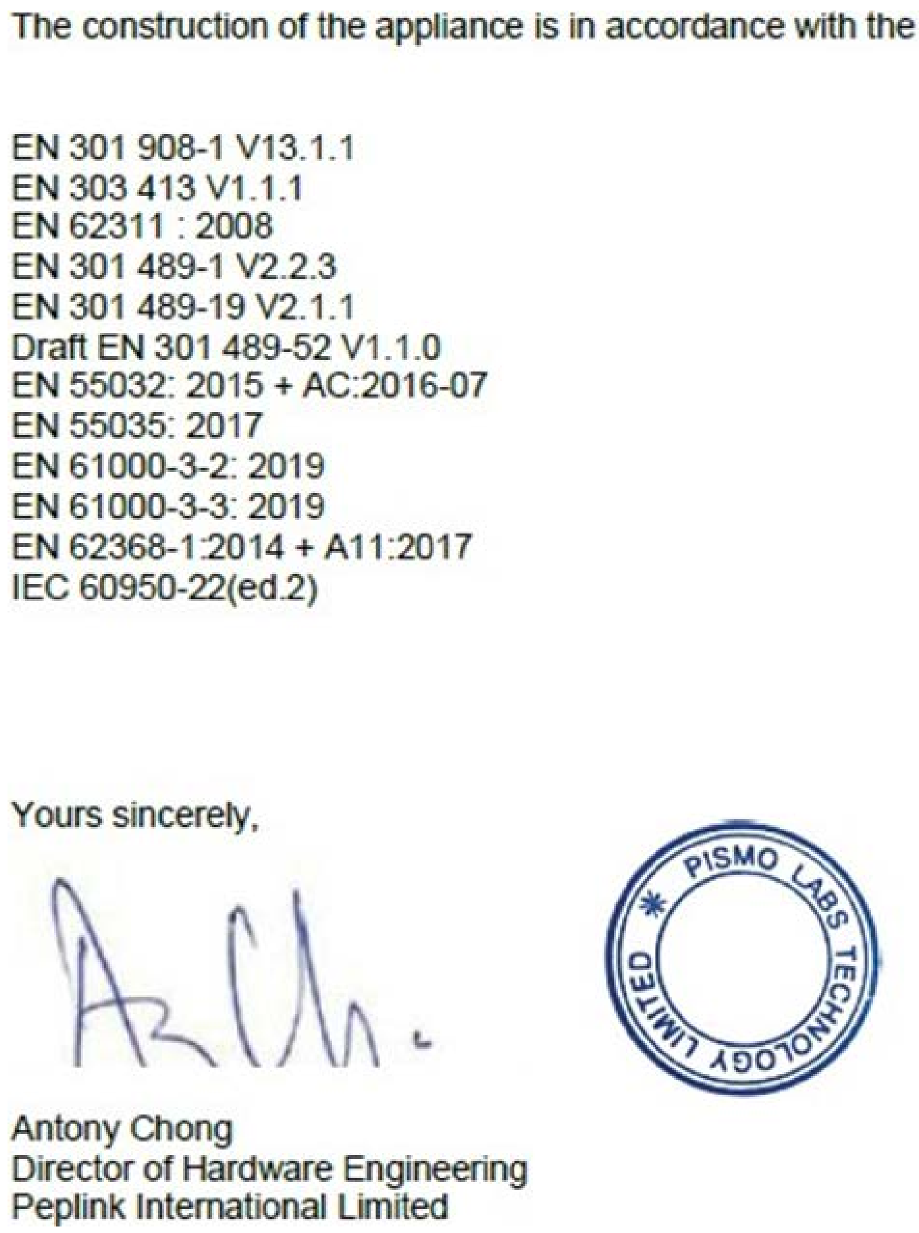
CE Statement for Pepwave Routers (MAX HD2 Dome)



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	Pepwave MAX HD1 Dome MAX HD1 Dome Peplink MAX HD1 Dome MAX HD1 Dome LTEA Pepwave MAX HD1 Dome LTEA Peplink MAX HD1 Dome LTEA MAX HD2 Dome Pepwave MAX HD2 Dome Peplink MAX HD2 Dome MAX HD2 Dome LTEA MAX-HD2-DOM-M-LTEA-K Peplink MAX HD2 Dome LTEA Pepwave MAX HD2 Dome LTEA Pismo825
Trade name of the appliance	PEPWAVE / PEPLINK



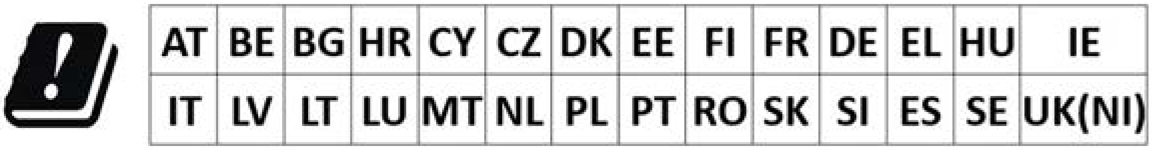
The construction of the appliance is in accordance with the following standards:

EN 301 908-1 V13.1.1
EN 303 413 V1.1.1
EN 62311 : 2008
EN 301 489-1 V2.2.3
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: 2019
EN 61000-3-3: 2019
EN 62368-1:2014 + A11:2017
IEC 60950-22(ed.2)

Yours sincerely,

PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



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

WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

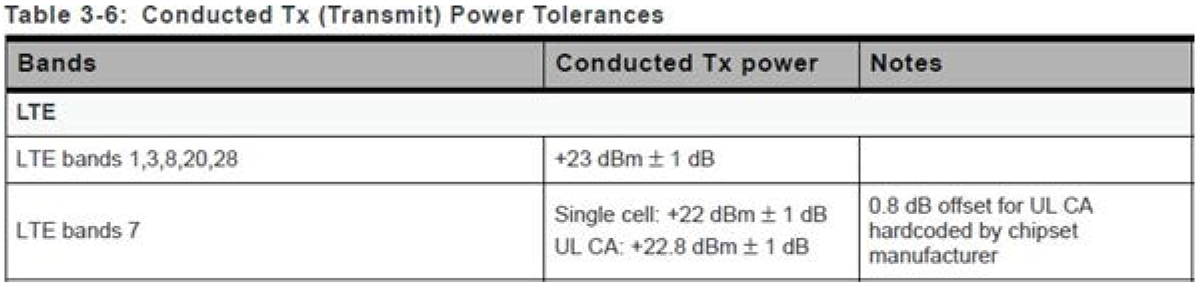


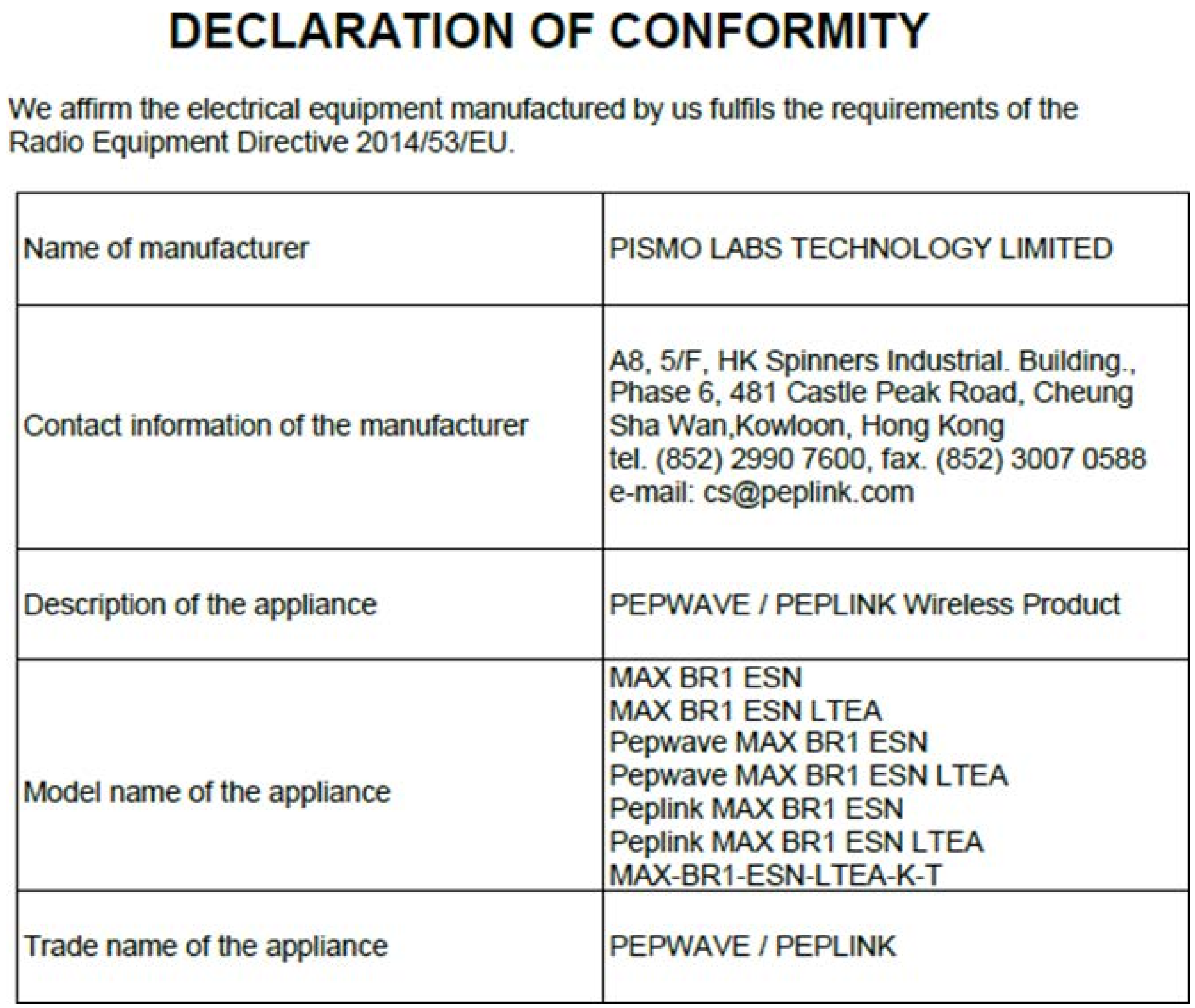
Table 3-6: Conducted Tx (Transmit) Power Tolerances

Bands	Conducted Tx power	Notes
LTE		
LTE bands 1,3,8,20,28	+23 dBm ± 1 dB	
LTE bands 7	Single cell: +22 dBm ± 1 dB UL CA: +22.8 dBm ± 1 dB	0.8 dB offset for UL CA hardcoded by chipset manufacturer

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/

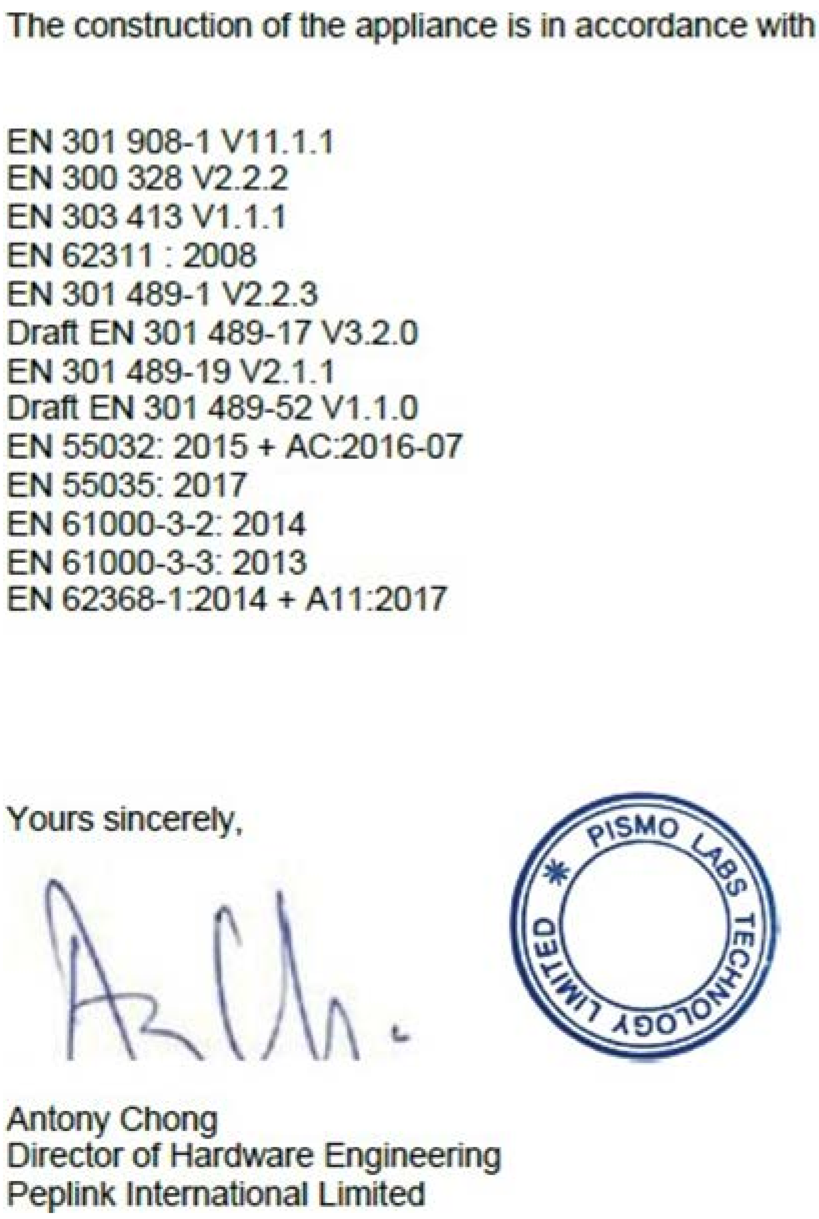
CE Statement for Pepwave Routers (MAX BR1 ESN)



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 MAX-BR1-ESN-LTEA-K-T
Trade name of the appliance	PEPWAVE / PEPLINK



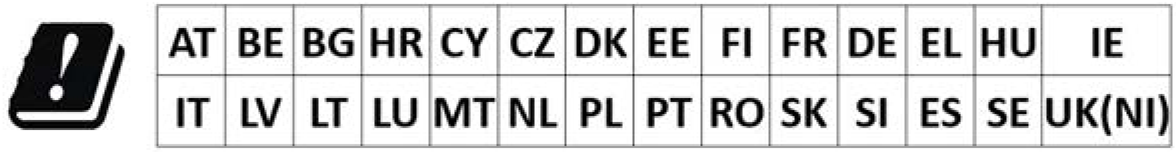
The construction of the appliance is in accordance with the following standards:

EN 301 908-1 V11.1.1
EN 300 328 V2.2.2
EN 303 413 V1.1.1
EN 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,

PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



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

2.4GHz (2412 - 2472 MHz) : 19.78 dBm

WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

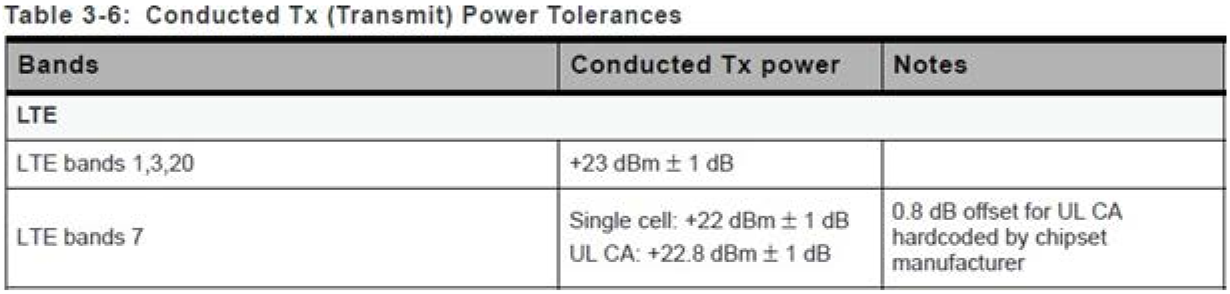


Table 3-6: Conducted Tx (Transmit) Power Tolerances

Bands	Conducted Tx power	Notes
LTE		
LTE bands 1,3,20	+23 dBm ± 1 dB	
LTE bands 7	Single cell: +22 dBm ± 1 dB UL CA: +22.8 dBm ± 1 dB	0.8 dB offset for UL CA hardcoded by chipset manufacturer

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

Federal Communication Commission Interference Statement

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 it is not installed and used in accordance with the instruction manual, it 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.

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 40 centimeters between the radiator and your body.

Industry Canada Statement (MAX HD4)

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Le present produit est conforme aux specifications techniques applicables d'Innovation, Sciences et Developpement economique Canada.

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions

(1) This device may not cause interference.

(2) This device must accept any interference, including interference that may cause undesired opera- tion of the device.

Le present appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio ex- empts de licence. L'exploitation est autorisee aux deux conditions suivantes

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioelectrique subi, meme si le brouillage est susceptible d'en

(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) For devices with detachable antenna(s), 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

The high-power radars are allocated as primary users (i.e. priority users) of the band 5725-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

(i) Le dispositif fonctionnant dans la bande 5150-5250 MHz est reserve uniquement pour une utilisation a l'interieur afin de reduire les risques de brouillage prejudiciable aux systemes de satellites mobiles utilisant les memes canaux;

(ii) Le gain maximal d'antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisant la bande 5725-5850 MHz doit se conformer a la limitation P.I.R.E specifiee pour l'exploitation point a point et non point a point, selon le cas.

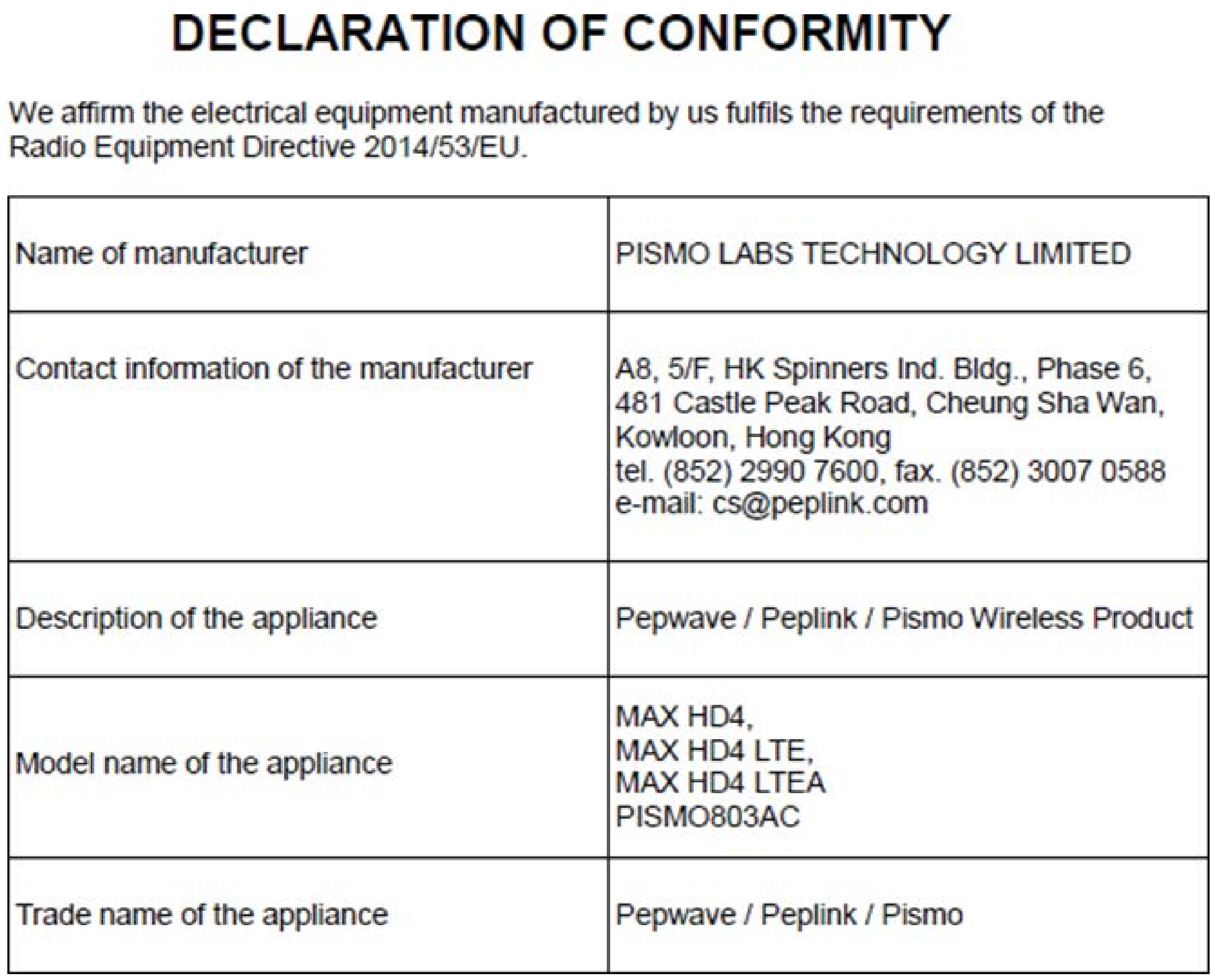
En outre, les utilisateurs devraient aussi etre avises que les utilisateurs de radars de haute puissance sont designes utilisateurs principaux (c.-a-d., qu'ils ont la priorite) pour les bande 5725-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Radiation Exposure Statement

This device complies with the ISED radiation exposure limit set forth for an uncontrolled environment. This device should be installed and operated with minimum distance 40cm between the radiator & your body.

Cet equipement est conforme avec l'exposition aux radiations ISED definies pour un environnement non controle. Cet equipement doit etre installe et utilise a une distance minimum de 40 cm entre le radiateur et votre corps.

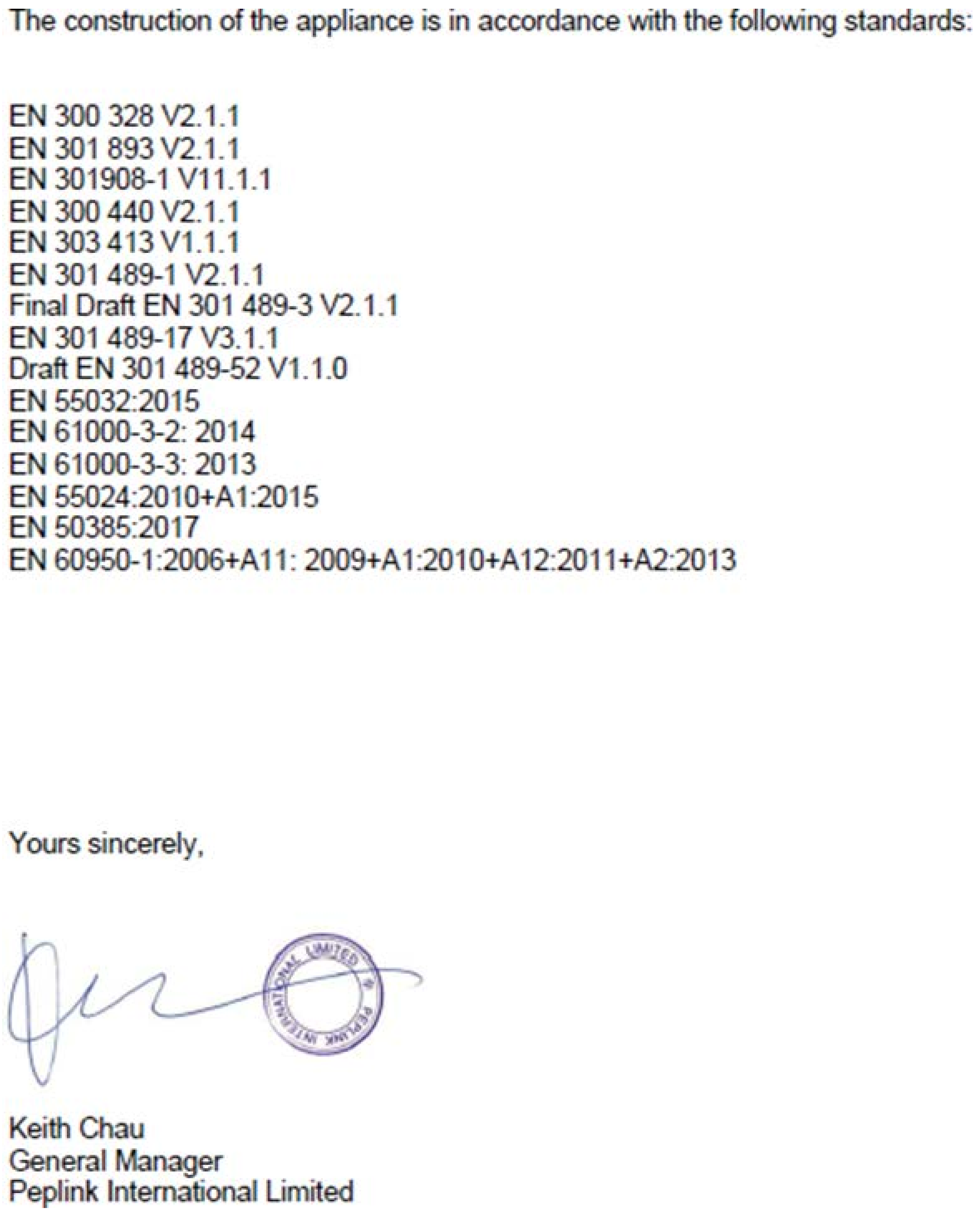
CE Statement for Pepwave Routers (MAX HD4)



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 HD4, MAX HD4 LTE, MAX HD4 LTEA PISMO803AC
Trade name of the appliance	Pepwave / Peplink / Pismo

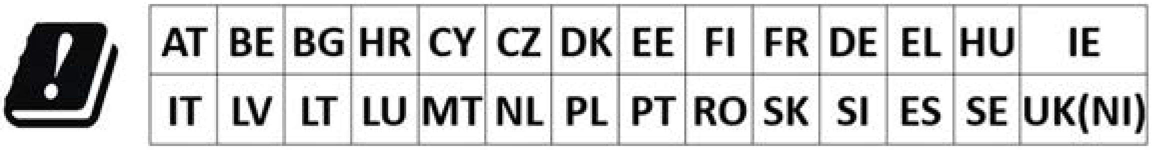


The construction of the appliance is in accordance with the following standards:

EN 300 328 V2.1.1
EN 301 893 V2.1.1
EN 301908-1 V11.1.1
EN 300 440 V2.1.1
EN 303 413 V1.1.1
EN 301 489-1 V2.1.1
Final Draft EN 301 489-3 V2.1.1
EN 301 489-17 V3.1.1
Draft EN 301 489-52 V1.1.0
EN 55032:2015
EN 61000-3-2: 2014
EN 61000-3-3: 2013
EN 55024:2010+A1:2015
EN 50385:2017
EN 60950-1:2006+A11: 2009+A1:2010+A12:2011+A2:2013

Yours sincerely,

Keith Chau
General Manager
Peplink International Limited

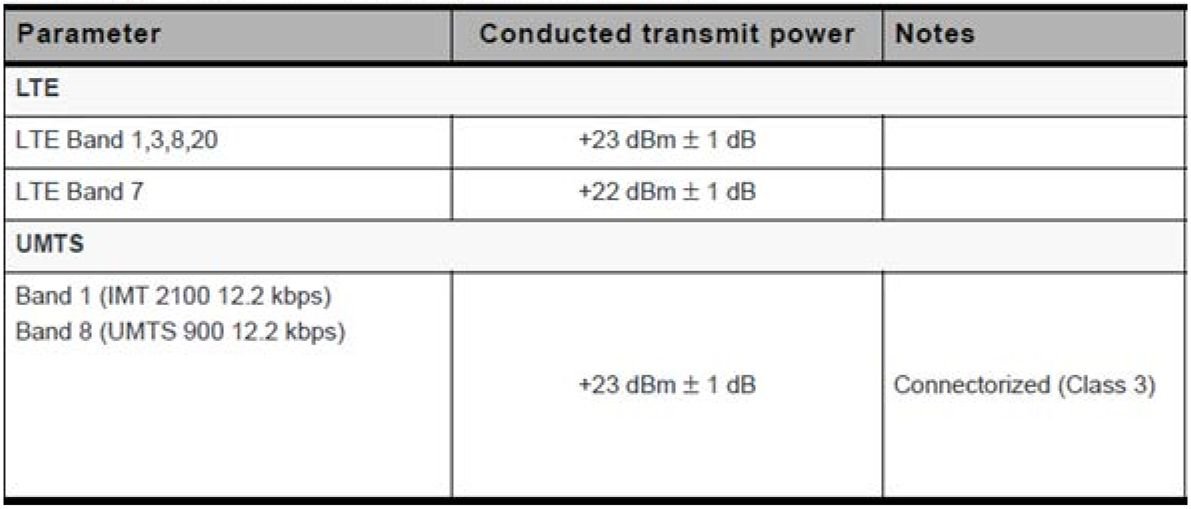


AT	BE	BG	HR	CY	CZ	DK	EE	FI	FR	DE	EL	HU	IE
IT	LV	LT	LU	MT	NL	PL	PT	RO	SK	SI	ES	SE	UK(NI)

2.4GHz (2412 - 2472 MHz) : 18.87 dBm
5GHz (5150 - 5250 MHz & 5725 - 5850 MHz) : 19.13 dBm

WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

Table 4-6: Conducted Tx (Transmit) Power Tolerances

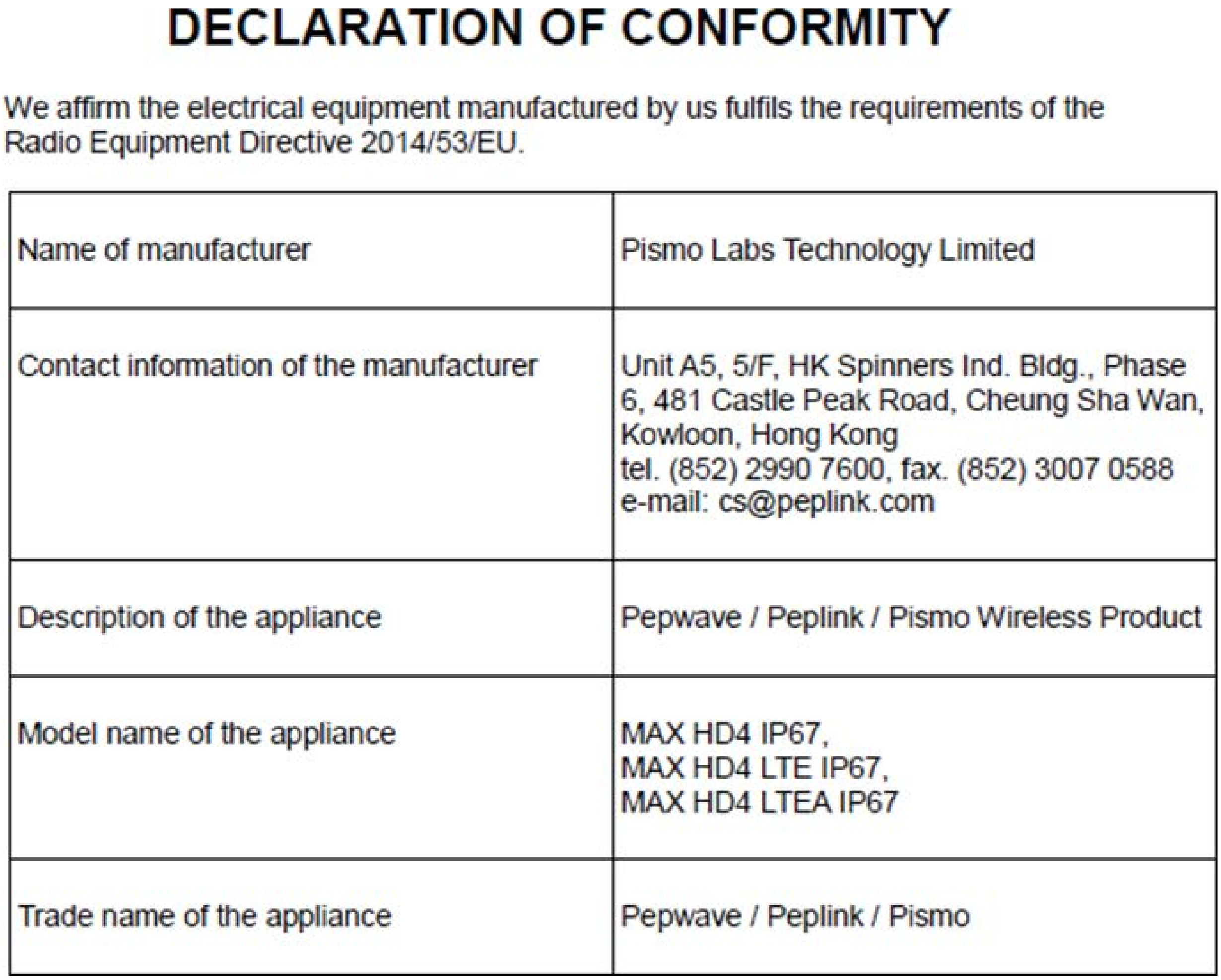


Parameter	Conducted transmit power	Notes
LTE		
LTE Band 1,3,8,20	+23 dBm ± 1 dB	
LTE Band 7	+22 dBm ± 1 dB	
UMTS		
Band 1 (IMT 2100 12.2 kbps) Band 8 (UMTS 900 12.2 kbps)	+23 dBm ± 1 dB	Connectorized (Class 3)

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/

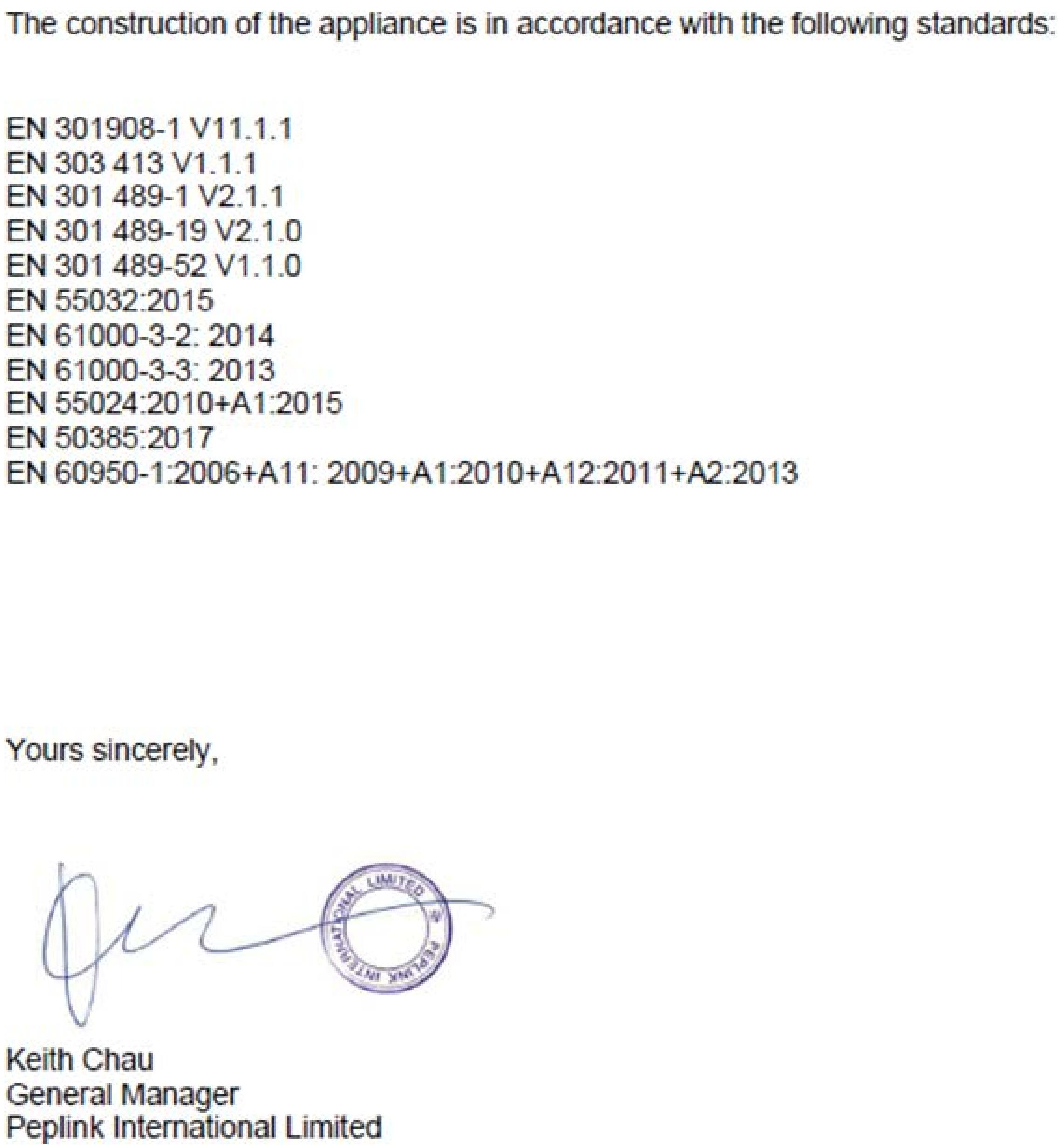
CE Statement for Pepwave Routers (MAX HD4 IP67)



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	Unit A5, 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 HD4 IP67, MAX HD4 LTE IP67, MAX HD4 LTEA IP67
Trade name of the appliance	Pepwave / Peplink / Pismo

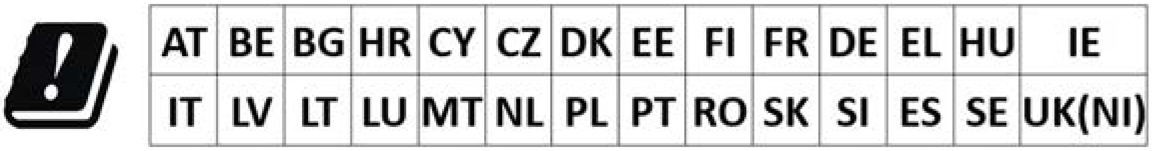


The construction of the appliance is in accordance with the following standards:

EN 301908-1 V11.1.1
EN 303 413 V1.1.1
EN 301 489-1 V2.1.1
EN 301 489-19 V2.1.0
EN 301 489-52 V1.1.0
EN 55032:2015
EN 61000-3-2: 2014
EN 61000-3-3: 2013
EN 55024:2010+A1:2015
EN 50385:2017
EN 60950-1:2006+A11: 2009+A1:2010+A12:2011+A2:2013

Yours sincerely,

Keith Chau
General Manager
Peplink International Limited



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

WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

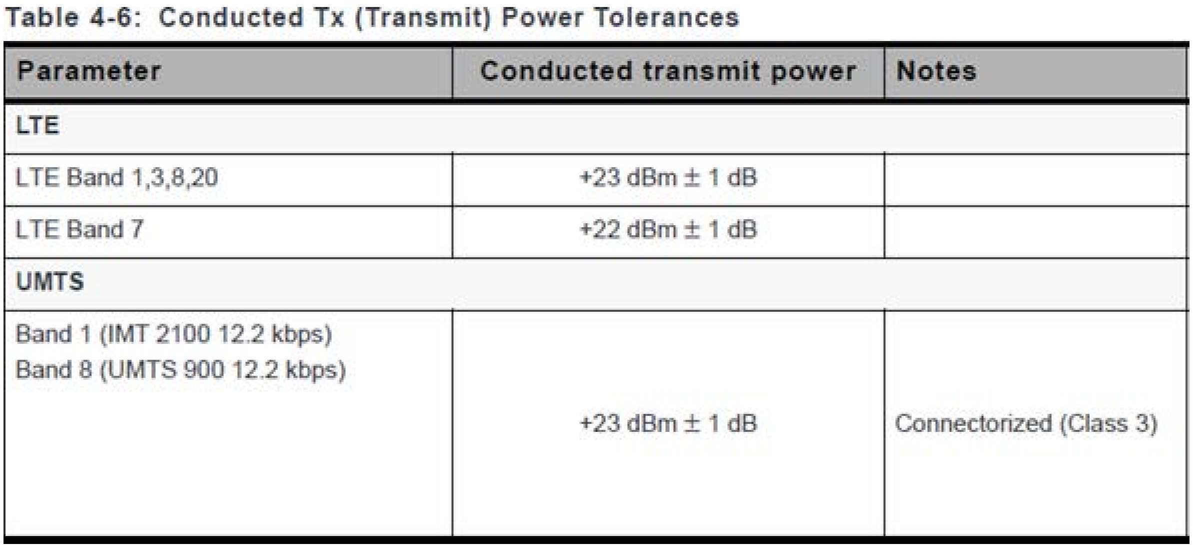


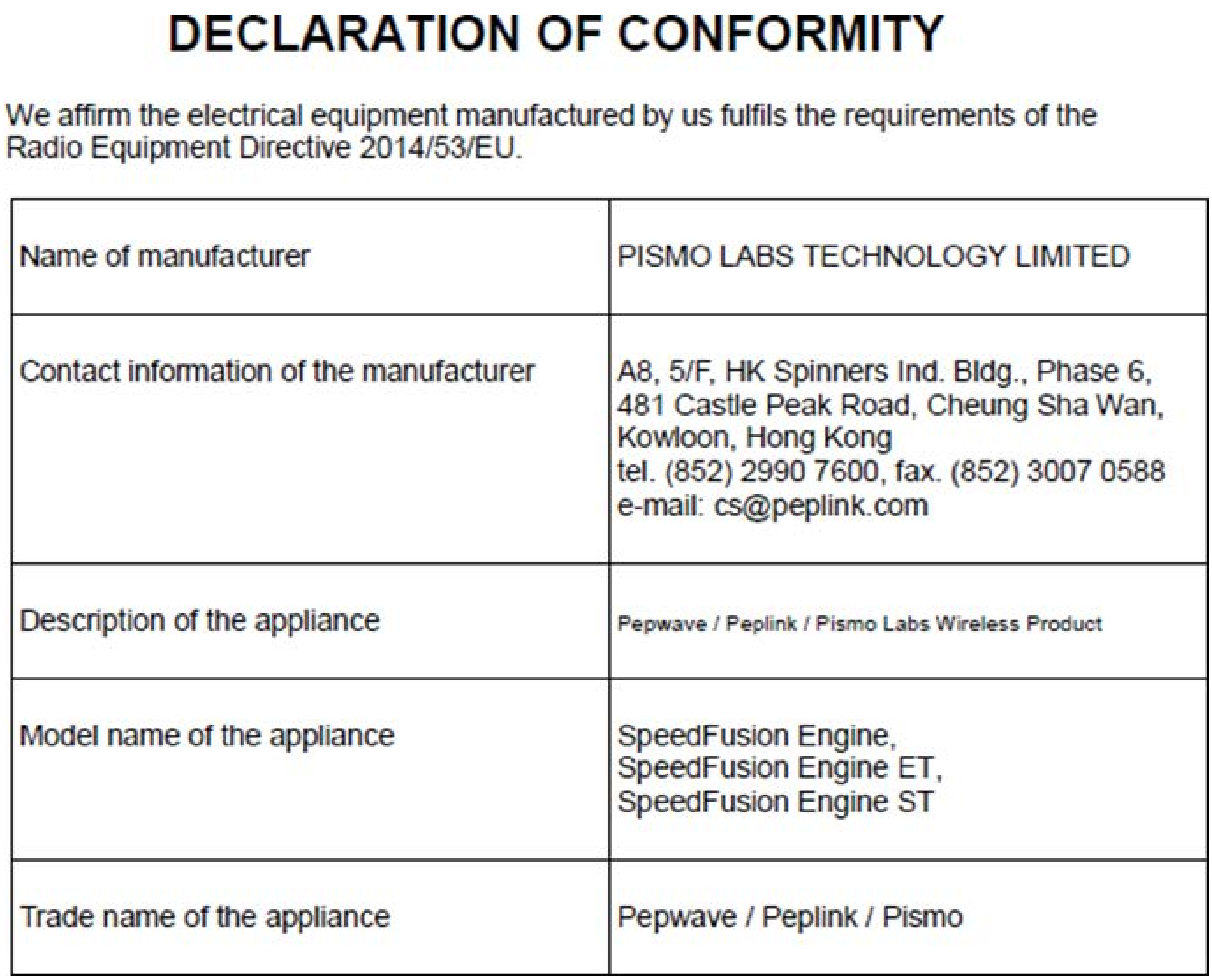
Table 4-6: Conducted Tx (Transmit) Power Tolerances

Parameter	Conducted transmit power	Notes
LTE		
LTE Band 1,3,8,20	+23 dBm ± 1 dB	
LTE Band 7	+22 dBm ± 1 dB	
UMTS		
Band 1 (IMT 2100 12.2 kbps) Band 8 (UMTS 900 12.2 kbps)	+23 dBm ± 1 dB	Connectorized (Class 3)

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/

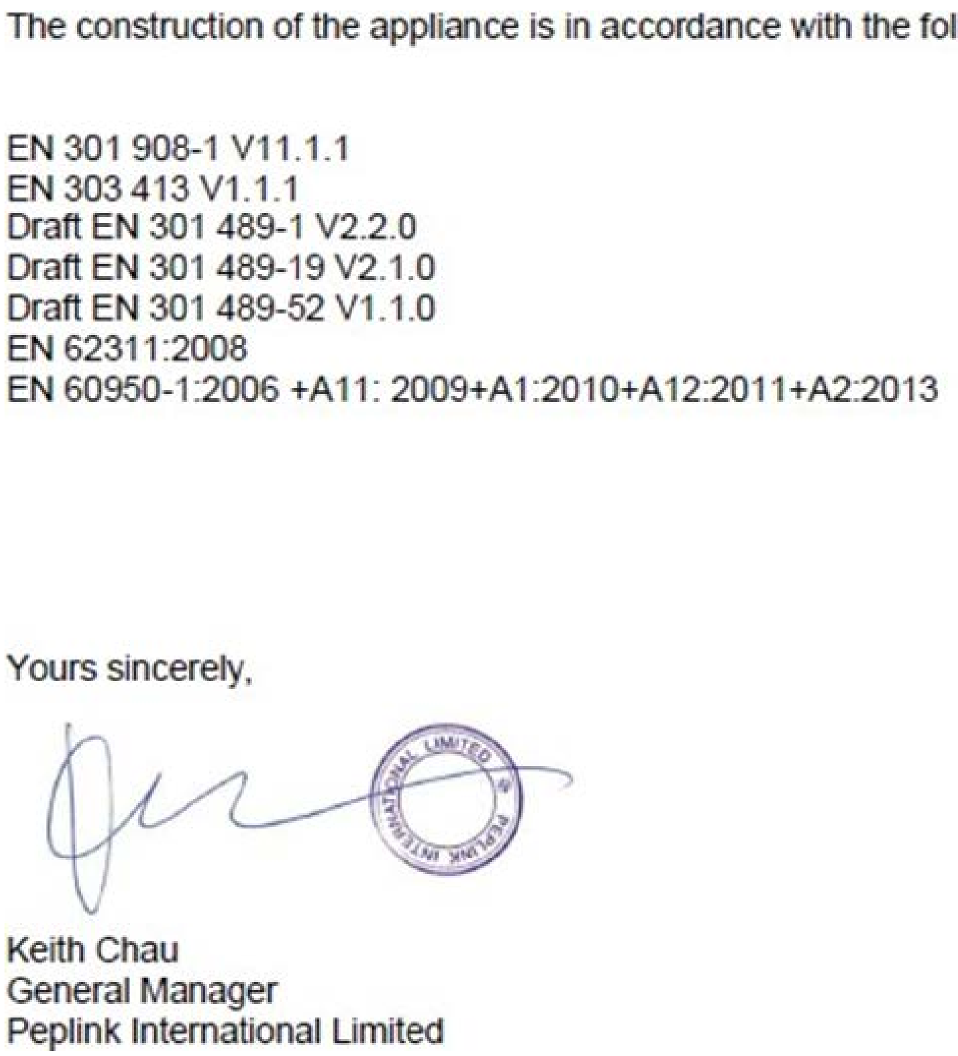
CE Statement for Pepwave Routers (SpeedFusion Engine)



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 Labs Wireless Product
Model name of the appliance	SpeedFusion Engine, SpeedFusion Engine ET, SpeedFusion Engine ST
Trade name of the appliance	Pepwave / Peplink / Pismo

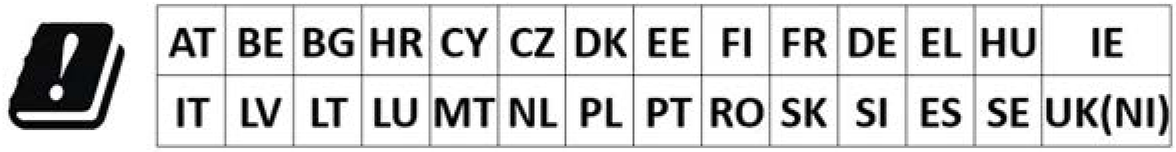


The construction of the appliance is in accordance with the following standards:

EN 301 908-1 V11.1.1
EN 303 413 V1.1.1
Draft EN 301 489-1 V2.2.0
Draft EN 301 489-19 V2.1.0
Draft EN 301 489-52 V1.1.0
EN 62311:2008
EN 60950-1:2006 +A11: 2009+A1:2010+A12:2011+A2:2013

Yours sincerely,

Keith Chau
General Manager
Peplink International Limited



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

WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

MC7455 module:

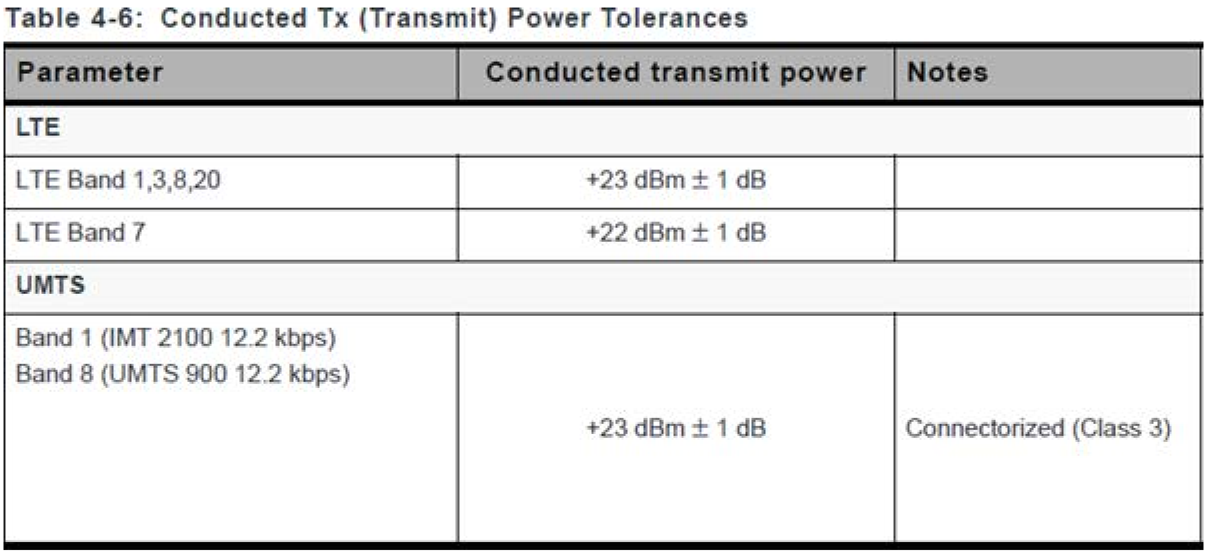
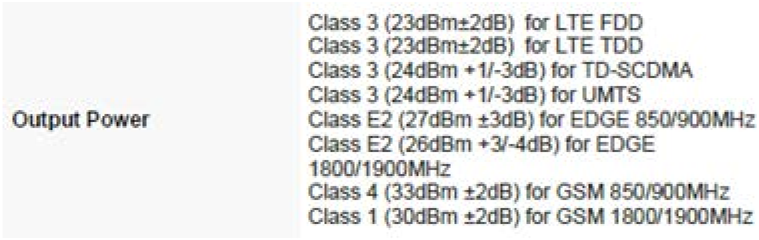


Table 4-6: Conducted Tx (Transmit) Power Tolerances

Parameter	Conducted transmit power	Notes
LTE		
LTE Band 1,3,8,20	+23 dBm ± 1 dB	
LTE Band 7	+22 dBm ± 1 dB	
UMTS		
Band 1 (IMT 2100 12.2 kbps) Band 8 (UMTS 900 12.2 kbps)	+23 dBm ± 1 dB	Connectorized (Class 3)

EC25-E module:



Output Power	Class 3 (23dBm±2dB) for LTE FDD Class 3 (23dBm±2dB) for LTE TDD Class 3 (24dBm +1/-3dB) for TD-SCDMA Class 3 (24dBm +1/-3dB) for UMTS Class E2 (27dBm ±3dB) for EDGE 850/900MHz Class E2 (26dBm +3/-4dB) for EDGE 1800/1900MHz Class 4 (33dBm ±2dB) for GSM 850/900MHz Class 1 (30dBm ±2dB) for GSM 1800/1900MHz

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 Transit, MAX Transit Duo

Federal Communication Commission Interference Statement

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 it is not installed and used in accordance with the instruction manual, it 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.

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the 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.

Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 24 centimeters between the radiator and your body.

Industry Canada Statement (MAX Transit, MAX Transit Duo)

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Le present produit est conforme aux specifications techniques applicables d'Innovation, Sciences et

Développement économique Canada.

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada’s licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference.

(2) This device must accept any interference, including interference that may cause undesired opera- tion of the device.

Le present appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio ex- empts de licence. L'exploitation est autorisee aux deux conditions suivantes:

(1) l’appareil ne doit pas produire de brouillage, et

(2) l’utilisateur de l’appareil doit accepter tout brouillage radioelectrique subi, meme si le brouillage est susceptible d’en

(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) For devices with detachable antenna(s), 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

The high-power radars are allocated as primary users (i.e. priority users) of the band 5725-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

(i) Le dispositif fonctionnant dans la bande 5150-5250 MHz est reserve uniquement pour une utilisation a l'interieur afin de reduire les risques de brouillage prejudiciable aux systemes de satellites mobiles utilisant les memes canaux;

(ii) Le gain maximal d'antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisant la bande 5725-5850 MHz doit se conformer a la limitation P.I.R.E specifiee pour l'exploitation point a point et non point a point, selon le cas.

En outre, les utilisateurs devraient aussi etre avises que les utilisateurs de radars de haute puissance sont designes utilisateurs principaux (c.-a-d., qu'ils ont la priorite) pour les bande 5725-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Radiation Exposure Statement

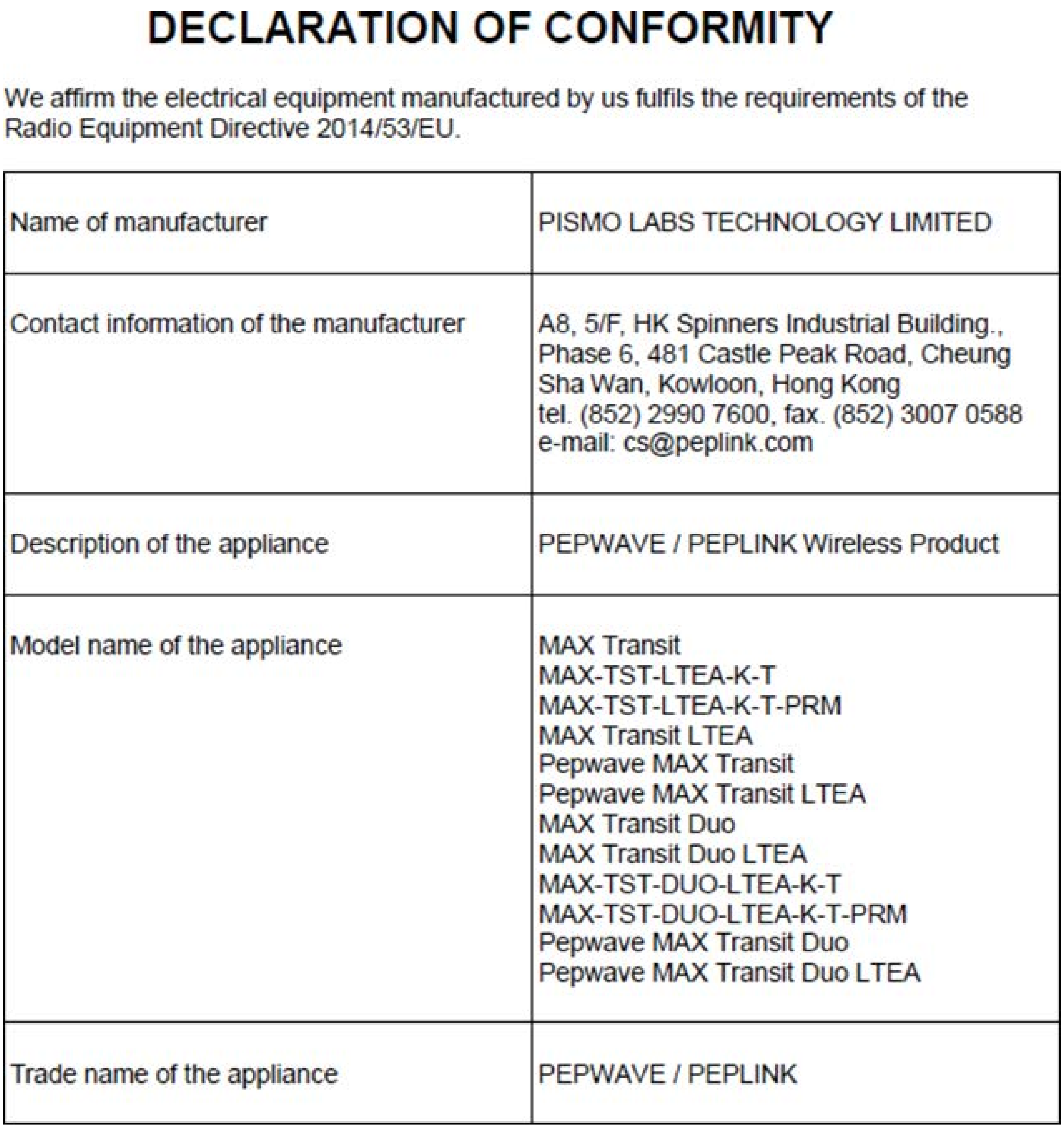
This device complies with the ISED radiation exposure limit set forth for an uncontrolled environment. This device should be installed and operated with minimum distance 30cm between the radiator & your body.

Cet equipement est conforme avec l'exposition aux radiations ISED definies pour un environnement non controle. Cet equipement doit etre installe et utilise a une distance minimum de 30 cm entre le radiateur et votre corps.

Battery Caution Statement

Risk of explosion if the battery is replaced by an incorrect type.

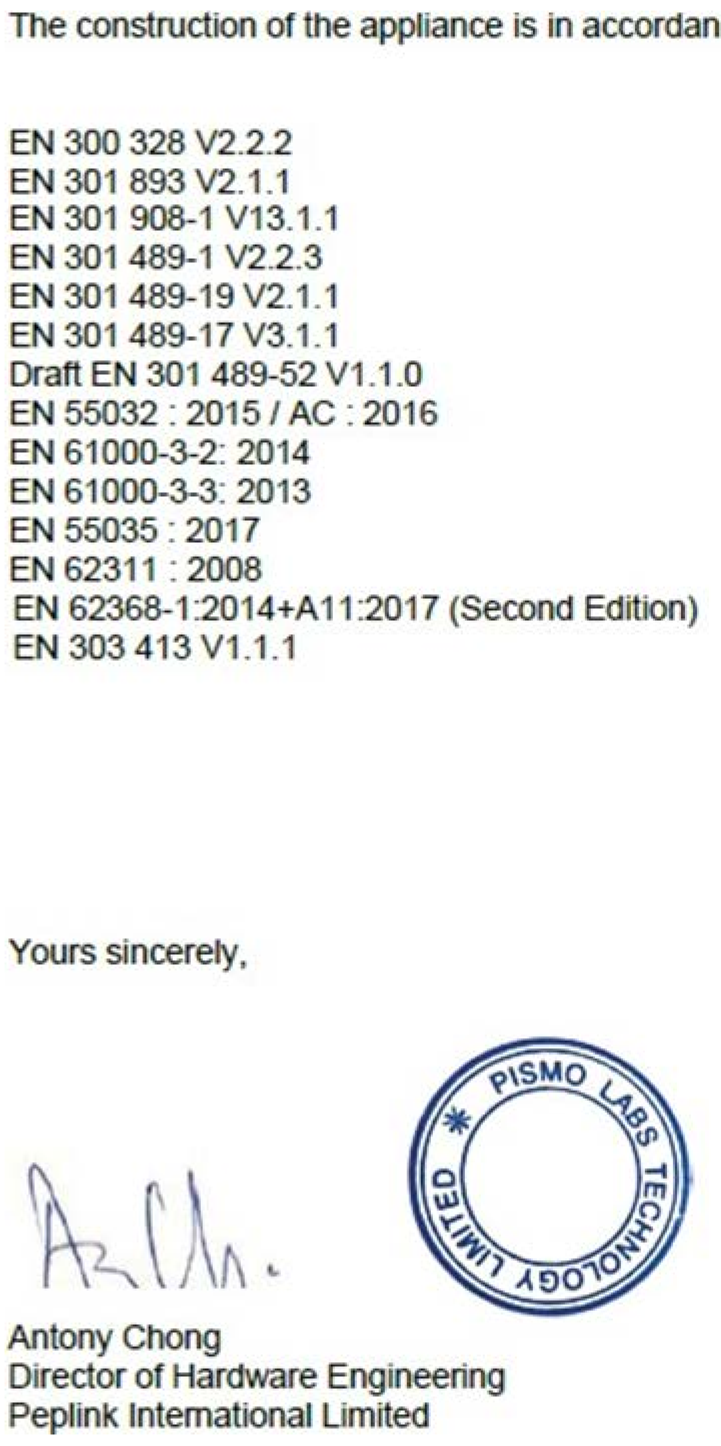
CE Statement for Pepwave Routers (MAX Transit / MAX Transit Duo For EM7565)



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 Transit MAX-TST-LTEA-K-T MAX-TST-LTEA-K-T-PRM MAX Transit LTEA Pepwave MAX Transit Pepwave MAX Transit LTEA MAX Transit Duo MAX Transit Duo LTEA MAX-TST-DUO-LTEA-K-T MAX-TST-DUO-LTEA-K-T-PRM Pepwave MAX Transit Duo Pepwave MAX Transit Duo LTEA
Trade name of the appliance	PEPWAVE / PEPLINK



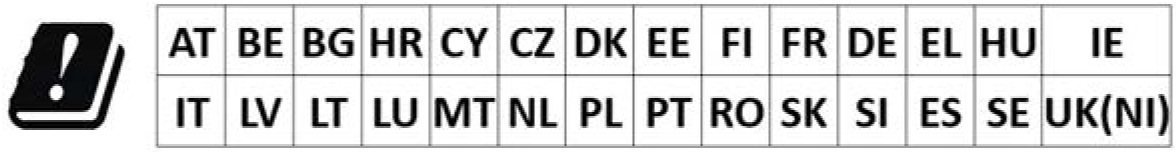
The construction of the appliance is in accordance with the following standards:

EN 300 328 V2.2.2
EN 301 893 V2.1.1
EN 301 908-1 V13.1.1
EN 301 489-1 V2.2.3
EN 301 489-19 V2.1.1
EN 301 489-17 V3.1.1
Draft EN 301 489-52 V1.1.0
EN 55032 : 2015 / AC : 2016
EN 61000-3-2: 2014
EN 61000-3-3: 2013
EN 55035 : 2017
EN 62311 : 2008
EN 62368-1:2014+A11:2017 (Second Edition)
EN 303 413 V1.1.1

Yours sincerely,

PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



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

2.4GHz (2412 - 2472 MHz) : 18.68 dBm
5GHz (5150 - 5250 MHz) : 18.19 dBm

WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

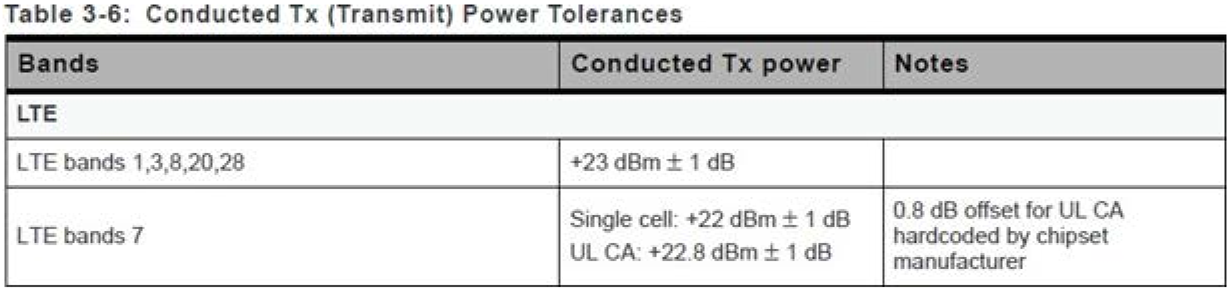


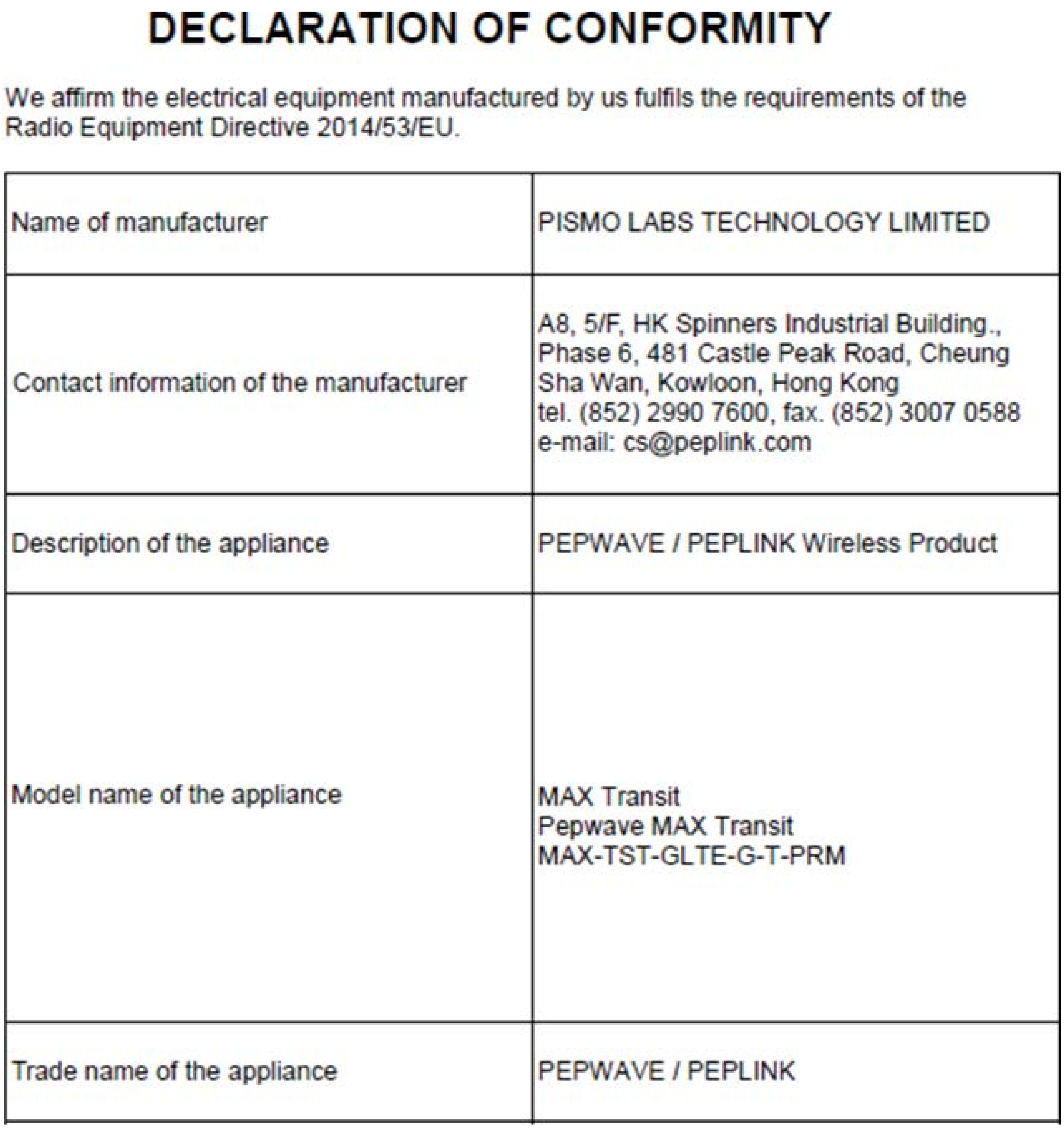
Table 3-6: Conducted Tx (Transmit) Power Tolerances

Bands	Conducted Tx power	Notes
LTE		
LTE bands 1,3,8,20,28	+23 dBm ± 1 dB	
LTE bands 7	Single cell: +22 dBm ± 1 dB UL CA: +22.8 dBm ± 1 dB	0.8 dB offset for UL CA hardcoded by chipset manufacturer

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/

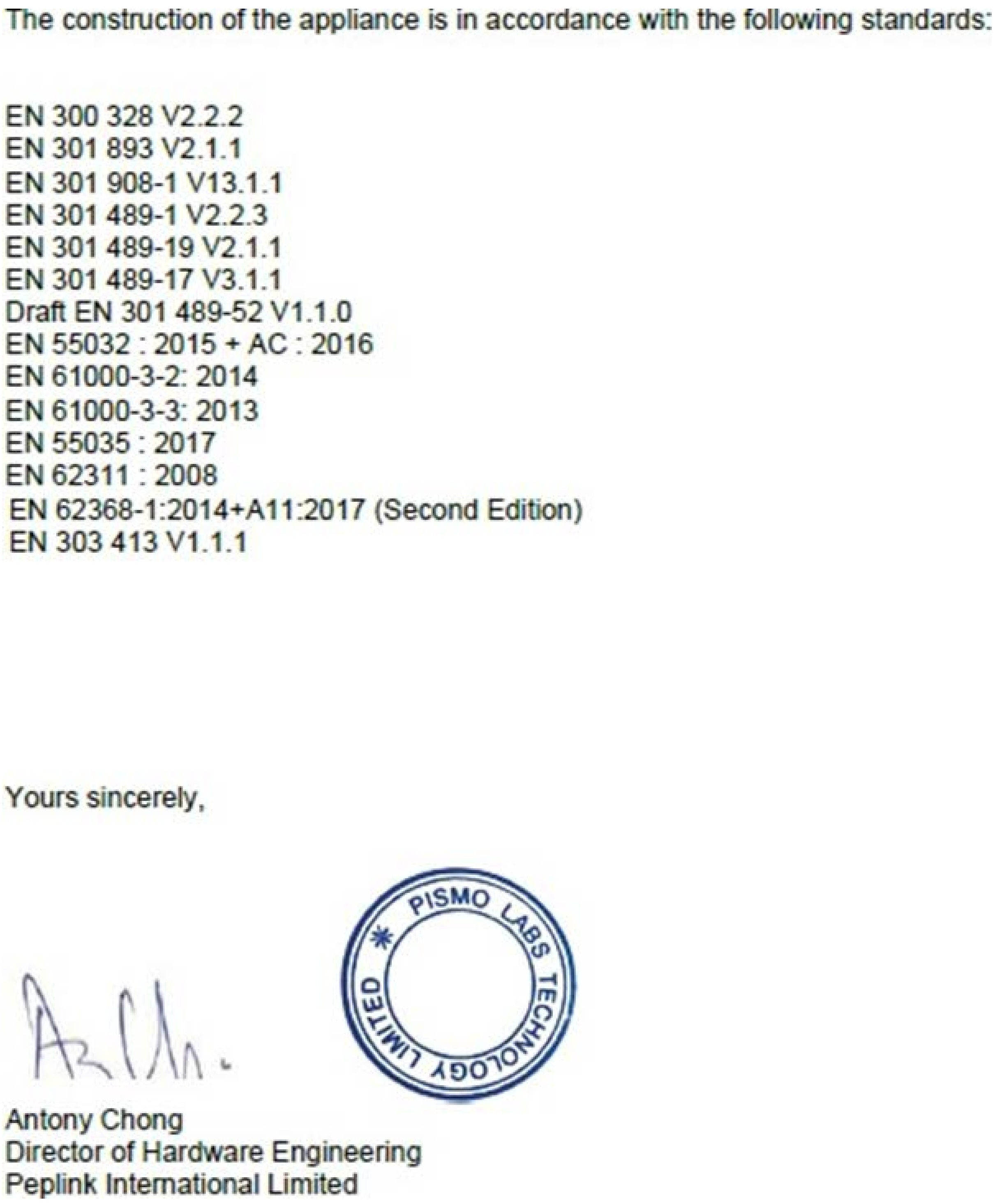
CE Statement for Pepwave Routers (MAX Transit For LM960A18)



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 Transit Pepwave MAX Transit MAX-TST-GLTE-G-T-PRM
Trade name of the appliance	PEPWAVE / PEPLINK



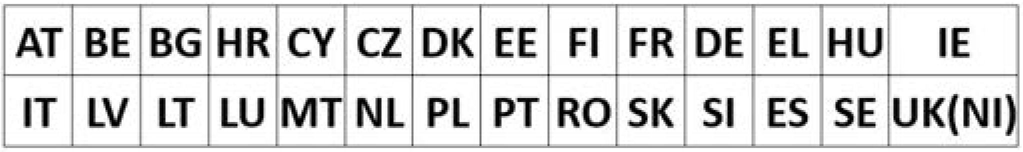
The construction of the appliance is in accordance with the following standards:

EN 300 328 V2.2.2
EN 301 893 V2.1.1
EN 301 908-1 V13.1.1
EN 301 489-1 V2.2.3
EN 301 489-19 V2.1.1
EN 301 489-17 V3.1.1
Draft EN 301 489-52 V1.1.0
EN 55032 : 2015 + AC : 2016
EN 61000-3-2: 2014
EN 61000-3-3: 2013
EN 55035 : 2017
EN 62311 : 2008
EN 62368-1:2014+A11:2017 (Second Edition)
EN 303 413 V1.1.1

Yours sincerely,

PISMO LABS TECHNOLOGY LIMITED

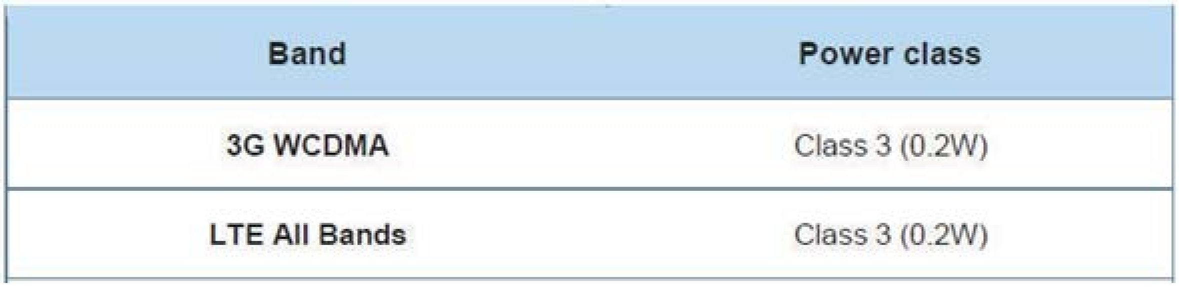
Antony Chong
Director of Hardware Engineering
Peplink International Limited



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

2.4GHz (2412 - 2472 MHz) : 18.68 dBm
5GHz (5150 - 5250 MHz) : 18.19 dBm

WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)



Band	Power class
3G WCDMA	Class 3 (0.2W)
LTE All Bands	Class 3 (0.2W)

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 Transit Mini

Federal Communication Commission Interference Statement

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 it is not installed and used in accordance with the instruction manual, it 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.

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Radiation Exposure Statement

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

Industry Canada Statement (MAX Transit Mini)

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Ce produit répond aux spécifications techniques applicables à l'innovation, Science et Développement économique Canada.

Radiation Exposure Statement

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

Cet équipement est conforme avec l'exposition aux radiations ISED définies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à une distance minimum de 20 cm entre le radiateur et votre corps.

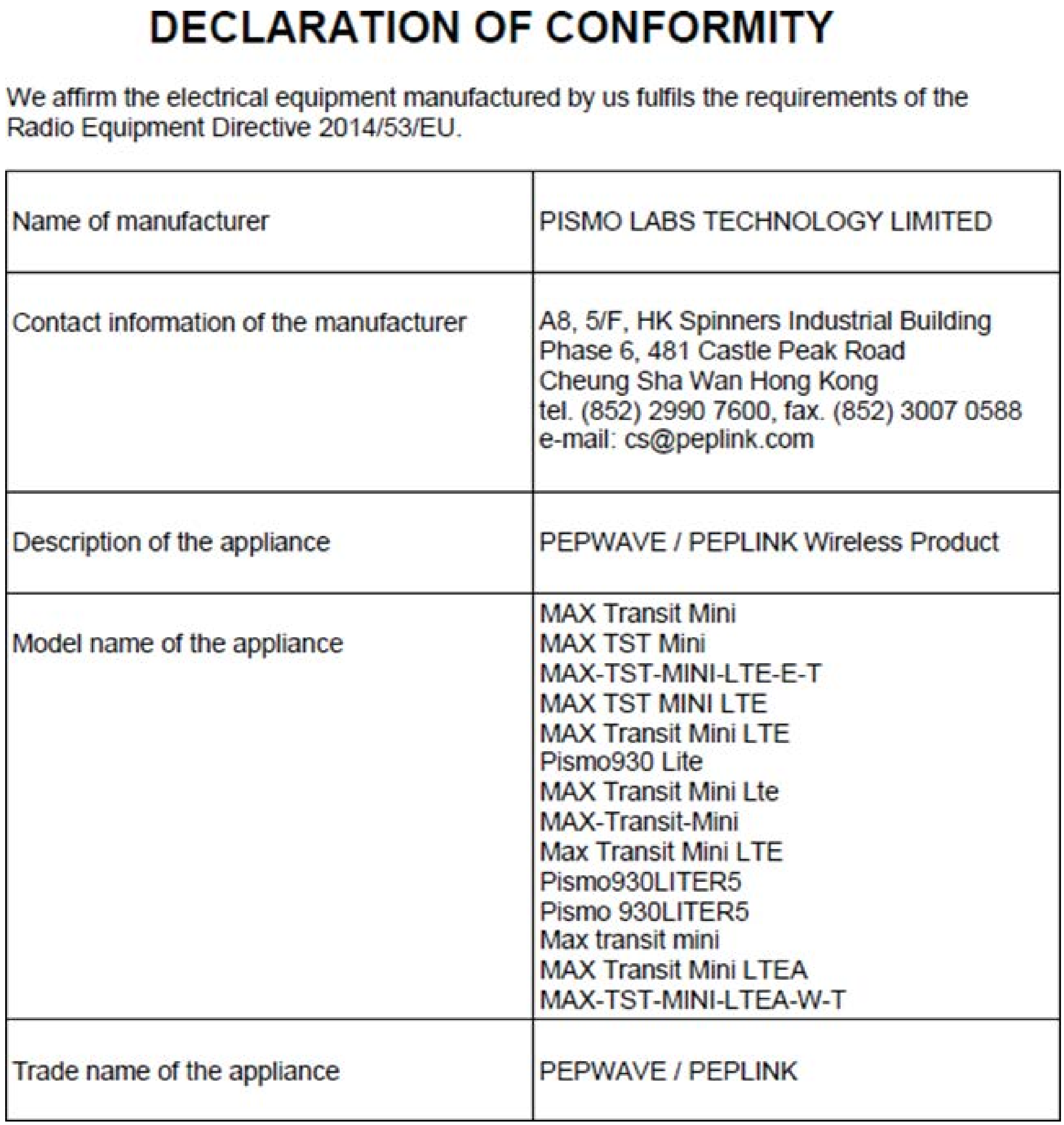
This radio transmitter has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Antenna types Replacement Antenna
Antenna gain (in dBi) 5.33 dBi

Innovation, Sciences et Developpement economique Canada a approuve l'utilisation de ce transmetteur radio avec les types d'antenne enumeres ci-dessous, le gain maximal admissible etant indique. Les types d'antennes non inclus dans cette liste qui ont un gain superieur au gain maximal indique pour tout type liste 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 Transit 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 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 Transit Mini MAX TST Mini MAX-TST-MINI-LTE-E-T MAX TST MINI LTE MAX Transit Mini LTE Pismo930 Lite MAX Transit Mini Lte MAX-Transit-Mini Max Transit Mini LTE Pismo930LITER5 Pismo 930LITER5 Max transit mini MAX Transit Mini LTEA MAX-TST-MINI-LTEA-W-T
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 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 62311 : 2008
EN 62368-1:2014/A11:2017
EN 301 489-19 V2.1.1

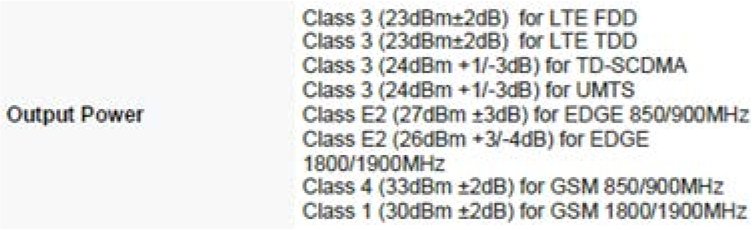
Yours sincerely,

PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited

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

2.4GHz (2412 - 2472 MHz) : 19.78 dBm
WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)



Output Power	Class 3 (23dBm±2dB) for LTE FDD Class 3 (23dBm±2dB) for LTE TDD Class 3 (24dBm +1/-3dB) for TD-SCDMA Class 3 (24dBm +1/-3dB) for UMTS Class E2 (27dBm ±3dB) for EDGE 850/900MHz Class E2 (26dBm +3/-4dB) for EDGE 1800/1900MHz Class 4 (33dBm ±2dB) for GSM 850/900MHz Class 1 (30dBm ±2dB) for GSM 1800/1900MHz

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 20 cm 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 PRO, MAX BR2 PRO, UBR LTE

Federal Communication Commission Interference Statement

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 it is not installed and used in accordance with the instruction manual, it 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.

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 23 centimeters between the radiator and your body.

Industry Canada Statement (MAX BR1 PRO, MAX BR2 PRO, UBR LTE)

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Le présent produit est conforme aux spécifications techniques applicables d'Innovation, Sciences et Développement économique Canada.

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada’s licence-exempt RSS(s). Operation is subject to the following two conditions:

(1) This device may not cause interference.

(2) This device must accept any interference, including interference that may cause undesired opera- tion of the device.

Le present appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio ex- empts de licence. L'exploitation est autorisee aux deux conditions suivantes:

(1) l’appareil ne doit pas produire de brouillage, et

(2) l’utilisateur de l’appareil doit accepter tout brouillage radioelectrique subi, meme si le brouillage est susceptible d’en

For licence exempt equipment with detachable antennas, the user manual shall also contain the following notice in a conspicuous location:

This radio transmitter 20682-P1941 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 I 2.44 dBi , 5GHz I 4.73 dBi
LTE Antenna type: Replacement Antenna (04-410055-00)
LTE Antenna gain: 4 dBi
LTE Antenna type: Replacement Antenna (04-410093-01)
LTE Antenna gain: 4.38 dBi

(i) The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potent for harmful interference to co-channel mobile satellite systems;

(ii) For devices with detachable antenna(s), 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 as appropriate; (detachable antenna only) ; and
The high-power radars are allocated as primary users (i.e. priority users) of the band 5725-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

(iii) where applicable, antenna type(s), antenna models(s), and worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in section 6.2.2.3 shall be clearly indicated.

(i) Le dispositif fonctionnant dans la bande 5150-5250 MHz est reserve uniquement pour utilisation a l'interieur afin de reduire les risques de brouillage prejudiciable aux systemes de satellites mobiles utilisant les memes canaux;

(ii) Le gain maximal d’antenne permis pour les dispositifs avec antenne(s) amovible(s) utilisant la bande 5725-5850 MHz doit se conformer à la limitation P.I.R.E spécifiée pour l’exploitation point à point et non point à point, selon le cas. (antenne détachable uniquement)

En outre, les utilisateurs devraient aussi etre avises que les utilisateurs de radars de haute puissance sont designes utilisateurs principaux (c.-a-d., qu'ils ont la priorite) pour les bande 5725-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

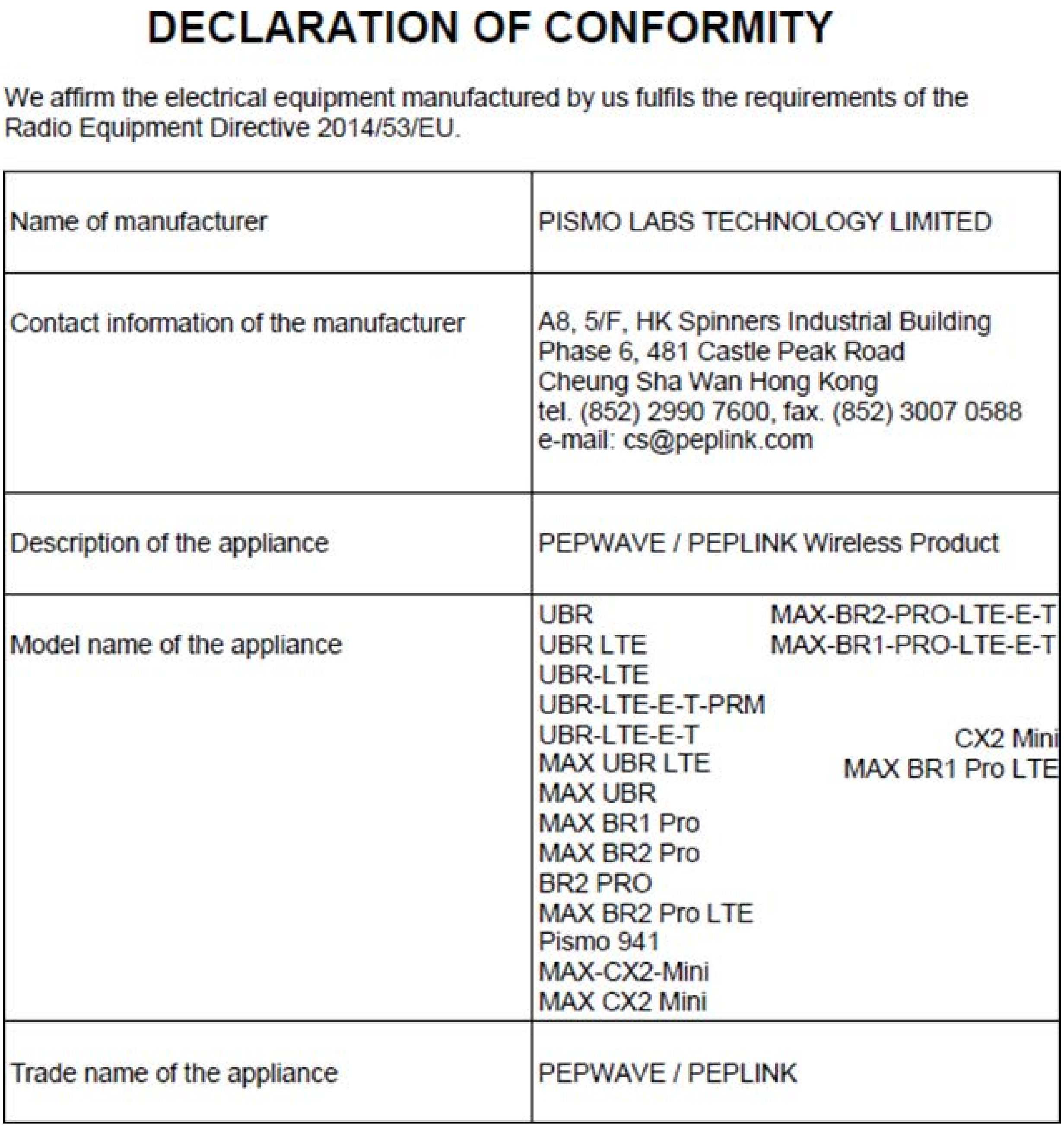
(iii) En outre, les utilisateurs devraient aussi etre avises que les utilisateurs de radars de haute puissance sont designes utilisateurs principaux (c.-a-d., qu'ils ont la priorite) pour les bande 5725-5850 MHz et

Radiation Exposure Statement

This device complies with the ISED radiation exposure limit set forth for an uncontrolled environment. This device should be installed and operated with minimum distance 23 cm between the radiator & your body.

Cet equipement est conforme avec l'exposition aux radiations ISED definies pour un environnement non controle. Cet equipement doit etre installe et utilise a une distance minimum de 23 cm entre le radiateur et votre corps.

CE Statement for Pepwave Routers (MAX BR1 PRO / MAX BR2 PRO / UBR LTE)



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	UBR UBR LTE UBR-LTE UBR-LTE-E-T-PRM UBR-LTE-E-T MAX UBR LTE MAX UBR MAX BR1 Pro MAX BR2 Pro BR2 PRO MAX BR2 Pro LTE Pismo 941 MAX-CX2-Mini MAX CX2 Mini MAX-BR2-PRO-LTE-E-T MAX-BR1-PRO-LTE-E-T CX2 Mini MAX BR1 Pro LTE
Trade name of the appliance	PEPWAVE / PEPLINK

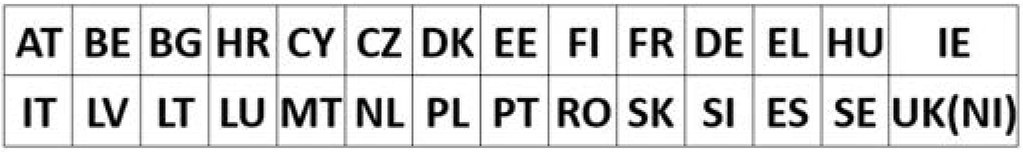
The construction of the appliance is in accordance with the following standards:

EN 300 328 V2.1.1
EN 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
EN 301 489-19 V2.1.1
EN 301 489-17 V3.1.1
Draft EN 301 489-52 V1.1.0
EN 55032: 2015 + AC:2016
EN 61000-3-3: 2013
EN 61000-3-2: 2014
EN 55035 : 2017
EN 62311 : 2008
EN 62368-1:2014/A11:2017

Yours sincerely,

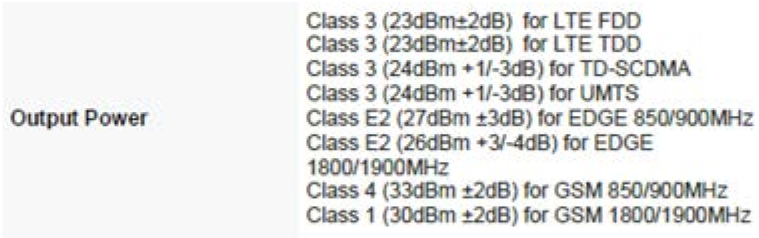
PISMO LABS TECHNOLOGY LIMITED

Antony Chong
Director of Hardware Engineering
Peplink International Limited



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

2.4GHz (2412 - 2472 MHz) : 19.94 dBm
5GHz (5150 - 5250 MHz) : 20.34 dBm
WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)



Output Power	Class 3 (23dBm±2dB) for LTE FDD Class 3 (23dBm±2dB) for LTE TDD Class 3 (24dBm +1/-3dB) for TD-SCDMA Class 3 (24dBm +1/-3dB) for UMTS Class E2 (27dBm ±3dB) for EDGE 850/900MHz Class E2 (26dBm +3/-4dB) for EDGE 1800/1900MHz Class 4 (33dBm ±2dB) for GSM 850/900MHz Class 1 (30dBm ±2dB) for GSM 1800/1900MHz

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 IP55, MAX BR2 IP55

Federal Communication Commission Interference Statement

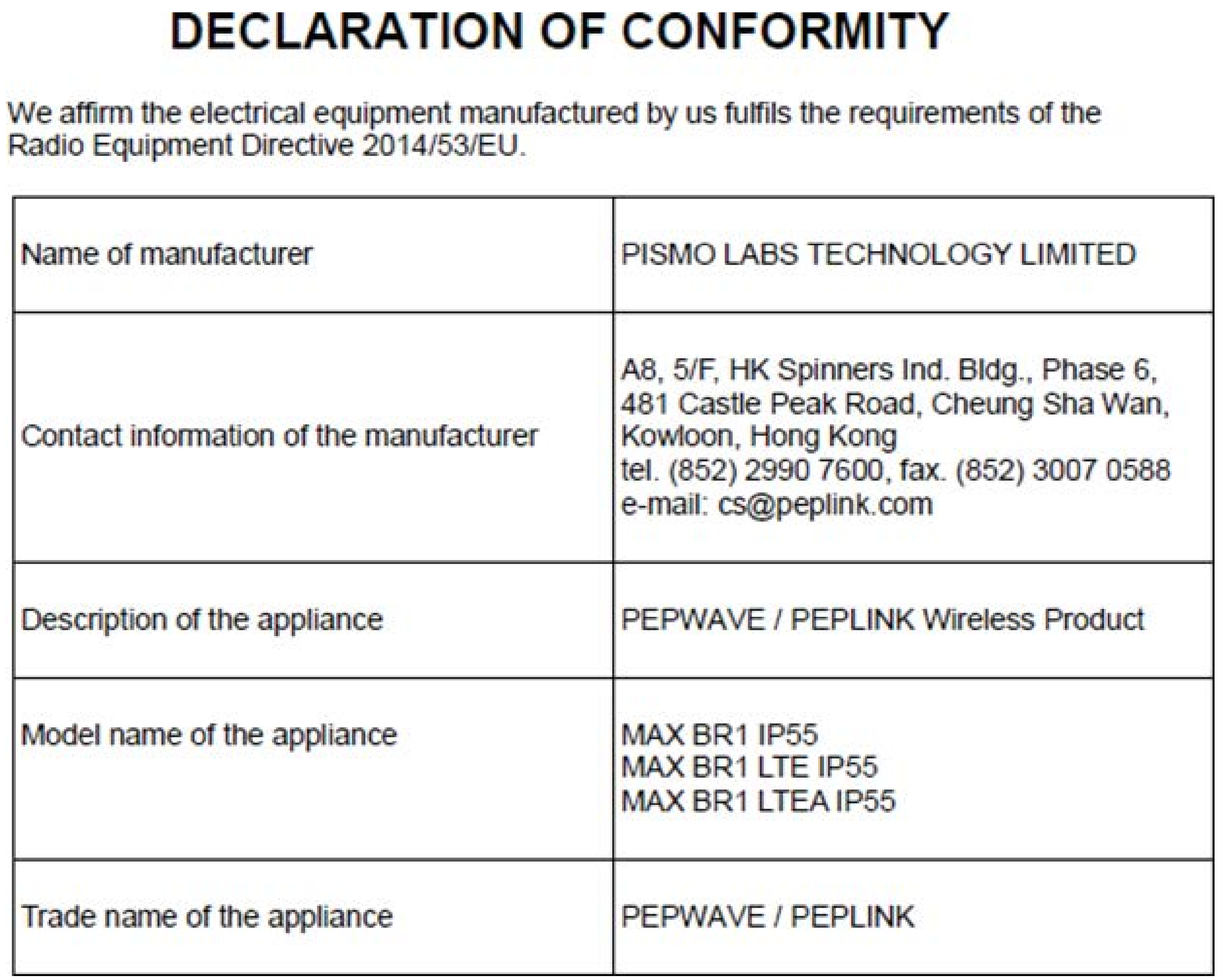
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if it is not installed and used in accordance with the instruction manual, it 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.

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Radiation Exposure Statement

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

CE Statement for Pepwave Routers (MAX BR1 IP55)



DECLARATION OF CONFORMITY

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

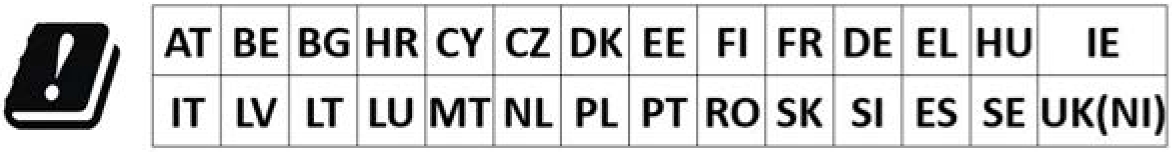
Name of manufacturer	PISMO LABS TECHNOLOGY LIMITED
Contact information of the manufacturer	A8, 5/F, HK Spinners Ind. Bldg., Phase 6, 481 Castle Peak Road, Cheung Sha Wan, Kowloon, Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	PEPWAVE / PEPLINK Wireless Product
Model name of the appliance	MAX BR1 IP55 MAX BR1 LTE IP55 MAX BR1 LTEA IP55
Trade name of the appliance	PEPWAVE / PEPLINK

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

EN 55032:2015
EN 55024:2010+A1:2015
EN 61000-3-2: 2014
EN 61000-3-3: 2013
Draft EN 301 489-1 V2.2.0
Draft EN 301 489-17 V3.2.0
Draft EN 301 489-52 V1.1.0
EN 300 328 V2.1.1
EN 301 893 V2.1.1
EN 301 908-1 V11.1.1
EN 300 440 V2.1.1
EN 62311: 2008
EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013

Yours sincerely,

Keith Chau
General Manager
Peplink International Limited



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

2.4GHz (2412 - 2472 MHz) : 18.16 dBm
5GHz (5150 - 5250 MHz) : 20.32 dBm
5GHz (5725 - 5850 MHz) : 13.00 dBm
WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

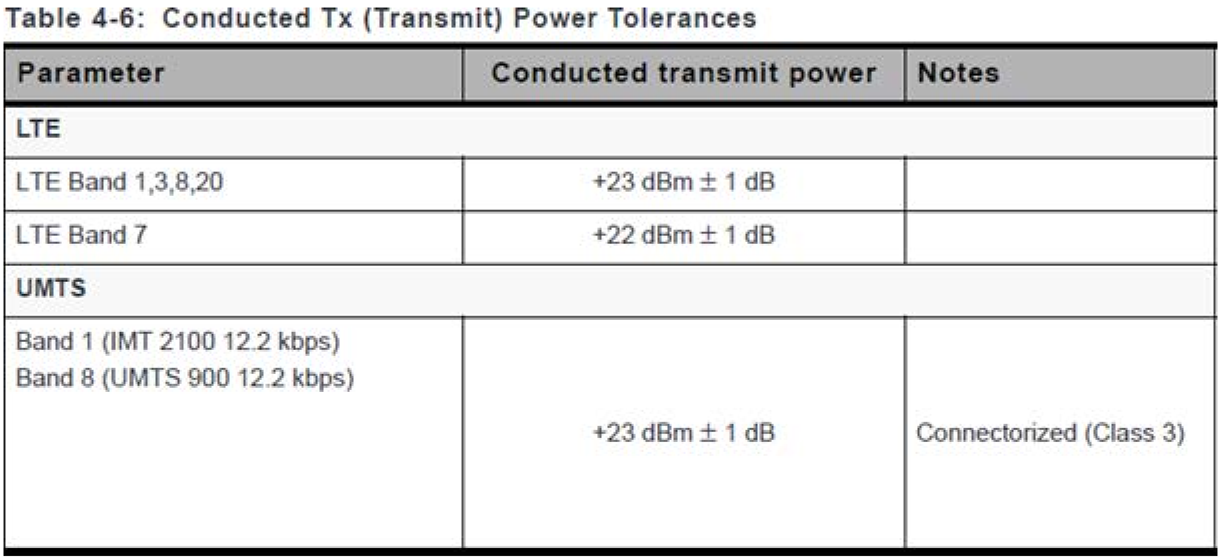


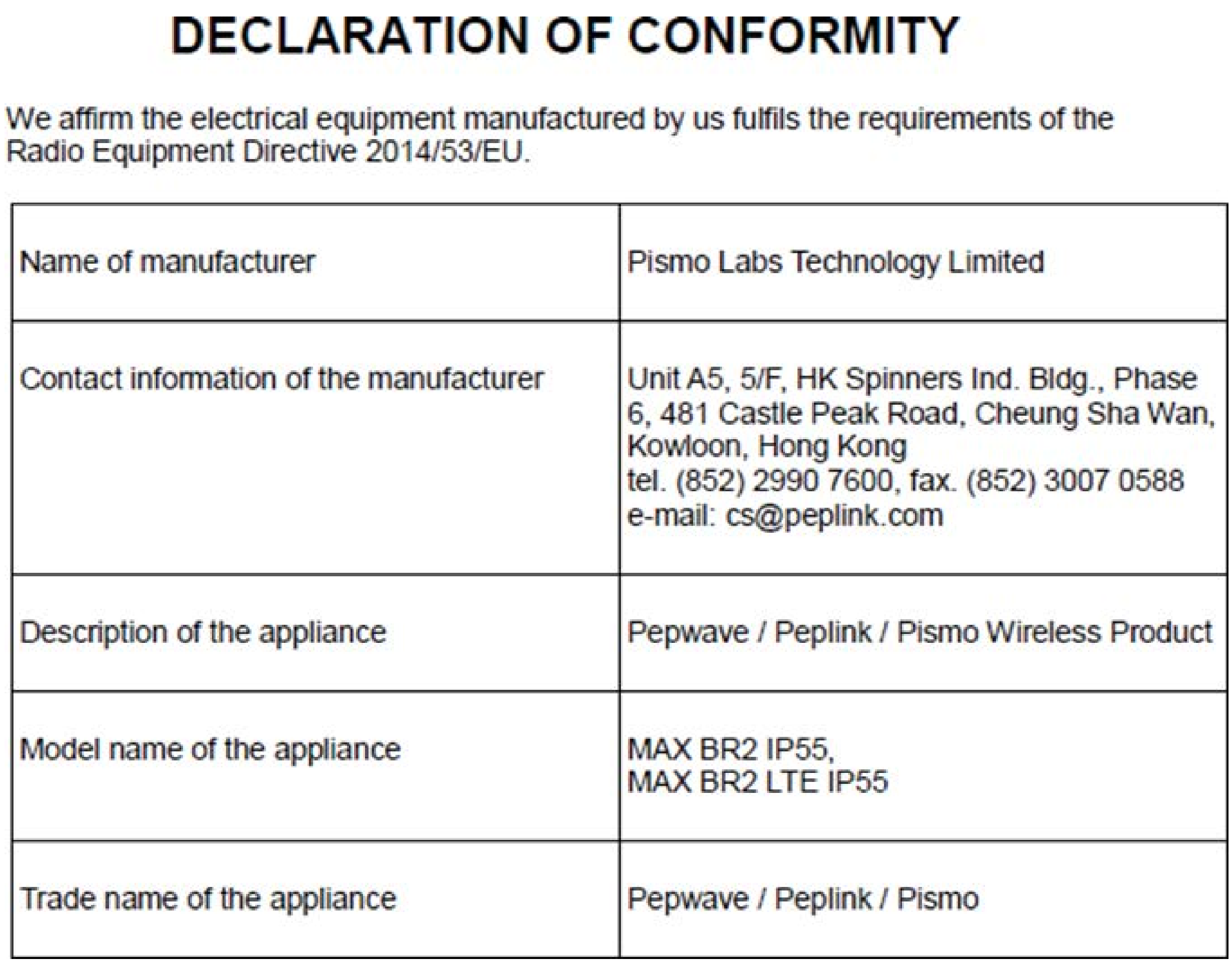
Table 4-6: Conducted Tx (Transmit) Power Tolerances

Parameter	Conducted transmit power	Notes
LTE		
LTE Band 1,3,8,20	+23 dBm ± 1 dB	
LTE Band 7	+22 dBm ± 1 dB	
UMTS		
Band 1 (IMT 2100 12.2 kbps) Band 8 (UMTS 900 12.2 kbps)	+23 dBm ± 1 dB	Connectorized (Class 3)

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 50cm between the radiator & your body.

contact as: https://www.peplink.com/

CE Statement for Pepwave Routers (MAX BR2 IP55)



DECLARATION OF CONFORMITY

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

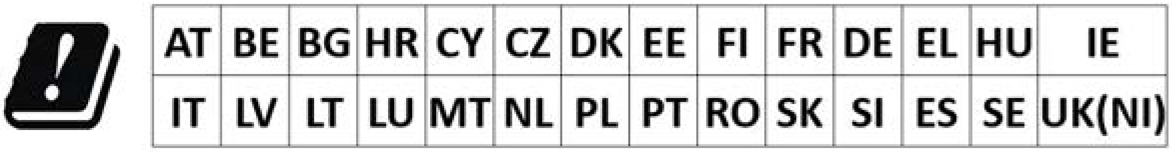
Name of manufacturer	Pismo Labs Technology Limited
Contact information of the manufacturer	Unit A5, 5/F, HK Spinners Ind. Bldg., Phase 6, 481 Castle Peak Road, Cheung Sha Wan, Kowloon, Hong Kong tel. (852) 2990 7600, fax. (852) 3007 0588 e-mail: cs@peplink.com
Description of the appliance	Pepwave / Peplink / Pismo Wireless Product
Model name of the appliance	MAX BR2 IP55, MAX BR2 LTE IP55
Trade name of the appliance	Pepwave / Peplink / Pismo

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

EN 55032:2015
EN 55024:2010+A1:2015
EN 61000-3-2: 2014
EN 61000-3-3: 2013
EN 301 489-1 V2.2.0
EN 301 489-17 V3.2.0
EN 301 489-52 V1.1.0
EN 300 328 V2.1.1
EN 301 893 V2.1.1
EN 301 908-1 V11.1.1
EN 300 440 V2.1.1
EN 62311: 2008
EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013

Yours sincerely,

Keith Chau
General Manager
Peplink International Limited



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

2.4GHz (2412 - 2472 MHz) : 18.99 dBm
5GHz (5150 - 5250 MHz) : 22.95 dBm
5GHz (5725 - 5850 MHz) : 12.80 dBm

WWAN : Refer 3GPP TS 36.521 -1 (UE Power class)

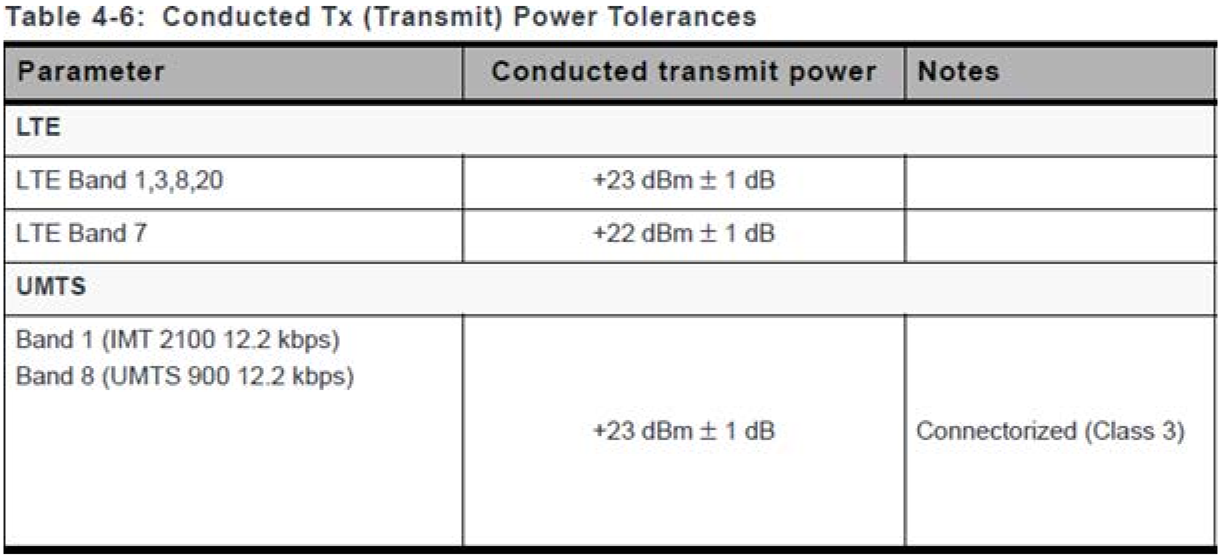


Table 4-6: Conducted Tx (Transmit) Power Tolerances

Parameter	Conducted transmit power	Notes
LTE		
LTE Band 1,3,8,20	+23 dBm ± 1 dB	
LTE Band 7	+22 dBm ± 1 dB	
UMTS		
Band 1 (IMT 2100 12.2 kbps) Band 8 (UMTS 900 12.2 kbps)	+23 dBm ± 1 dB	Connectorized (Class 3)

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 50cm 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 Transit Pro E / MAX Transit LTEA

FCC 15.21:

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

FCC 15.105

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, it 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.

RF exposure warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

ICES Statement

This product meets the applicable Innovation, Science and Economic Development Canada technical specifications.

Le présent produit est conforme aux spécifications techniques applicables d'Innovation, Sciences et Développement économique Canada.

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the following two conditions:

1. This device may not cause interference.

2. This device must accept any interference, including interference that may cause undesired operation of the device.

Le present appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence.

L'exploitation est autorisee aux deux conditions suivantes:

1. l'appareil ne doit pas produire de brouillage, et

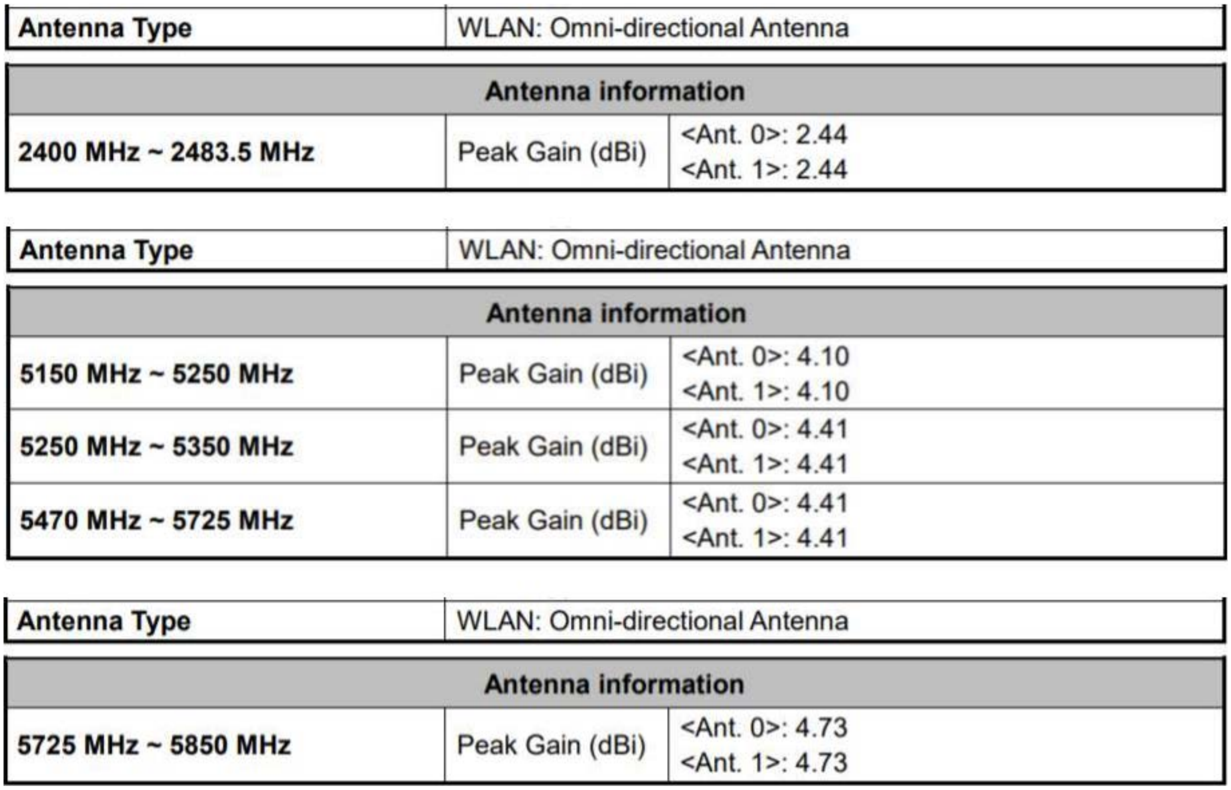
2. l'utilisateur de l'appareil doit accepter tout brouillage radioelectrique subi, meme si le brouillage est susceptible d'en

RF exposure warning

This device complies with the ISED radiation exposure limit set forth for an uncontrolled environment. This device 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.

Cet équipement est conforme avec l'exposition aux radiations ISED définies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à une distance minimum de 20 cm entre le radiateur et votre corps. Cet émetteur ne doit pas être colocalisées ou opérant en conjonction avec une autre antenne ou transmetteur.

This radio transmitter IC: 20682-P1835 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 Type	WLAN: Omni-directional Antenna

Antenna information		
2400 MHz ~ 2483.5 MHz	Peak Gain (dBi)	<Ant. 0>: 2.44 <Ant. 1>: 2.44

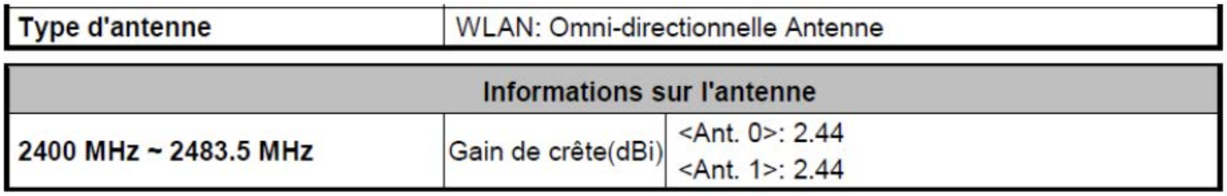
Antenna Type	WLAN: Omni-directional Antenna

Antenna information		
5150 MHz ~ 5250 MHz	Peak Gain (dBi)	<Ant. 0>: 4.10 <Ant. 1>: 4.10
5250 MHz ~ 5350 MHz	Peak Gain (dBi)	<Ant. 0>: 4.41 <Ant. 1>: 4.41
5470 MHz ~ 5725 MHz	Peak Gain (dBi)	<Ant. 0>: 4.41 <Ant. 1>: 4.41

Antenna Type	WLAN: Omni-directional Antenna

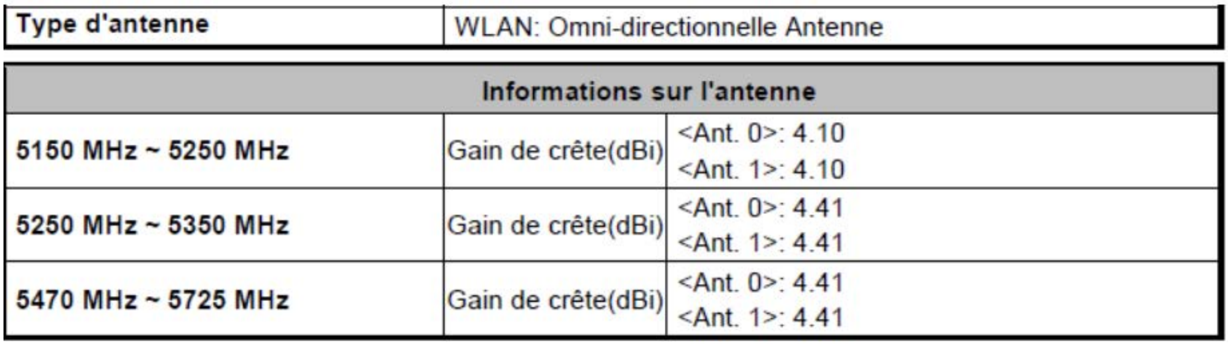
Antenna information		
5725 MHz ~ 5850 MHz	Peak Gain (dBi)	<Ant. 0>: 4.73 <Ant. 1>: 4.73

Cet émetteur radio IC : 20682-P1835 a été approuvé par Innovation, Sciences et Développement économique Canada doit fonctionner avec les types d'antennes énumérés ci-dessous, avec le gain maximal admissible indiqué. Les types d'antenne non inclus dans cette liste qui ont un gain supérieur au gain maximum indiqué pour tout type répertorié sont strictement interdits pour une utilisation avec cet appareil.



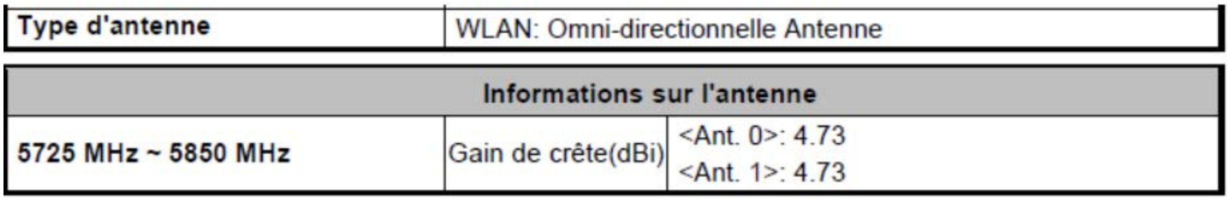
Type d'antenne	WLAN: Omni-directionnelle Antenne

Informations sur l'antenne		
2400 MHz ~ 2483.5 MHz	Gain de crête(dBi)	<Ant. 0>: 2.44 <Ant. 1>: 2.44



Type d'antenne	WLAN: Omni-directionnelle Antenne

Informations sur l'antenne		
5150 MHz ~ 5250 MHz	Gain de crête(dBi)	<Ant. 0>: 4.10 <Ant. 1>: 4.10
5250 MHz ~ 5350 MHz	Gain de crête(dBi)	<Ant. 0>: 4.41 <Ant. 1>: 4.41
5470 MHz ~ 5725 MHz	Gain de crête(dBi)	<Ant. 0>: 4.41 <Ant. 1>: 4.41



Type d'antenne	WLAN: Omni-directionnelle Antenne

Informations sur l'antenne		
5725 MHz ~ 5850 MHz	Gain de crête(dBi)	<Ant. 0>: 4.73 <Ant. 1>: 4.73

USB WAN Modem Port Specification

MAX Series

	MAX 700	MAX HD2 / MAX HD2 Media Fast	MAX HD2 Mini	MAX HD2 / HD4 MBX	MAX BR1 ENT MAX BR1NT	MAX HD4 / MAX HD4 Media Fast / MediaFast 200
Output Rating	**5V DC, 2A**	**5V DC, 2A**	**5V DC, 2A**	**5V DC, 0.5A**	**5V DC, 2A**	**5V DC, 2A**