MAX Series

User Manual

Pepwave Products:

MAX 700 / HD2 / HD2 IP67 / HD2 Mini / HD2 MBX / HD Dome / HD Dome Pro / HD4 / HD4 MBX / MBX Mini / HD4 IP67 / Transit / Transit Duo / Transit 5G / Transit Core / Transit Mini / Transit Pro E / Transit Pro / BR1 Classic / BR1 MK2 / BR1 Slim / BR1 ENT / BR1 M2M / / BR1 Mini (HW2) / BR1 Mini (HW3) / BR1 Mini Core / BR1 ESN / BR1 Pro LTE / BR1 Pro (CAT-20) / BR1 Pro 5G / BR2 Pro / BR1 IP55 / BR1 IP67 / BR2 IP55 / On-The-Go / HD2 with MediaFast / HD4 with MediaFast / SpeedFusion Engine / UBR LTE / UBR Plus / PDX

Pepwave Firmware 8.2.1
November 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

 Copyright @ 2021 Peplink

 Copyright @ 2021 Peplink

 Copyright @ 2021 Peplink

 Copyright @ 2021 Peplink

 Copyright @ 2021 Peplink

 Copyright @ 2021 Peplink

Introduction and Scope

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

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

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

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

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

 Copyright @ 2021 Peplink

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

 Copyright @ 2021 Peplink

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

 Copyright @ 2021 Peplink

- 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

 Copyright @ 2021 Peplink

- 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

 Copyright @ 2021 Peplink

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

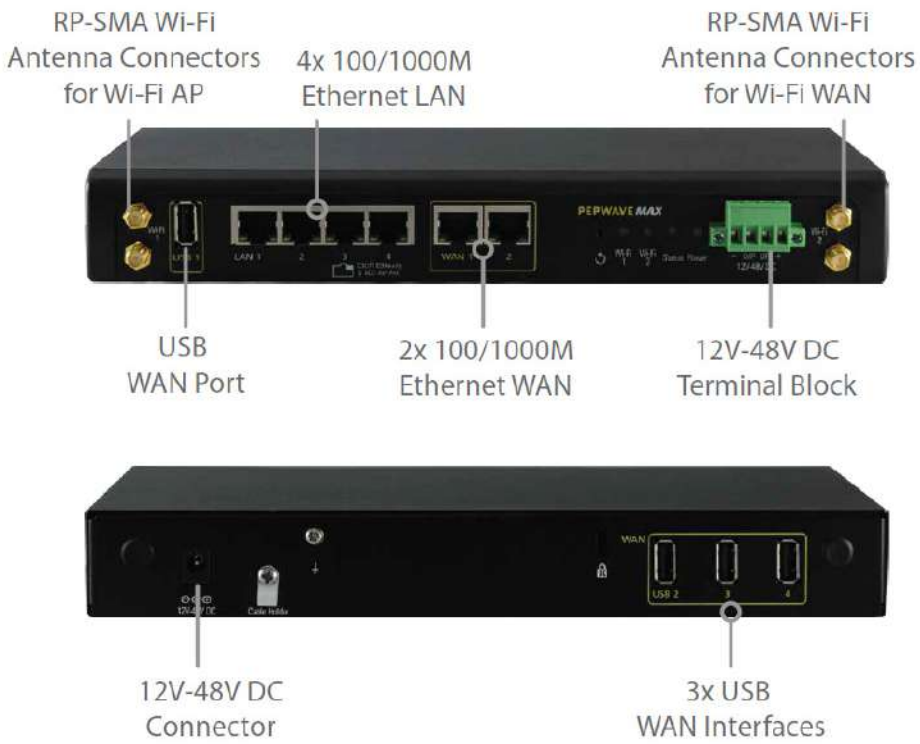
* Not supported on MAX Surf-On-The-Go, and BR1 variants

 Copyright @ 2021 Peplink

2 Pepwave MAX Mobile Router Overview

2.1 MAX 700

2.1.1 Panel Appearance



Note:

- For proper Wi-Fi performance and operations, please ensure all 4 Wi-Fi antenna connectors (labeled Wi-Fi 1 and Wi-Fi 2) have antennas attached.
- The LED indicators of Wi-Fi 1 & 2 shown as below is referring to the default settings of Wi-Fi Operation mode is WAN + AP under the AP.

 Copyright @ 2021 Peplink

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 Indicators		
Wi-Fi 1	OFF	WiFi AP is disabled.
	ON	WiFi AP is enabled.

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

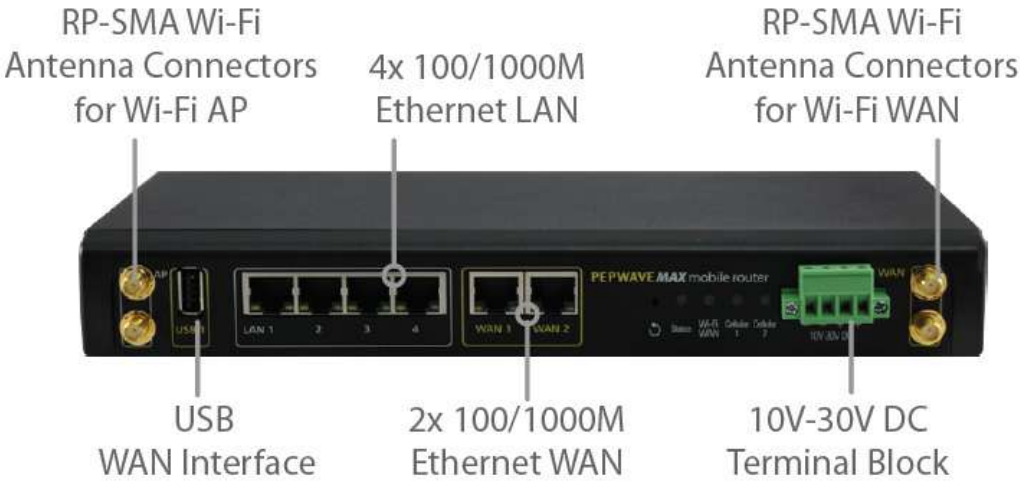
LAN and Ethernet WAN Ports		
Green LED	ON	10 / 100/ 1000 Mbps
Orange LED	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

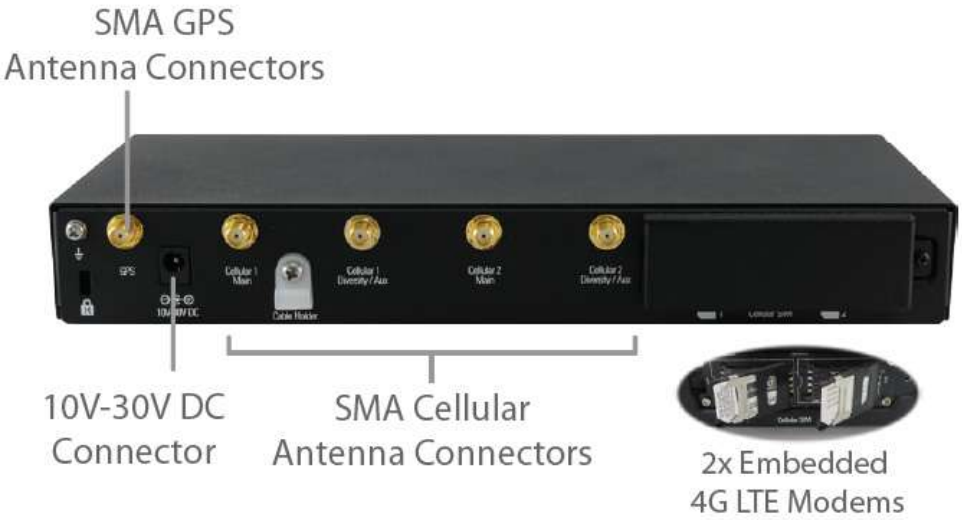
 Copyright @ 2021 Peplink

2.2 MAX HD2

For certification information, please refer to Appendix B: Declaration

2.2.1 Panel Appearance





 Copyright @ 2021 Peplink

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 WAN Indicators		
Wi-Fi WAN	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

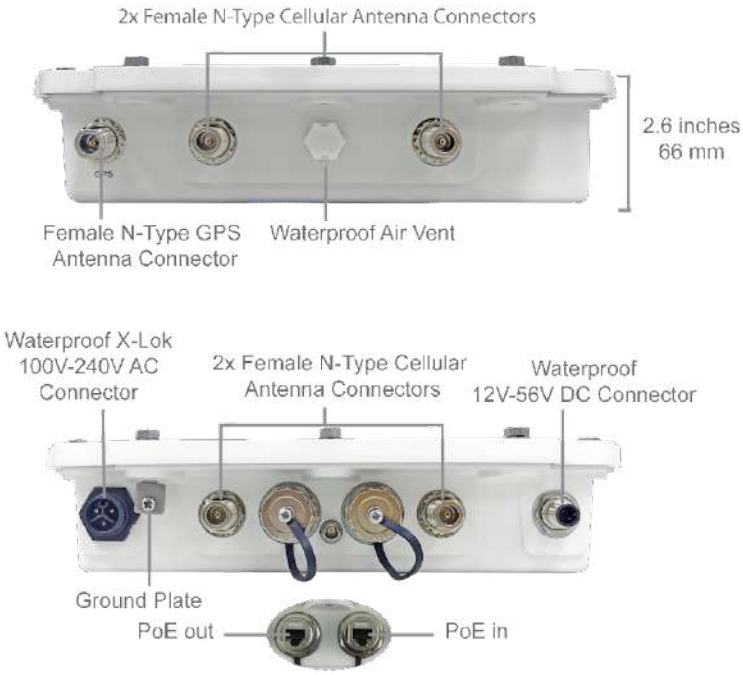
Cellular Indicators		
Cellular 1 / Cellular 2	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

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	

 Copyright @ 2021 Peplink

2.3 MAX HD2 IP67

2.3.1 Panel Appearance



2.3.2 LED Indicators

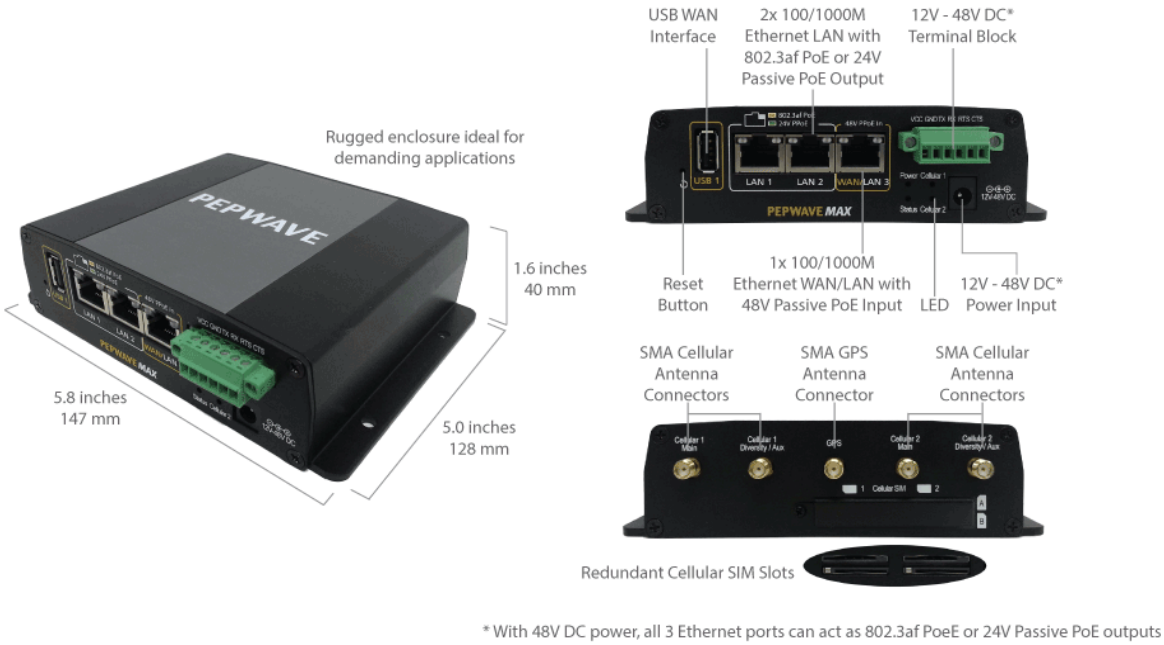
The statuses indicated by the front panel LEDs are as follows:

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

 Copyright @ 2021 Peplink

2.4 MAX HD2 mini

2.4.1 Panel Appearance



* 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)

 Copyright @ 2021 Peplink

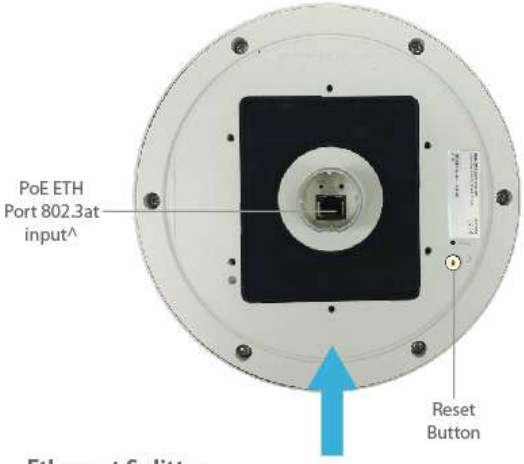
LAN and Ethernet WAN Ports		
Green LED	ON	POE Enabled
	OFF	POE Disabled
Orange LED	Blinking	10 / 100 / 1000 Mbps and Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

2.5 MAX HD Dome

2.5.1 Panel Appearance

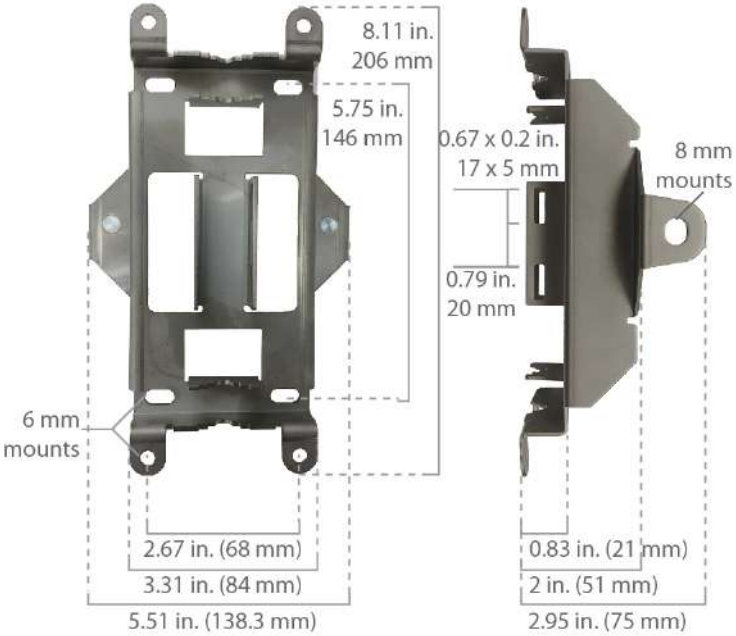
 Copyright @ 2021 Peplink

HD2 Dome



Ethernet Splitter

Mounting Bracket



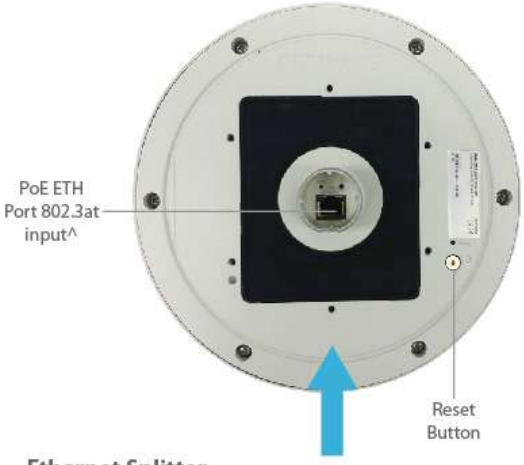
 Copyright @ 2021 Peplink

2.6 MAX HD Dome Pro

2.6.1 Panel Appearance

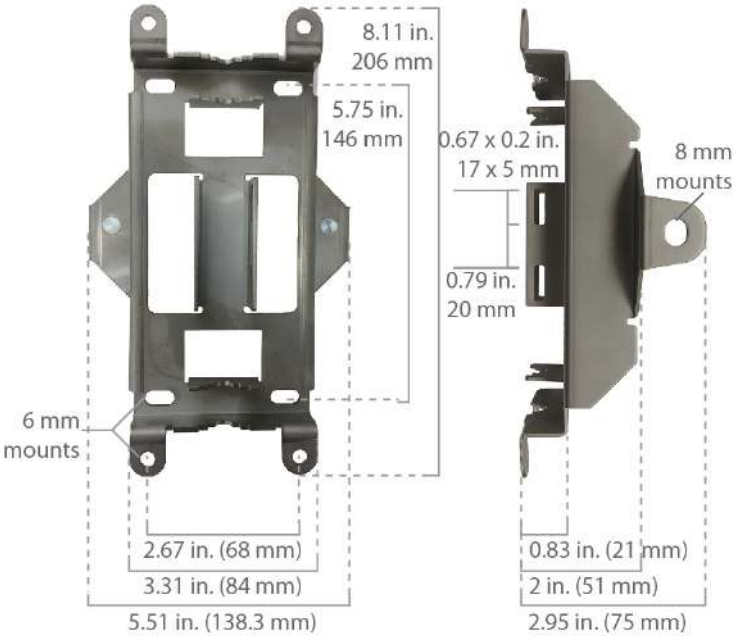
#SIM Injector is available separately
^Ethernet LAN port can be split into two LAN ports
using the included splitter (1x LAN 802.3af PoE out, 1x LAN PoE in)

 Copyright @ 2021 Peplink



Ethernet Splitter

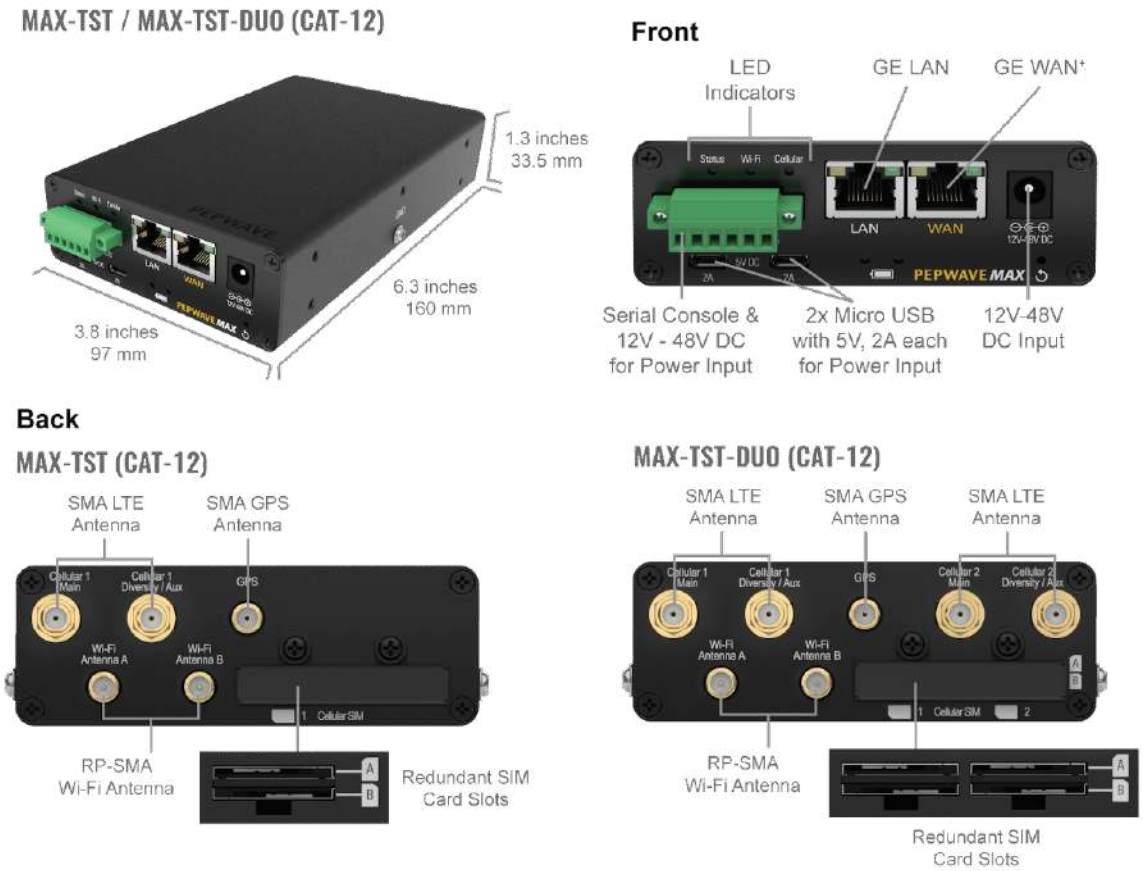
Mounting Bracket



 Copyright @ 2021 Peplink

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

2.7.1 Panel Appearance



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

 Copyright @ 2021 Peplink

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

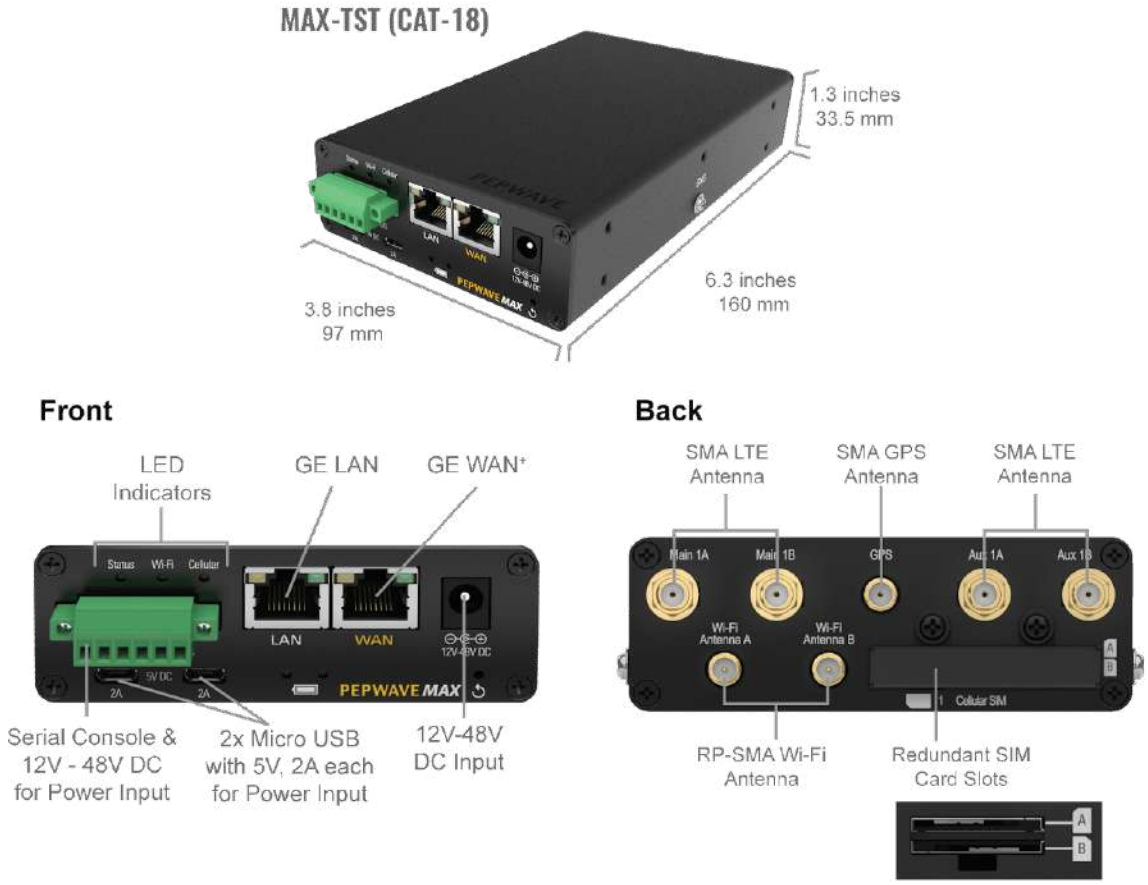
Wi-Fi Indicators		
Wi-Fi	OFF	Wi-Fi AP is turn off
	Blinking	Wi-Fi AP is turn on

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	

 Copyright @ 2021 Peplink

2.8 MAX Transit (CAT-18)

2.8.1 Panel Appearance



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

 Copyright @ 2021 Peplink

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	

 Copyright @ 2021 Peplink

2.9 MAX Transit 5G

2.9.1 Panel Appearance

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

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

 Copyright @ 2021 Peplink

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	

2.10 MAX Transit Mini

2.10.1 Panel Appearance

2.10.2 LED indicators

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

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

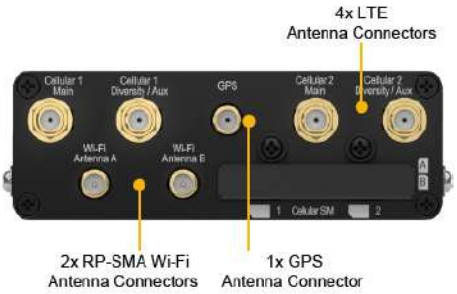
Wi-Fi Indicators		
Wi-Fi	OFF	Disabled intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

 Copyright @ 2021 Peplink

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 Pro E

2.11.1 Panel Appearance



2.11.2 LED indicators

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

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

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

 Copyright @ 2021 Peplink

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)

2.12 MAX Transit Core

2.12.1 Panel Appearance

 Copyright @ 2021 Peplink

2.12.2 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

 Copyright @ 2021 Peplink

2.13 MAX Transit Pro

2.13.1 Panel Appearance

2.13.2 LED indicators

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

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

Cellular Indicators		
Cellular 1 / Cellular 2*	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

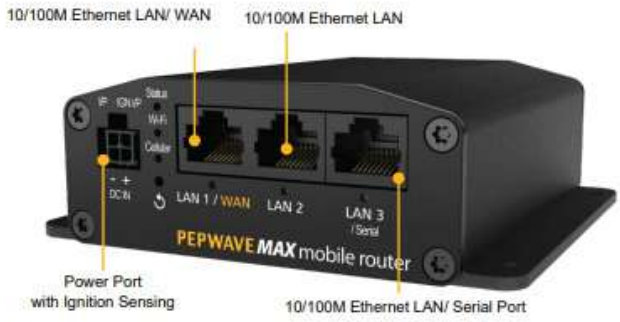
 Copyright @ 2021 Peplink

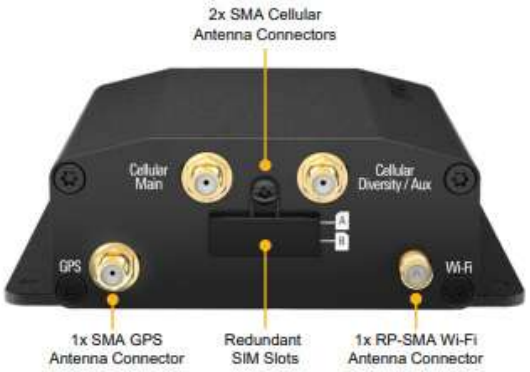
LAN and Ethernet WAN Ports		
Green LED	ON	1000 Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

 Copyright @ 2021 Peplink

2.14 MAX BR1 ESN

2.14.1 Panel Appearance





2.14.2 LED indicators

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

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

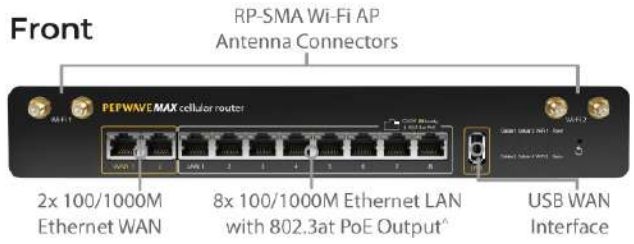
Wi-Fi Indicators		
Wi-Fi	OFF	Disabled intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

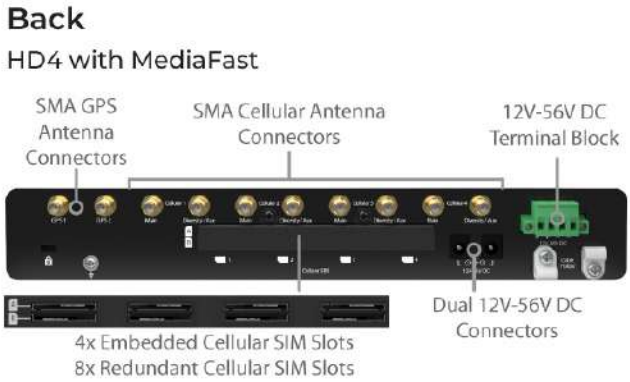
Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

 Copyright @ 2021 Peplink

2.15 MAX HD2 and HD4 with MediaFast

2.15.1 Panel Appearance





Note:

- For proper Wi-Fi performance and operations, please ensure all 4 Wi-Fi antenna connectors (labeled Wi-Fi 1 and Wi-Fi 2) have antennas attached.
- The LED indicators of Wi-Fi 1 & 2 shown as below is referring to the default settings of Wi-Fi Operation mode is WAN + AP under the AP. For more details, please refer to the section 25.4.

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

 Copyright @ 2021 Peplink

Wi-Fi WAN Indicators		
Wi-Fi 1	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

Wi-Fi AP Indicators		
Wi-Fi 2	OFF	WiFi AP is disabled.
	ON	WiFi AP is enabled.

Cellular Indicators		
Cellular 1 / 2 / 3 / 4	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

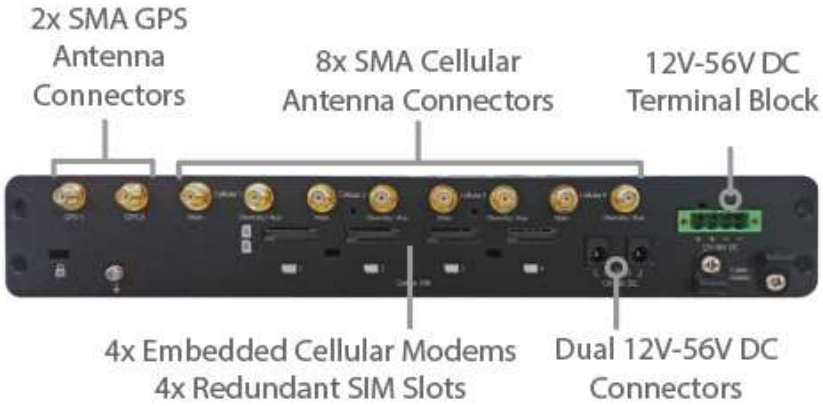
LAN Ports		
Green LED	ON	POE Enabled
	OFF	POE Disabled
Orange LED	Blinking	10 / 100 / 1000 Mbps and Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

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	

Copyright @ 2021 Peplink

2.16 MAX HD4

2.16.1 Panel Appearance



Note:

- For proper Wi-Fi performance and operations, please ensure all 4 Wi-Fi antenna connectors (labeled Wi-Fi 1 and Wi-Fi 2) have antennas attached.
- The LED indicators of Wi-Fi 1 & 2 shown as below is referring to the default settings of Wi-Fi Operation mode is WAN + AP under the AP. For more details, please refer to the section 25.4

 Copyright @ 2021 Peplink

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 WAN Indicators		
Wi-Fi 1	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

Wi-Fi AP Indicators		
Wi-Fi 2	OFF	WiFi AP is disabled.
	ON	WiFi AP is enabled.

Cellular Indicators		
Cellular 1 / 2 / 3 / 4	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

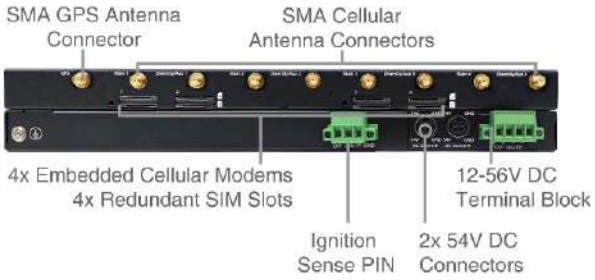
 Copyright @ 2021 Peplink

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

2.17 MAX HD4 MBX (CAT-12)

For certification information, please refer to Appendix B: Declaration

2.17.1 Panel Appearance



*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

Note:

- For proper Wi-Fi performance and operations, please ensure all 4 Wi-Fi antenna connectors (labeled Wi-Fi 1 and Wi-Fi 2) have antennas attached.

 Copyright @ 2021 Peplink

- The LED indicators of Wi-Fi 1 & 2 shown as below is referring to the default settings of Wi-Fi Operation mode is WAN + AP under the AP. For more details, please refer to the section 25.4

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

Wi-Fi AP Indicators		
Wi-Fi 2	OFF	WiFi AP is disabled.
	ON	WiFi AP is enabled.

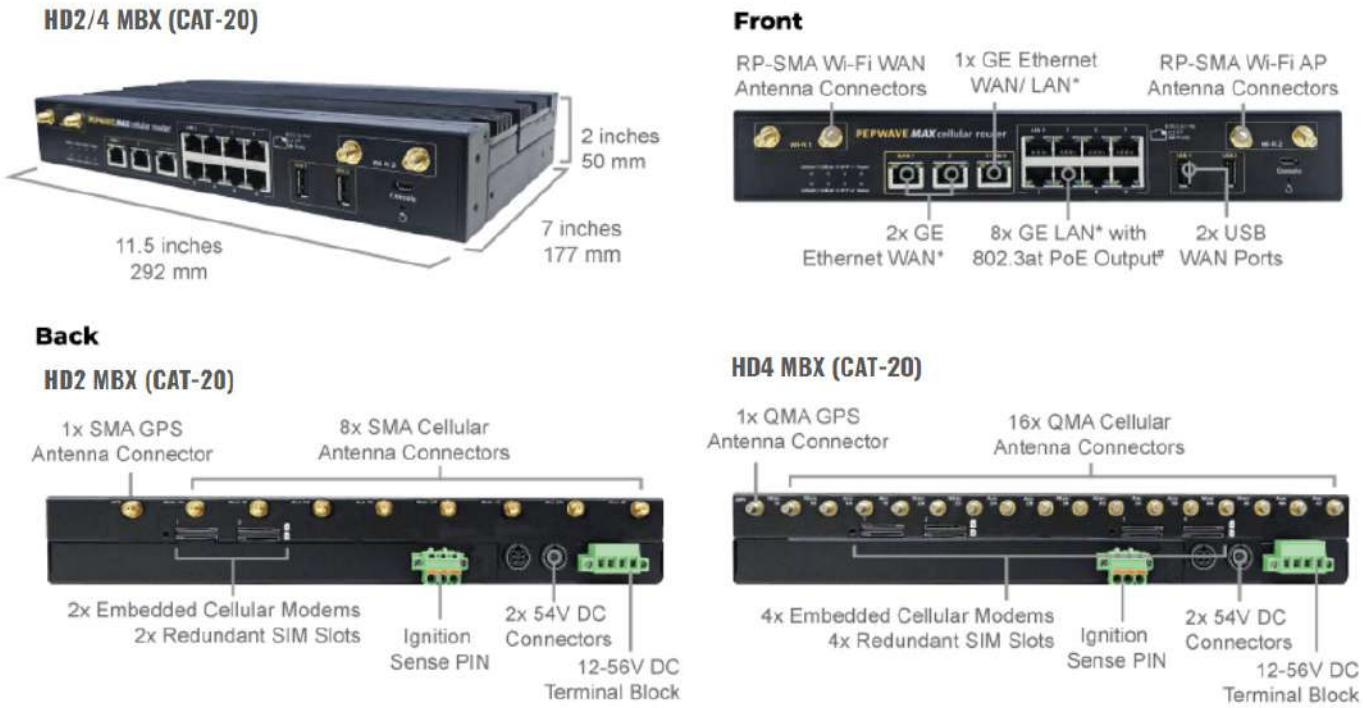
Cellular Indicators		
Cellular 1 / 2 / 3 / 4	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

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	

 Copyright @ 2021 Peplink

2.18 MAX HD2/4 MBX (CAT-20)

2.18.1 Panel Appearance



Note:

- For proper Wi-Fi performance and operations, please ensure all 4 Wi-Fi antenna connectors (labeled Wi-Fi 1 and Wi-Fi 2) have antennas attached.
- The LED indicators of Wi-Fi 1 & 2 shown as below is referring to the default settings of Wi-Fi Operation mode is WAN + AP under the AP. For more details, please refer to the section 25.4

2.18.2 LED Indicators

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

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

 Copyright @ 2021 Peplink

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

Wi-Fi AP Indicators		
Wi-Fi 2	OFF	WiFi AP is disabled.
	ON	WiFi AP is enabled.

Cellular Indicators		
Cellular 1 / 2 / 3 / 4	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

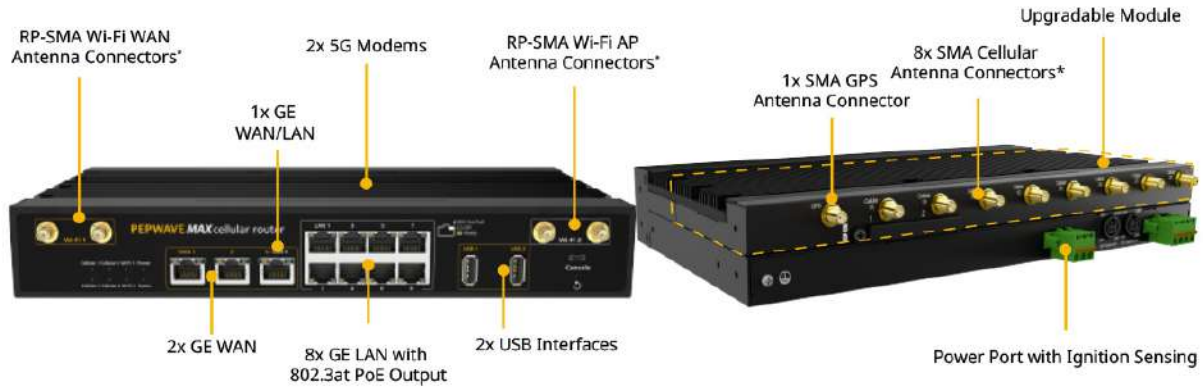
LAN and Ethernet WAN Ports		
Green LED	ON	10 / 100 / 1000 Mbps
Orange LED	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

 Copyright @ 2021 Peplink

2.19 MAX HD2/4 MBX (5G)

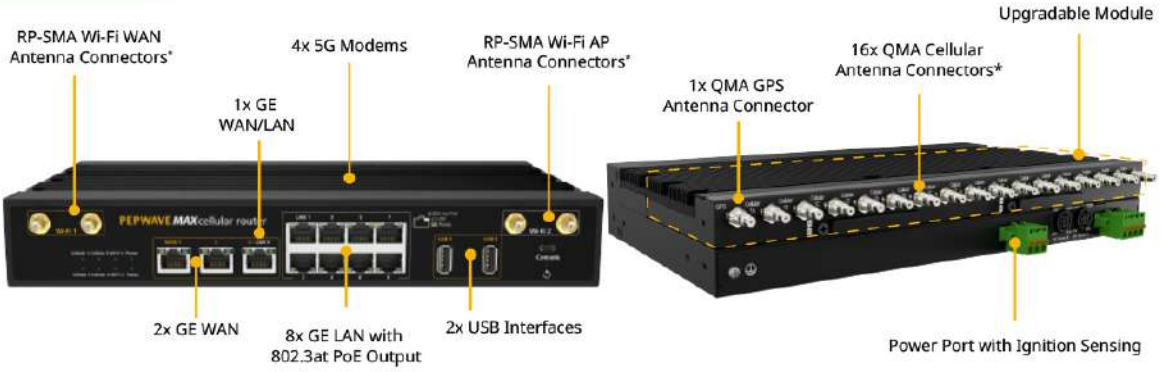
2.19.1 Panel Appearance

HD2 MBX 5G



* For the best performance and reliability, all RF connectors must be connected to the same type and performance antennas.

HD4 MBX 5G



* For the best performance and reliability, all RF connectors must be connected to the same type and performance antennas.

Note:

- For proper Wi-Fi performance and operations, please ensure all 4 Wi-Fi antenna connectors (labeled Wi-Fi 1 and Wi-Fi 2) have antennas attached.
- The LED indicators of Wi-Fi 1 & 2 shown as below is referring to the default settings of Wi-Fi Operation mode is WAN + AP under the AP. For more details, please refer to the section 25.4

 Copyright @ 2021 Peplink

2.19.2 LED Indicators

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

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

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

Wi-Fi AP Indicators		
Wi-Fi 2	OFF	WiFi AP is disabled.
	ON	WiFi AP is enabled.

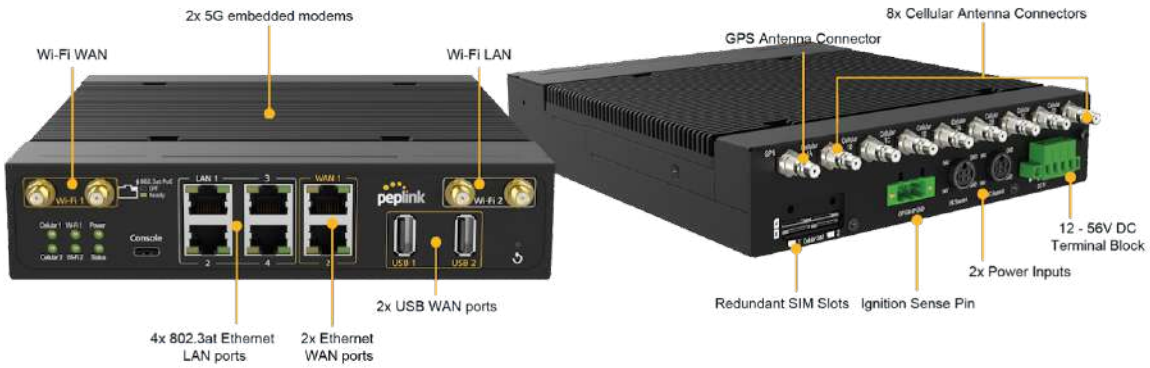
Cellular Indicators		
Cellular 1 / 2 / 3 / 4	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

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	

 Copyright @ 2021 Peplink

2.20 MAX MBX Mini

2.20.1 Panel Appearance



Note:

- For proper Wi-Fi performance and operations, please ensure all 4 Wi-Fi antenna connectors (labeled Wi-Fi 1 and Wi-Fi 2) have antennas attached.
- The LED indicators of Wi-Fi 1 & 2 shown as below is referring to the default settings of Wi-Fi Operation mode is WAN + AP under the AP. For more details, please refer to the section 25.4

2.20.2 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

 Copyright @ 2021 Peplink

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

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

Wi-Fi AP Indicators		
Wi-Fi 2	OFF	WiFi AP is disabled.
	ON	WiFi AP is enabled.

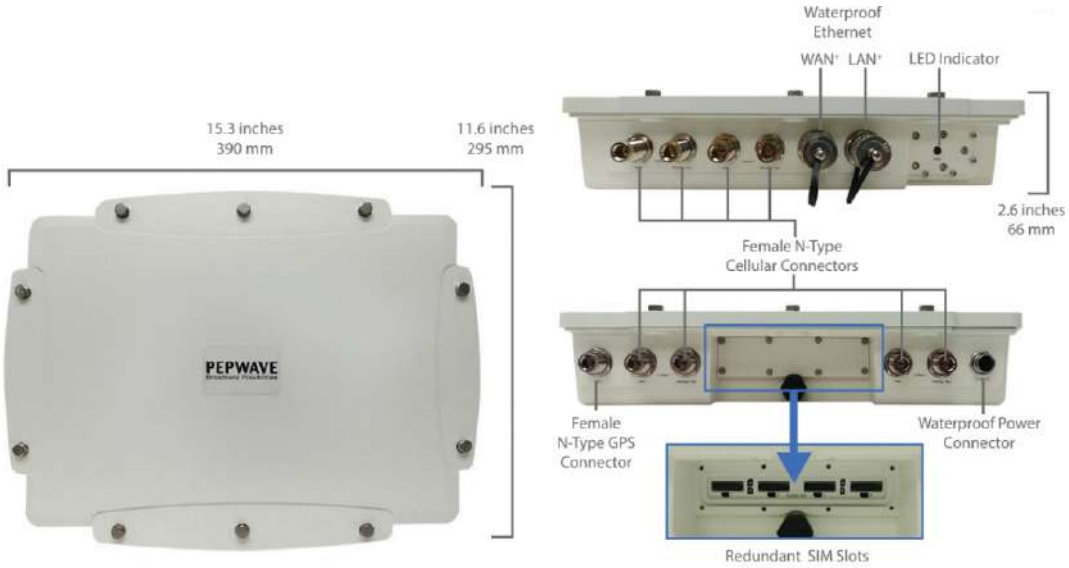
Cellular Indicators		
Cellular 1 / 2	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

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

 Copyright @ 2021 Peplink

2.21 MAX HD4 IP67

2.21.1 Panel Appearance



2.21.2 LED Indicators

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

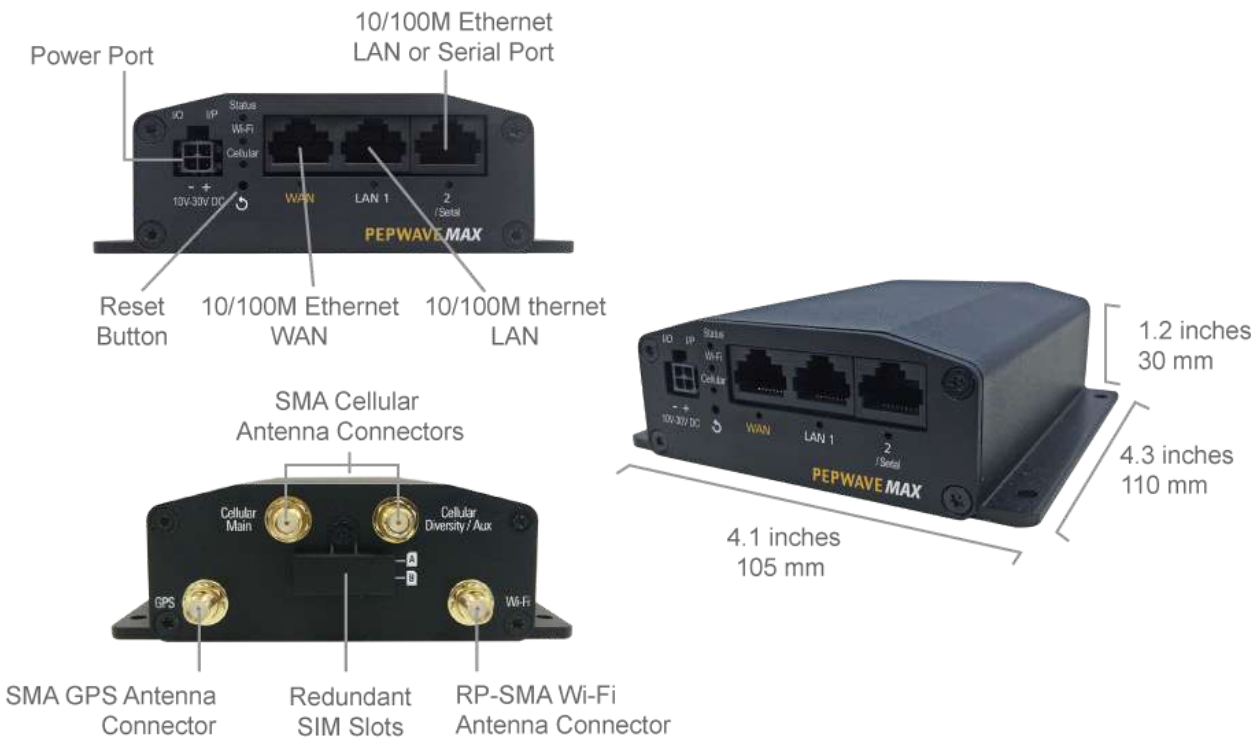
Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Blinking red	Boot up error
	Green	Ready

 Copyright @ 2021 Peplink

2.22 MAX BR1 Classic

For certification information, please refer to Appendix B: Declaration

2.22.1 Panel Appearance



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

 Copyright @ 2021 Peplink

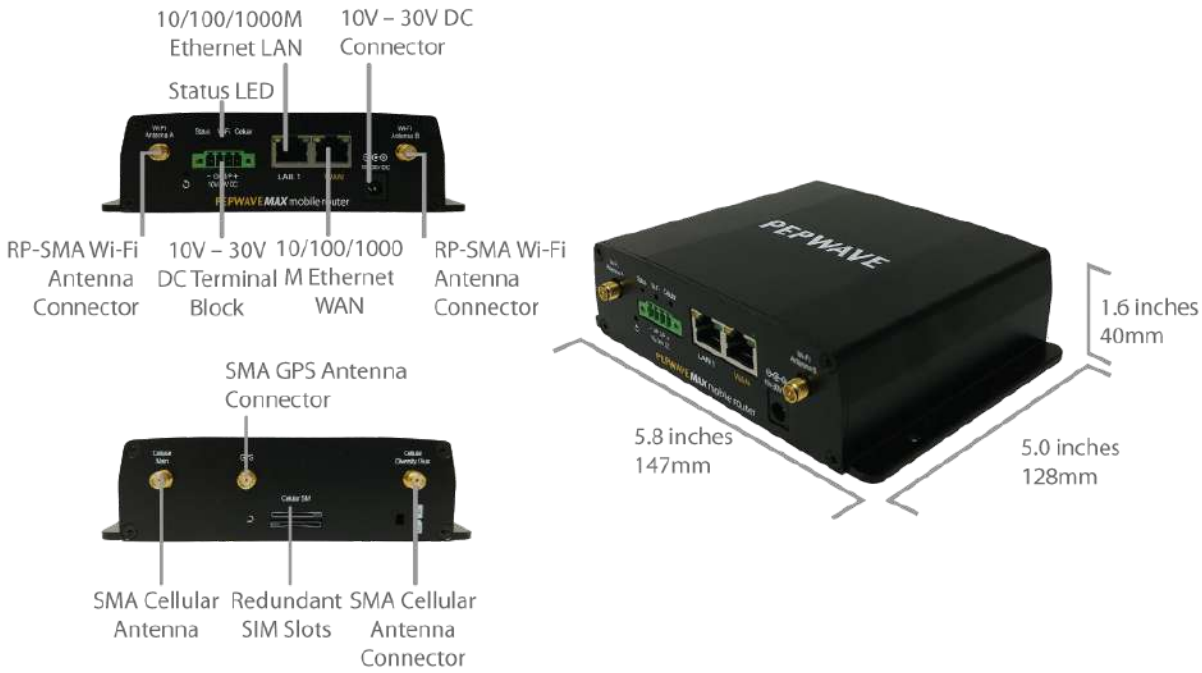
Wi-Fi Indicators		
Wi-Fi	OFF	Disabled intermittent
	Blinking slowly	Connecting to wireless network(s)
	Blinking	Connected to wireless network(s) with traffic
	ON	Connected to wireless network(s) without traffic

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

2.23 MAX BR1 MK2

For certification information, please refer to Appendix B: Declaration

2.23.1 Panel Appearance



 Copyright @ 2021 Peplink

2.23.2 LED Indicators

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

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

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

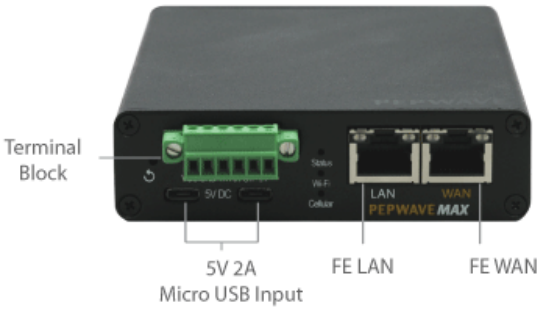
Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

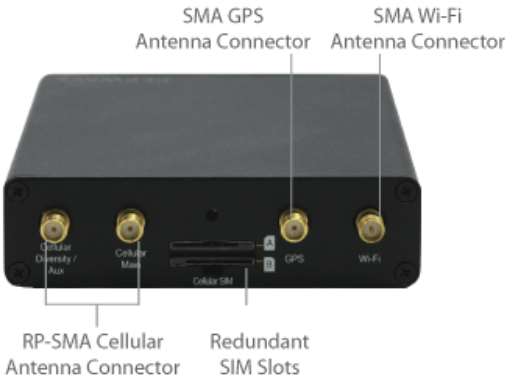
LAN and Ethernet WAN Ports		
Green LED	ON	1000 Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

 Copyright @ 2021 Peplink

2.24 MAX BR1 Slim

2.24.1 Panel Appearance





2.24.2 LED Indicators

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

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

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)

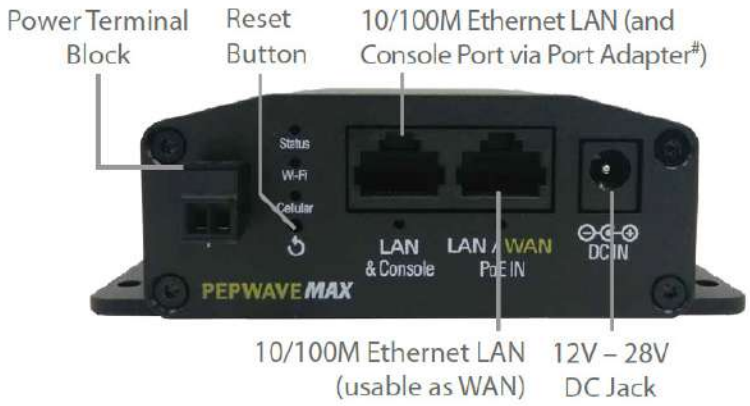
 Copyright @ 2021 Peplink

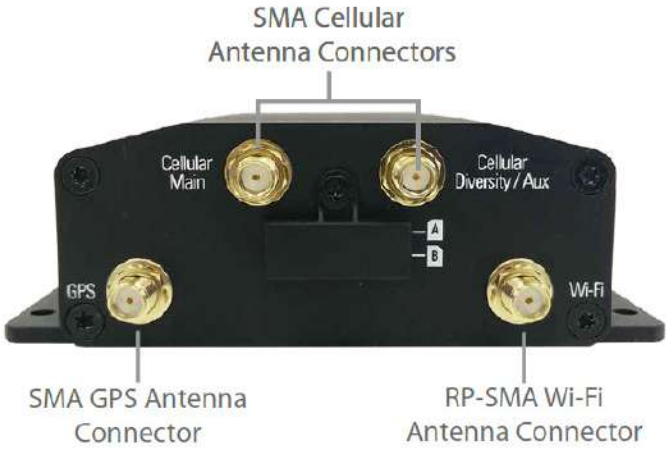
LAN and Ethernet WAN Ports		
Green LED	ON	100 Mbps
	OFF	10 Mbps
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	Port is not connected
Port Type	Auto MDI/MDI-X ports	

2.25 MAX BR1 Mini (HW2)

For certification information, please refer to Appendix B: Declaration

2.25.1 Panel Appearance





 Copyright @ 2021 Peplink

2.25.2 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

 Copyright @ 2021 Peplink

2.26 MAX BR1 Mini (HW3)

2.26.1 Panel Appearance

2.26.2 LED Indicators

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

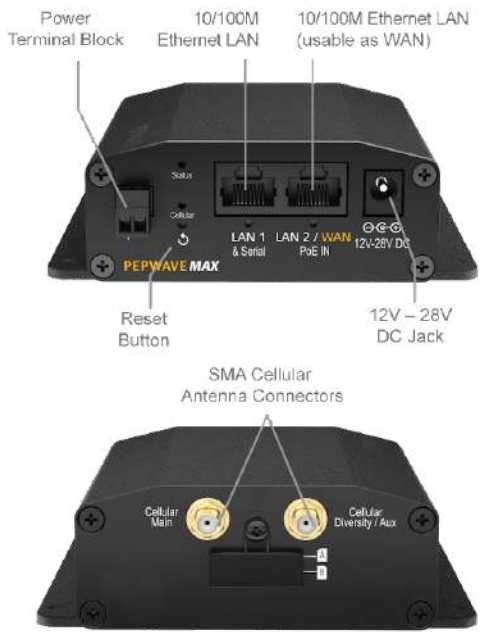
Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

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

 Copyright @ 2021 Peplink

2.27 MAX BR1 Mini Core

2.27.1 Panel Appearance



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)

 Copyright @ 2021 Peplink

2.28 MAX BR1 M2M

2.28.1 Panel Appearance

2.28.2 LED Indicators

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

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

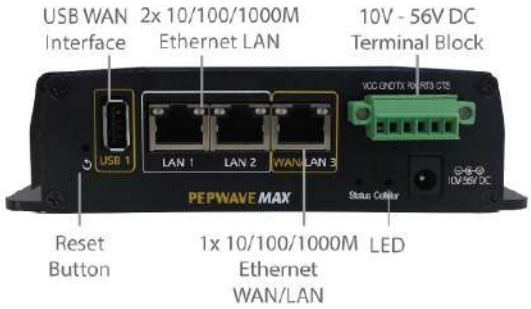
Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

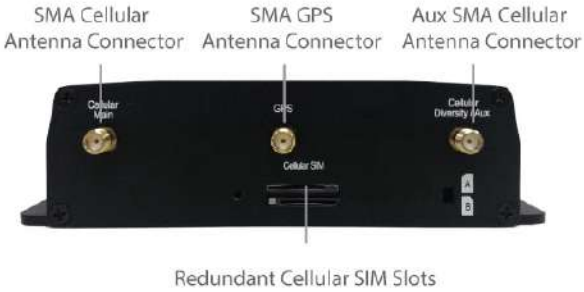
 Copyright @ 2021 Peplink

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	

2.29 MAX BR1 ENT

2.29.1 Panel Appearance





2.29.2 LED Indicators

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

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

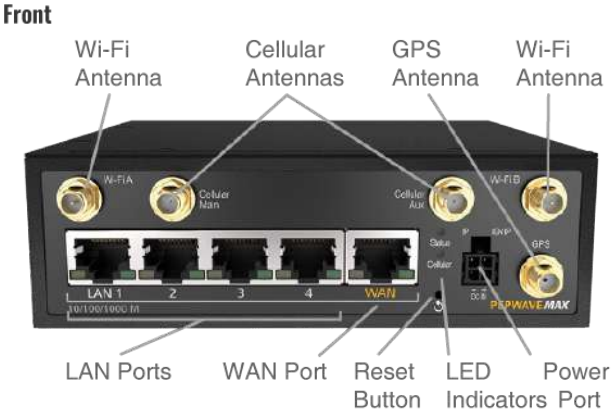
Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	Blinking slowly	Connecting to network(s)
	Green	Connected to network(s)

 Copyright @ 2021 Peplink

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	

2.30 MAX BR1 Pro

2.30.1 Panel Appearance



2.30.2 LED Indicators

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

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

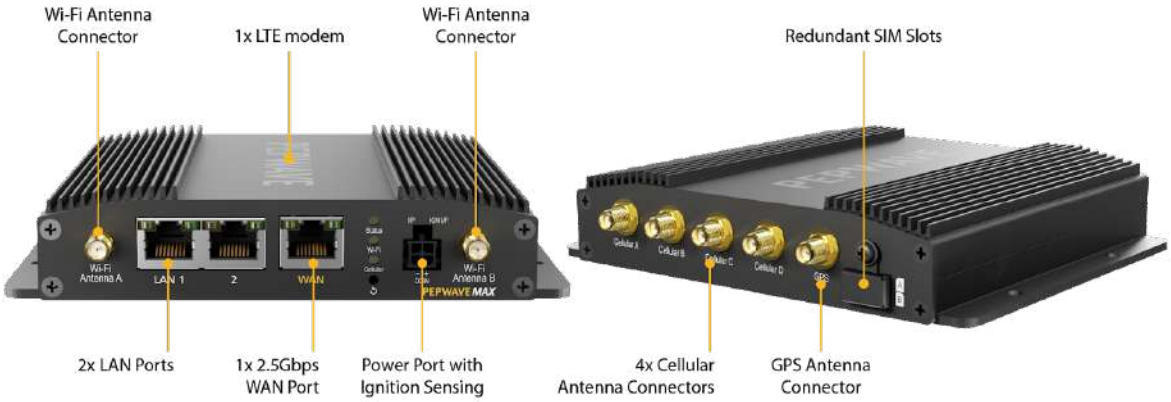
 Copyright @ 2021 Peplink

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	

2.31 MAX BR1 Pro (CAT-20)

2.31.1 Panel Appearance



2.31.2 LED Indicators

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

 Copyright @ 2021 Peplink

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)

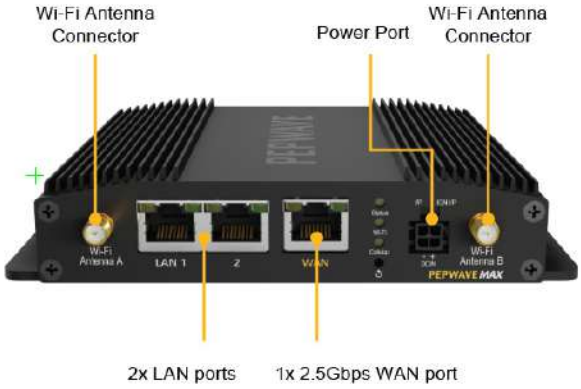
LAN Ports		
Green LED	ON	1000 Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

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	

 Copyright @ 2021 Peplink

2.32 MAX BR1 Pro 5G

2.32.1 Panel Appearance



2.32.2 LED Indicators

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

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

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

 Copyright @ 2021 Peplink

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	

 Copyright @ 2021 Peplink

2.33 MAX BR2 Pro

2.33.1 Panel Appearance

2.33.2 LED Indicators

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

Status Indicators		
Status	OFF	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

 Copyright @ 2021 Peplink

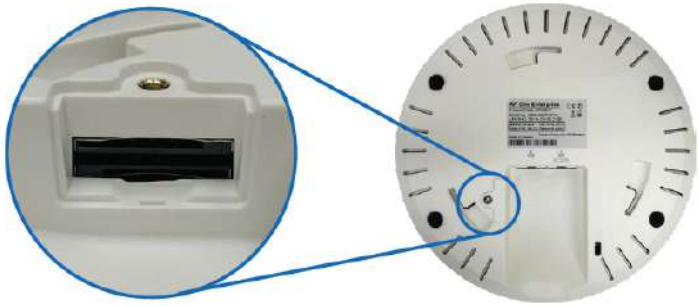
	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

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	

2.34 MAX Hotspot

2.34.1 Panel Appearance

 Copyright @ 2021 Peplink



Screw Open the Panel to
Reveal Redundant SIM Slots

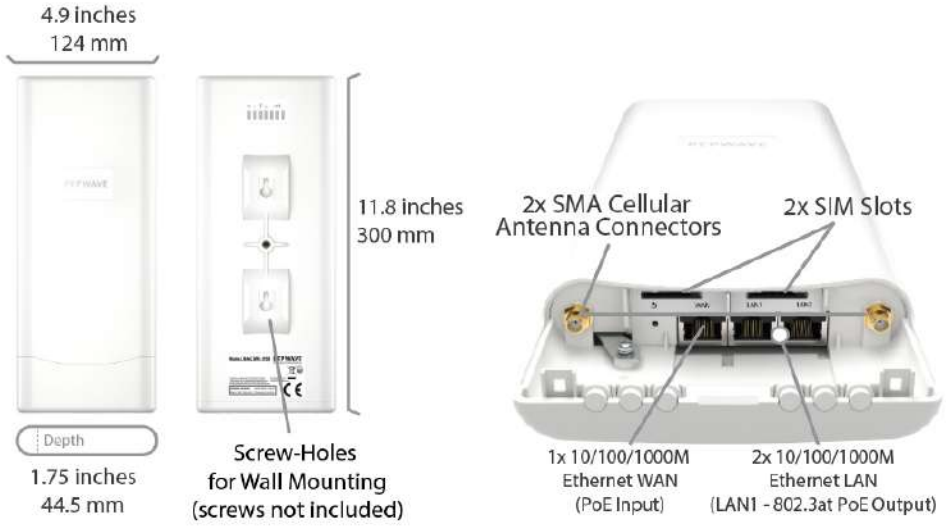
2.34.2 LED Indicators

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	

2.35 MAX BR1 IP55

2.35.1 Panel Appearance



 Copyright @ 2021 Peplink

2.35.2 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	

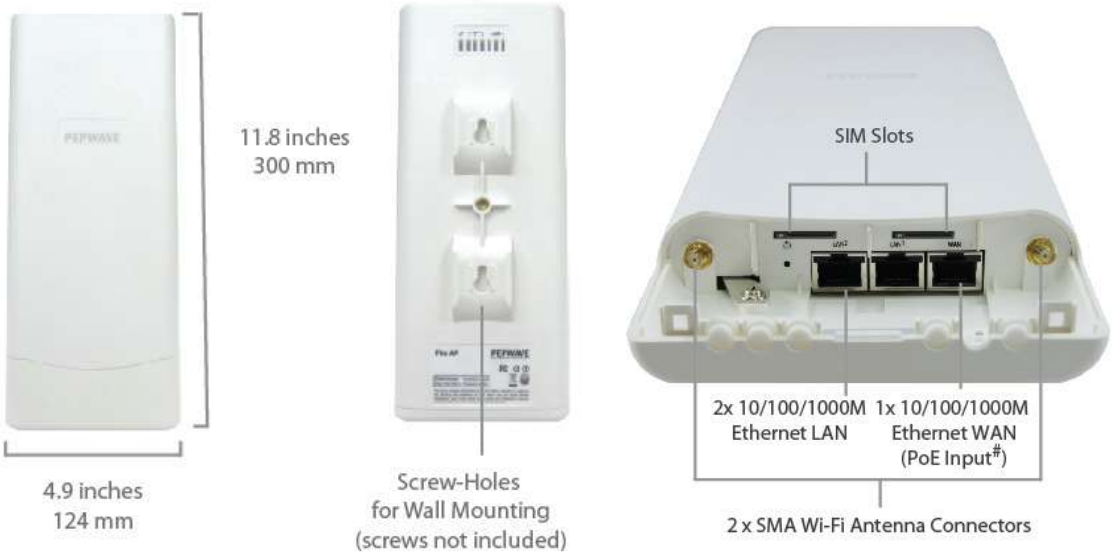
Cellular Indicators		
Cellular 	OFF	Disabled or no SIM card inserted
	Blinking	Connecting to network(s) in Standby Mode
	Green	Connected to network(s) in Priority 1 (Active)

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

 Copyright @ 2021 Peplink

2.36 MAX BR2 IP55

2.36.1 Panel Appearance



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

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

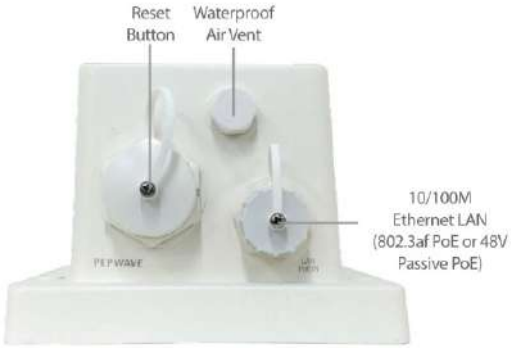
Cellular Indicators		
Cellular	OFF	Disabled or no SIM card inserted
	ON	Connecting or connected to network(s)

 Copyright @ 2021 Peplink

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	

2.37 MAX BR1 IP67

2.37.1 Panel Appearance



 Copyright @ 2021 Peplink

2.38 MAX On-The-Go

2.38.1 Panel Appearance

2.38.2 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

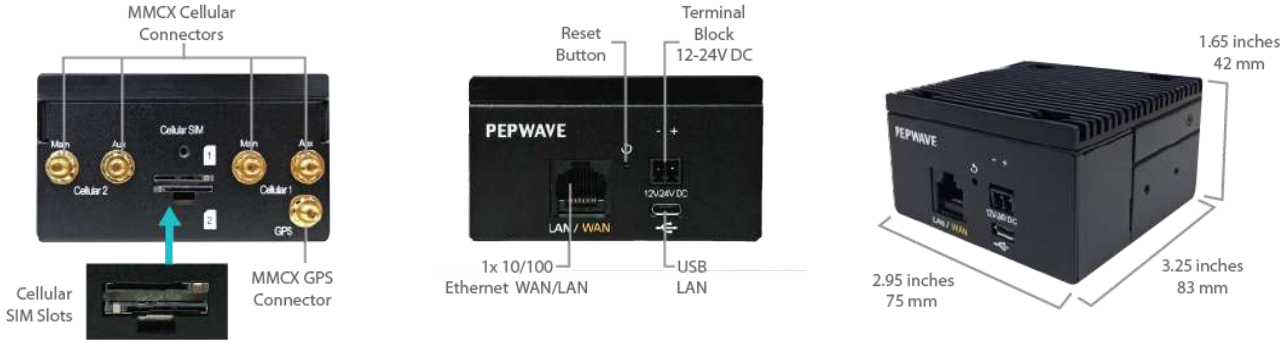
Status Indicators		
Status	OFF	System initializing
	Red	Booting up or busy
	Green	Ready

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	

 Copyright @ 2021 Peplink

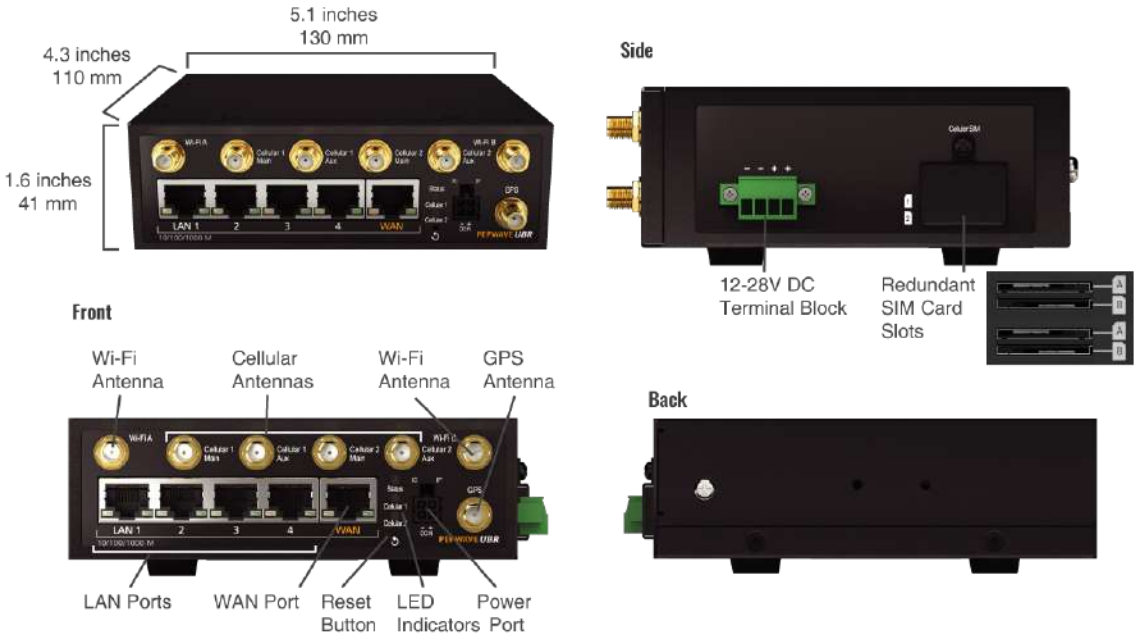
2.39 SpeedFusion Engine

2.39.1 Panel Appearance



2.40 UBR LTE

2.40.1 Panel Appearance



 Copyright @ 2021 Peplink

2.40.2 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

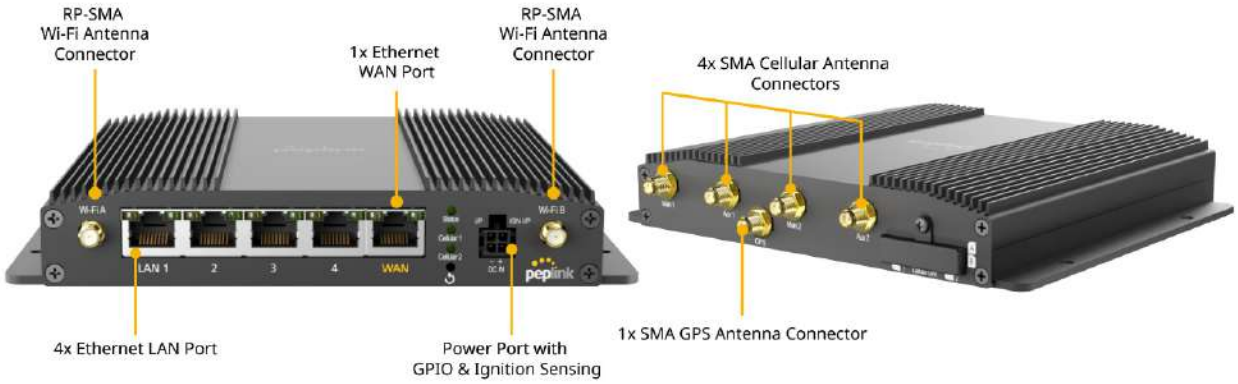
LAN and Ethernet WAN Ports		
Green LED	ON	1000 Mbps
	OFF	10 Mbps / 100 Mbps or port is not connected
Orange LED	ON	Port is connected without traffic
	Blinking	Data is transferring
	OFF	No data is being transferred or port is not connected
Port Type	Auto MDI/MDI-X ports	

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

 Copyright @ 2021 Peplink

2.41 UBR Plus

2.41.1 Panel Appearance



2.41.2 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

 Copyright @ 2021 Peplink

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

2.42 PDX

2.42.1 Panel Appearance

2.42.2 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

 Copyright @ 2021 Peplink

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.

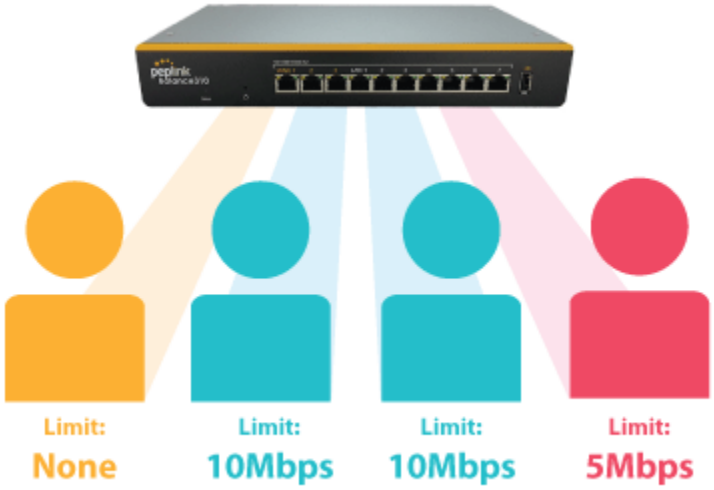
Note: Drop-in mode is compatible for All MAX models except MAX BR1 IP67

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.

 Copyright @ 2021 Peplink

3.3 Per-User Bandwidth Control



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

3.4 High Availability via VRRP

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

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

 Copyright @ 2021 Peplink

3.5 USB Modem and Android Tethering

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

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

3.6 Built-In Remote User VPN Support

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

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

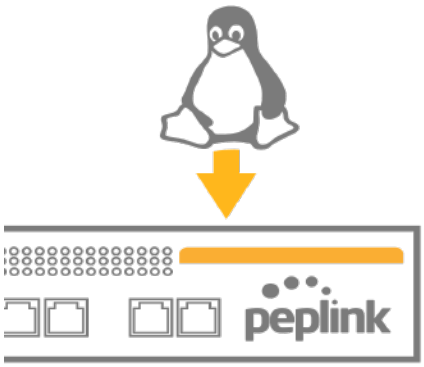
 Copyright @ 2021 Peplink

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

 Copyright @ 2021 Peplink

3.9 DPI Engine

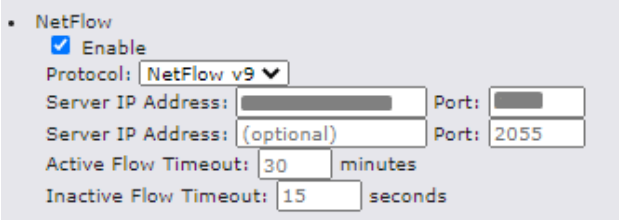
The DPI report written in the updated KB article will show further information on InControl2 through breaking down application categories into subcategories.

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.

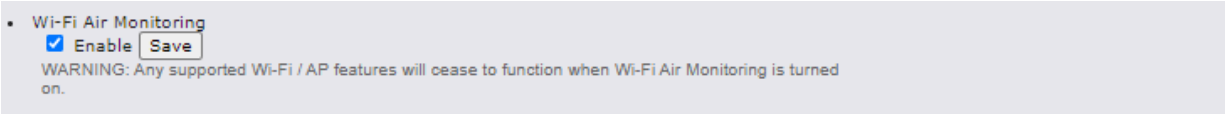
Note: To enable this feature, go to https://<Device's IP>/cgi-bin/MANGA/support.cgi



3.11 Wi-Fi Air Monitoring

Pepwave routers support Wi-Fi “Air Monitoring Mode” which is 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



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).

 Copyright @ 2021 Peplink

3.13 Peplink Relay

Cloud Service Providers often restrict access to certain applications. With SFC Relay, you can route traffic before going out to the Internet, allowing access to previously restricted applications experienced with the public SpeedFusion Cloud nodes. Available as an add-on for your home router or as an upgradable license to your Peplink router, SFC Relay is sure to impress you and any peers you give access to.

https://forum.peplink.com/t/configure-speedfusion-cloud-relay-server-and-client/6215ca9b017e48e0f3ff2479/

3.14 DNS over HTTPS (DoH)

DoH provides the benefits of communicating DNS information over a secure HTTPS connection in an encrypted manner. The protocol offers increased privacy and confidentiality by preventing data interception and man-in-the-middle attacks.

3.15 Peplink InTouch

InTouch is Peplink's zero-touch remote network management solution, leveraging InControl 2 and a SpeedFusion Connect (formerly known as SpeedFusion Cloud) data plan. This service extends a network administrator's ability to reach any device UI backed by a Peplink/Pepwave router. To configure InTouch, all you need is a valid InControl 2 subscription, a SpeedFusion Connect data plan, and a Peplink/Pepwave router (which requires the latest 8.2.0 firmware).

To watch a demonstration and read the FAQ, visit
https://www.peplink.com/enterprise-solutions/intouch/

Or learn to configure InTouch at **https://youtu.be/zg0iavHGkJw**

 Copyright @ 2021 Peplink

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.

 Copyright @ 2021 Peplink

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**.

 Copyright @ 2021 Peplink

5 Mounting the Unit

5.1 Wall Mount

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

The Pepwave MAX BR1 requires four screws for wall mounting.

5.2 Car Mount

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

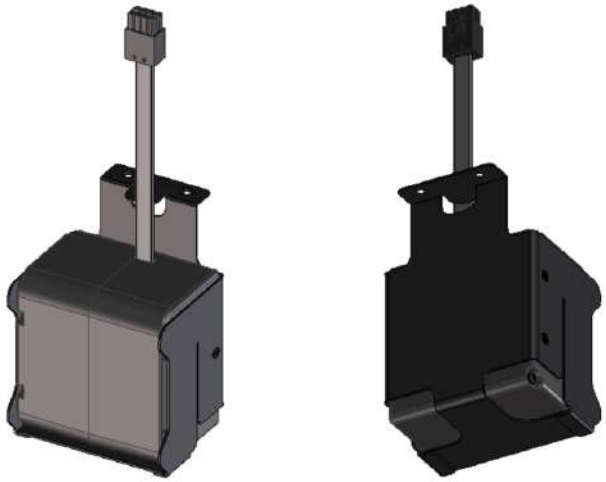
5.3 IP67 Installation Guide

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

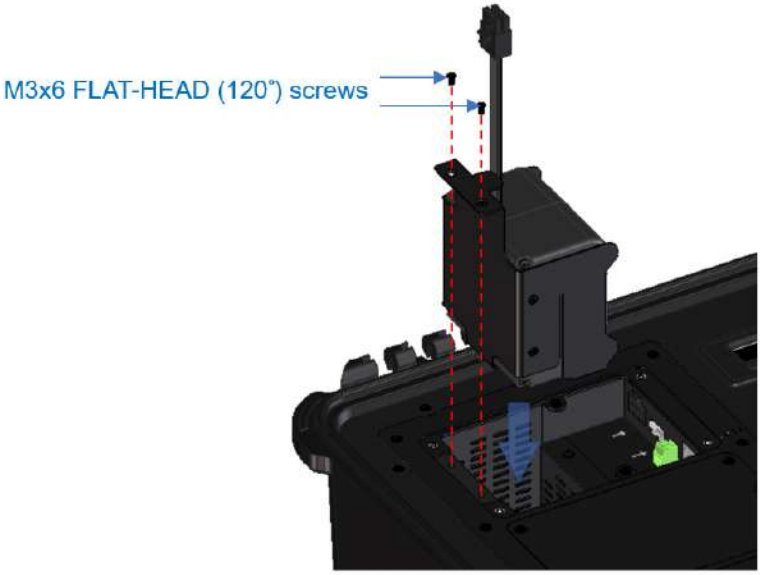
 Copyright @ 2021 Peplink

5.4 PDX Accessory Kit Installation Guide

5.4.1 Battery Set appearance



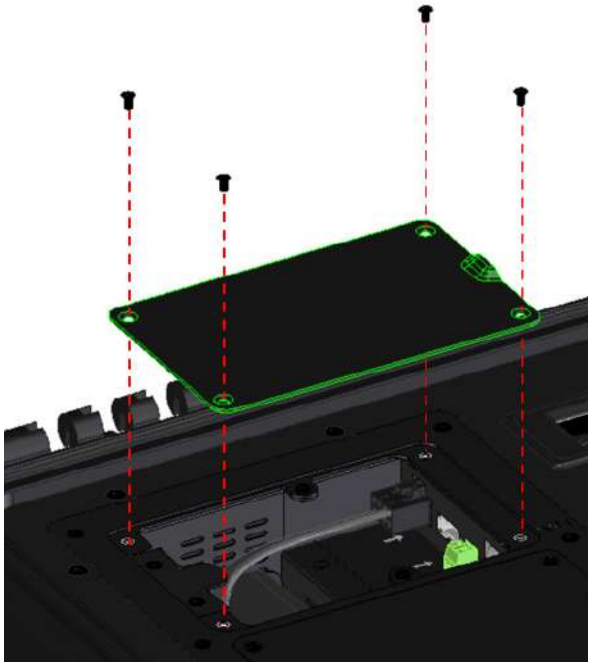
- Step 1: Lock the battery set in the slot with 2 pcs M3 screws.



- Step 2: Plug power cable into the socket

 Copyright @ 2021 Peplink

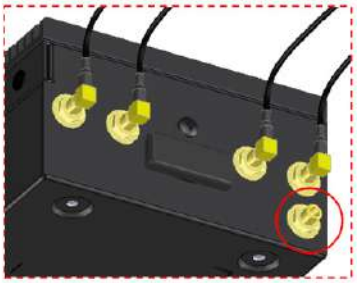
- STEP 3: Lock the slot cover with 4 pcs M3 screws.



 Copyright @ 2021 Peplink

5.4.2 SFE-DUO Set appearance

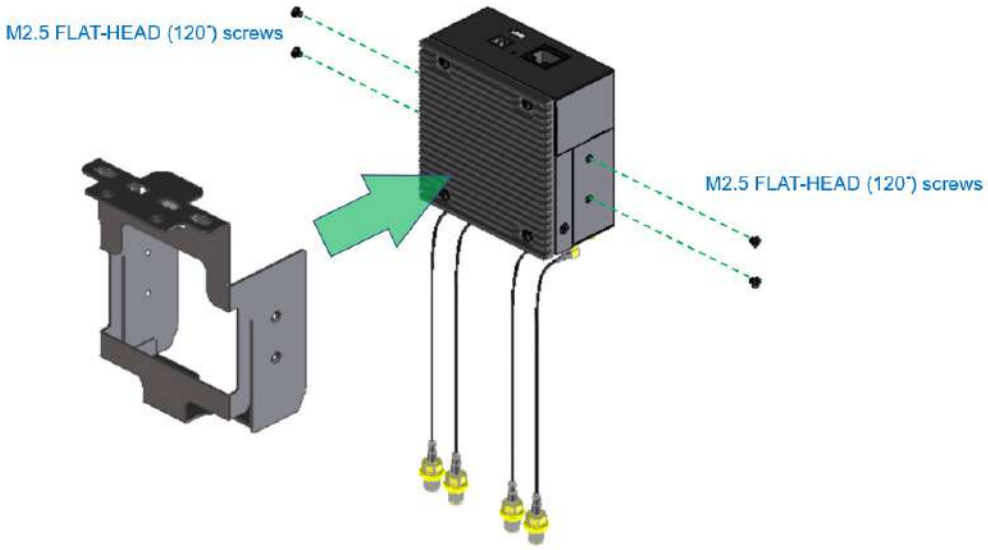
- STEP 1: Assemble SMA cables to the device

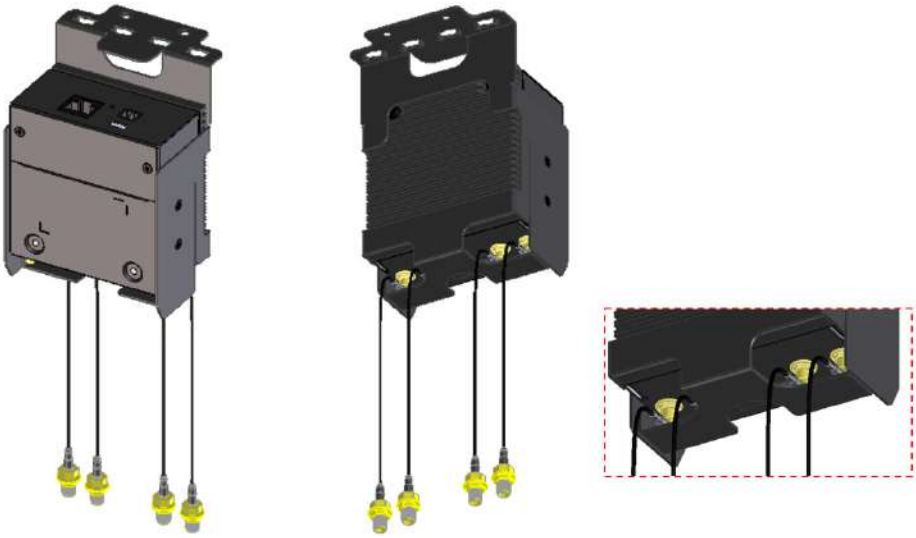


GPS port not in use

- STEP 2: Assemble bracket to the device

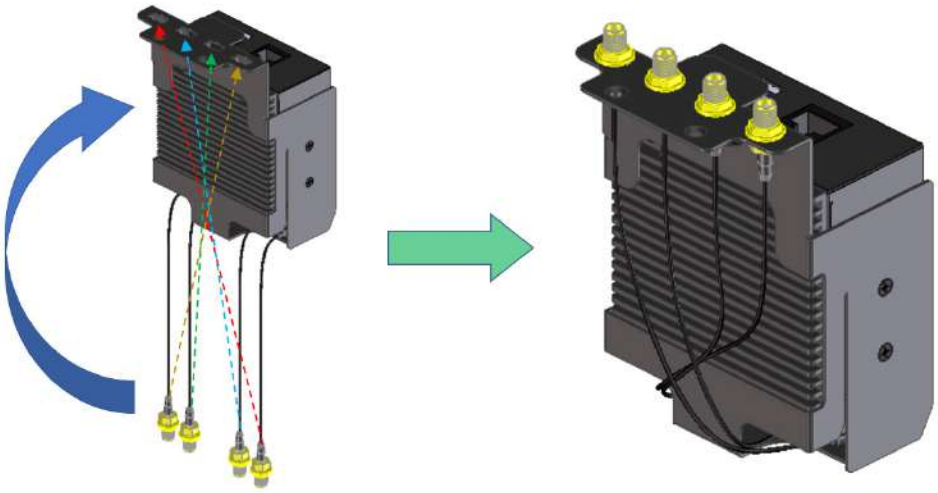
 Copyright @ 2021 Peplink

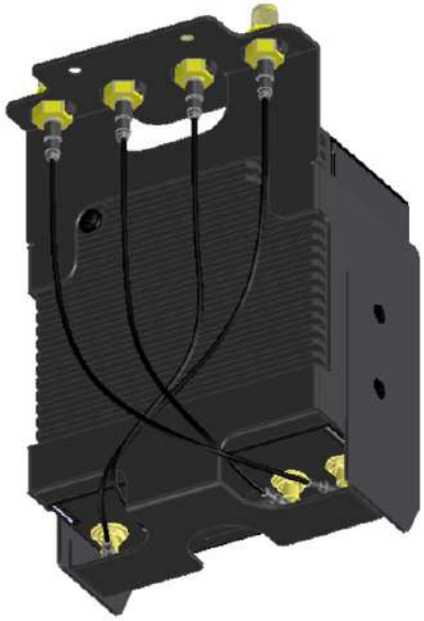


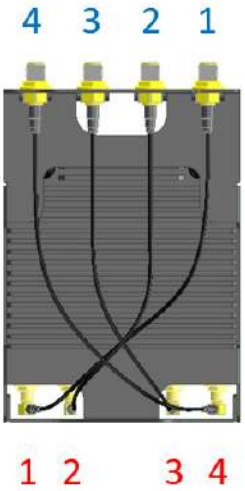


- STEP 3: Assemble SMA connectors to the bracket

 Copyright @ 2021 Peplink

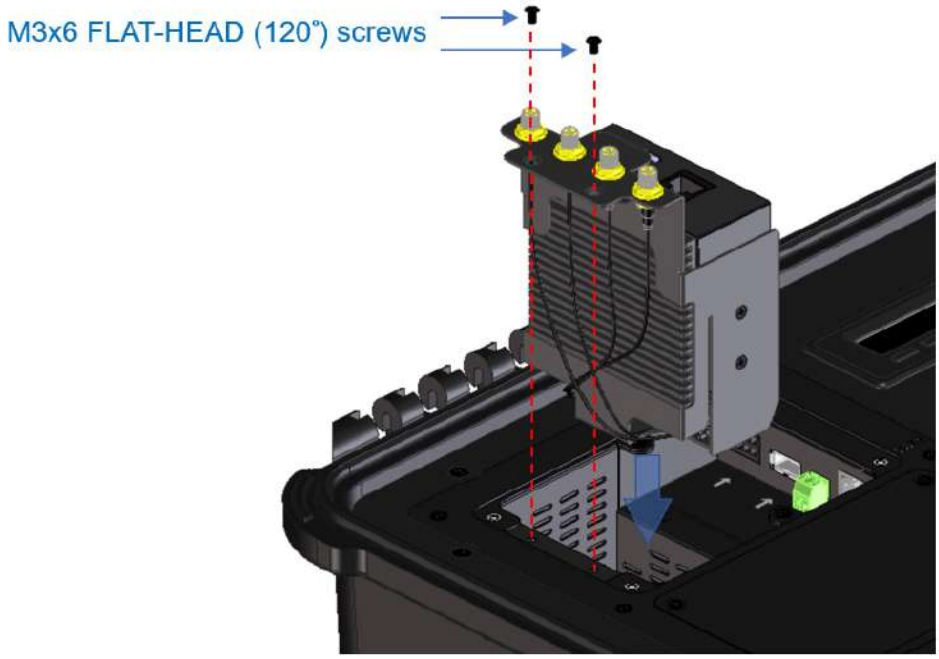




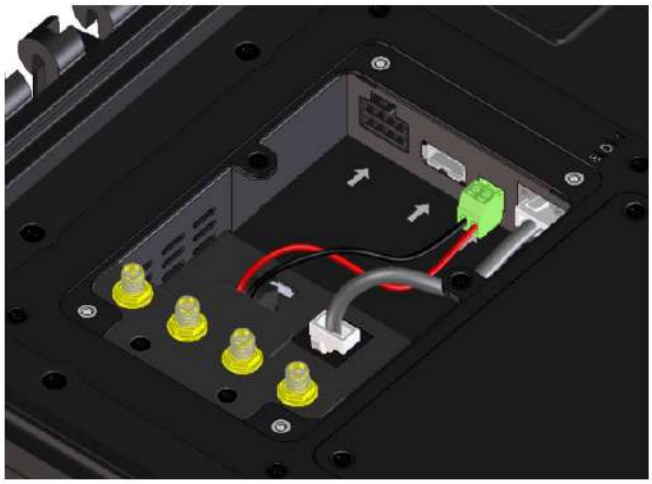


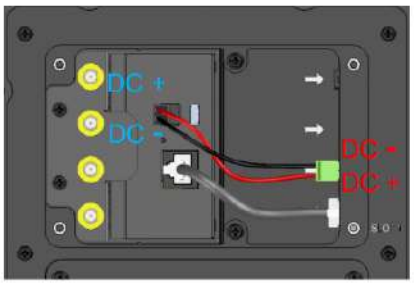
- STEP 4: Lock the SFE-Duo set in the slot with 2 pcs M3 screws.

 Copyright @ 2021 Peplink



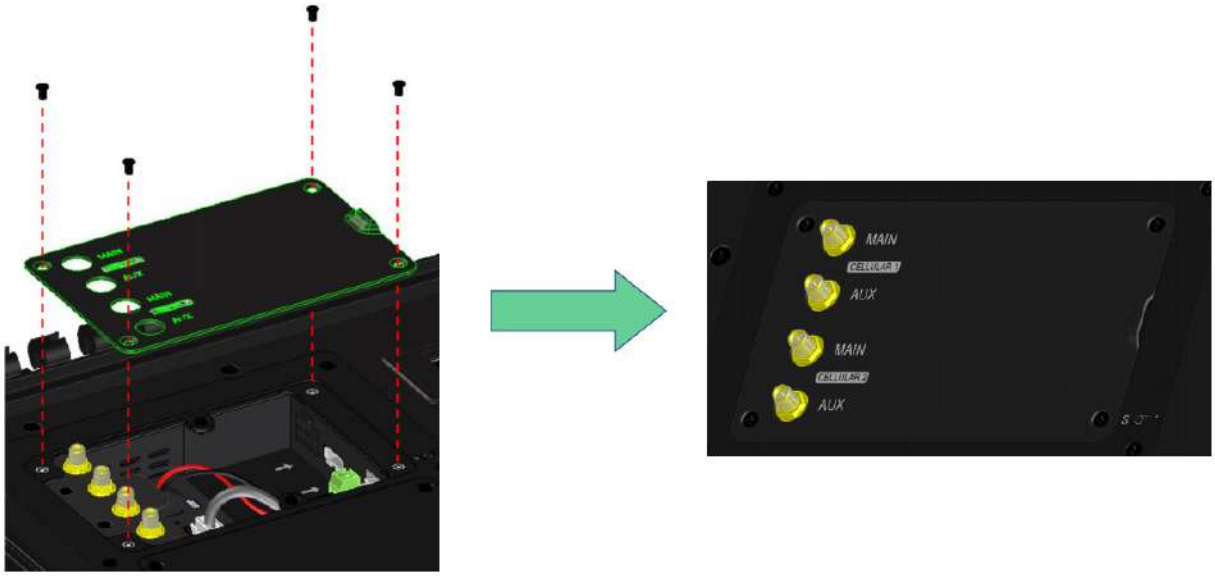
- STEP 5: Connect DC power & ETH port





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

 Copyright @ 2021 Peplink



0

 Copyright @ 2021 Peplink

6 Connecting to the Web Admin Interface

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

   http://192.168.50.1

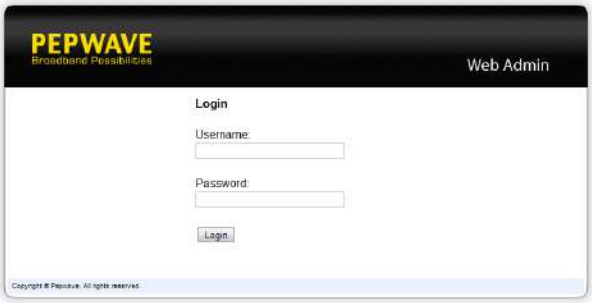
   (This is the default LAN IP address for Pepwave routers.)

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

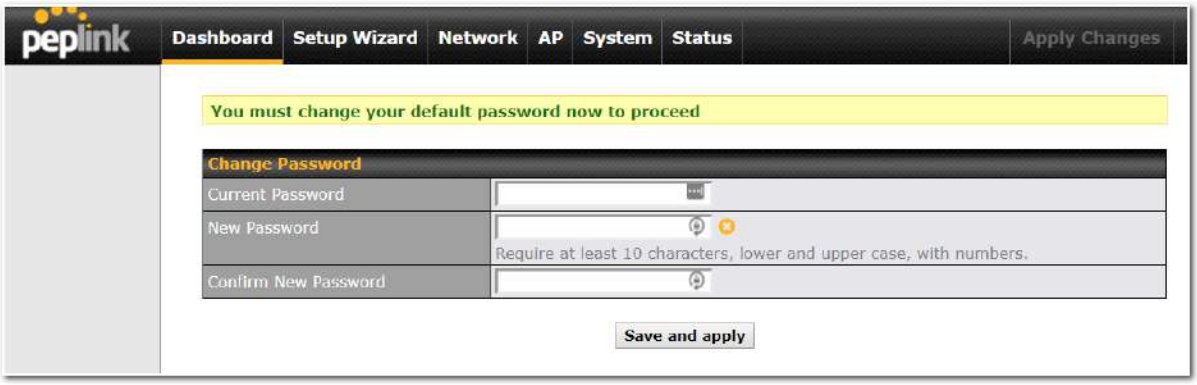
   Username: admin

   Password: admin

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

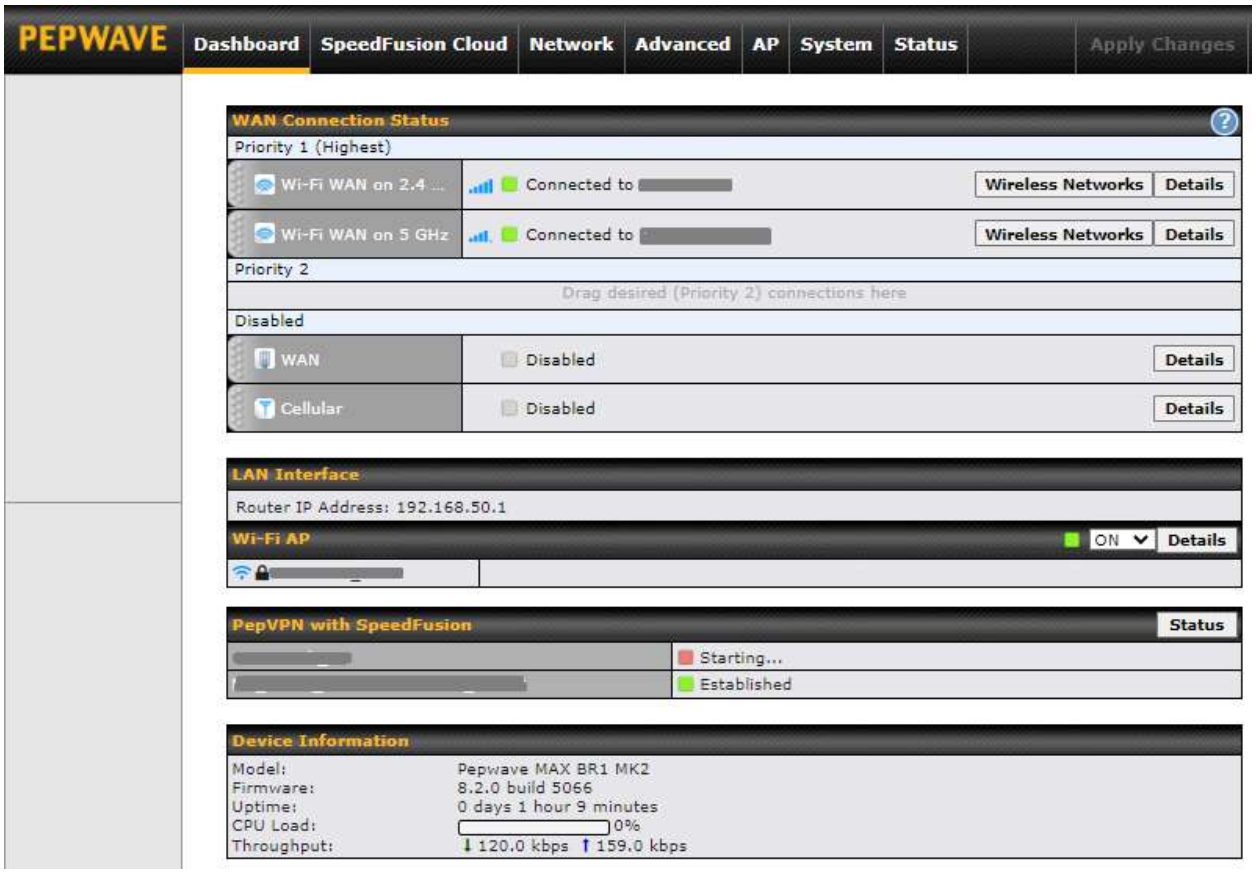


- You must change the default password on the first successful logon.
- Password requirements are: A minimum of 10 lower AND upper case characters, including at least 1 number.
- When HTTP is selected, the URL will be redirected to HTTPS by default.



 Copyright @ 2021 Peplink

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



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

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

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

 Copyright @ 2021 Peplink

7 SpeedFusion Connect

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

*SpeedFusion Connect is supported in firmware version 8.1.0 and above. SpeedFusion Connect is a subscription basis. SpeedFusion Connect license can be purchased at https://estore.peplink.com/ **> SpeedFusion Service > SpeedFusion Connect**.

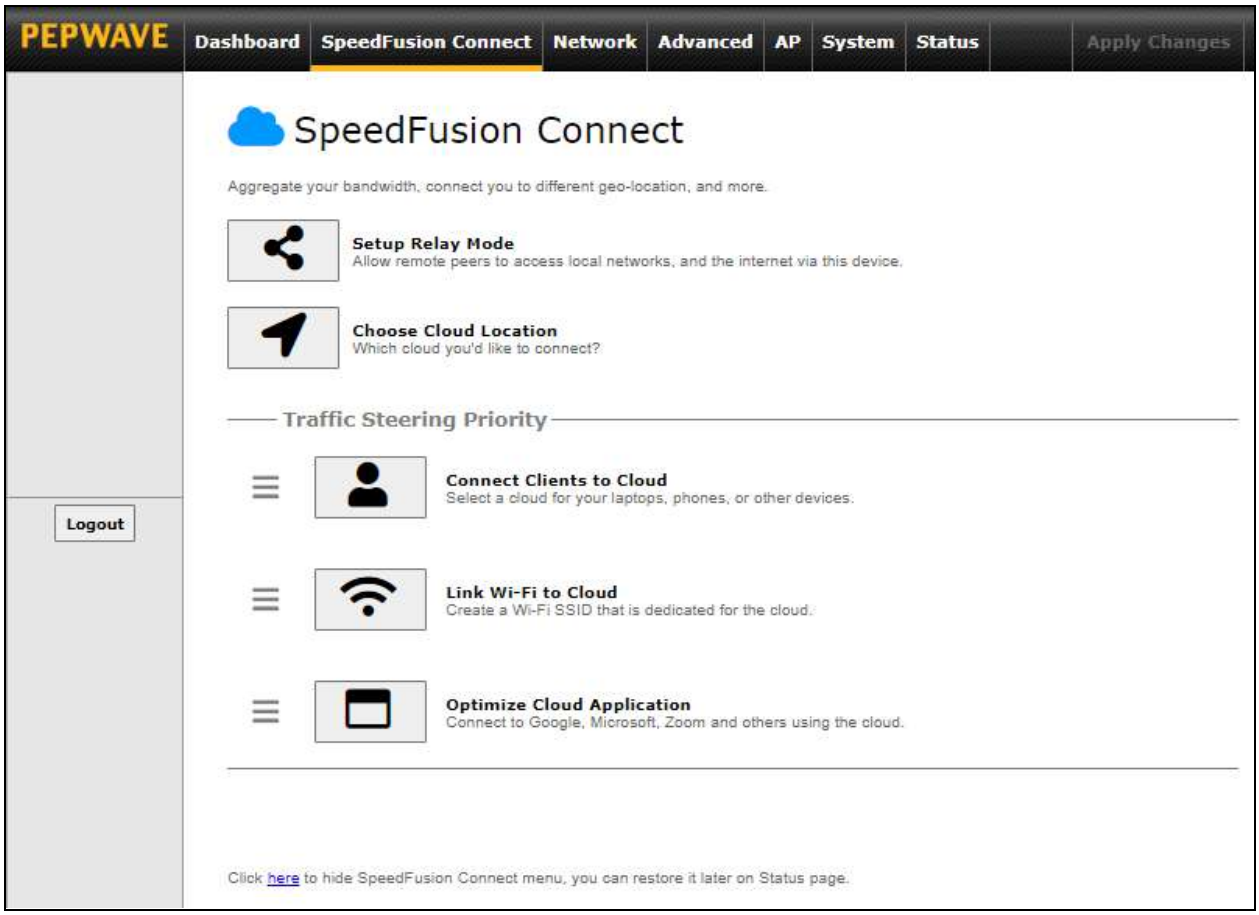
7.1 Activate SpeedFusion Connect Service

All Care plans now come with SpeedFusion Connect included. This data allowance will automatically begin and end in accordance with your warranty. No activation is required.

 Copyright @ 2021 Peplink

7.2 Enable SpeedFusion Connect

Access the Web Admin of the device you want to create as the Peplink Relay Server, navigating to the "**SpeedFusion Connect**" tab.

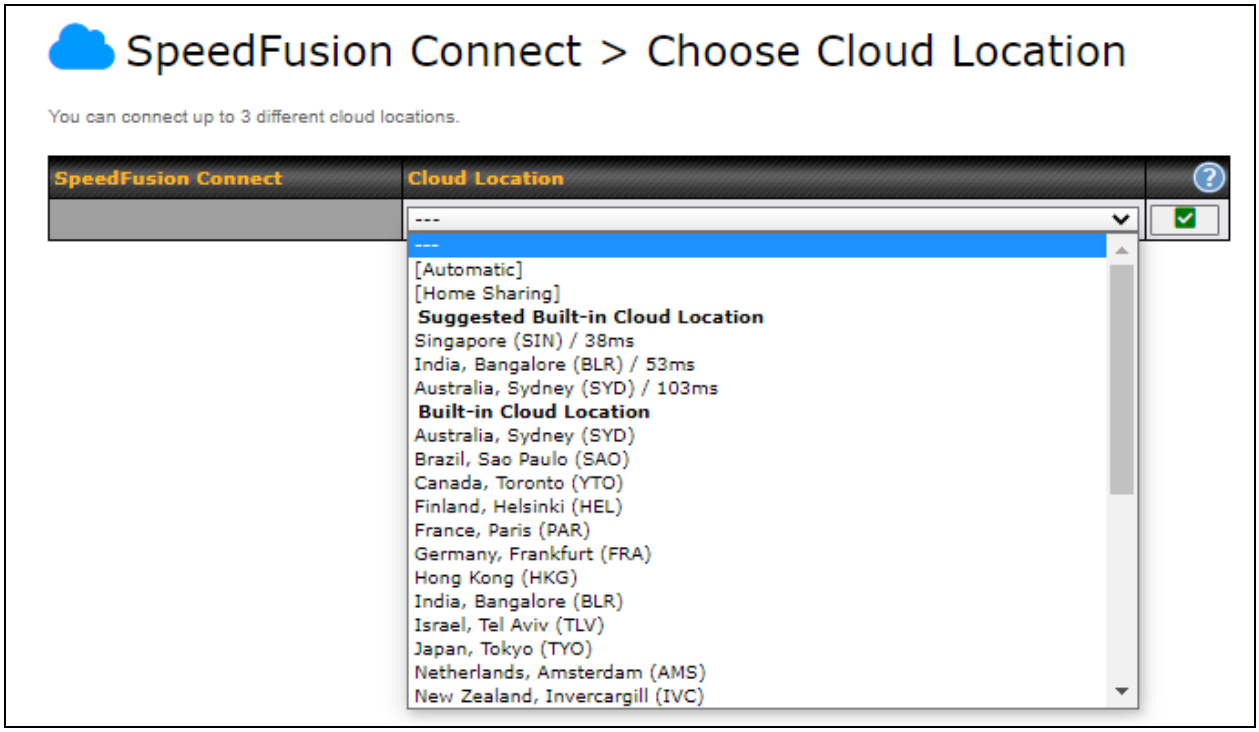


To set up a Peplink Relay Server, select "**Setup Home Sharing**" > Choose the **Cloud Location** you wish to connect to > Click on the **green tick button** to confirm the change.

 Copyright @ 2021 Peplink

The Relay Sharing Code will be generated and other peers can use this code to establish a SpeedFusion Connect connection that will forward the traffic to this device, allowing them to access local networks and the Internet via your WAN connection.

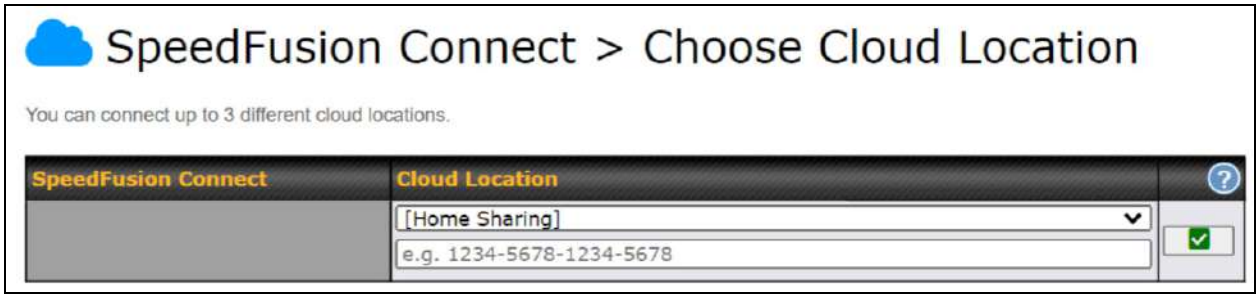
To connect to SpeedFusion Cloud, you can select a **Cloud Location** of your choice, or simply **Automatic**, then the device will establish a connection to the nearest cloud server.



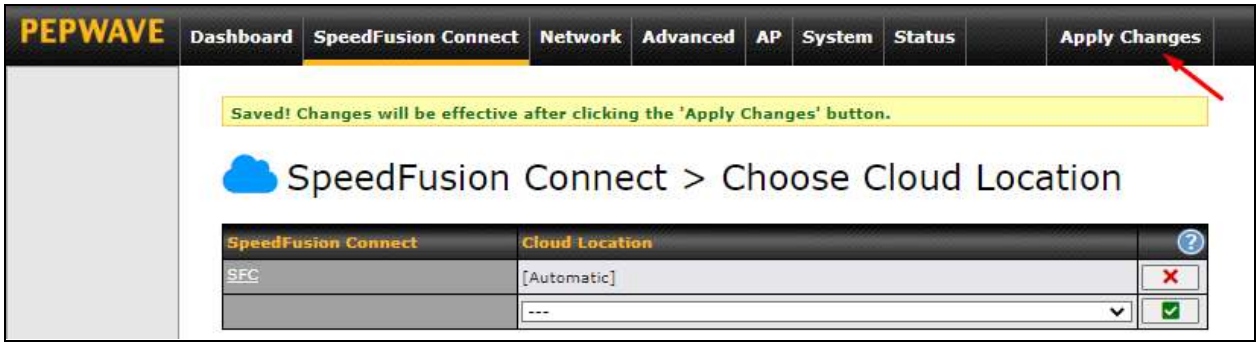
Choose **Automatic > Click on the green tick button** to confirm the change.

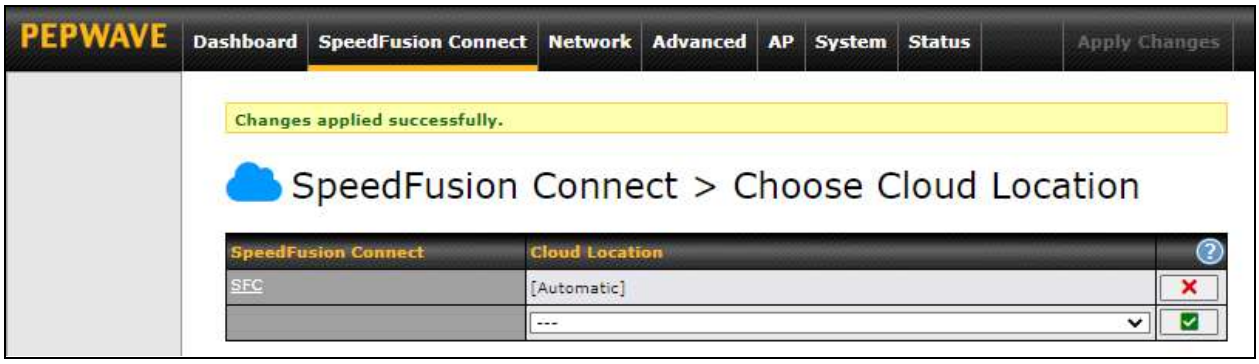
 Copyright @ 2021 Peplink

Or you may select **Home Sharing** and use your **Relay Sharing Code** to create a profile if you have set up a Peplink Relay Client on another device.



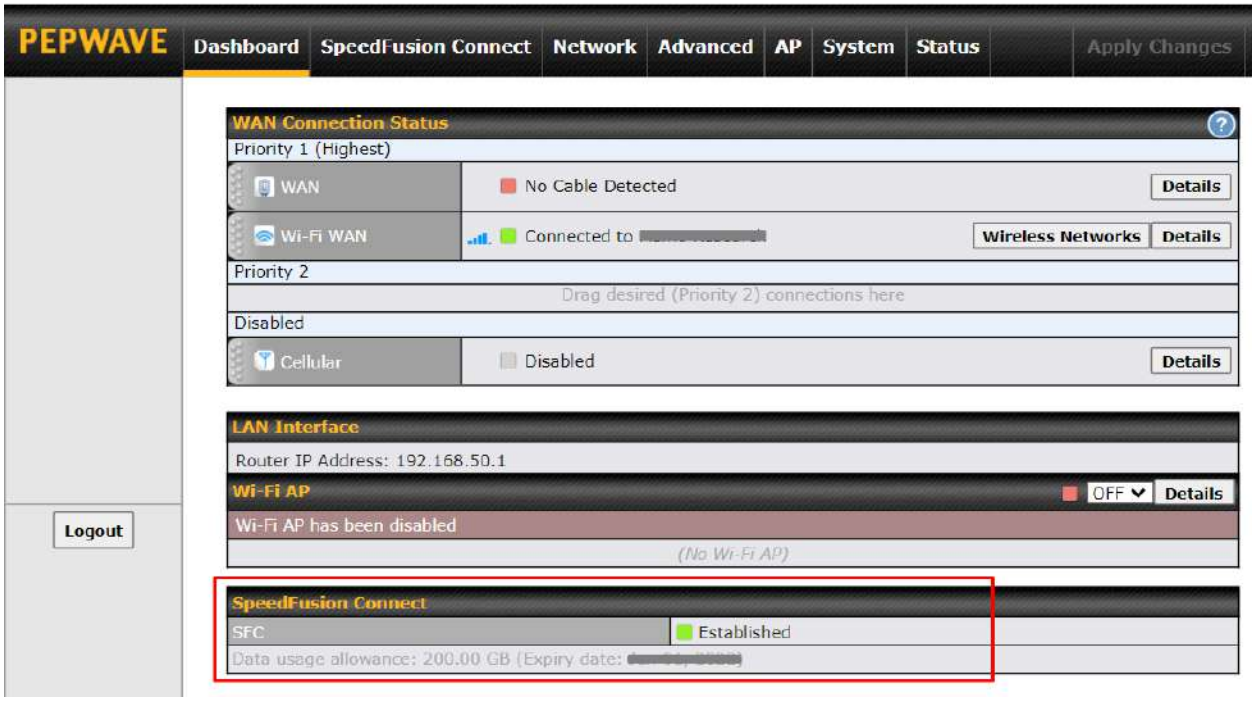
Click on **Apply Changes** to save the change.





 Copyright @ 2021 Peplink

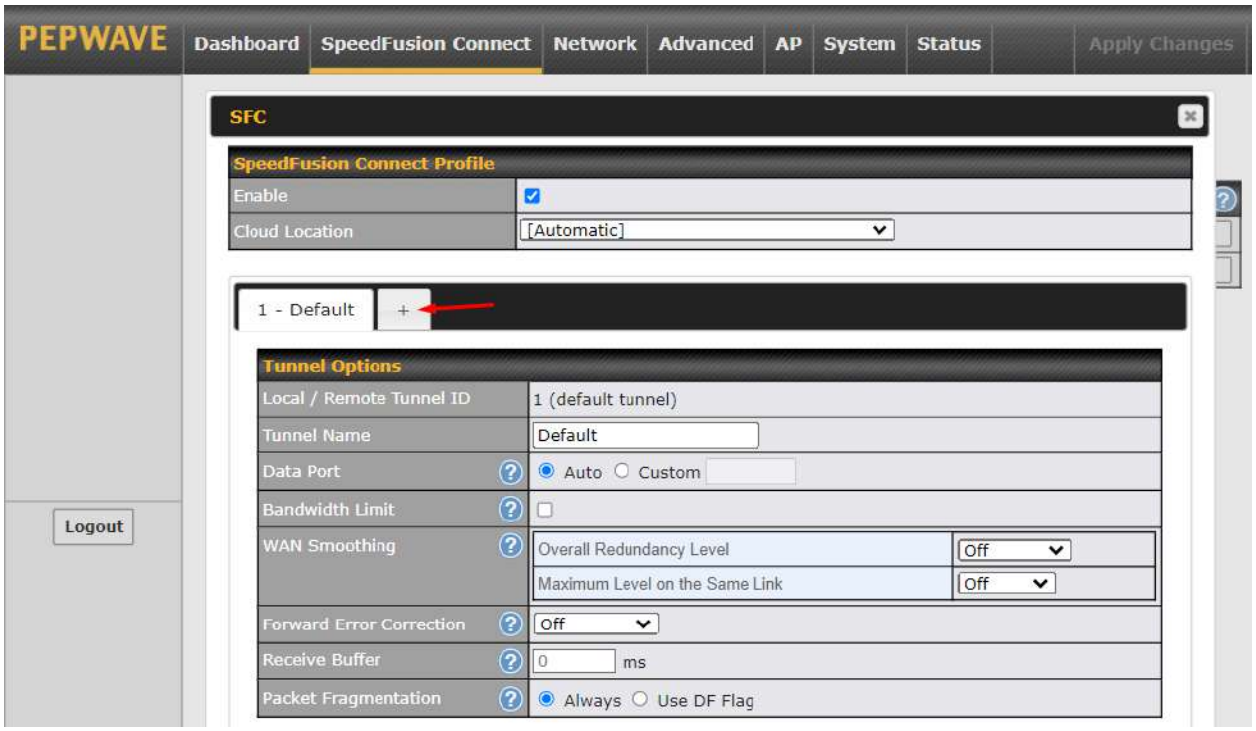
By default, the router will build a SpeedFusion tunnel to the SpeedFusion Cloud.

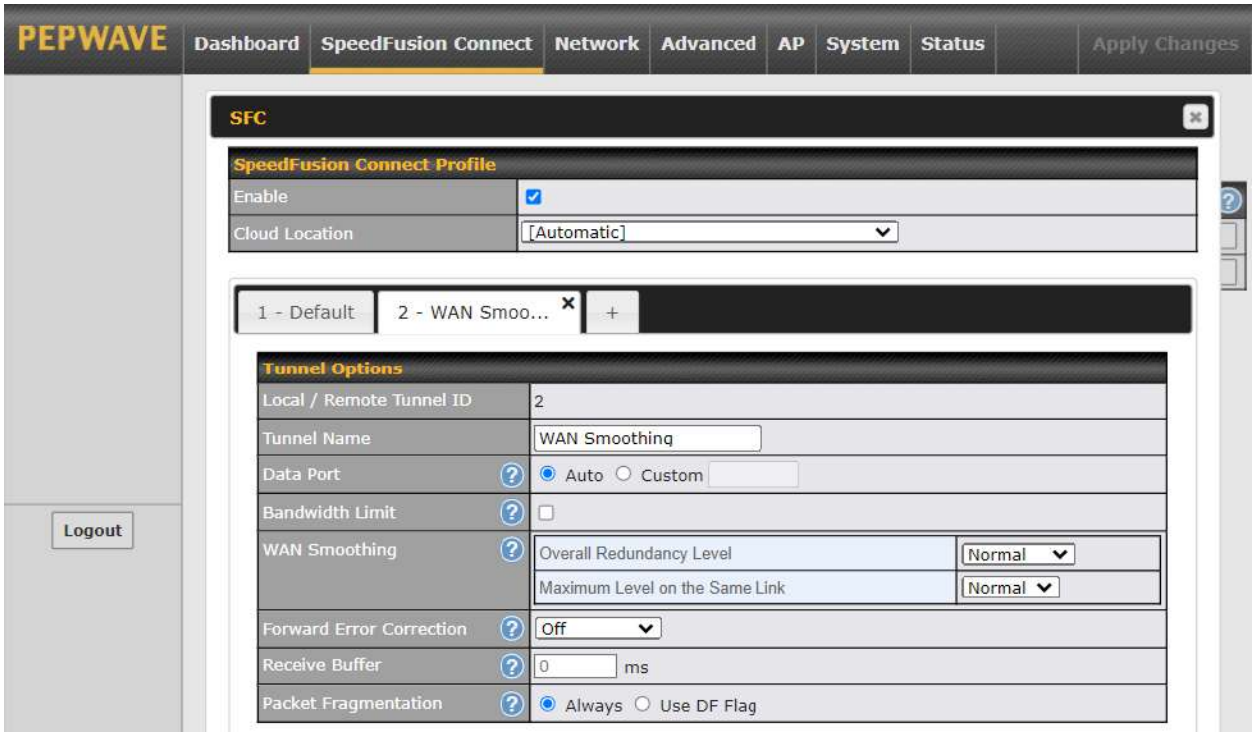


If you are running a latency sensitive service like video streaming or VOIP, a WAN Smoothing sub-tunnel can be created. Navigate to **Speedfusion Connect > Choose a cloud location > SFC**.

 Copyright @ 2021 Peplink

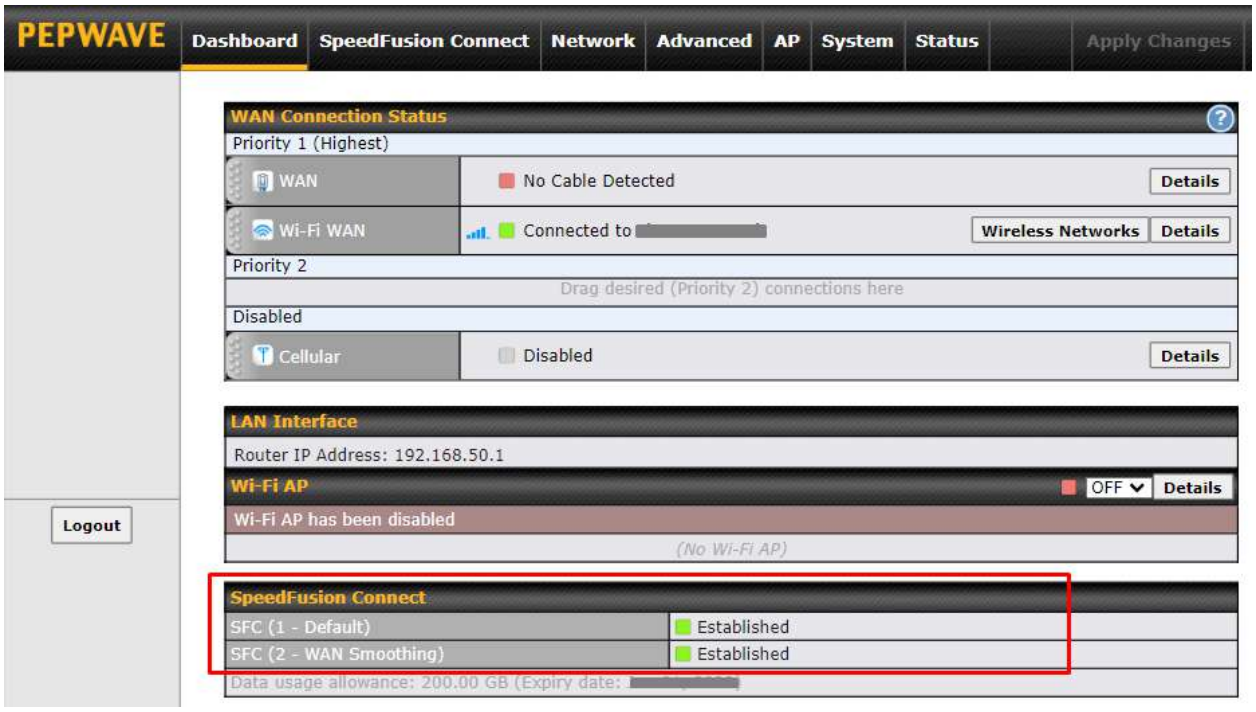
A SpeedFusion tunnel configuration window will pop out. Click on the **+** sign to create the WAN Smoothing sub-tunnel.





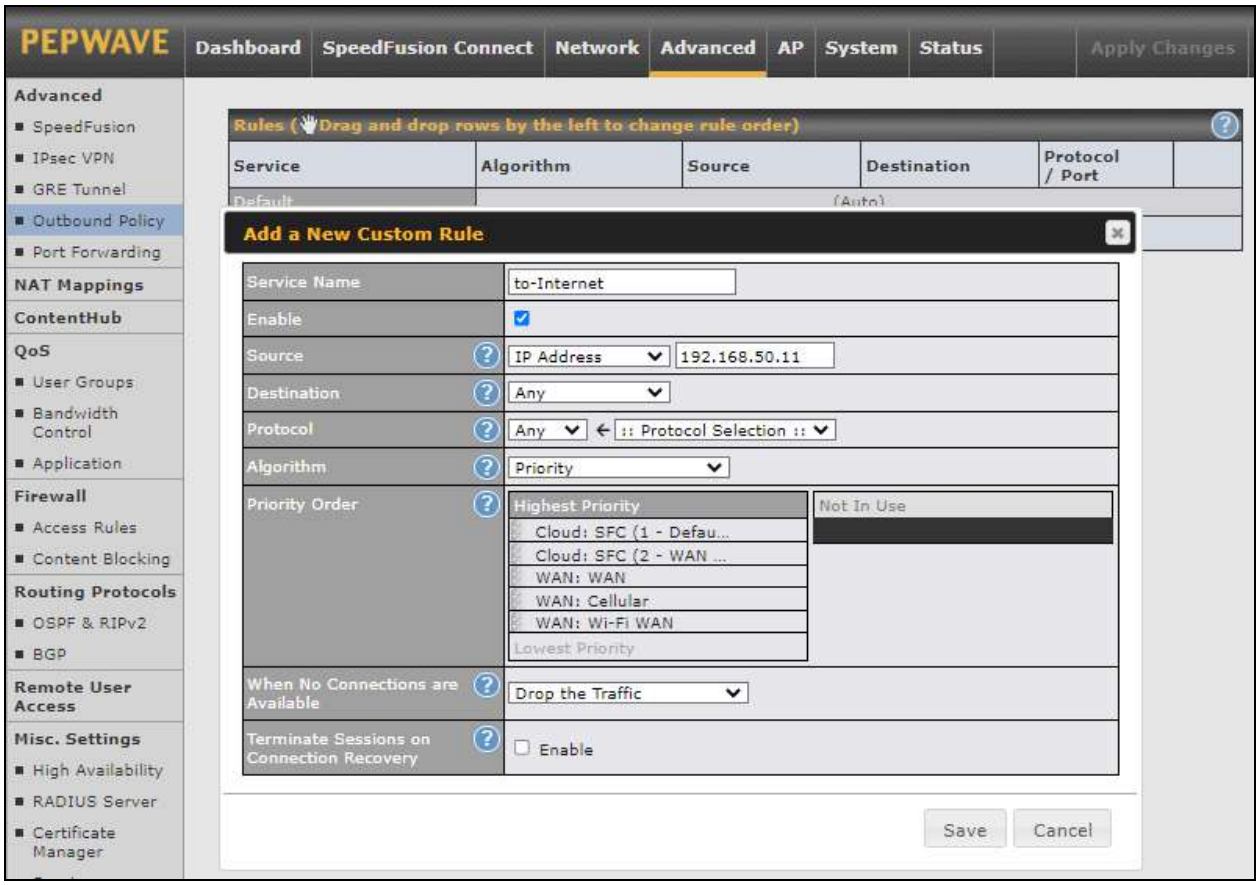
 Copyright @ 2021 Peplink

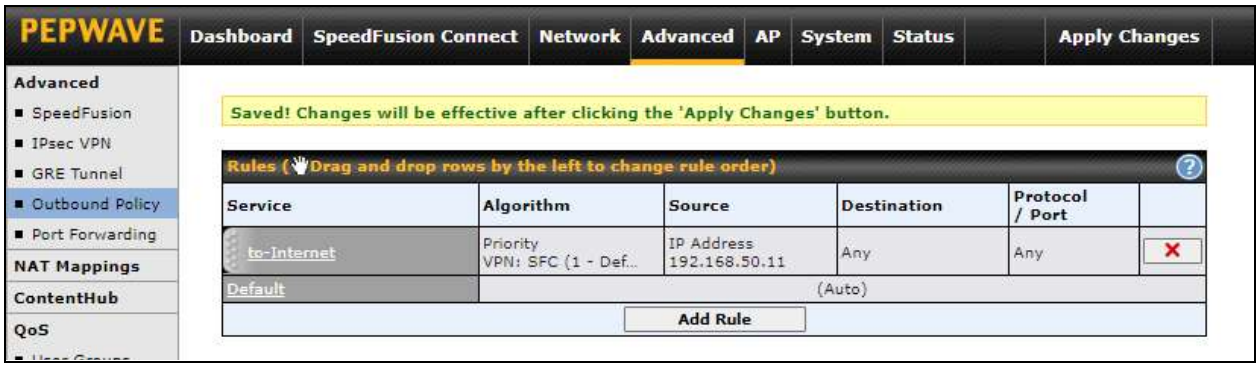
Click on **Save** and **Apply Changes** to save the configuration. Now, the router has 2 Speedfusion tunnels to the SpeedFusion Cloud.



 Copyright @ 2021 Peplink

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.

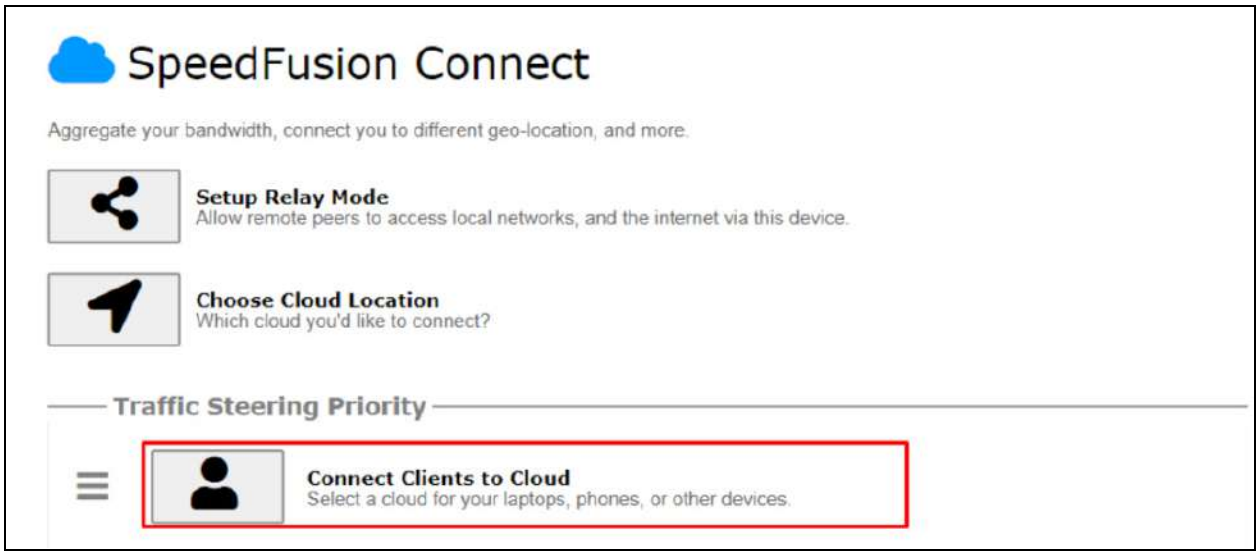




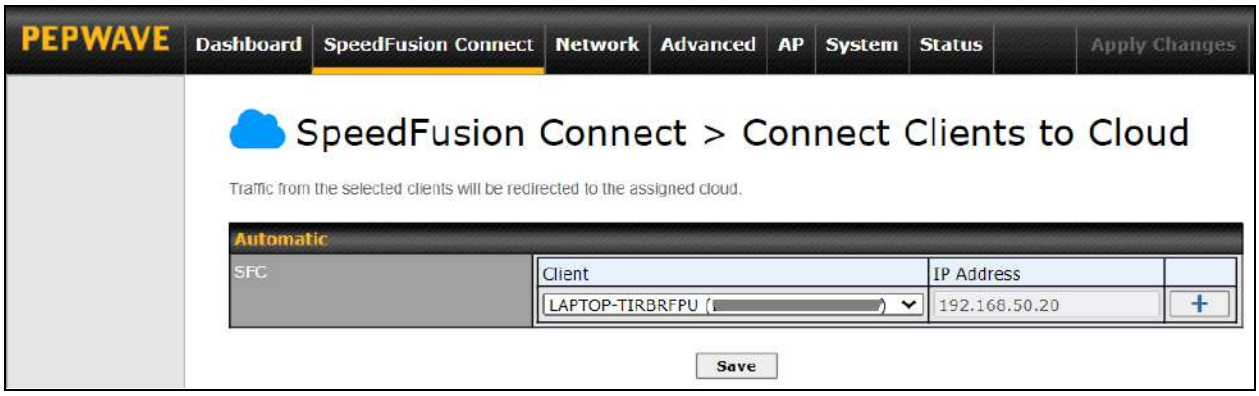
 Copyright @ 2021 Peplink

7.3 Connect Clients to Cloud

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



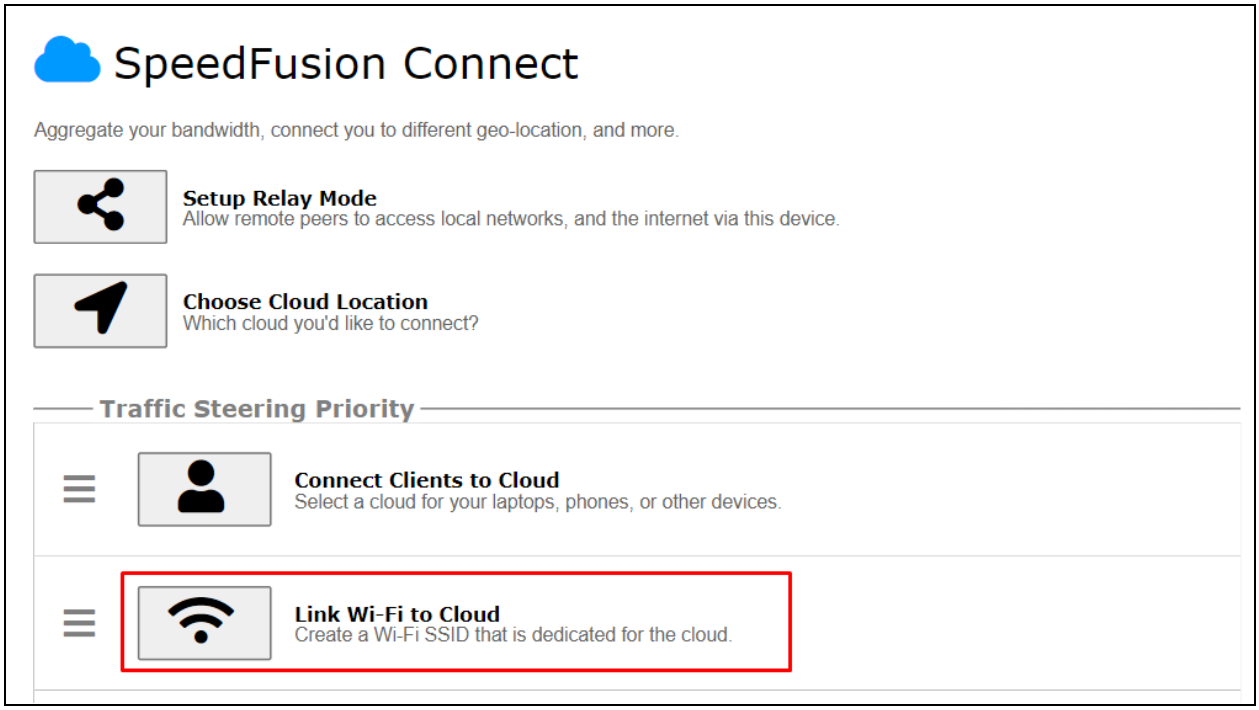
Choose a client from the drop down list > Click + > Save > Apply Changes.



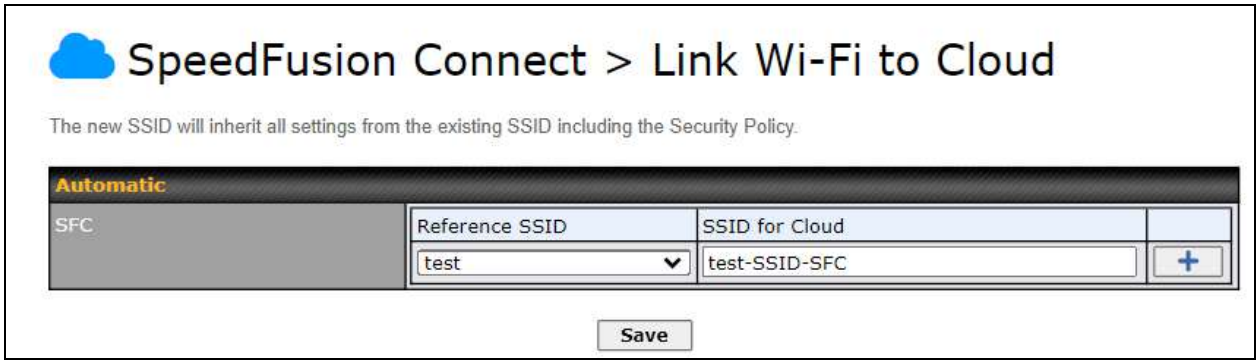
 Copyright @ 2021 Peplink

7.4 Link Wi-Fi to Cloud

SpeedFusion Connect provides a convenient way to route the Wi-Fi client to the cloud from **SpeedFusion Connect > Link Wi-Fi to Cloud**.

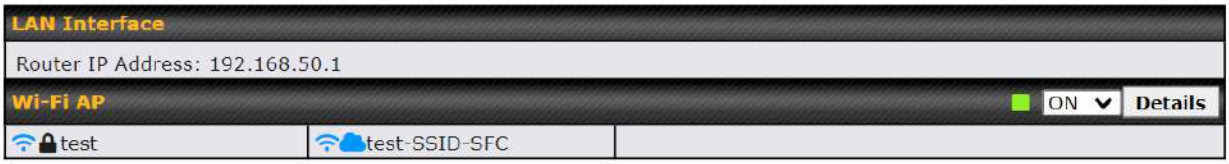


Create a new SSID for SpeedFusion Connect. The new SSID will inherit all settings from one of the existing SSIDs including the Security Policy. Then click **Save** followed by **Apply Changes**.



 Copyright @ 2021 Peplink

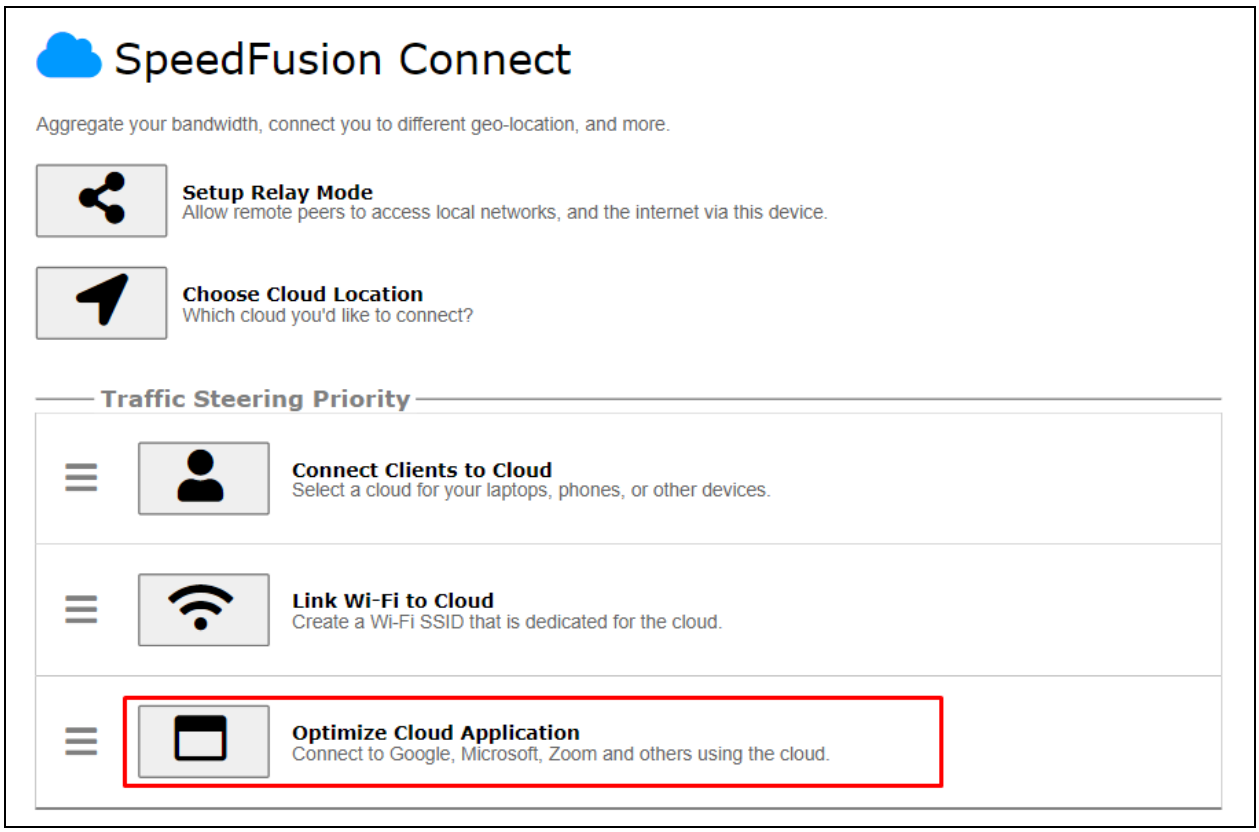
SpeedFusion Connect SSID will be shown on **Dashboard**.



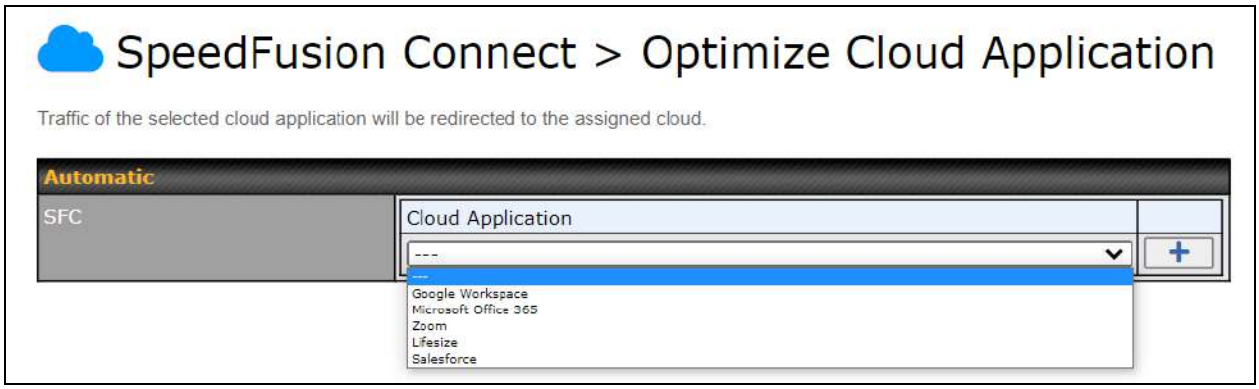
 Copyright @ 2021 Peplink

7.5 Optimize Cloud Application

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



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.

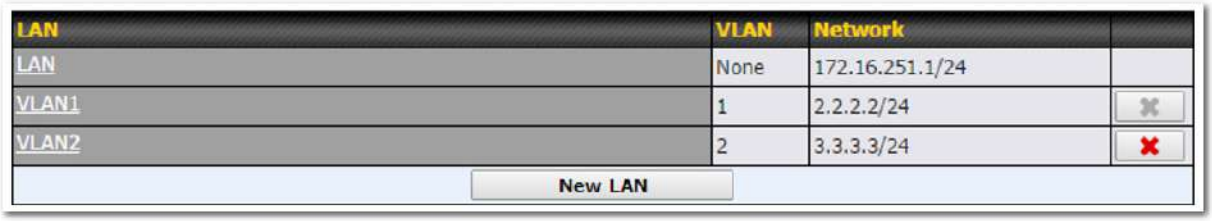


 Copyright @ 2021 Peplink

8 Configuring the LAN Interface(s)

8.1 Basic Settings

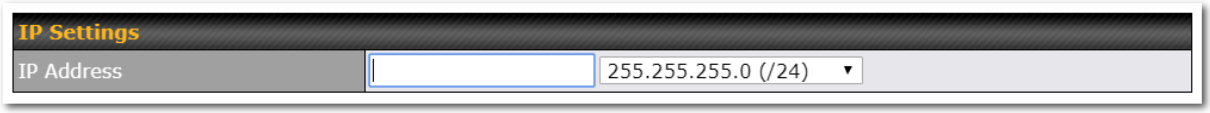
LAN interface settings are located at **Network>LAN>Network Settings**. Navigating to that page will show the following dashboard:



This represents the LAN interfaces that are active on your router (including VLAN). A gray "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 gray "X".

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

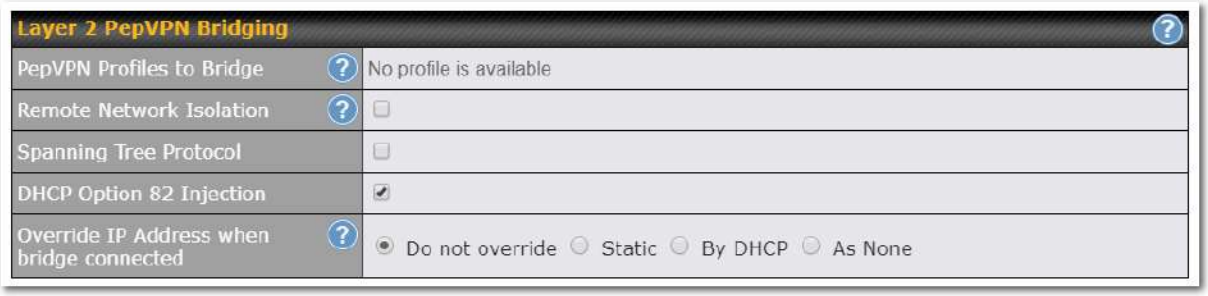
Clicking on any of the existing LAN interfaces (or creating a new one) will show the following :



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

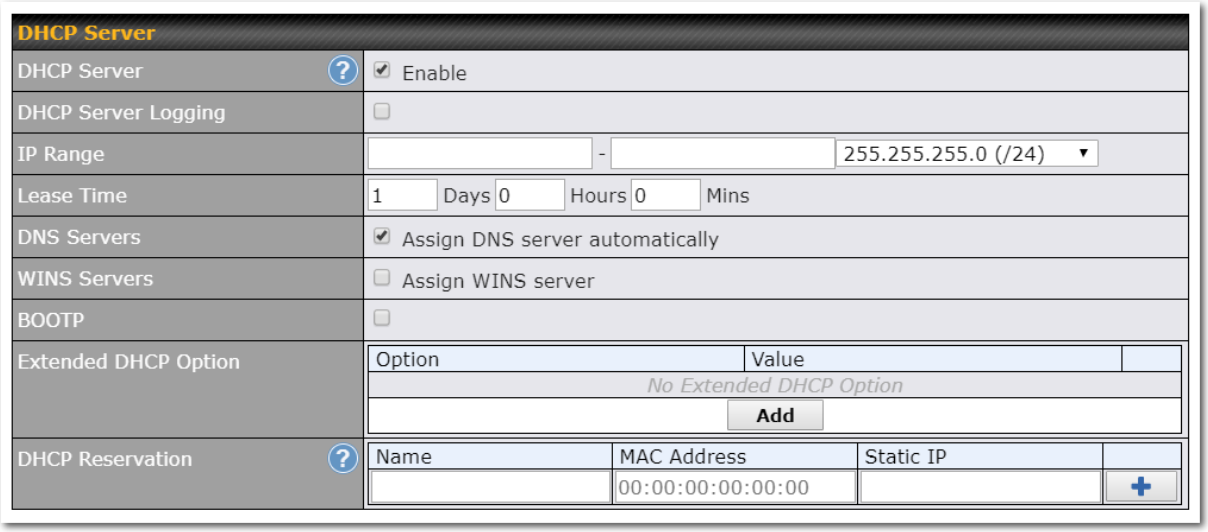
Network Settings	
Name	Enter a name for the LAN.
VLAN ID	Enter a number for your VLAN.
Inter-VLAN routing	Check this box to enable routing between virtual LANs.

 Copyright @ 2021 Peplink



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 the 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.

 Copyright @ 2021 Peplink

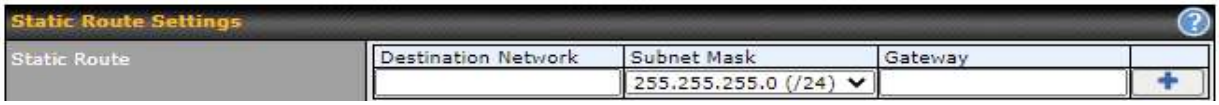


DHCP Server Settings	
DHCP Server	When this setting is enabled, the DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Pepwave router's DHCP server can prevent IP address collision on the LAN.
DHCP Server Logging	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™, 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

 Copyright @ 2021 Peplink

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

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



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

[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.

 Copyright @ 2021 Peplink

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.

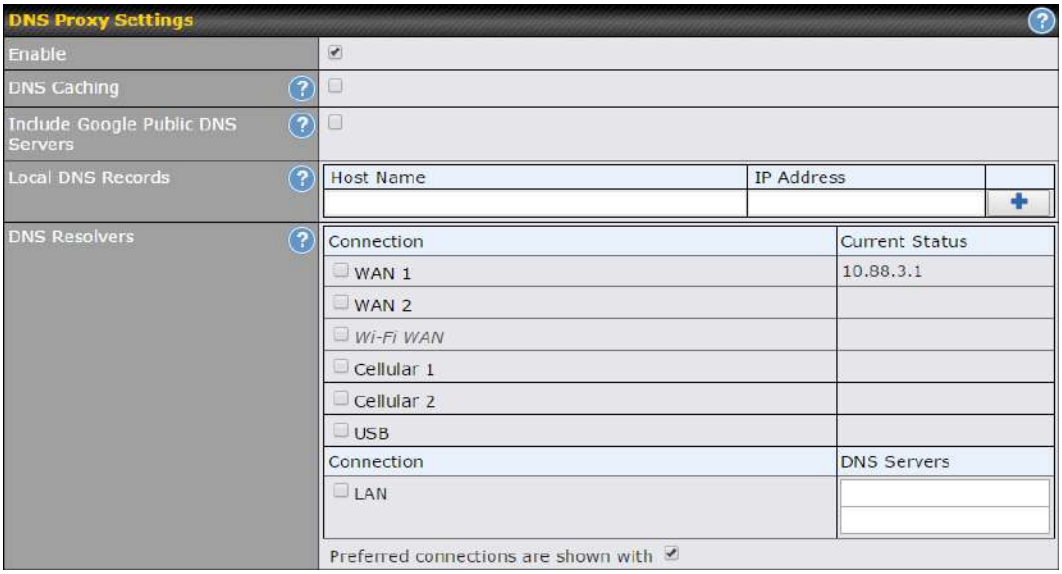
For further details on virtual network mapping watch this video:

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

 Copyright @ 2021 Peplink



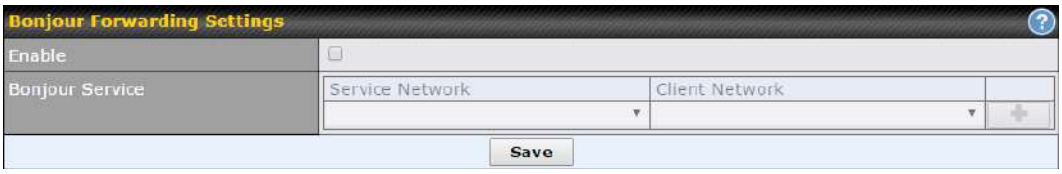
DNS Proxy Settings	
Enable	To enable the DNS proxy feature, check this box, and then set up the feature at **Network>LAN>DNS Proxy Settings**. A DNS proxy server can be enabled to serve DNS requests originating from LAN/PPTP/SpeedFusion™ peers. Requests are forwarded to the **DNS servers/resolvers**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

 Copyright @ 2021 Peplink

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

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

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



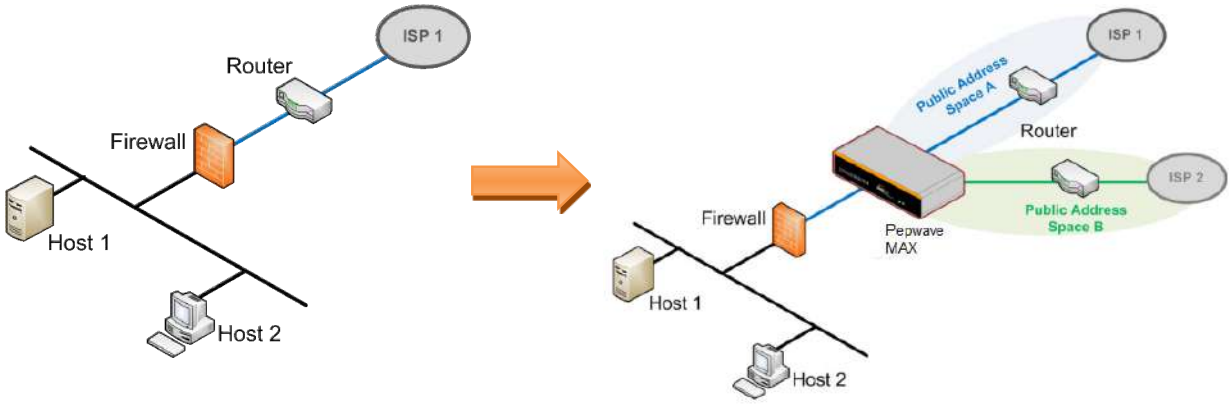
Bonjour Forwarding Settings	
Enable	Check this box to turn on Bonjour forwarding.
Bonjour Service	Choose **Service** and **Client** networks from the drop-down menus, and then click + to add the networks. To delete an existing Bonjour listing, click ✖.

 Copyright @ 2021 Peplink

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:



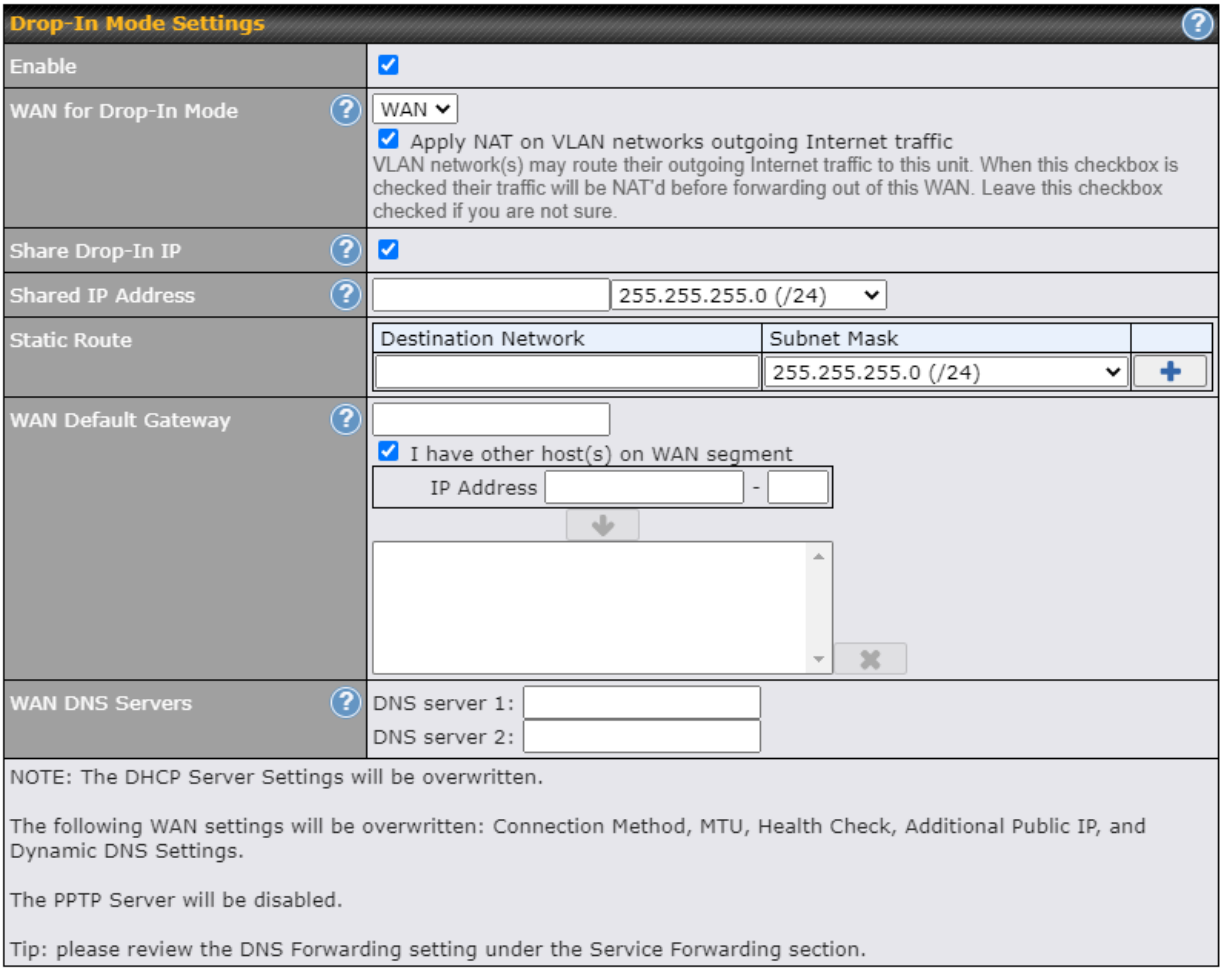
Check the box Enable to enable the Drop-in Mode. After enabling this feature and selecting the WAN for Drop-in mode, various settings including the WAN's connection method and IP address will be automatically updated.

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.

 Copyright @ 2021 Peplink



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

 Copyright @ 2021 Peplink

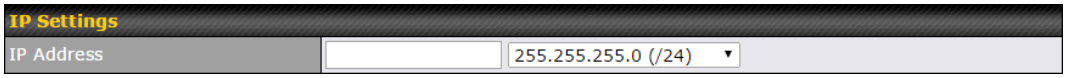
Address[A]	not serving the service being accessed. The shared IP address will be used in connecting to hosts on the WAN (e.g., email notification, remote syslog, etc.) The device will also listen on the IP address when hosts on the WAN access services served on this device (e.g., web admin accesses from 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.

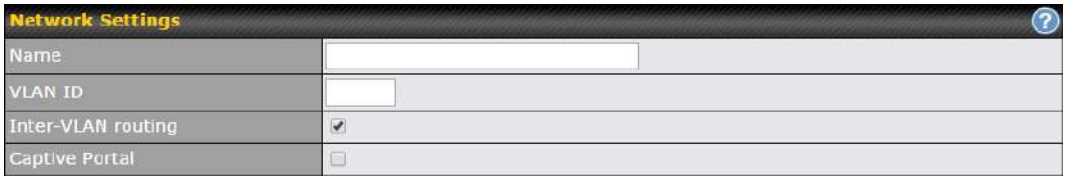
To add a new LAN, click the **New LAN** button. To change LAN settings, click the name of the LAN to change under the **LAN** heading.

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

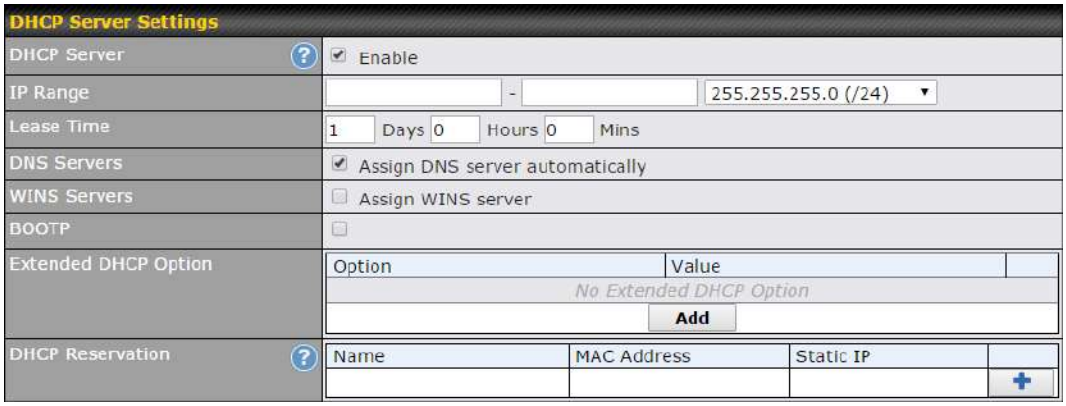


IP Settings	
IP Address & Subnet Mask	Enter the Pepwave router's IP address and subnet mask values to be used on the LAN.

 Copyright @ 2021 Peplink



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.

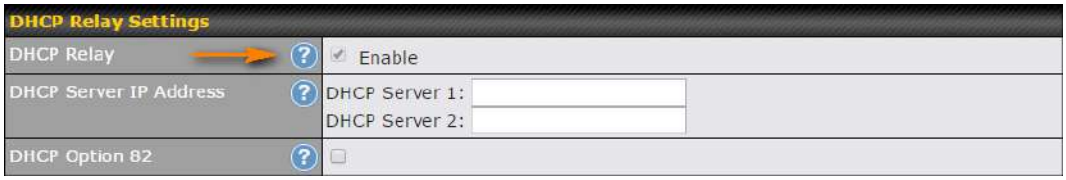


DHCP Server Settings	
DHCP Server	When this setting is enabled, the Pepwave router's DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Pepwave router's DHCP server can prevent IP address collisions on the LAN. 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.

 Copyright @ 2021 Peplink

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

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



DHCP Relay Settings	
Enable	Check this box to turn on DHCP relay. Click the icon to disable DHCP relay.
DHCP Server IP	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

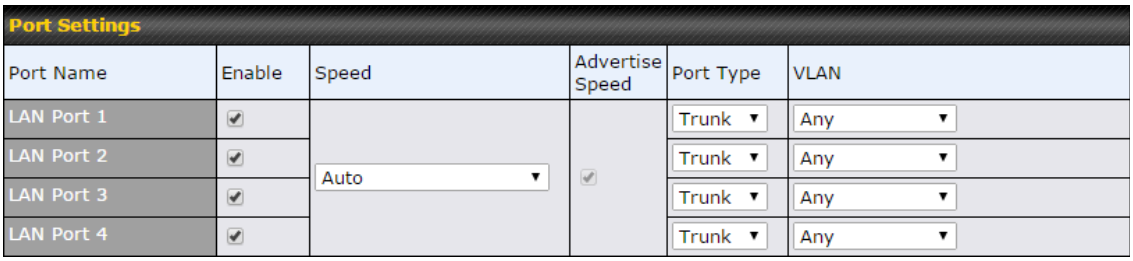
 Copyright @ 2021 Peplink

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**

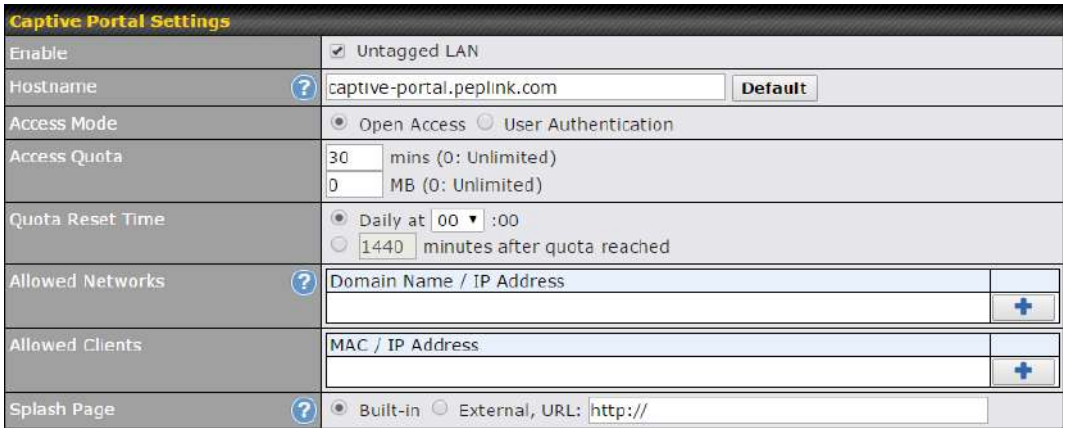


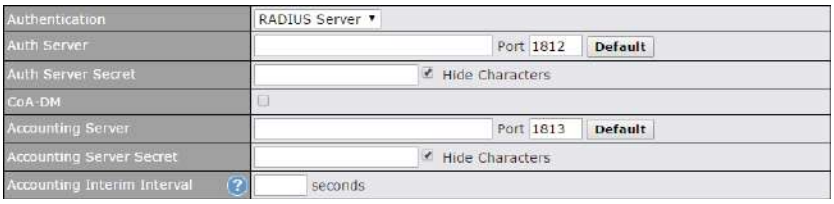
On this screen, you can enable specific ports, as well as determine the speed of the LAN ports, whether each port is a trunk or access port, can well as which VLAN each link belongs to, if any.

 Copyright @ 2021 Peplink

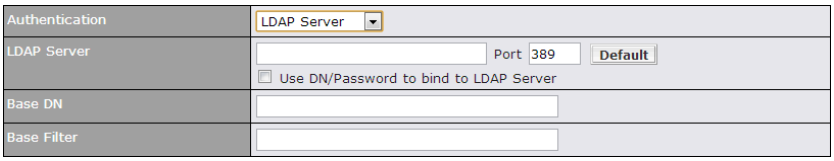
8.3 Captive Portal

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**.



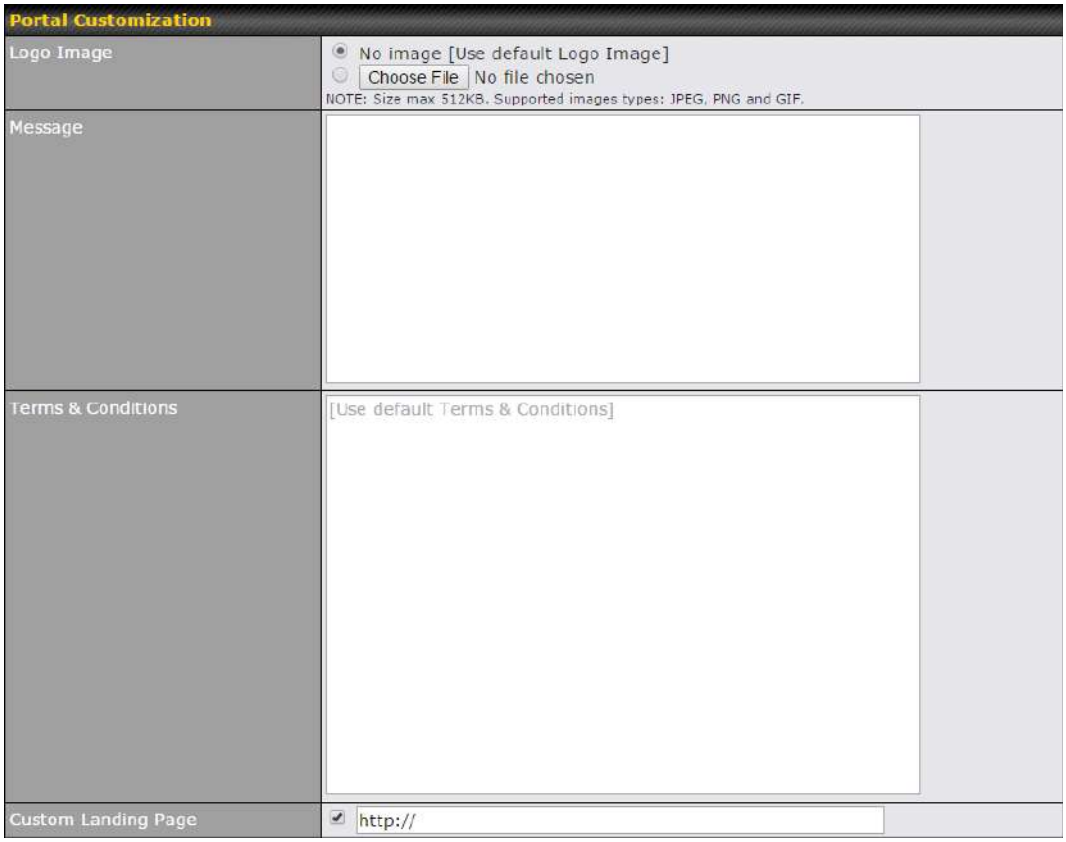
Captive Portal Settings	
Enable	Check **Enable** and then, optionally, select the LANs/VLANs that will use the captive portal.
Hostname	To customize the portal's form submission and redirection URL, enter a new URL in this field. To reset the URL to factory settings, click **Default**.
Access Mode	Click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

 Copyright @ 2021 Peplink

	 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:

 Copyright @ 2021 Peplink

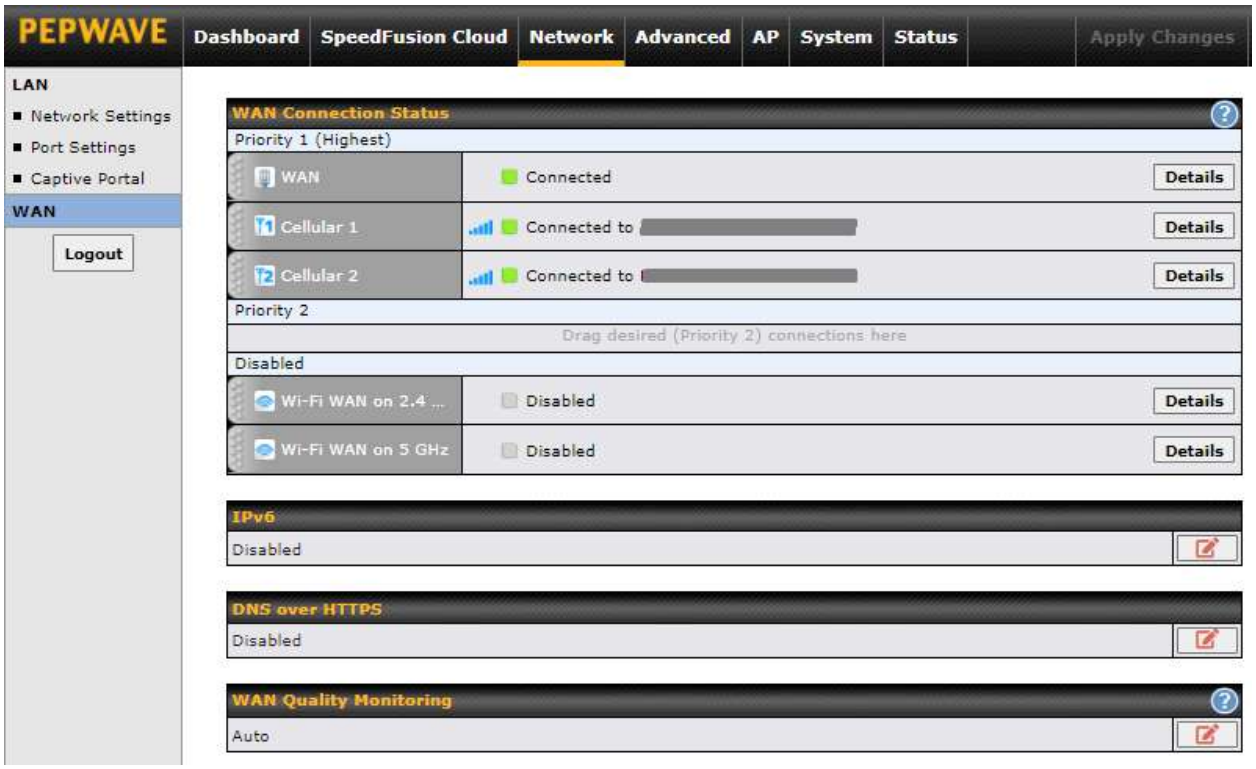


Portal Customization	
Logo Image	Click the **Choose File** button to select a logo to use for the built-in portal.
Message	If you have any additional messages for your users, enter them in this field.
Terms & Conditions	If you would like to use your own set of terms and conditions, please enter them 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.

 Copyright @ 2021 Peplink

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.



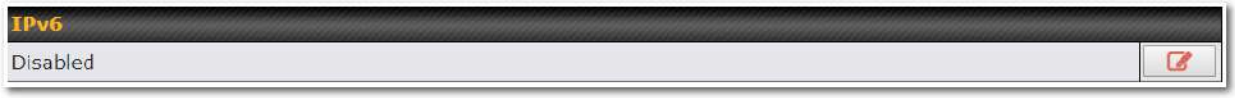
To able a particular WAN connection, drag on the appropriate WAN by holding the left mouse button, move it the **Disabled** row, and drop it by releasing the mouse button.

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.

 Copyright @ 2021 Peplink

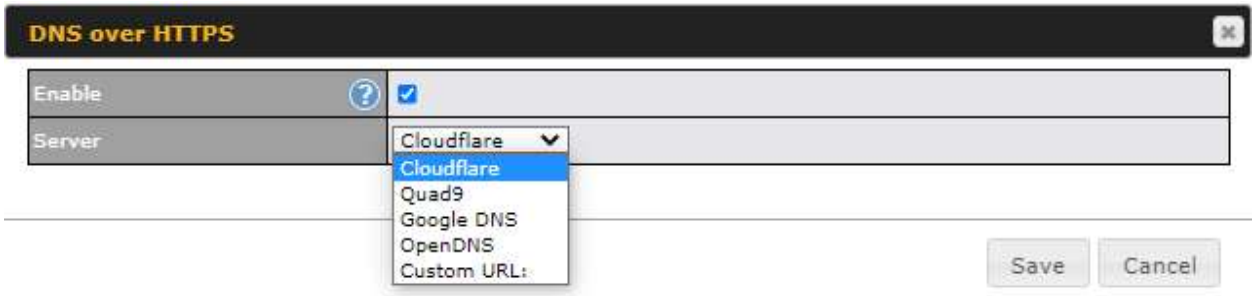
IPv6



You can also enable IPv6 support in this section.

DNS over HTTPS (DoH)

You can enable DoH (DNS over HTTPS) support in this section.



DNS over HTTPS	
Enable	When this option is enabled, the DNS proxy server will use HTTPS connections to forward DNS requests to the DoH resolver; it will not fallback to traditional UDP DNS options.
Server	The options to configure DoH with a predefined server are: • Cloudflare - The DNS server IP addresses for **Cloudflare** will be using 1.1.1.1, which is unfiltered. • Quad9 - The DNS server IP addresses for **Quad9** will be using 9.9.9.9 and 142.112.112.112, which is malware blocking and DNSSEC. • Google DNS - The DNS server IP addresses for **Google DNS** will be using 8.8.8.8 and 8.8.4.4, which is RFC8484 standard. • OpenDNS - The DNS server IP addresses for **OpenDNS** will be using 208.67.222.222 and 208.67.220.220, which is standard DNS. • Custom URL - You may select **Custom URL:**, and enter the **resolver URL** and **IP address**.

 Copyright @ 2021 Peplink

WAN Quality Monitoring

This settings advice how WAN Quality information is being gathered.

By default, WAN Quality will always be observed and gathered automatically. With customized choice of WAN connections, the device will always observe WAN Quality of those selected WAN connections. Other WAN connections may stop observing WAN Quality information if it is not necessary for the underlying features.

 Copyright @ 2021 Peplink

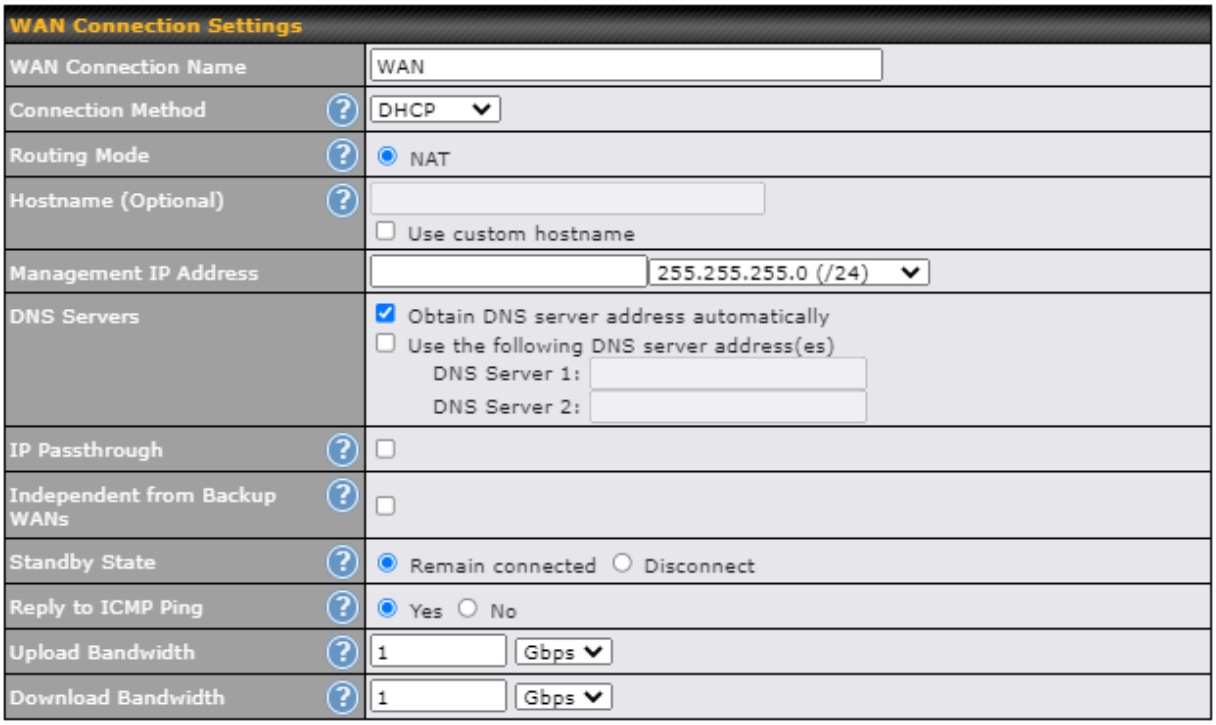
9.1 Ethernet WAN

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.).



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.

 Copyright @ 2021 Peplink

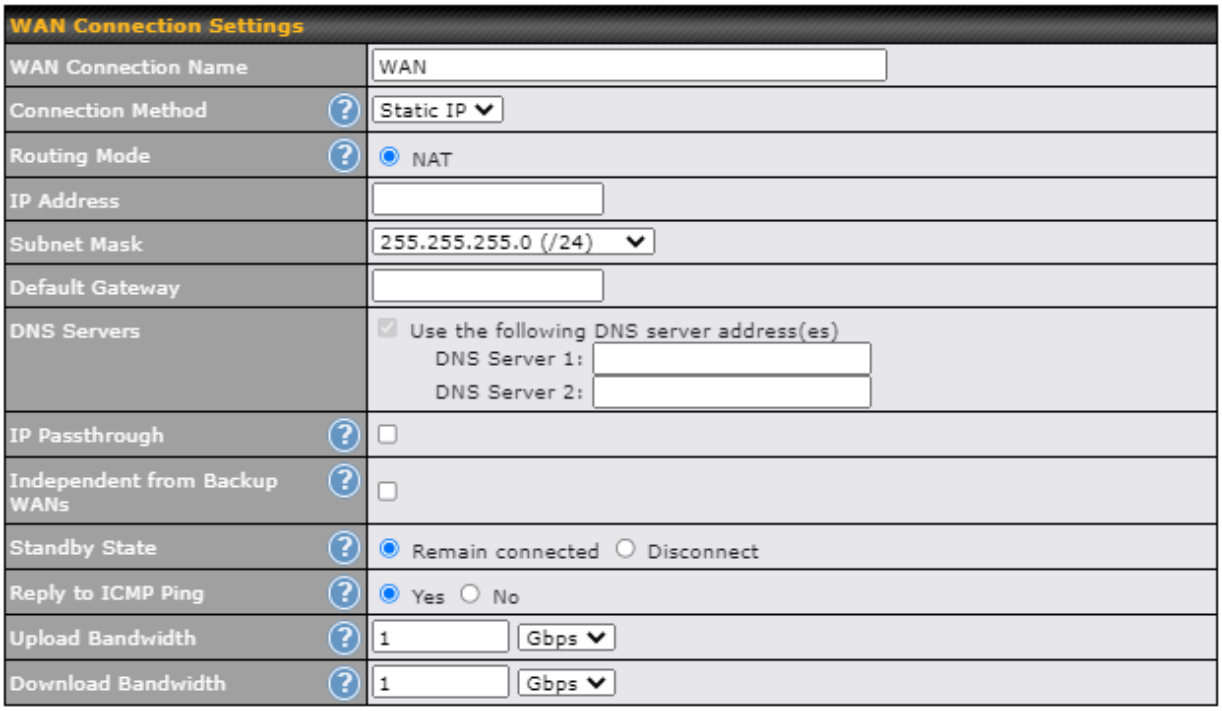
Management IP Address	**Management IP Address** is available for configuration when you click the link in the help icon via the Hostname. This option allows you to configure the management IP address for the DHCP WAN connection.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This 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

 Copyright @ 2021 Peplink

	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.



 Copyright @ 2021 Peplink

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.

 Copyright @ 2021 Peplink

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

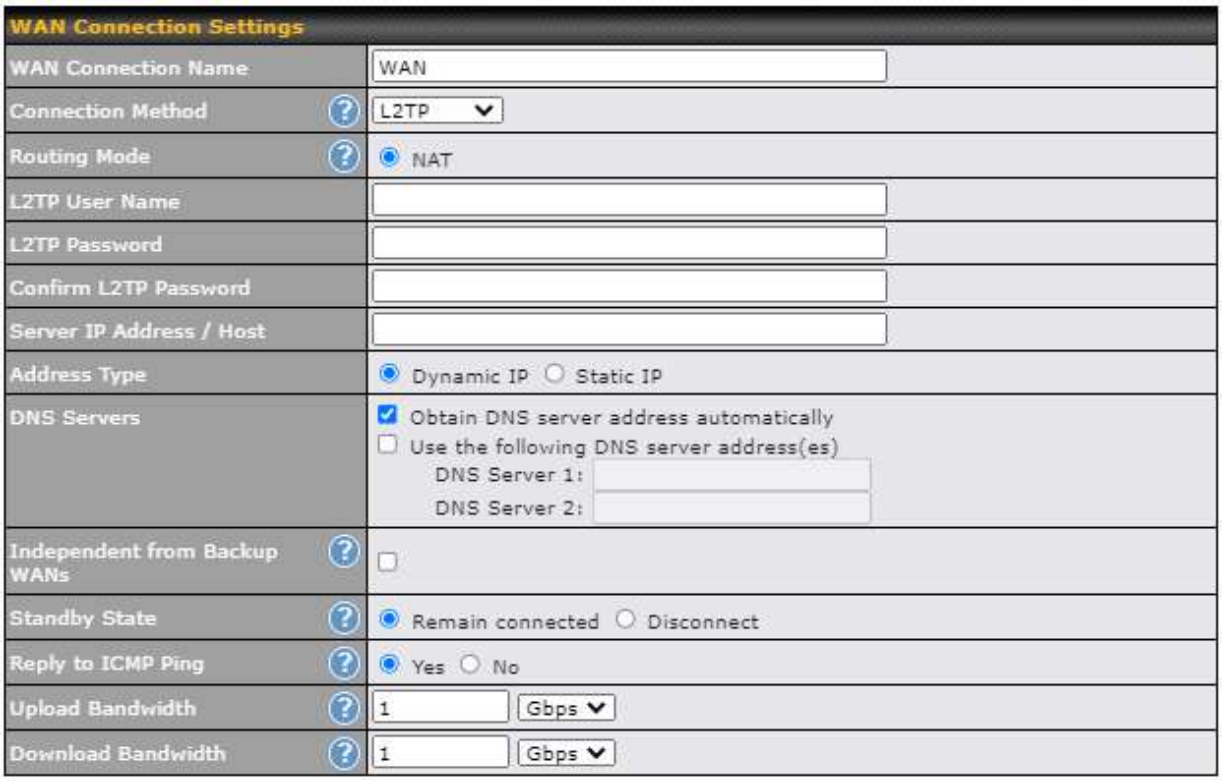
PPPoE Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the **IP Forwarding** option, if your network requires it.
PPPoE Username / Password	Enter the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

 Copyright @ 2021 Peplink

(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.



 Copyright @ 2021 Peplink

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.

 Copyright @ 2021 Peplink

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.

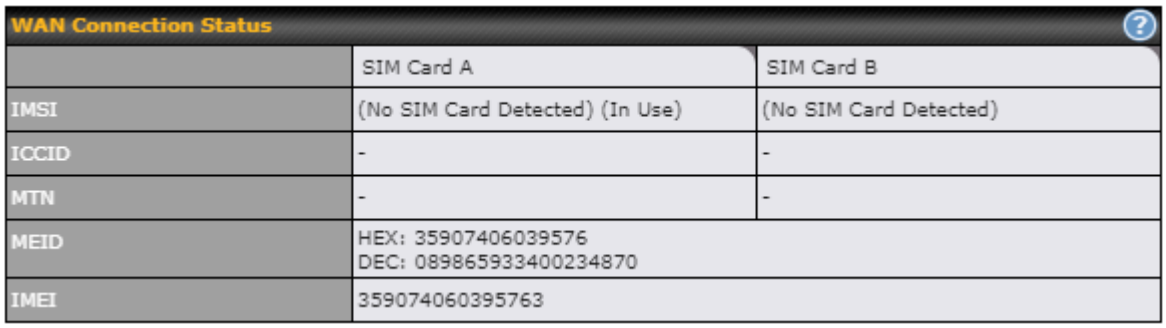
 Copyright @ 2021 Peplink

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.

 Copyright @ 2021 Peplink

9.2 Cellular WAN

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

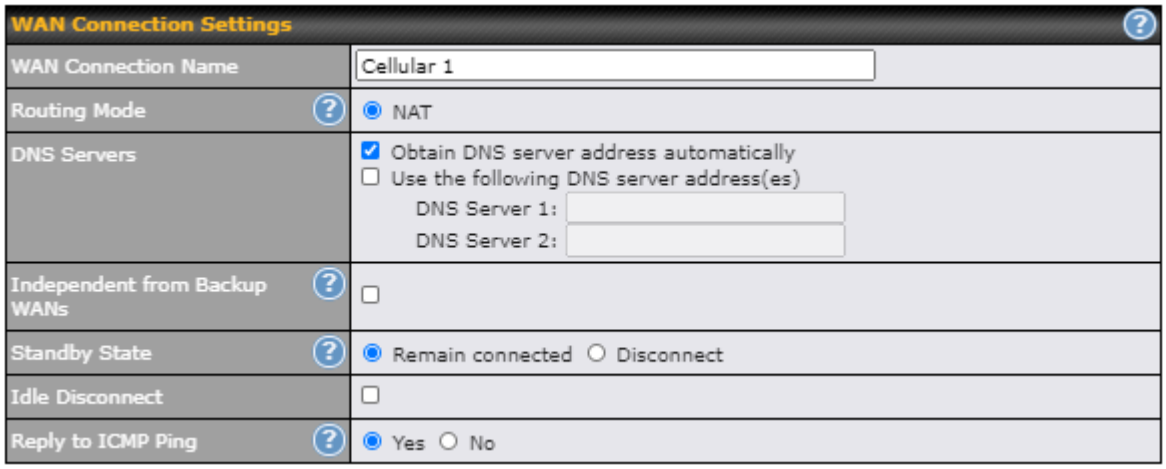


WAN Connection Status

	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.

 Copyright @ 2021 Peplink



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.

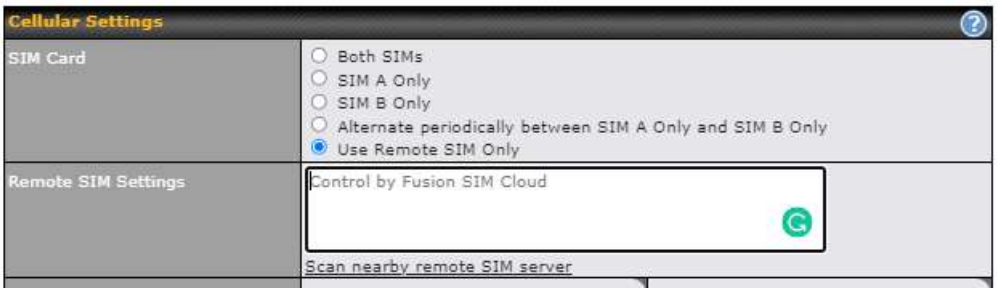
 Copyright @ 2021 Peplink

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

 Copyright @ 2021 Peplink

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.  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**.

 Copyright @ 2021 Peplink

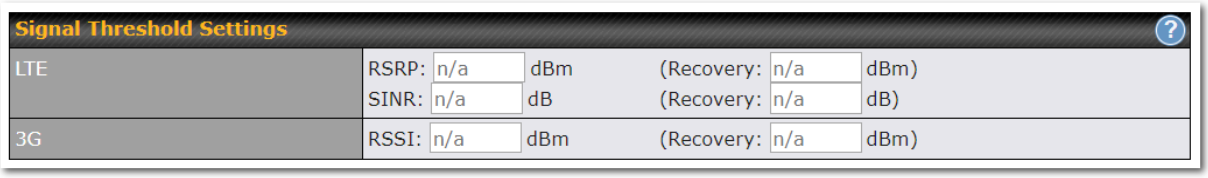
APN / Login / Password / SIM PIN	When **Auto** is selected, the information in these fields will be filled automatically. Select **Custom** to customize these parameters. The parameter values are determined by and can be obtained from the ISP.
Bandwidth Allowance Monitor	Check the box Enable to enable 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.



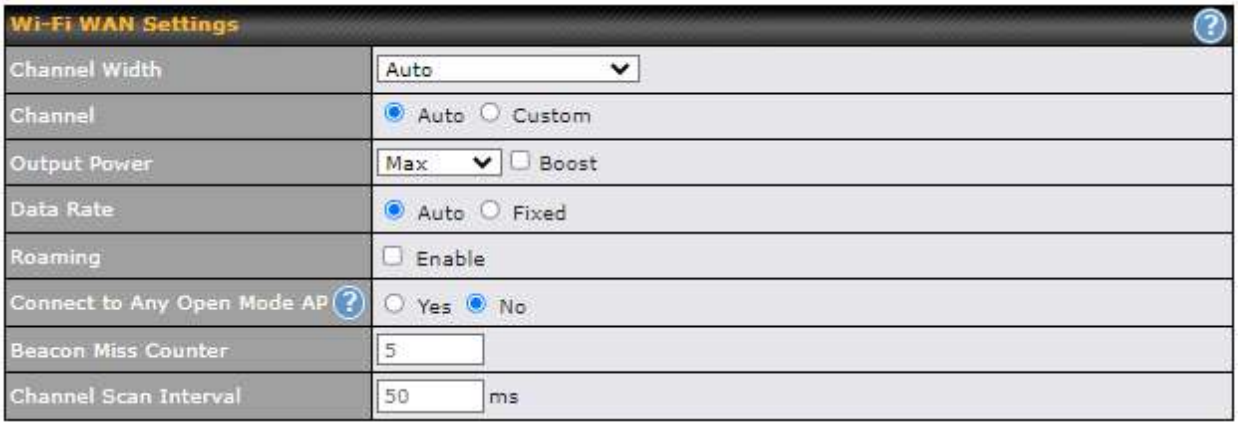
 Copyright @ 2021 Peplink

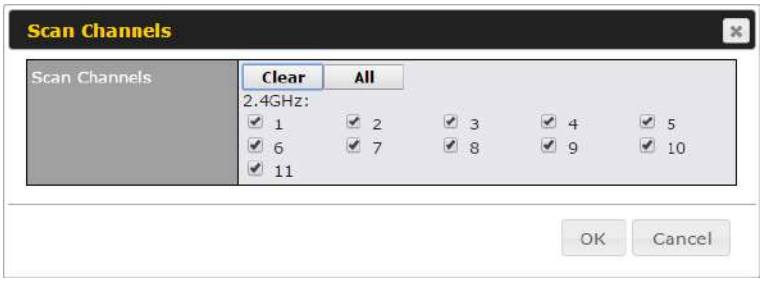
9.3 Wi-Fi WAN

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

WAN Connection Settings	
WAN Connection Name	Enter a name to represent this WAN connection.
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.

 Copyright @ 2021 Peplink

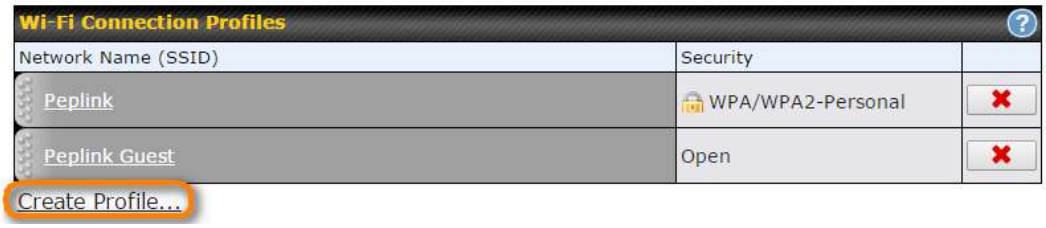


Wi-Fi WAN Settings	
Channel Width	Select the channel width for this Wi-Fi WAN. 20MHz will have greater support for older devices using 2.4Ghz, while 40MHz is appropriate for networks with newer devices that connect using 5Ghz
Channel	Determine whether the channel will be automatically selected. If you select custom, the following table will appear: 
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.
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.
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.
Channel Scan Interval	Configure Channel Scan Interval in ms.

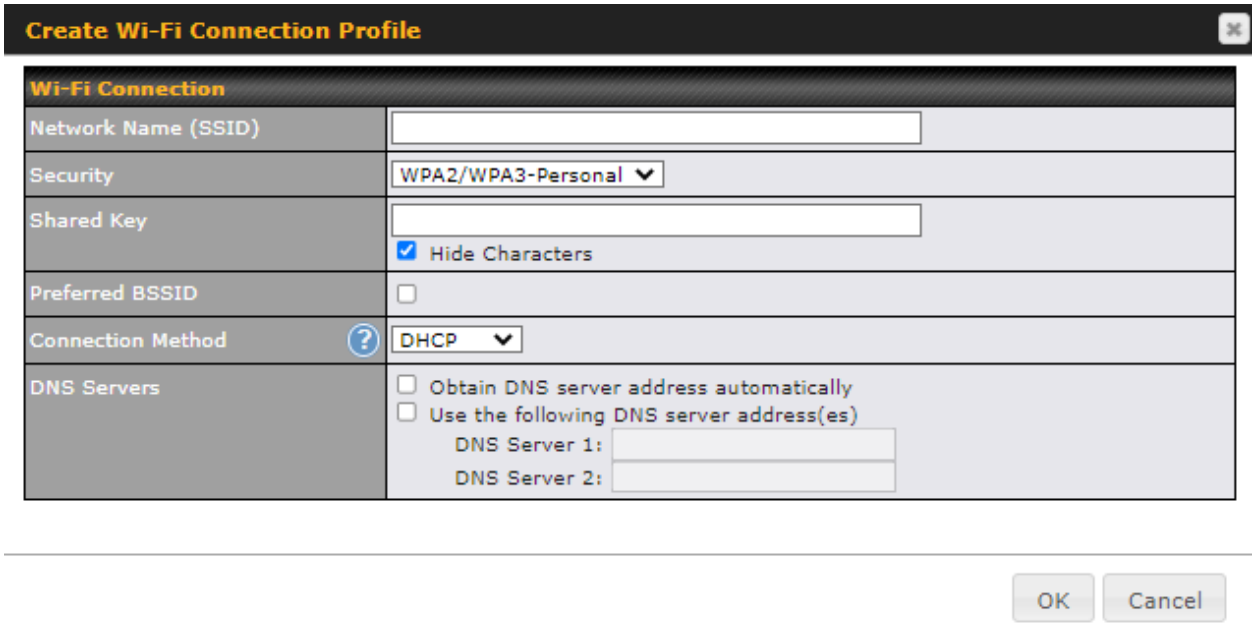
 Copyright @ 2021 Peplink

9.3.1 Creating Wi-Fi Connection Profiles

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



This will open a window similar to the one shown below



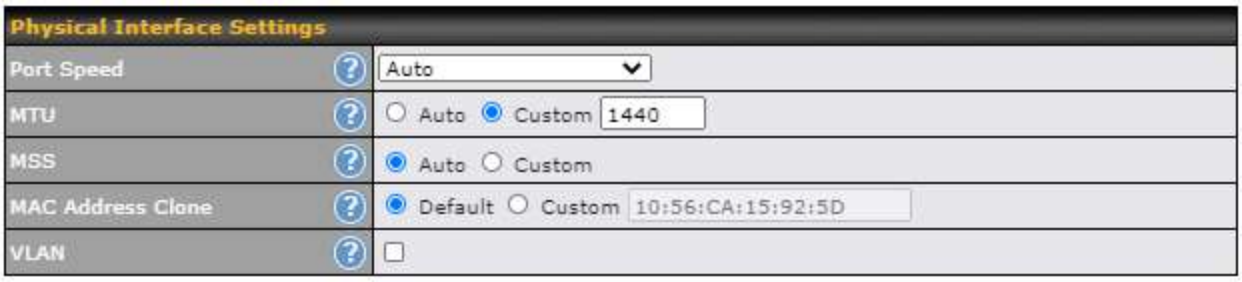
Wi-Fi Connection Profile Settings	
Type	Select whether the network will connect automatically or manually.
Network Name (SSID)	Enter a name to represent this Wi-Fi connection.

 Copyright @ 2021 Peplink

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**
Shared Key	Enter the password for the wireless network.
Preffered BSSID	Configure the BSSID. The BSSID is the MAC address of the wireless access point (WAP).
Connected Method	Choose DHCP or Static IP.
DNS Servers	Configure the DNS servers that this WAN connection should use.

9.4 WAN Connection Settings (Common)

The remaining WAN-related settings are common to the WAN connection:



Physical Interface Settings	
Speed	This is the port speed of the WAN connection. It should be set to the same speed as the connected device in case of any port negotiation problems. When a static speed is set, you may choose whether to advertise its speed to the peer device or not. Advertise Speed is selected by default. You can choose not to advertise the port speed if the port has difficulty in negotiating with the peer device. Default: Auto

 Copyright @ 2021 Peplink

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. Default value is 1440.
MSS	This field is for specifying the Maximum Segment Size of the WAN connection. When Auto is selected, MSS will be depended on the MTU value. When Custom is selected, you may enter a value for MSS. This value will be announced to remote TCP servers for maximum data that it can receive during the establishment of TCP connections. Some Internet servers are unable to listen to MTU setting if ICMP is filtered by firewall between the connections. Normally, MSS equals to MTU minus 40. You are recommended to reduce the MSS only if changing of the MTU value cannot effectively inform some remote servers to size down data size. Default: Auto
MAC Address Clone	Some service providers (e.g. cable network) identify the client's MAC address and require client to always use the same MAC address to connect to the network. If it is the case, you may change the WAN interface's MAC address to the client PC's one by entering the PC's MAC address to this field. If you are not sure, click the Default button to restore to the default value.
VLAN	Check the box to assign a VLAN to the interface.

9.5 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	
	
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.	

 Copyright @ 2021 Peplink

Health Check Method: PING

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

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

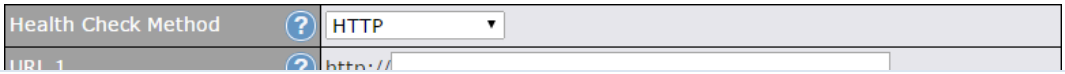
Health Check Method: DNS Lookup

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

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.

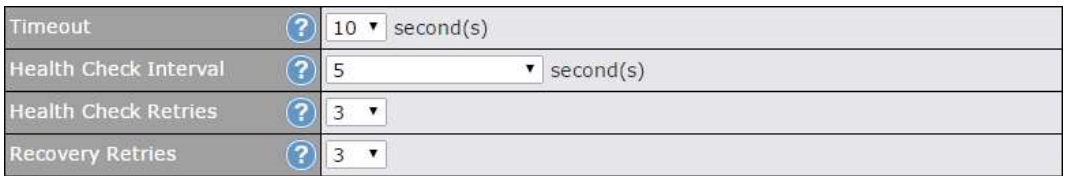
Health Check Method: HTTP

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



 Copyright @ 2021 Peplink

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

Automatic Public DNS Server Check on DNS Test Failure

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

 Copyright @ 2021 Peplink

⚠ **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.**

9.6 Bandwidth Allowance Monitoring

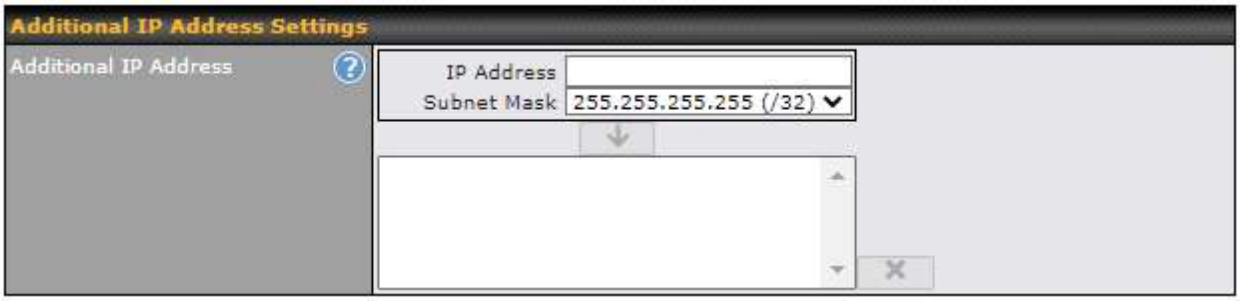
Bandwidth Allowance Monitor	
Bandwidth Allowance Monitor	☑ Enable
Action	Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling Email Notification. ☑ Disconnect when usage hits 100% of monthly allowance
Start Day	On 1st of each month at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

Bandwidth Allowance Monitor	
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.

Disclaimer
Due to different network protocol overheads and conversions, the amount of data reported by this Peplink device is not representative of actual billable data usage as metered by your network provider. Peplink disclaims any obligation or responsibility for any events arising from the use of the numbers shown here.

 Copyright @ 2021 Peplink

9.7 Additional Public IP address



Additional Public IP Settings	
IP Address List	**IP Address List** represents the list of fixed Internet IP addresses assigned by the ISP in the event that more than one Internet IP address is assigned to this WAN connection. Enter the fixed Internet IP addresses and the corresponding subnet mask, and then click the **Down Arrow** button to populate IP address entries to the **IP Address List**.

9.8 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**.

 Copyright @ 2021 Peplink

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

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

Important Note

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

 Copyright @ 2021 Peplink

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	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.

 Copyright @ 2021 Peplink

	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**.

 Copyright @ 2021 Peplink

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**.

 Copyright @ 2021 Peplink

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.

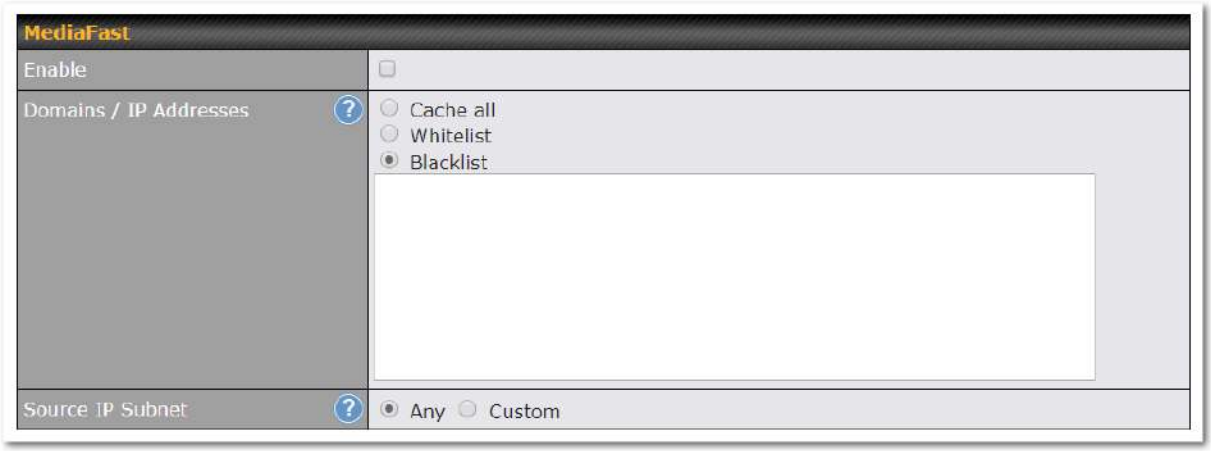
 Copyright @ 2021 Peplink

11 MediaFast Configuration

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

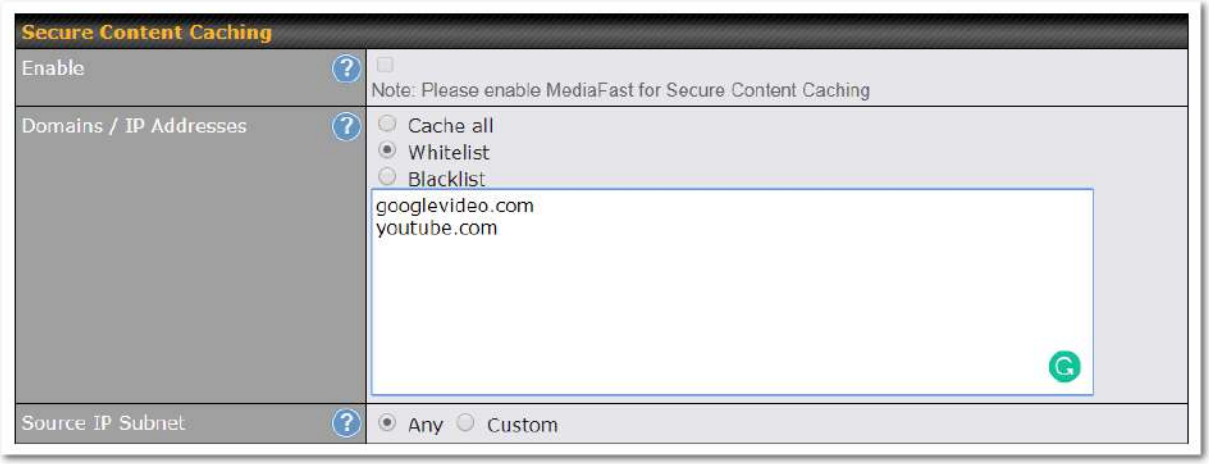
11.1 Setting Up MediaFast Content Caching

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



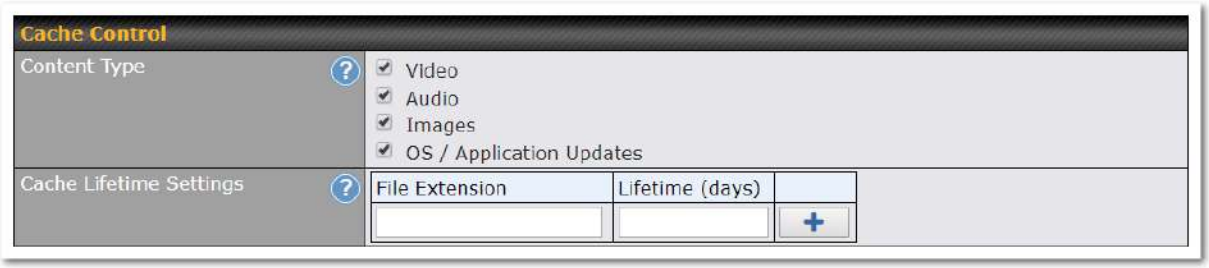
MediaFast	
Enable	Click the checkbox to enable MediaFast content caching.
Domains / IP Addresses	Choose to **Cache on all domains**, or enter domain names and then choose either **Whitelist** (cache the specified domains only) or **Blacklist** (do not cache the specified domains).
Source IP Subnet	This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

 Copyright @ 2021 Peplink



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

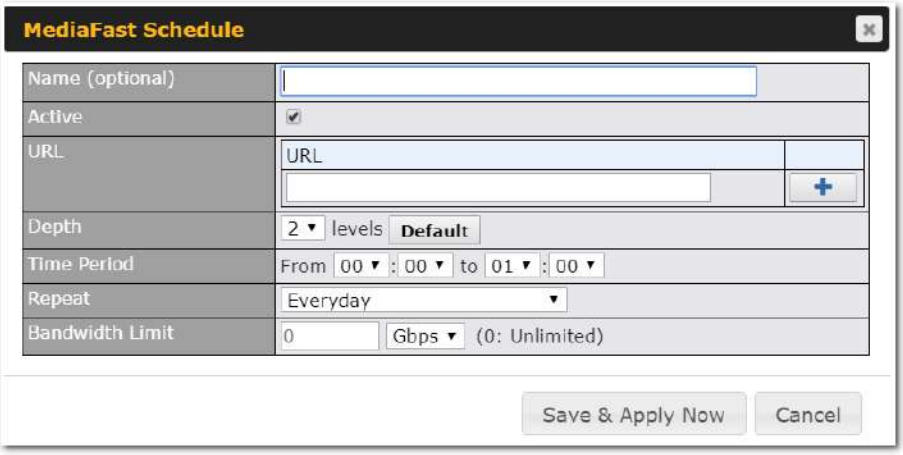
 Copyright @ 2021 Peplink

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 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 .

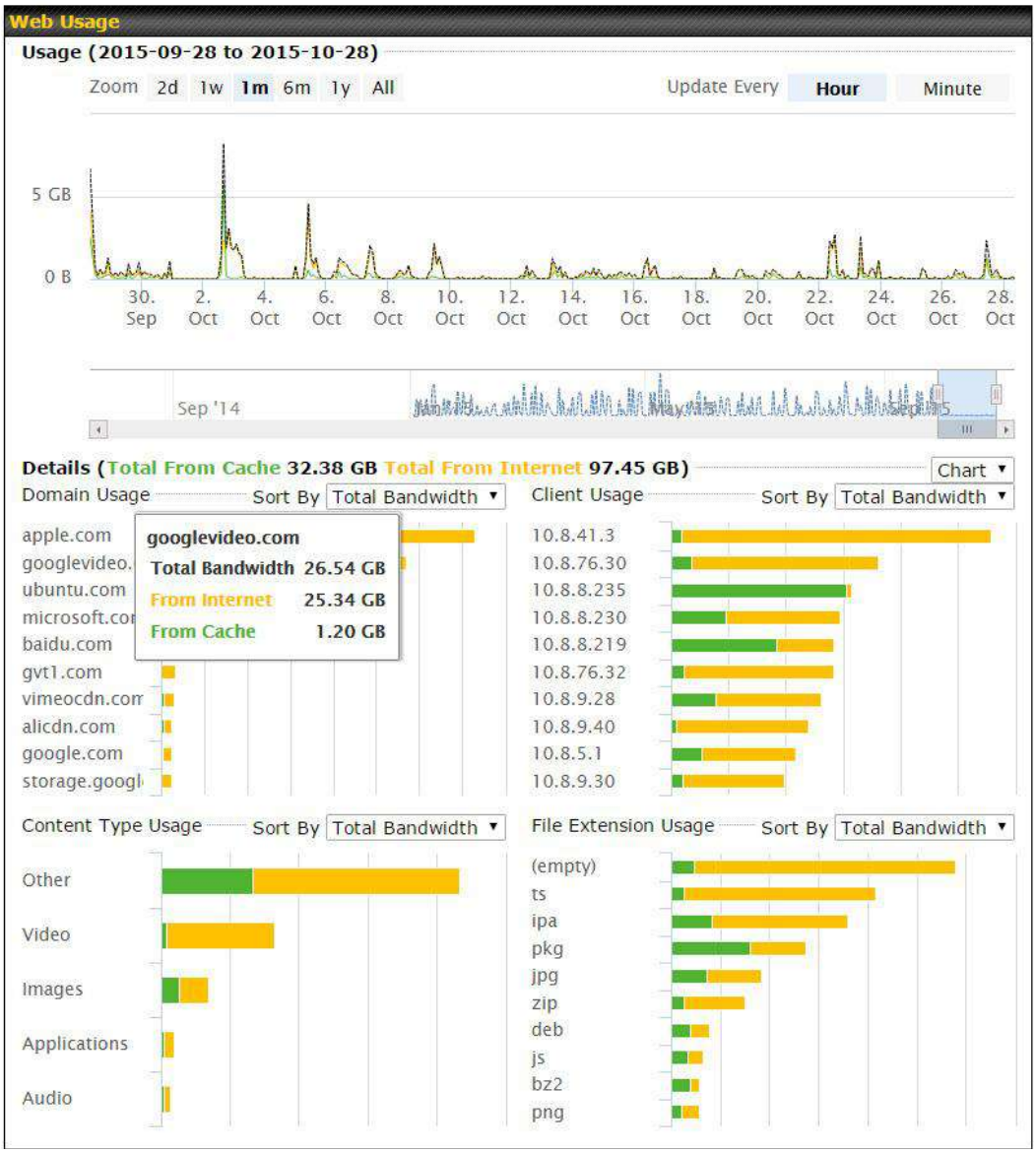
 Copyright @ 2021 Peplink

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

 Copyright @ 2021 Peplink

11.3 Viewing MediaFast Statistics

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



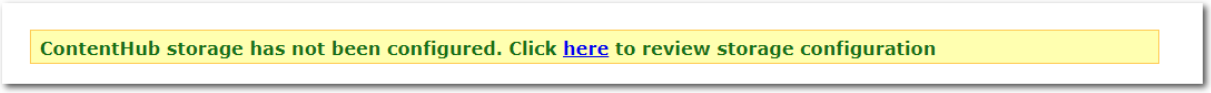
 Copyright @ 2021 Peplink

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.



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

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

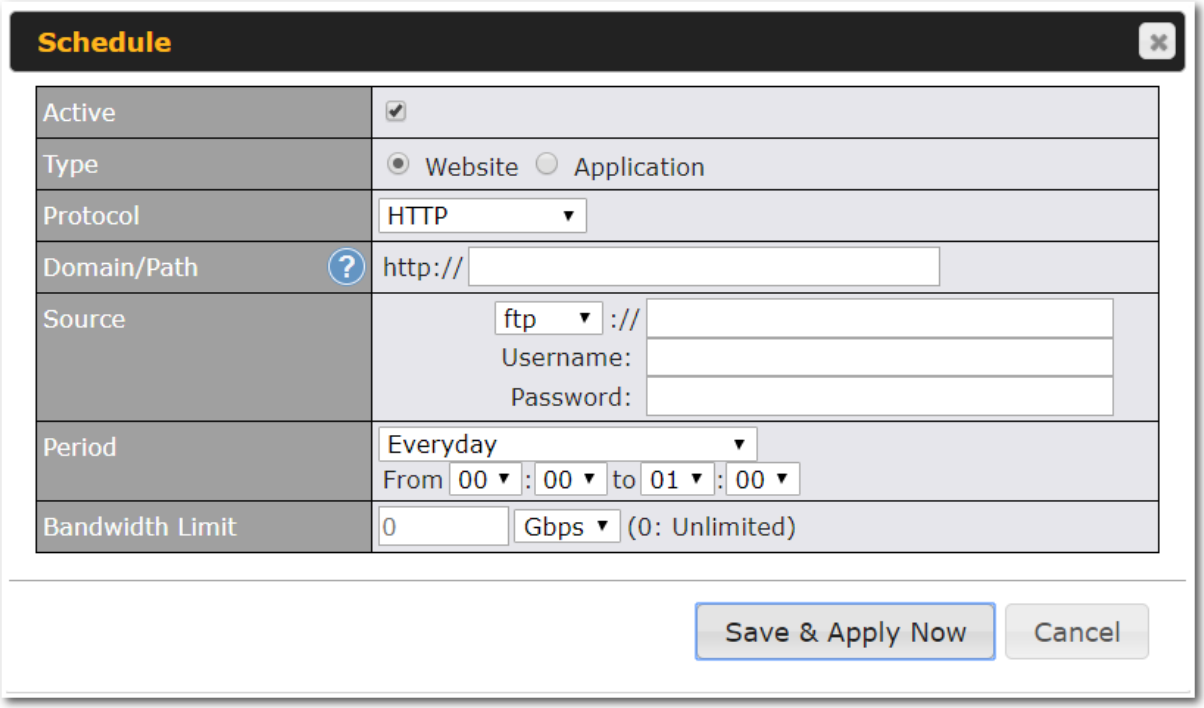
To configure a website or application as content, follow the steps below.

12.2 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.

 Copyright @ 2021 Peplink

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



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.

 Copyright @ 2021 Peplink

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

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:

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).

12.3 Configure an application for ContentHub

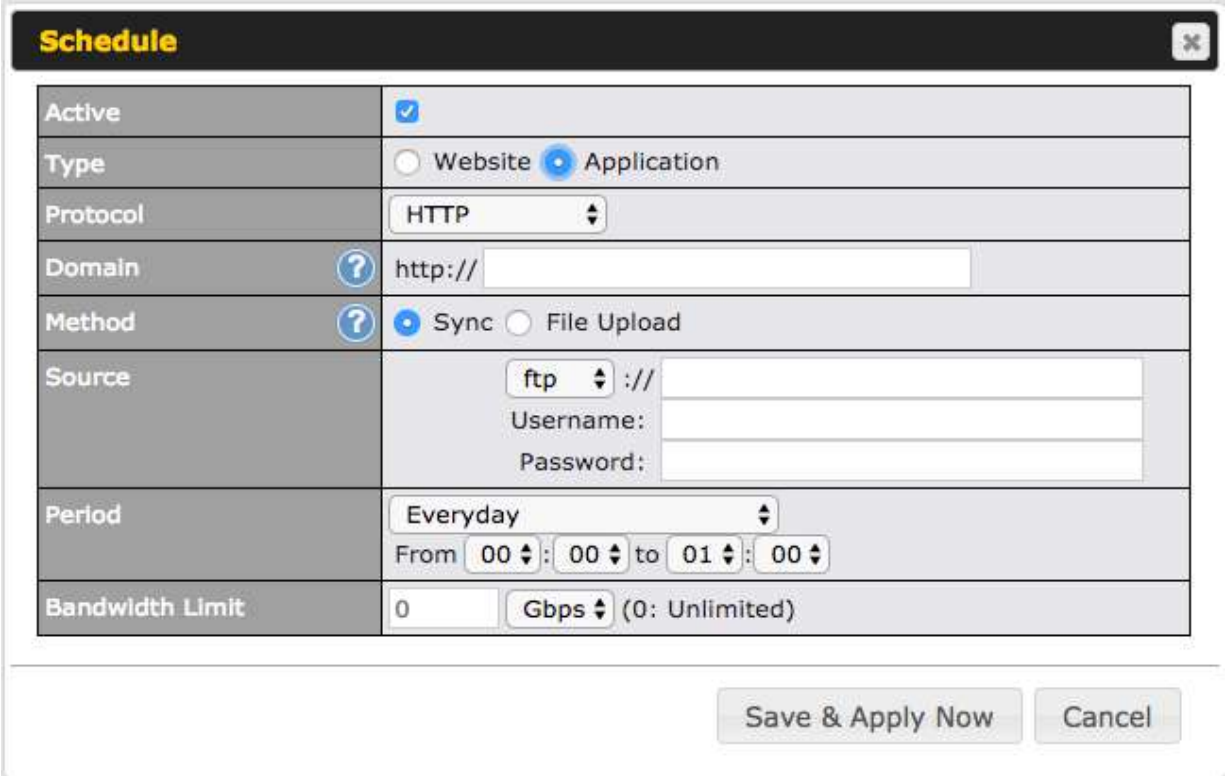
MediaFast routers allow you to configure and publish any application from the router itself by using one of the supported frameworks below:

- 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:

 Copyright @ 2021 Peplink

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



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

 Copyright @ 2021 Peplink

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.

 Copyright @ 2021 Peplink

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

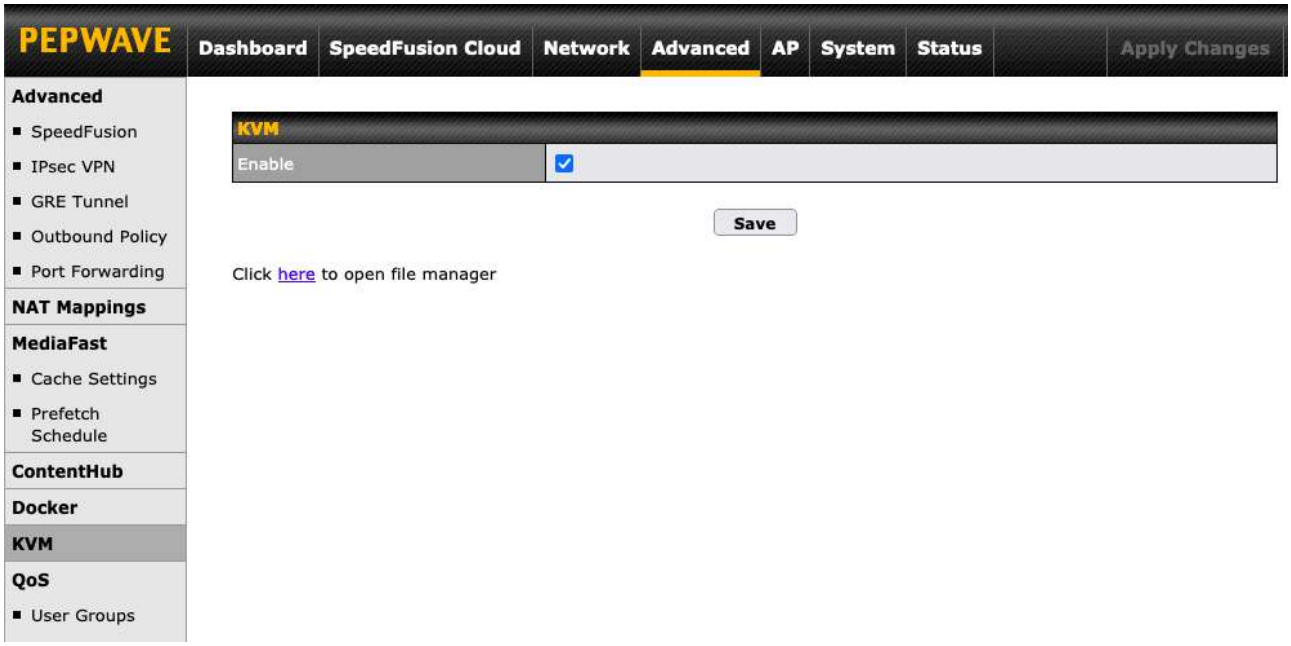
For detailed configuration instructions, refer to our knowledge base:

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

 Copyright @ 2021 Peplink

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.



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**

 Copyright @ 2021 Peplink

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.

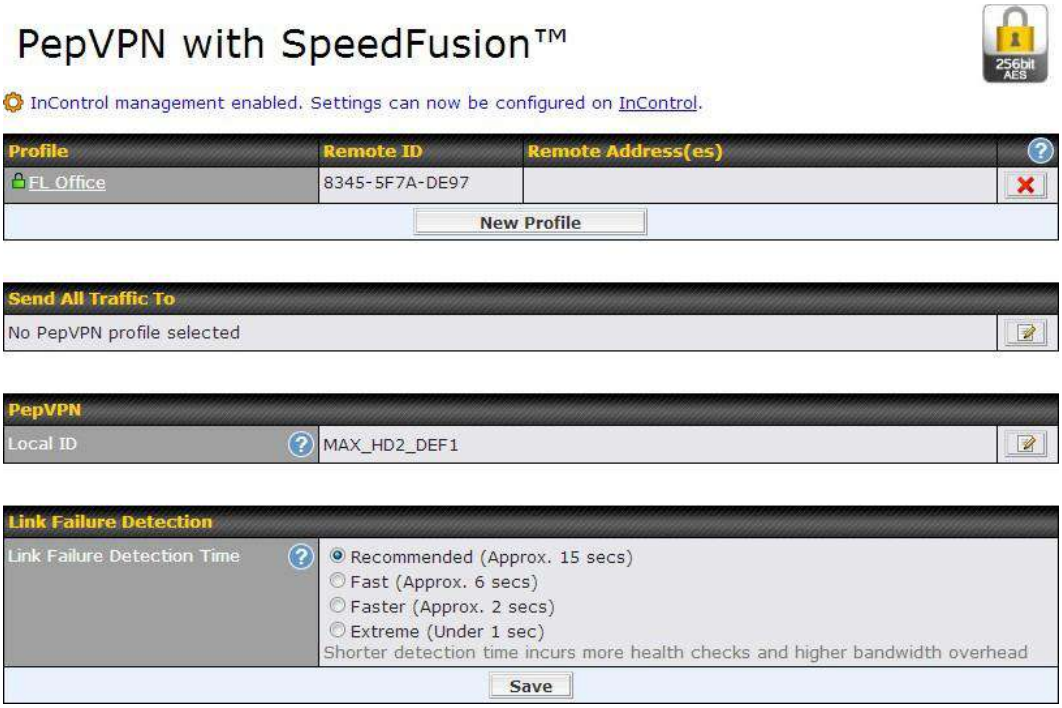
Pepwave routers can aggregate all WAN connections' bandwidth for routing SpeedFusion™ traffic. Unless all the WAN connections of one site are down, Pepwave routers can keep the VPN up and running.

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.

 Copyright @ 2021 Peplink

15.1 PepVPN

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



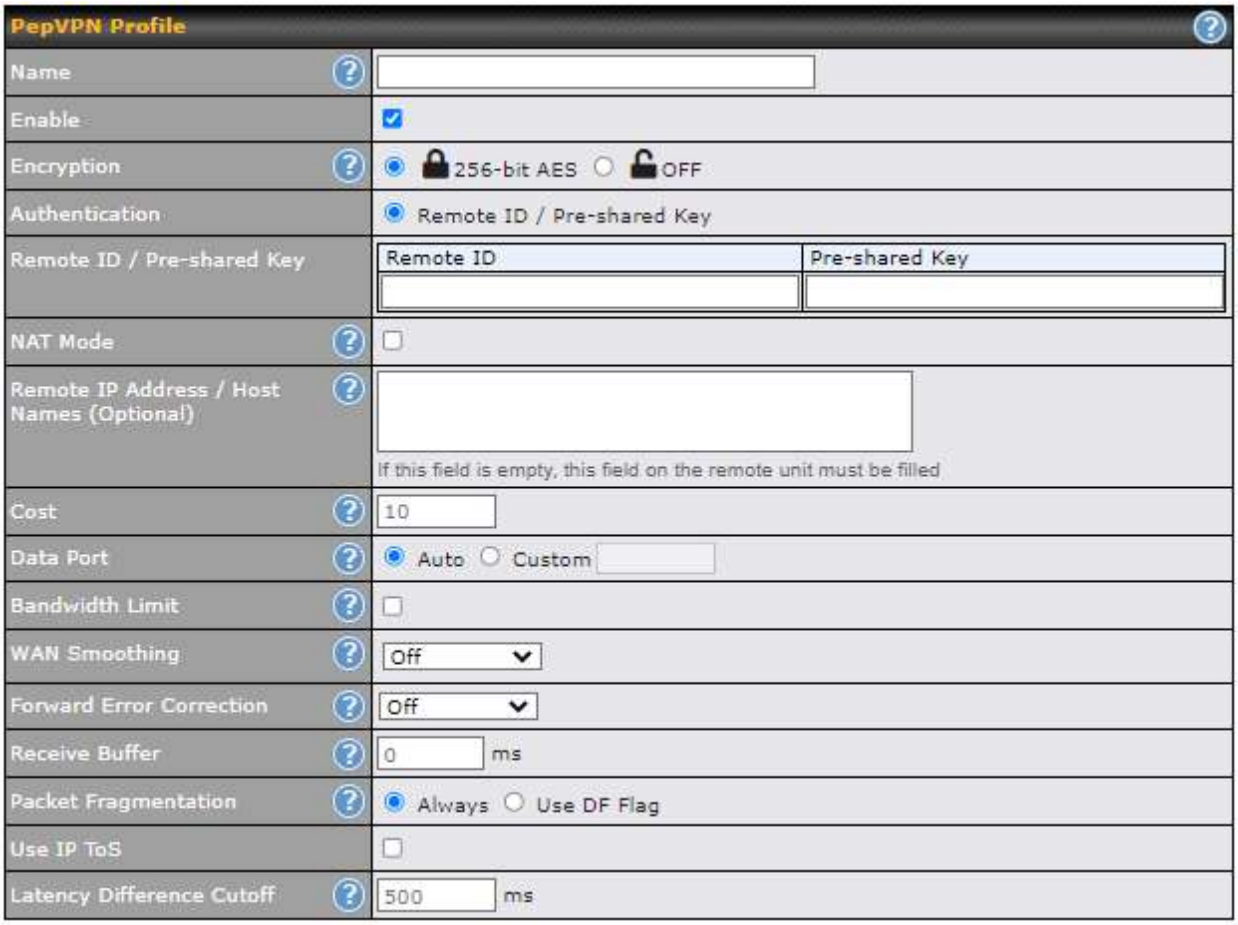
The local LAN subnet and subnets behind the LAN (defined under **Static Route** on the LAN settings page) will be advertised to the VPN. All VPN members (branch offices and headquarters) will be able to route to local subnets.

Note that all LAN subnets and the subnets behind them must be unique. Otherwise, VPN members will not be able to access each other.

All data can be routed over the VPN using the 256-bit AES encryption standard. To configure, navigate to **Advanced>SpeedFusion™** or **Advanced>PepVPN** and click the **New Profile** button to create a new VPN profile (you may have to first save the displayed default profile in order to 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.

 Copyright @ 2021 Peplink



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

 Copyright @ 2021 Peplink

	match. When the peer is running firmware 5.0+, this setting will be ignored. Enter Remote IDs either by typing out each Remote ID and Pre-shared Key, or by pasting a CSV. If you wish to paste a CSV, click the icon next to the "Remote ID / Preshared Key" setting.
Remote ID/Remote Certificate	These optional fields become available when **X.509** is selected as the Pepwave 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.
WAN Smoothing	While using PepVPN, utilize multiple WAN links to reduce the impact of packet loss and get the lowest possible latency at the expense of extra bandwidth consumption. This is suitable for streaming applications where the average bitrate requirement is much lower than the WAN's available bandwidth.

 Copyright @ 2021 Peplink

	Off - Disable WAN Smoothing. Normal - The total bandwidth consumption will be at most 2x of the original data traffic. Medium - The total bandwidth consumption will be at most 3x of the original data traffic. High - The total bandwidth consumption depends on the number of connected active tunnels.
Forward Error Correction	Forward Error Correction (FEC) can help to recover packet loss by using extra bandwidth to send redundant data packets. Higher FEC level will recover packets on a higher loss rate link. The expected overhead of Low is 13.3% and High is 26.7%. Require peer using PepVPN version 8.0.0 and above.
Receive Buffer	Receive Buffer can help to reduce out-of-order packets and jitter, but will introduce extra latency to the tunnel. Default is 0 ms, which disables the buffer, and maximum buffer size is 2000 ms.
Packet Fragmentation	If the packet size is larger than the tunnel's MTU, it will be fragmented inside the tunnel in order to pass through. Select Always to fragment any packets that are too large to send, or Use DF Flag to only fragment packets with Don't Fragment bit cleared. This can be useful if your application does Path MTU Discovery, usually sending large packets with DF bit set, if allowing them to go through by fragmentation, the MTU will not be detected correctly.
Use IP ToS[A]	Checking this button enables the use of IP ToS header field.
Latency Difference Cutoff[A]	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.

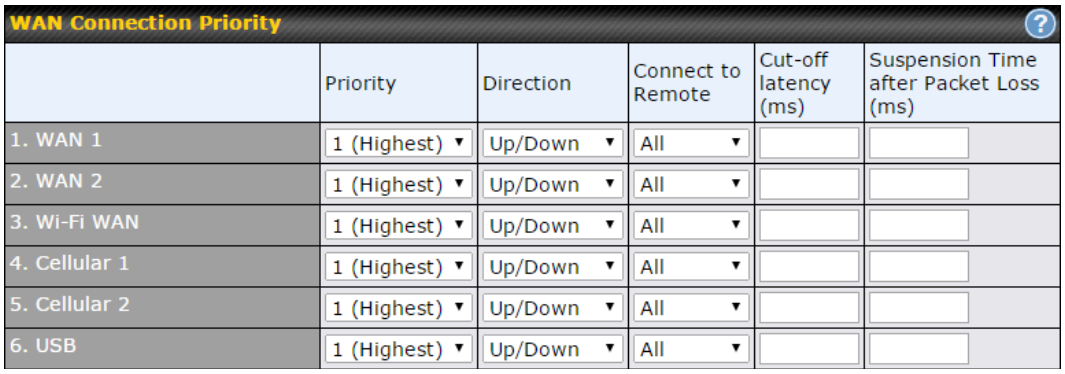
To enable Layer 2 Bridging between PepVPN profiles, navigate to **Network>LAN>Basic Settings>*LAN Profile Name*** and refer to instructions in section 9.1

 Copyright @ 2021 Peplink

Traffic Distribution	
Policy	Dynamic Weighted Bonding
Congestion Latency Level	Default
Ignore Packet Loss Event	☐
Disable Bufferbloat Handling	☐
Disable TCP ACK Optimization	☐
Packet Jitter Buffer	150 ms

Traffic Distribution	
Policy	This option allows you to select the desired out-bound traffic distribution policy: ● Bonding - Aggregate multiple WAN-to-WAN links into a single higher throughput tunnel. ● Dynamic Weighted Bonding - Aggregates WAN-to-WAN links with similar latencies. By default, Bonding is selected as a traffic distribution policy.
Congestion Latency Level	For most WANs, especially on cellular networks, the latency will increase when the link becomes more congested. Setting the **Congestion Latency Level** to **Low** will treat the link as congested more aggressively. Setting it to **High** will allow the latency to increase more before treating it as congested.
Ignore Packet Loss Event	By default, when there is packet loss, it is considered as a congestion event. If this is not the case, select this option to ignore the packet loss event.
Disable Bufferbloat Handling	Bufferbloat is a phenomenon on the WAN side when it is congested. The latency can become very high due to buffering on the uplink. By default, the Dynamic Weighted Bonding policy will try its best to mitigate bufferbloat by reducing TCP throughput when the WAN is congested. However, as a side effect, the tunnel might not achieve maximum bandwidth. Selecting this option will **disable** the bufferbloat handling mentioned above.
Disable TCP ACK Optimization	By default, TCP ACK will be forwarded to remote peers as fast as possible. This will consume more bandwidth, but may help to improve TCP performance as well. Selecting this option will **disable** the TCP ACK optimization mentioned above.
Packet Jitter Buffer	The default jitter buffer is 150ms, and can be modified from 0ms to 500ms. The jitter buffer may increase the tunnel latency. If you want to keep the latency as low as possible, you can set it to 0ms to disable the buffer. **Note**: If the Receive Buffer is set, the Packet Jitter Buffer will be automatically disabled.

 Copyright @ 2021 Peplink



WAN Connection Priority

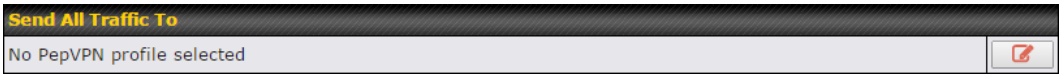
	Priority	Direction	Connect to Remote	Cut-off latency (ms)	Suspension Time after Packet Loss (ms)
1. WAN 1	1 (Highest)	Up/Down	All		
2. WAN 2	1 (Highest)	Up/Down	All		
3. Wi-Fi WAN	1 (Highest)	Up/Down	All		
4. Cellular 1	1 (Highest)	Up/Down	All		
5. Cellular 2	1 (Highest)	Up/Down	All		
6. USB	1 (Highest)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

WAN Connection Priority

WAN Connection Priority

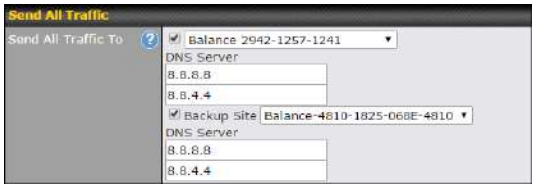
If your device supports it, you can specify the priority of WAN connections to be used for making VPN connections. WAN connections set to **OFF** will never be used. Only available WAN connections with the highest priority will be used.

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



Send All Traffic To

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



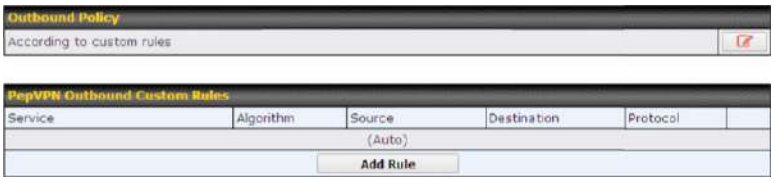
You could also specify a DNS server to resolve incoming DNS requests. Click the checkbox next to **Backup Site** to designate a backup SpeedFusion profile that will take over, should the main PepVPN connection fail.

Outbound Policy/PepVPN Outbound Custom Rules

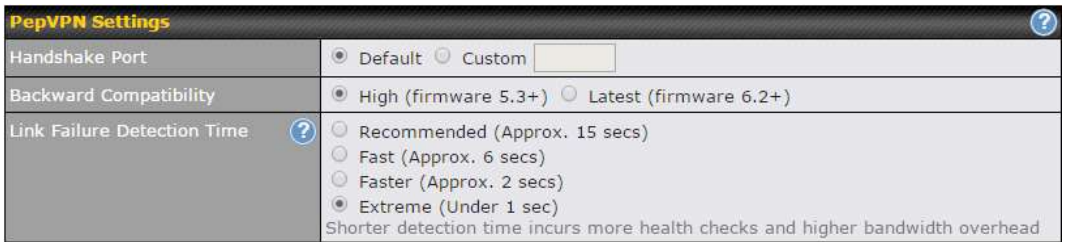
Some models allow you to set outbound policy and custom outbound rules from **Advanced>PepVPN**.

 Copyright @ 2021 Peplink

See **Section 14** for more information on outbound policy settings.



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



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

 Copyright @ 2021 Peplink

	When **Extreme** is selected, a health check packet is sent every 0.1 second, and the expected detection time is less than one second.

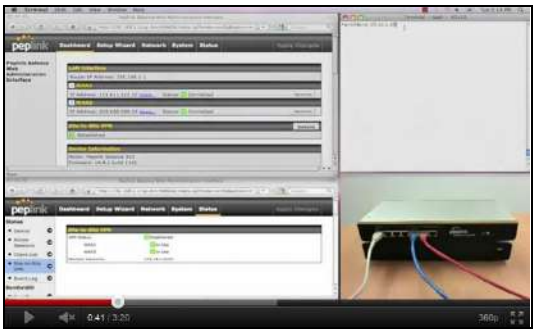
[A] - Advanced feature, please click the button on the top right-hand corner to activate.

Important Note

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

Tip

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



http://youtu.be/TLQgdpPSY88

 Copyright @ 2021 Peplink

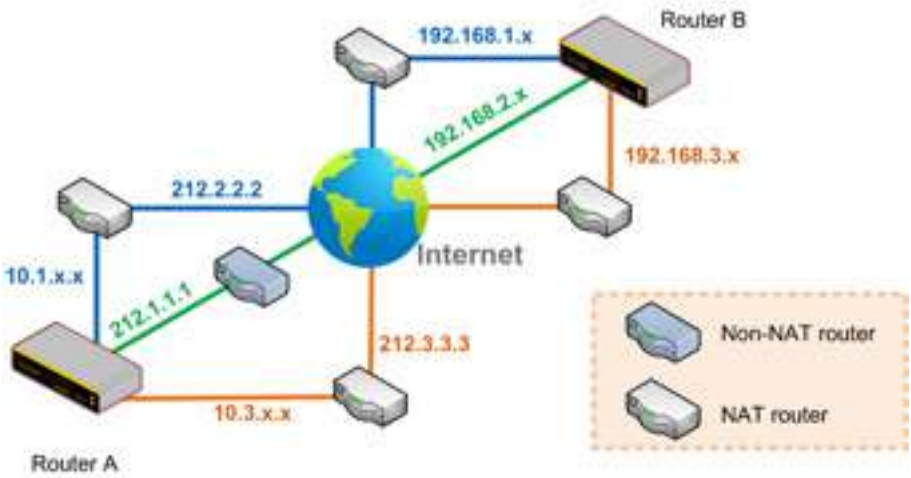
15.2 The Pepwave Router Behind a NAT Router

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.

 Copyright @ 2021 Peplink

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™ table, you will be forwarded to **Status>SpeedFusion™**, where you can view subnet and WAN connection information for each VPN peer. Please refer to **Section 22.6** for details.

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

 Copyright @ 2021 Peplink

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.**

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.

 Copyright @ 2021 Peplink

Name	
Active	☑
IKE Version	◉ IKEv1 ○ IKEv2
Connect Upon Disconnection of	☑ WAN
Remote Gateway IP Address / Host Name	
IPsec Type	◉ Policy-based ○ Route-based
Local Networks	Propose the following networks to remote gateway: ☑ 192.168.50.0/24 ☐ Apply the following NAT policies: ☐ Local Network ➔ NAT Network
Remote Networks	Network: ; Subnet Mask: 255.255.255.0 (/24) +
Authentication	◉ Preshared Key
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	1 Group 2 2 -----
Phase 1 SA Lifetime	3600 seconds
Phase 2 (ESP) Proposal	1 AES-256 & SHA1 2 -----
Phase 2 PFS Group	None
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.

 Copyright @ 2021 Peplink

IKE Version	Two versions of the IKE standards are available: • IKEv1 • IKEv2
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.
IPsec Type	Policy-based - (default) All the matched traffic as defined in Local Networks and Remote Networks will be routed to this IPsec connection, this cannot be overridden by other routing methods. Route-based - Outbound Policy rule is required to route traffic to this tunnel and comes with more flexibility to control how to route traffic compared to Policy-based. If you want to modify the traffic selector instead of using the default (0.0.0.0/0). **Note**: This option is available for certain following models only: • MAX: BR1 ENT, Transit, 700 HW3 or above, HD2 HW5 or above, HD4
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	Enter the LAN and subnets that are located at the remote site here.

 Copyright @ 2021 Peplink

Networks	
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.

 Copyright @ 2021 Peplink

	Group 2: 1024-bit Diffie-Hellman group. The larger the group number, the higher the security. **Group 5**: **1536-bit** is the third option.
Phase 2 SA Lifetime	This setting specifies the lifetime limit of this Phase 2 Security Association. By default, it is set at **28800** seconds.

WAN Connection Priority	
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

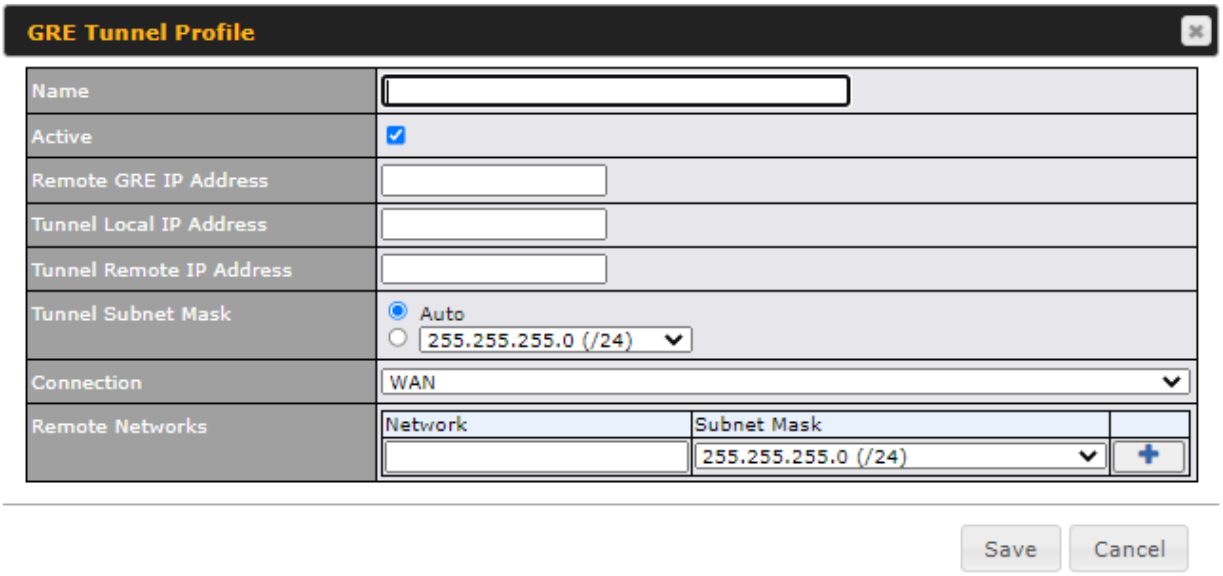
Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. A GRE tunnel is similar to IPSec or PepVPN.

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

GRE Tunnel Profiles	Remote Networks	
No GRE profile defined		
New Profile		

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.

 Copyright @ 2021 Peplink



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.

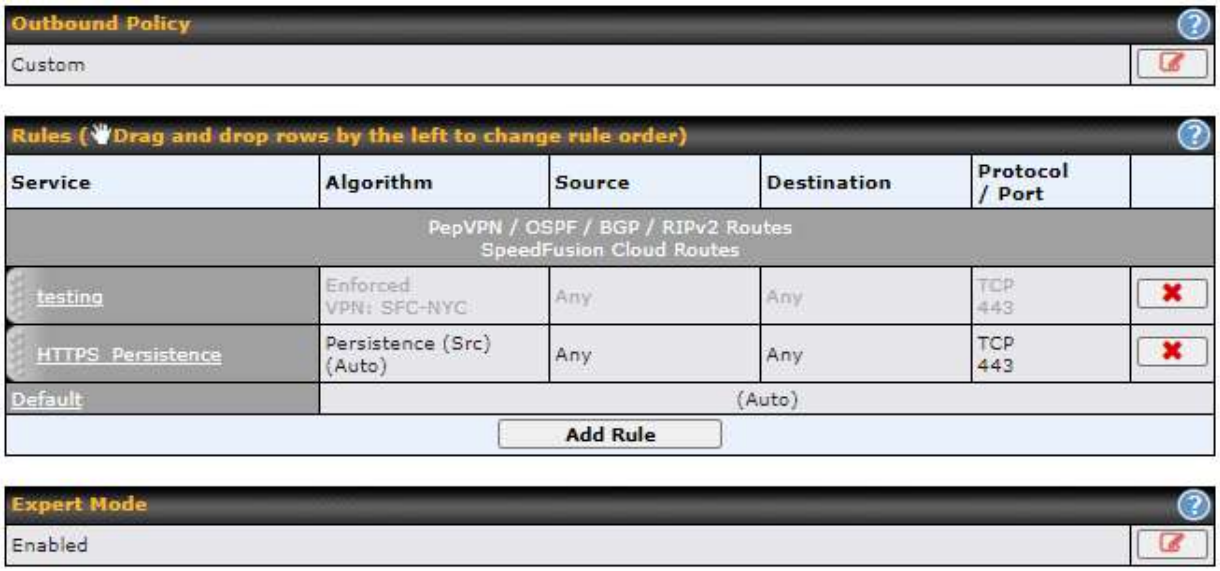
 Copyright @ 2021 Peplink

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.

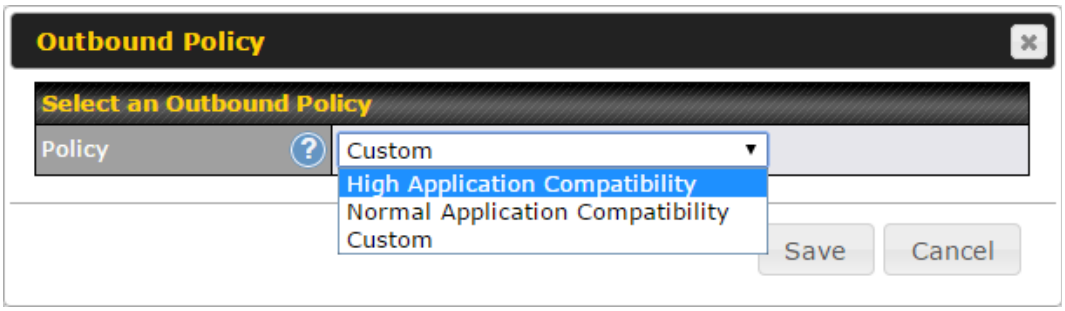


 Copyright @ 2021 Peplink

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:



There are three main selections for the outbound traffic policy:

- High Application Compatibility
- Normal Application Compatibility
- Custom

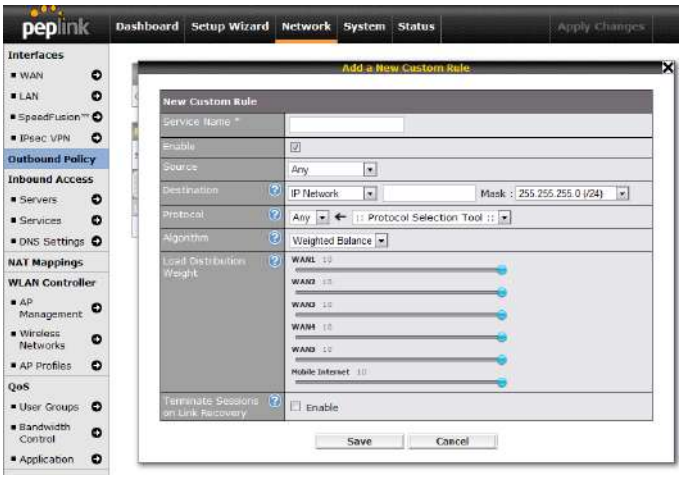
Note that some Pepwave routers provide only the **Send All Traffic To** setting here. See **Section 12.1** for details.

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!

 Copyright @ 2021 Peplink



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)

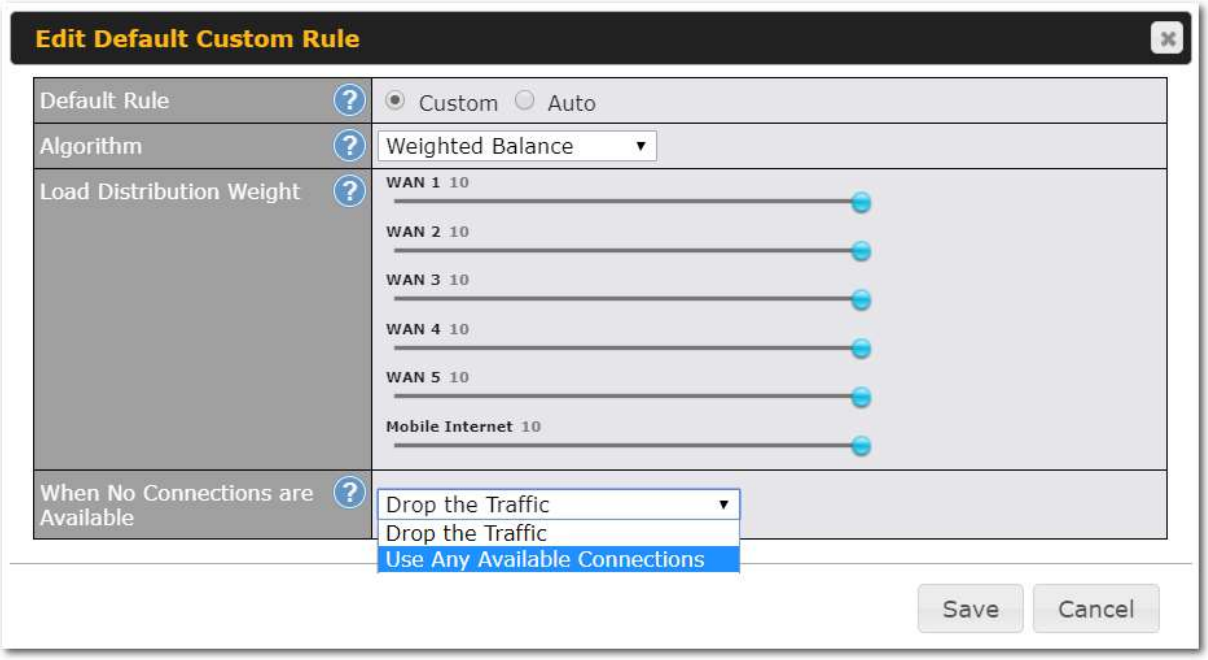
Service	Algorithm	Source	Destination	Protocol / Port	
HTTPS_Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	✖
Default	(Auto)				

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.

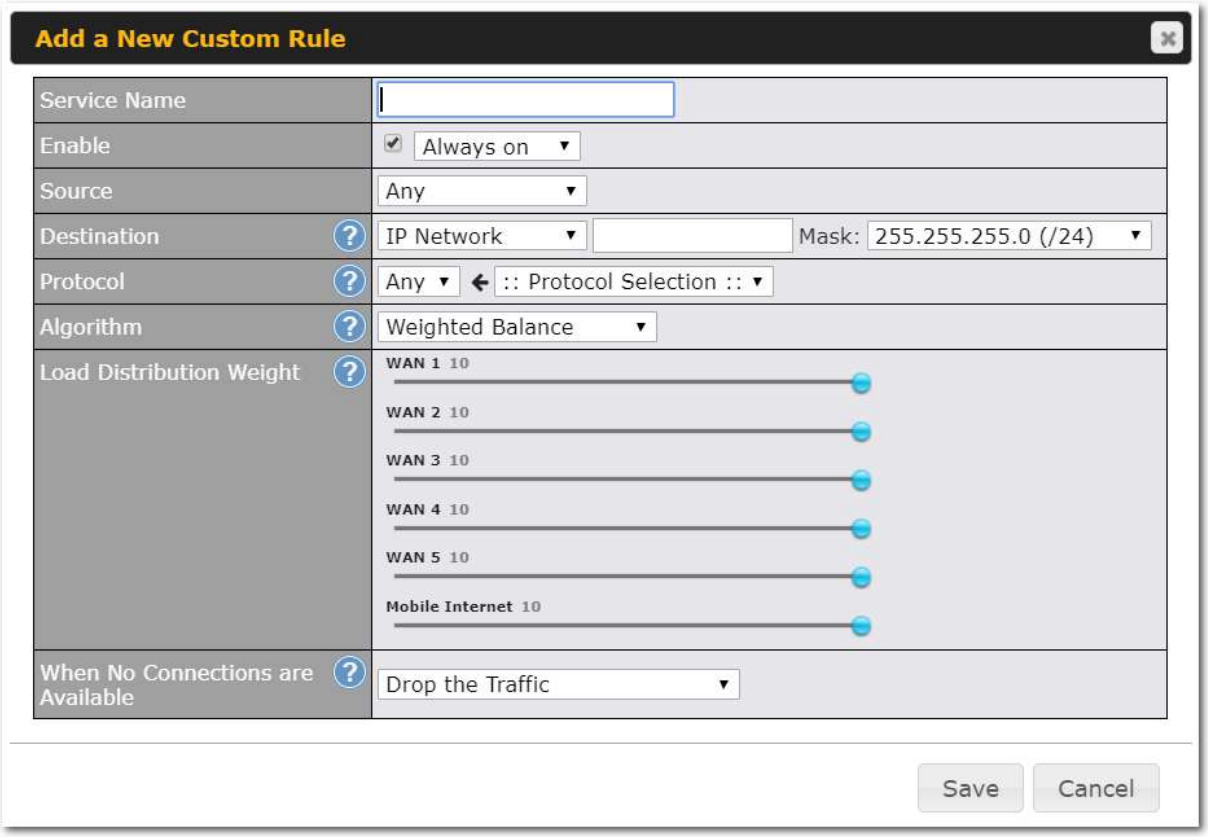
 Copyright @ 2021 Peplink

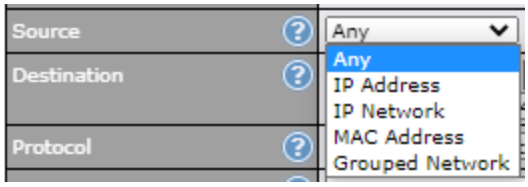


By default, **Auto** is selected as the **Default Rule**. You can select **Custom** to change the algorithm to be used. Please refer to the upcoming sections for the details on the available algorithms.

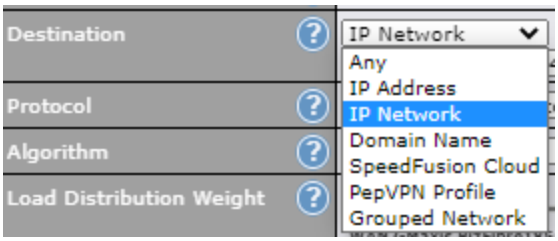
To create a custom rule, click **Add Rule** at the bottom of the table.

 Copyright @ 2021 Peplink



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. 
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.

 Copyright @ 2021 Peplink

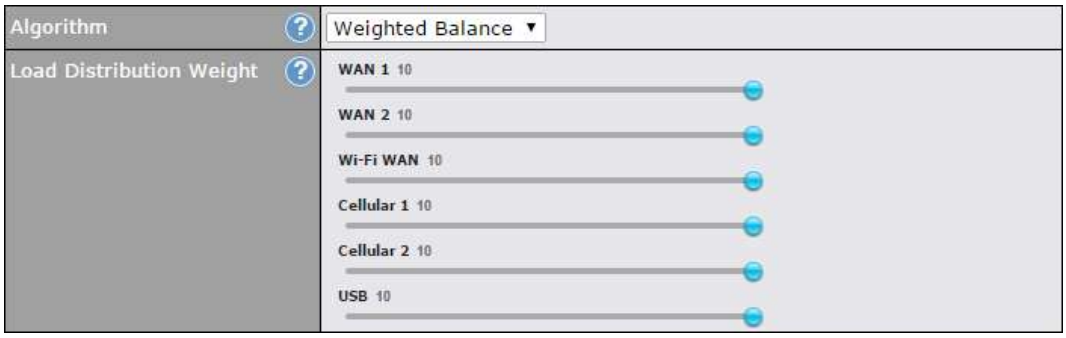
	 If **Domain Name** is chosen and a domain name, such as *foobar.com*, is entered, any outgoing accesses to *foobar.com* and **.foobar.com* will match this criterion. You may enter a wildcard (.*) at the end of a domain name to match any host with a name having the domain name in the middle. If you enter *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.

 Copyright @ 2021 Peplink

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**.



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

 Copyright @ 2021 Peplink

- 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%.

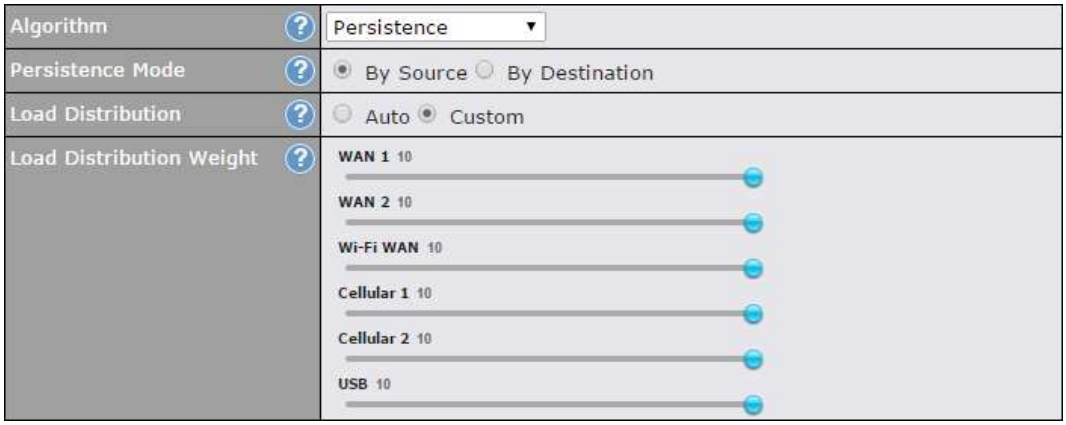
17.2.2 Algorithm: Persistence

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.



 Copyright @ 2021 Peplink

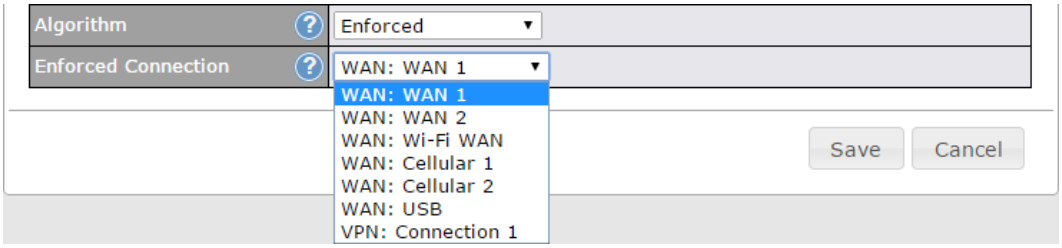
There are two persistent modes: **By Source** and **By Destination**.

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**.

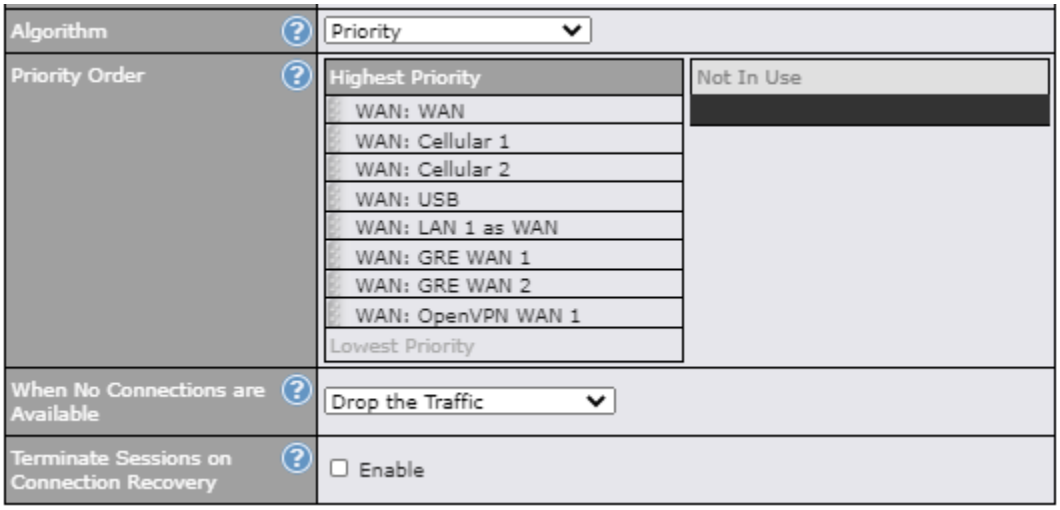


Matching traffic will be routed through the specified WAN connection, regardless of the health check status of the WAN connection. Starting from Firmware 5.2, outbound traffic can be enforced to go through a specified SpeedFusion™ connection.

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.

 Copyright @ 2021 Peplink

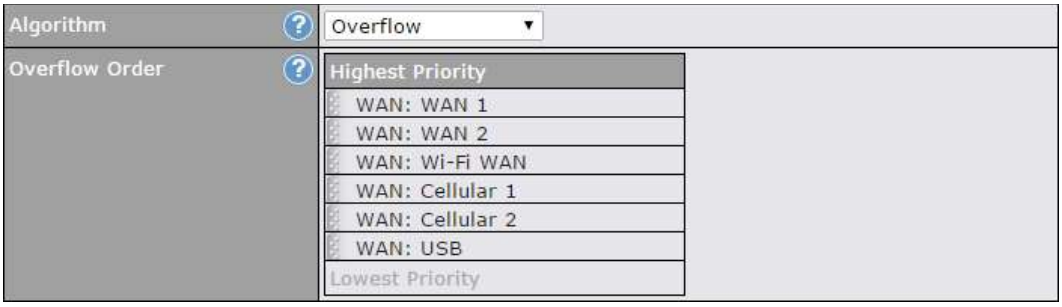


Starting from Firmware 5.2, outbound traffic can be prioritized to go through SpeedFusion™ connection(s). By default, VPN connections are not included in the priority list.

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

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.



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.

 Copyright @ 2021 Peplink

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

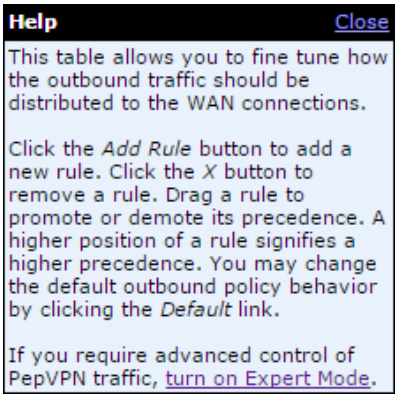
The roundtrip time of a 6M down/640k uplink can be higher than that of a 2M down/2M up link because the overall round trip time is lengthened by its slower upload bandwidth, despite its higher downlink speed. Therefore, this algorithm is good for two scenarios:

- 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.

 Copyright @ 2021 Peplink

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**.



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

above the bar to override the SpeedFusion™ routes.

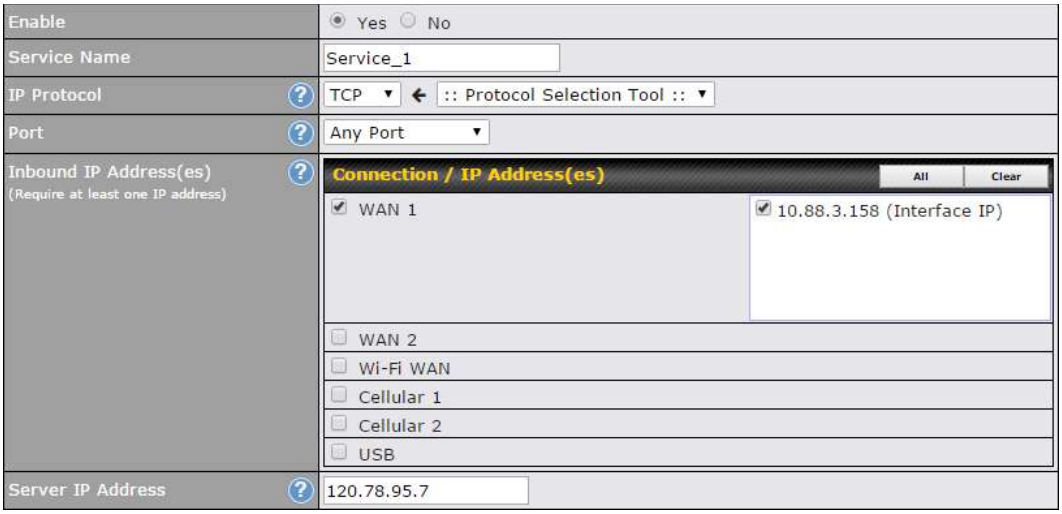
Upon disabling Expert Mode, all rules above the bar will be removed.

 Copyright @ 2021 Peplink

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**.

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



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

 Copyright @ 2021 Peplink

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**  **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.  **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 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 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.)  **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.

 Copyright @ 2021 Peplink

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.

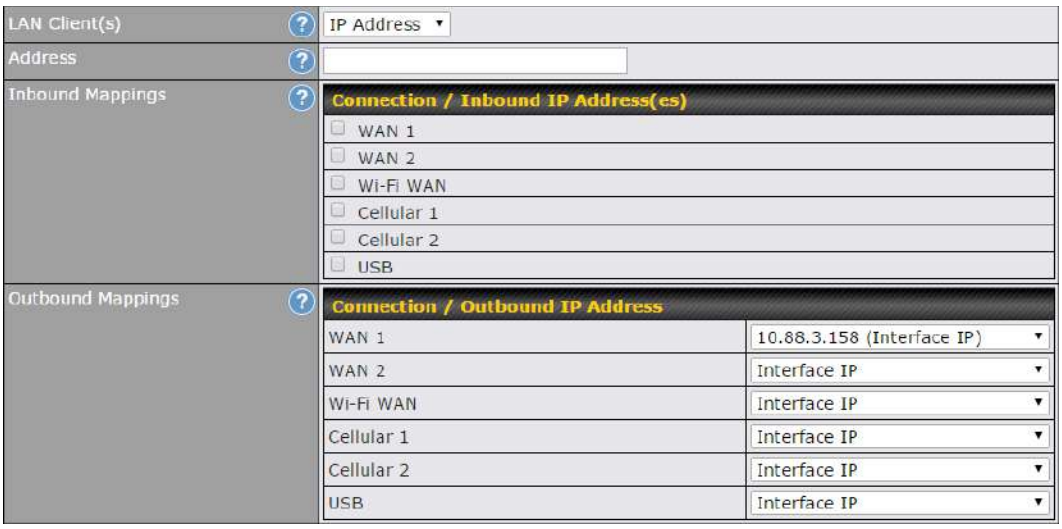
When the options are enabled, a table listing all the forwarded ports under these two protocols can be found at **Status > UPnP / NAT-PMP**.

 Copyright @ 2021 Peplink

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**.

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



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

 Copyright @ 2021 Peplink

	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.

 Copyright @ 2021 Peplink

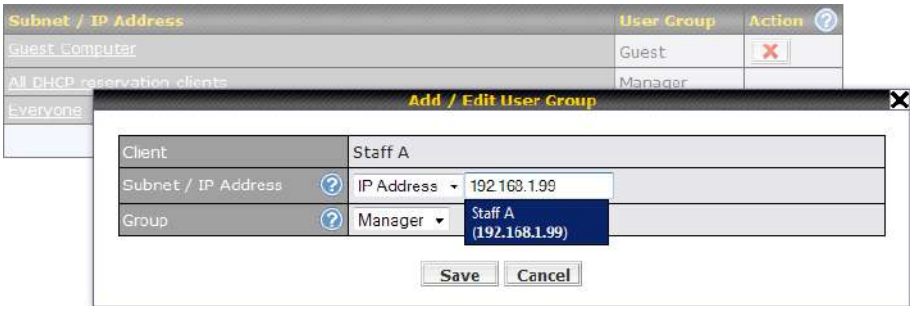
20 QoS

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.



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.

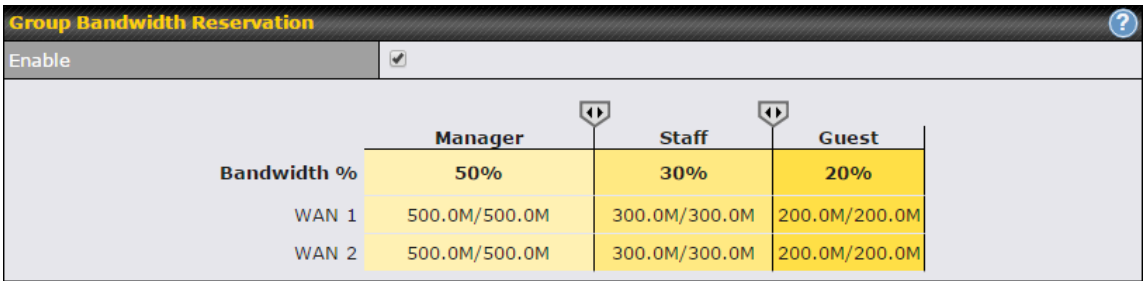
Once users have been assigned to a user group, their internet traffic will be restricted by rules defined for that particular group. Please refer to the following two sections for details.

 Copyright @ 2021 Peplink

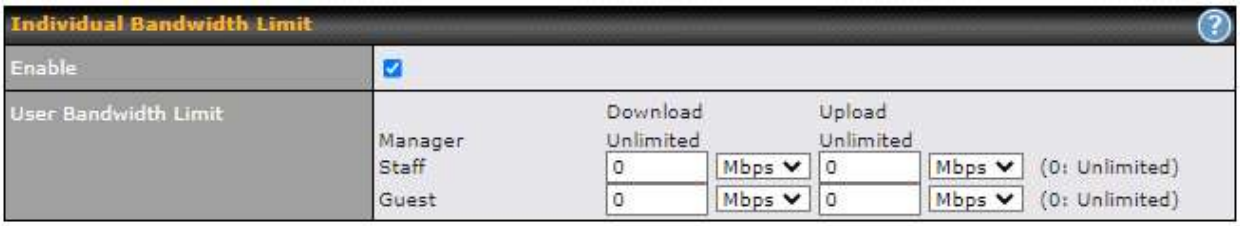
20.2 Bandwidth Control

This section is to define how much minimum bandwidth will be reserved to each user group when a WAN connection is **in full load**. When this feature is enabled, a slider with two indicators will be shown. You can move the indicators to adjust each group's weighting. The lower part of the table shows the corresponding reserved download and uploads bandwidth value of each connection.

By default, **50%** of bandwidth has been reserved for Manager, **30%** for Staff, and **20%** for Guest.



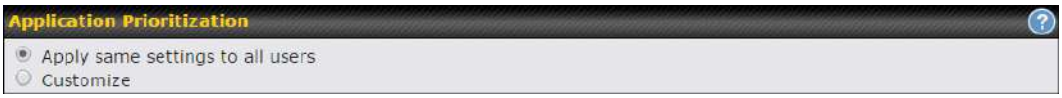
You can define a maximum download speed (over all WAN connections) and upload speed (for each WAN connection) that each individual Staff and Guest member can consume. No limit can be imposed on individual Managers. By default, download and upload bandwidth limits are set to unlimited (set as **0**).



20.3 Application

20.3.1 Application Prioritization

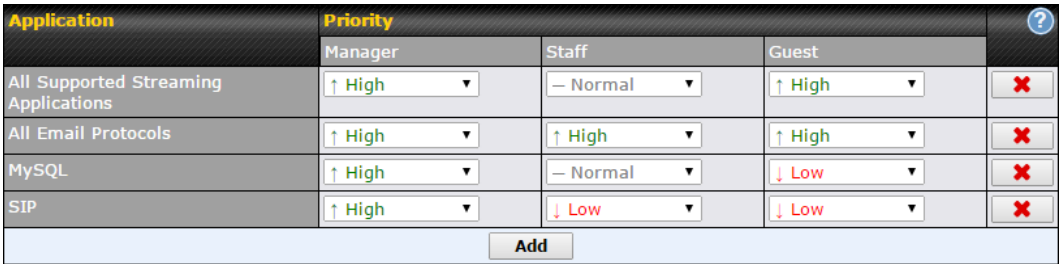
On many Pepwave routers, you can choose whether to apply the same prioritization settings to all user groups or customize the settings for each group.



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

 Copyright @ 2021 Peplink

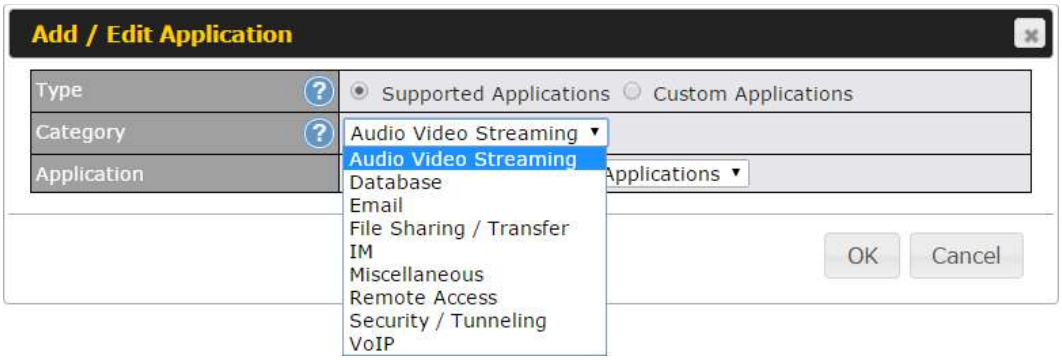
the bottom.

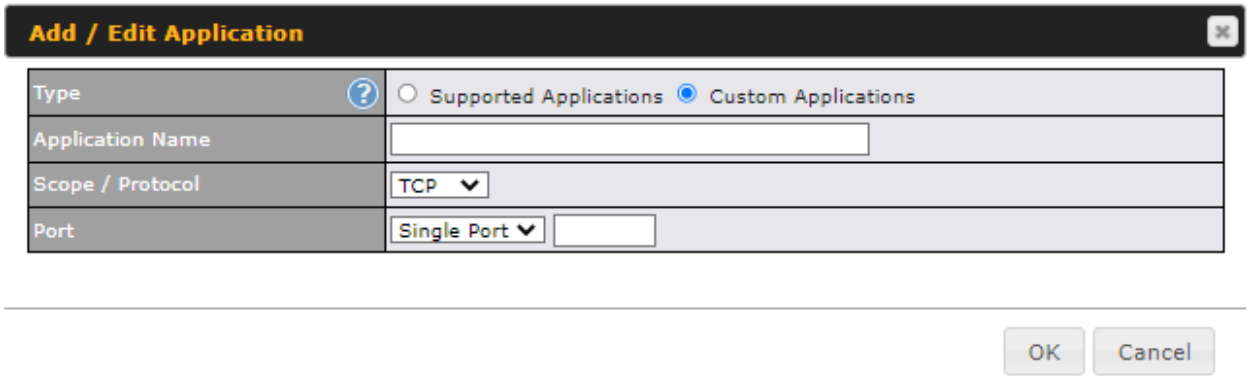


20.3.2 Prioritization for Custom Applications

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.

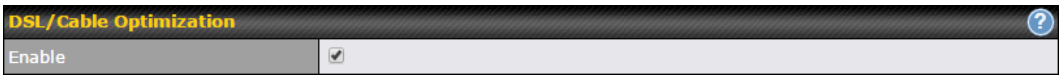




 Copyright @ 2021 Peplink

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.



 Copyright @ 2021 Peplink

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.

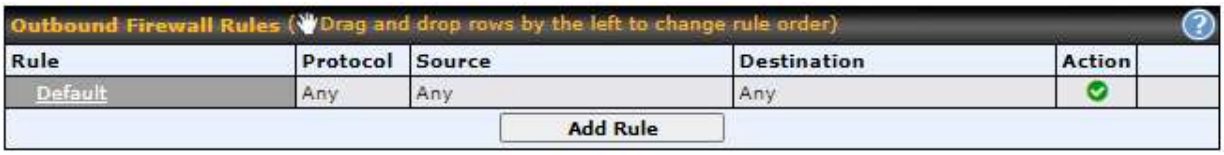
The firewall functionality of Pepwave routers supports the selective filtering of data traffic in both directions:

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



 Copyright @ 2021 Peplink

21.1 Outbound and Inbound Firewall Rules

21.1.1 Access Rules

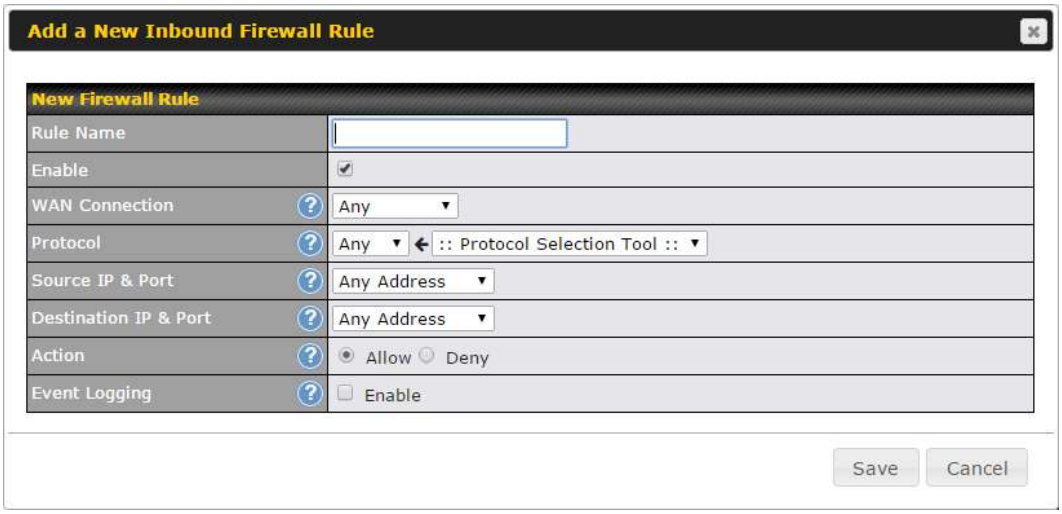
The outbound firewall settings are located at **Advanced>Firewall>Access Rules>Outbound Firewall Rules.**

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

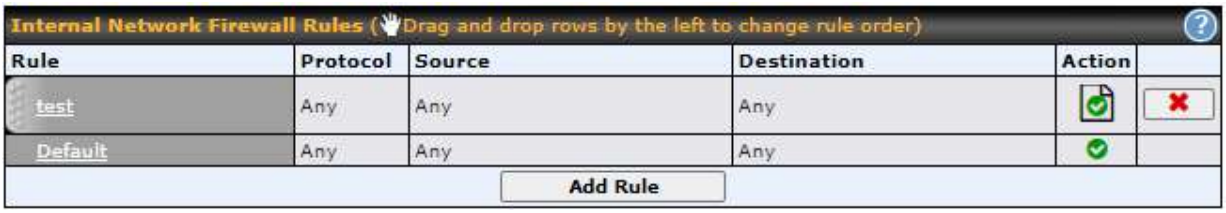
Inbound firewall settings are located at **Advanced>Firewall>Access Rules>Inbound Firewall Rules.**

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

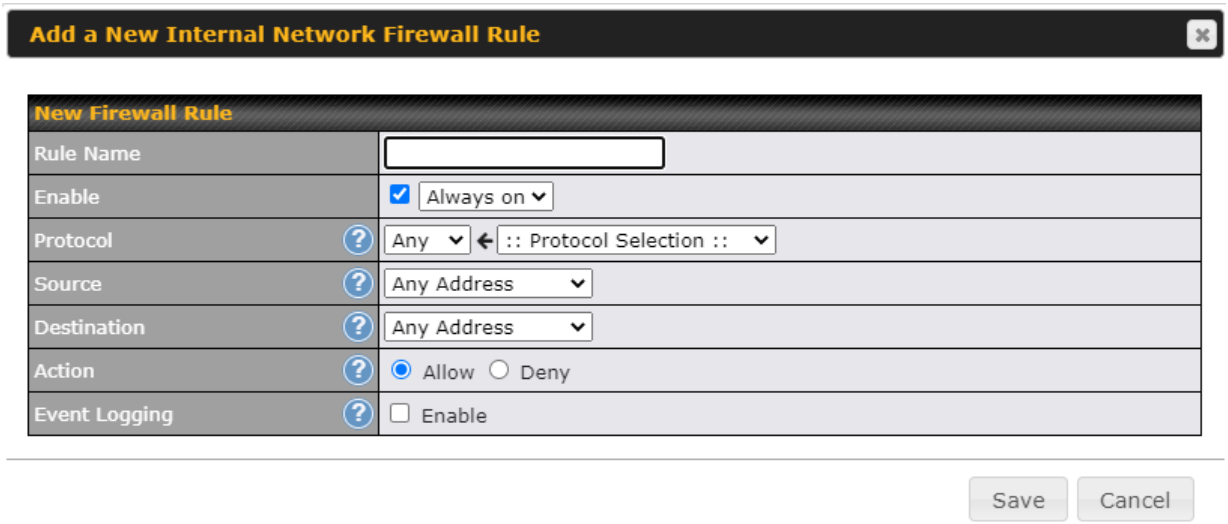
 Copyright @ 2021 Peplink



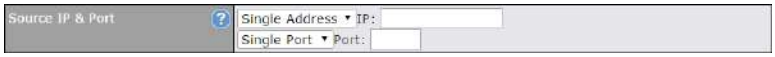
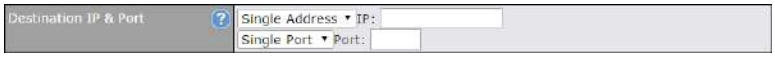
Internal Network firewall settings are located at **Advanced>Firewall>Access Rules>Internal Network Firewall Rules.**



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



 Copyright @ 2021 Peplink

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:  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:  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

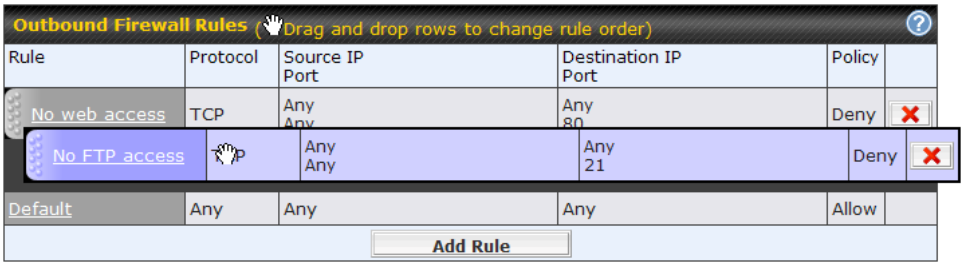
 Copyright @ 2021 Peplink

	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.



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.

 Copyright @ 2021 Peplink

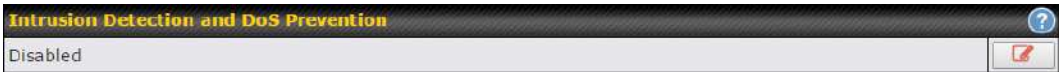
Tip

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

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



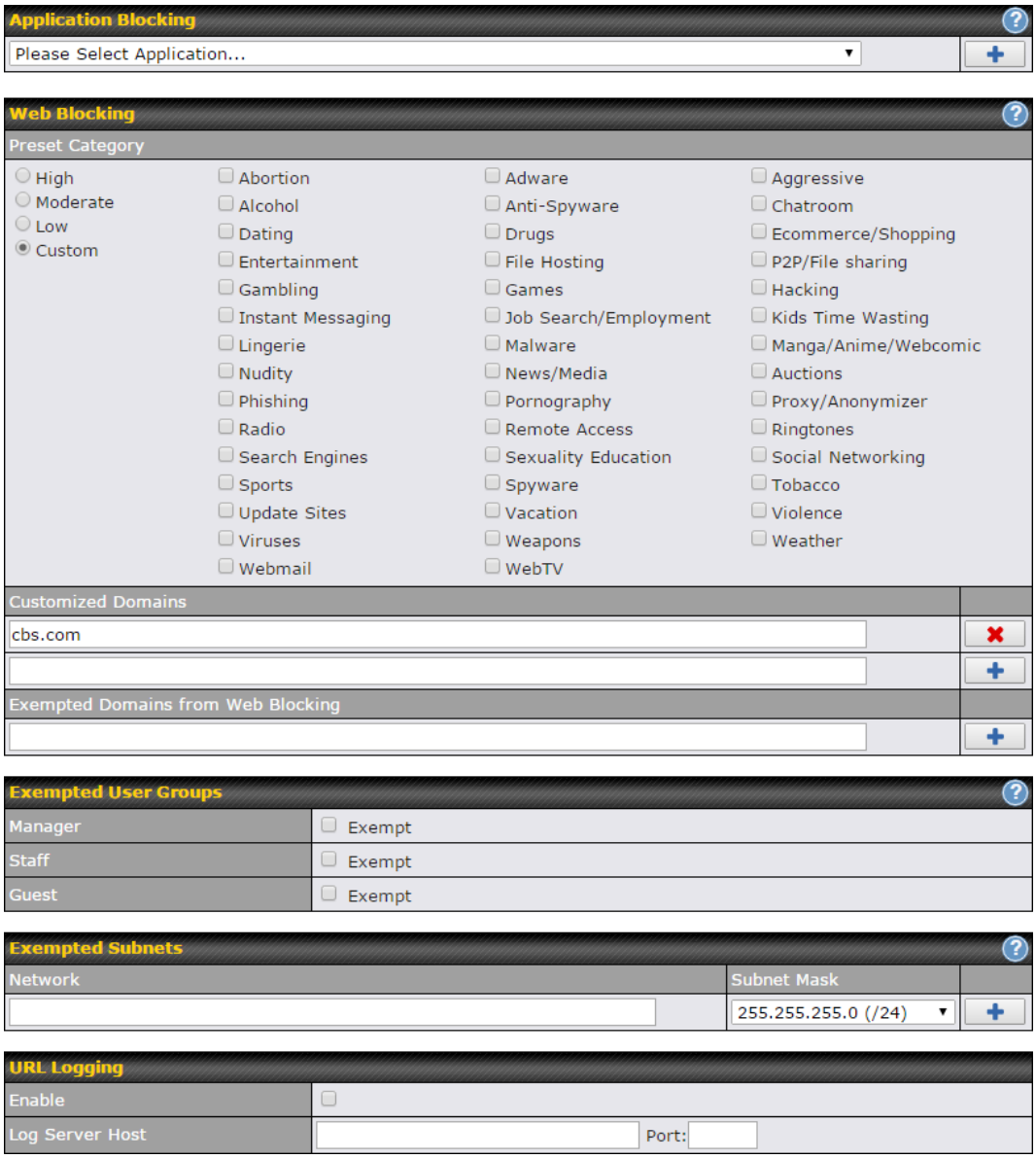
Pepwave routers can detect and prevent intrusions and denial-of-service (DoS) attacks from the Internet. To turn on this feature, click , check the **Enable** check box, and press the **Save** button.

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

 Copyright @ 2021 Peplink

21.2 Content Blocking



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

 Copyright @ 2021 Peplink

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

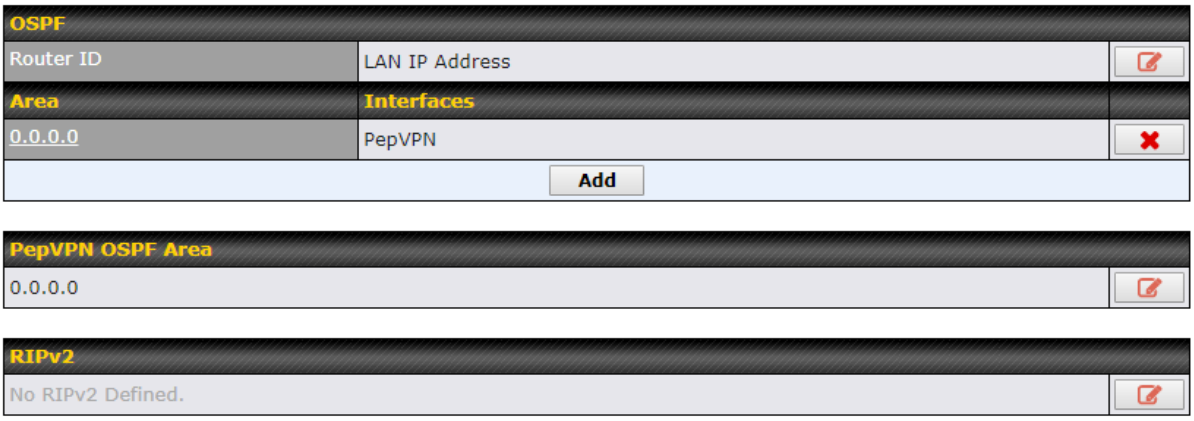
Click **enable**, and the enter the ip address and port (if applicable) where your remote syslog server is located.

 Copyright @ 2021 Peplink

22 Routing Protocols

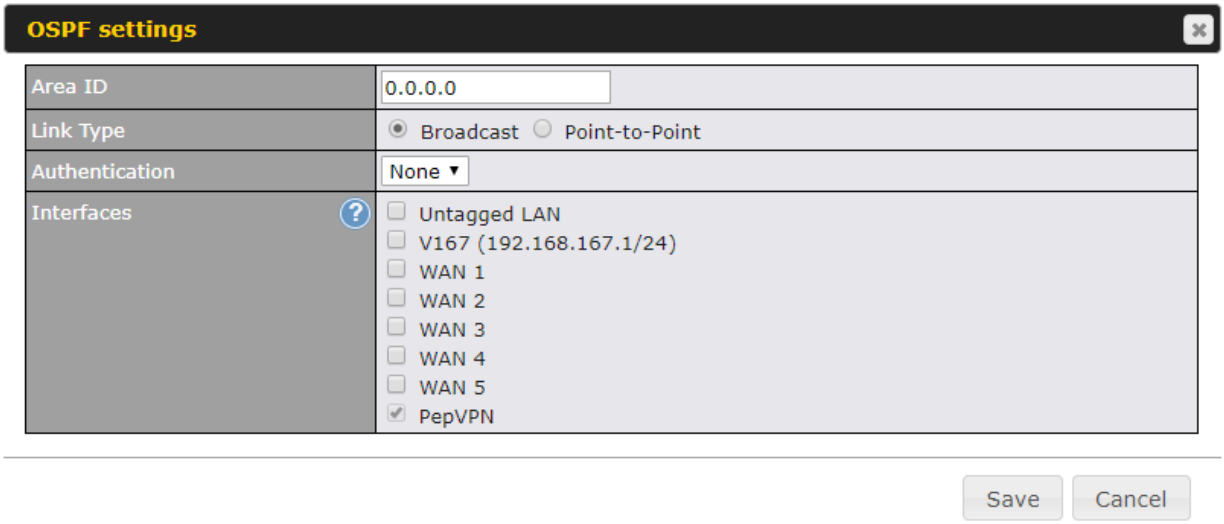
22.1 OSPF & RIPv2

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:



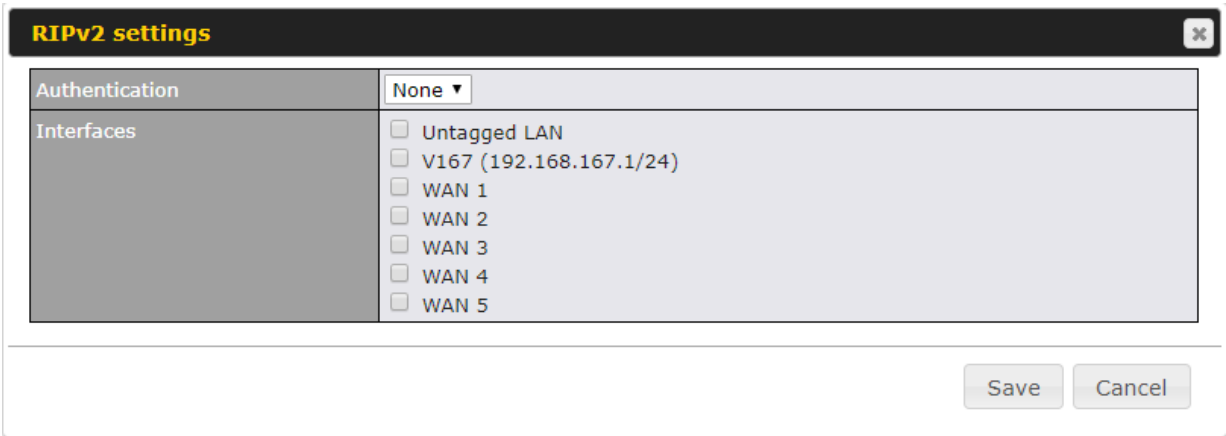
OSPF	
Router ID	This field determines the ID of the router. By default, this is specified as the WAN IP address. If you want to specify your own ID, enter it into the **Custom** field.
Area	This is an overview of the OSPF areas that you have defined. Clicking on the name under Area allows you to configure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

 Copyright @ 2021 Peplink



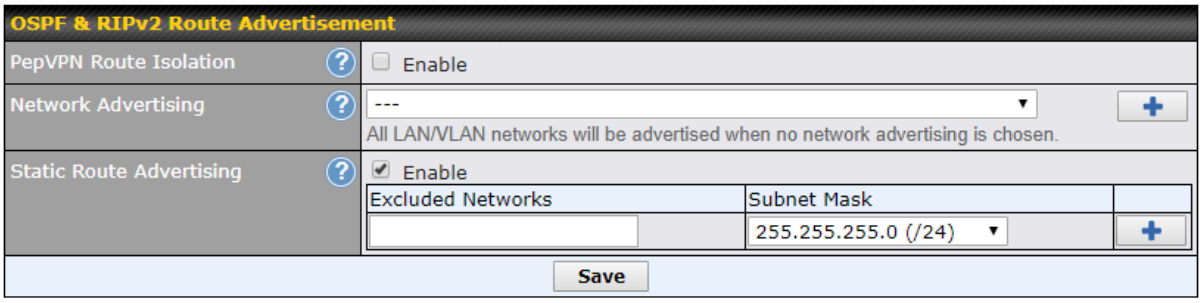
OSPF Settings	
Area ID	Assign a name to be applied to this group. Machines linked to this group will send and receive related OSPF packets, while unlinked machines will ignore them.
Link Type	Choose the type of network that this area will use.
Authentication	If an authentication method is used, select 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 .



 Copyright @ 2021 Peplink

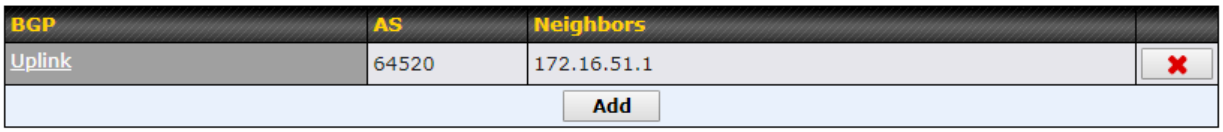
RIPv2 Settings	
Authentication	If an authentication method is used, select one from this drop-down menu. Available options are **MD5** and **Text**. Authentication key(s) may be input next to the drop-down menu after selecting an authentication method.
Interfaces	Select the interface(s) that this area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



OSPF & RIPv2 Route Advertisement	
PepVPN Route Isolation	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

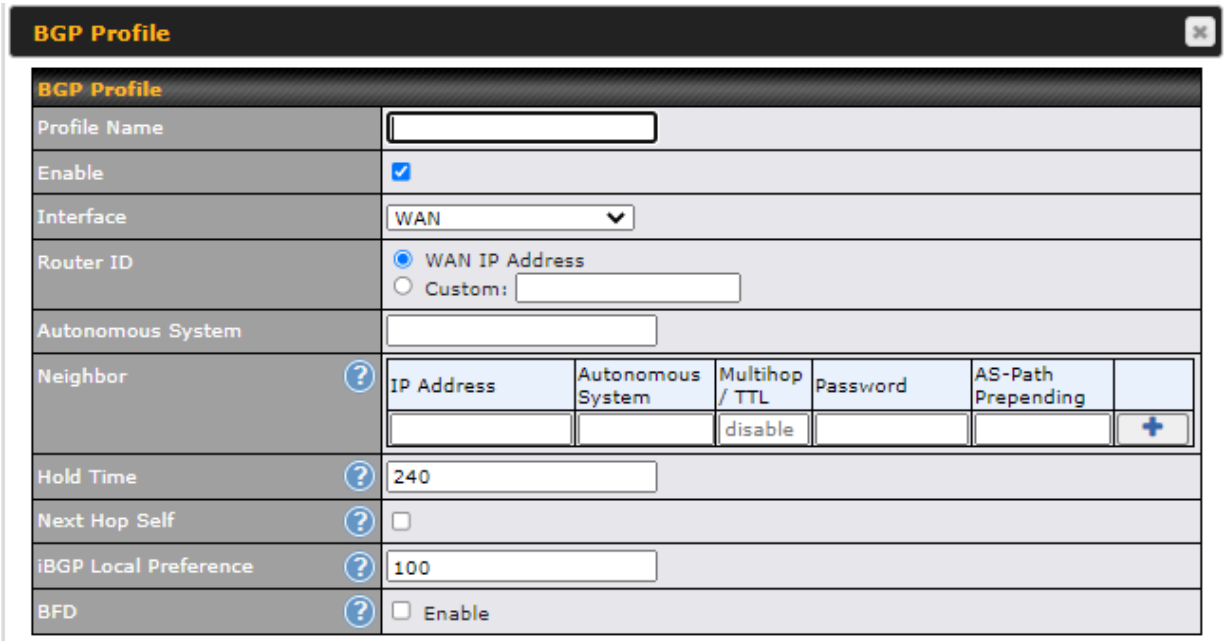
Click the **Network** tab along the top bar, and then click the **BGP** item on the sidebar to configure BGP.



Click the "**x**" to delete a BGP profile.

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

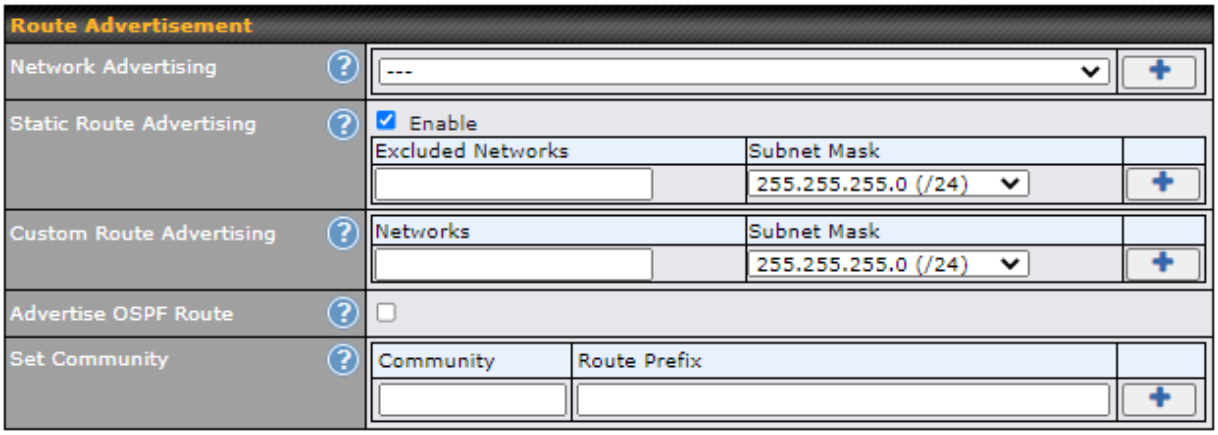
 Copyright @ 2021 Peplink



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.

 Copyright @ 2021 Peplink

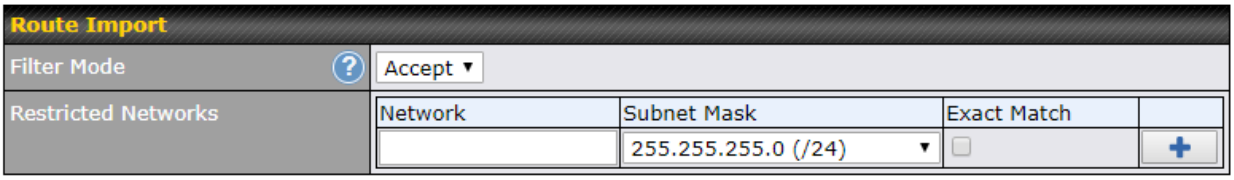
Hold Time	Wait time in seconds for a keepalive message from a Neighbor before considering the BGP connection as stalled. The value must be either 0 (infinite hold time) or between 3 and 65535 inclusively. Default: 240
Next Hop Self	Enable this option to advertise your own source address as the next hop 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.



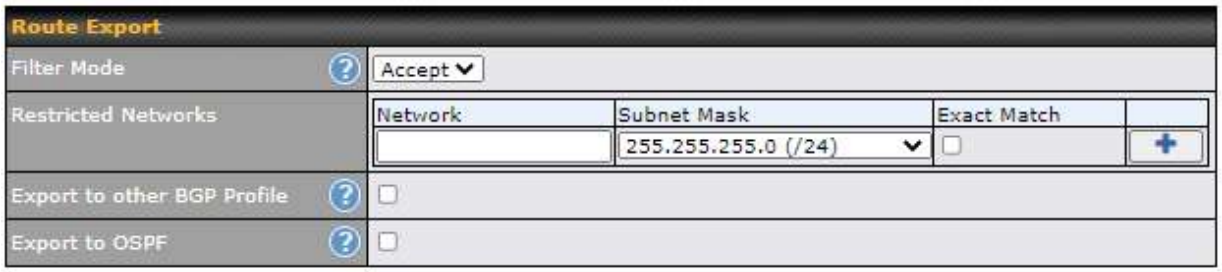
Network Advertising	Select the Networks that will be advertised to the BGP Neighbor.
Static Route Advertising	Enable this option to advertise static LAN routes. Static routes that match the Excluded Networks table will not be advertised.
Custom Route Advertising	Additional routes to be advertised to 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:

 Copyright @ 2021 Peplink

	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



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.



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

 Copyright @ 2021 Peplink

	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.

 Copyright @ 2021 Peplink

23 Remote User Access

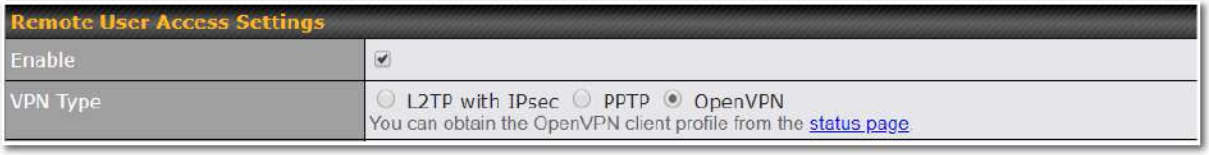
A remote-access VPN connection allows an individual user to connect to a private business network from a remote location using a laptop or desktop computer connected to the Internet. Networks routed by a Pepwave router can be remotely accessed via OpenVPN, L2TP with IPsec or PPTP. To configure this feature,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

23.1 L2TP with IPsec

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



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.

 Copyright @ 2021 Peplink

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.

 Copyright @ 2021 Peplink

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.

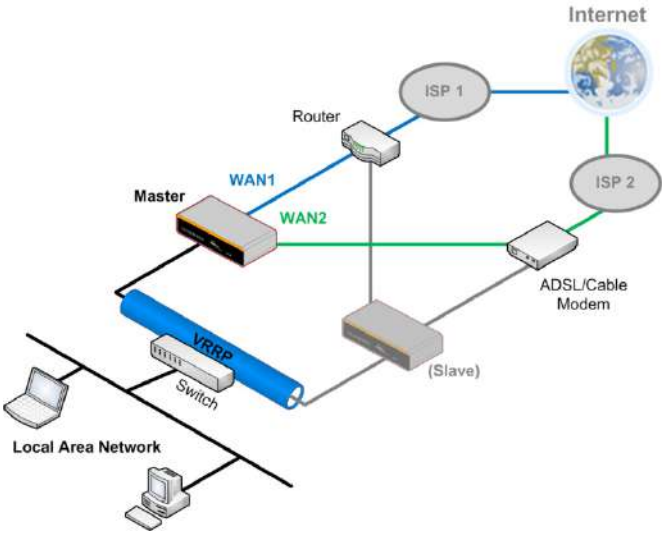
 Copyright @ 2021 Peplink

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

 Copyright @ 2021 Peplink

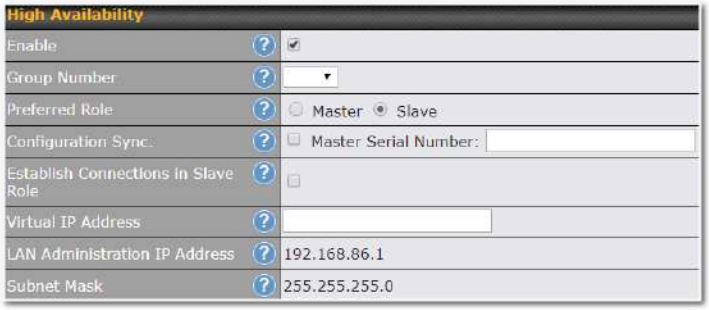
configured LAN IP address.

- 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

Interface for Slave Router



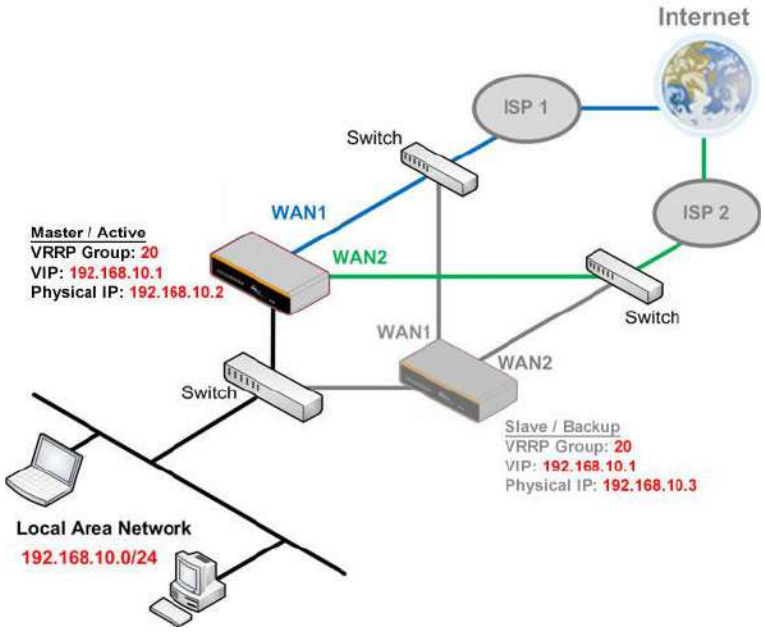
High Availability	
Enable	Checking this box specifies that the Pepwave router is part of a high availability configuration.
Group Number	This number identifies a pair of Pepwave routers operating in a high availability configuration. The two Pepwave routers in the pair must have the same **Group Number** 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**

 Copyright @ 2021 Peplink

	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.

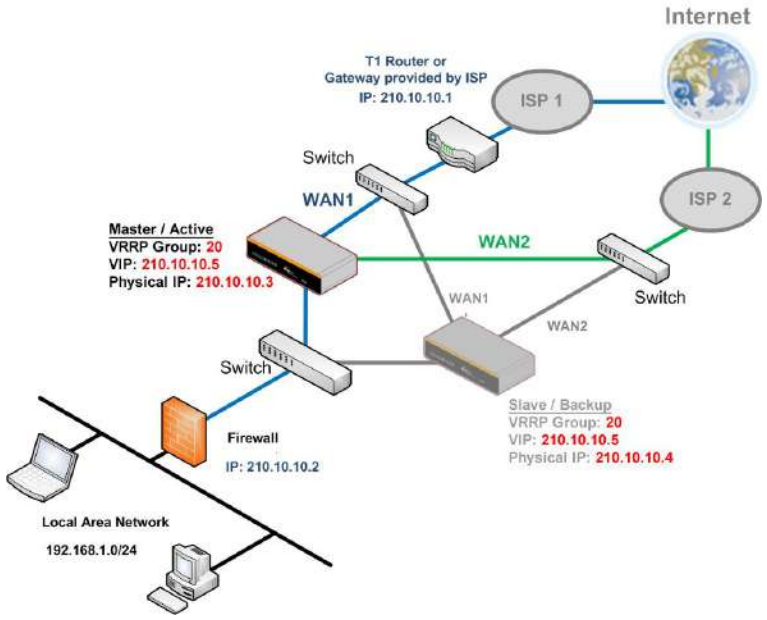
Important Note

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.



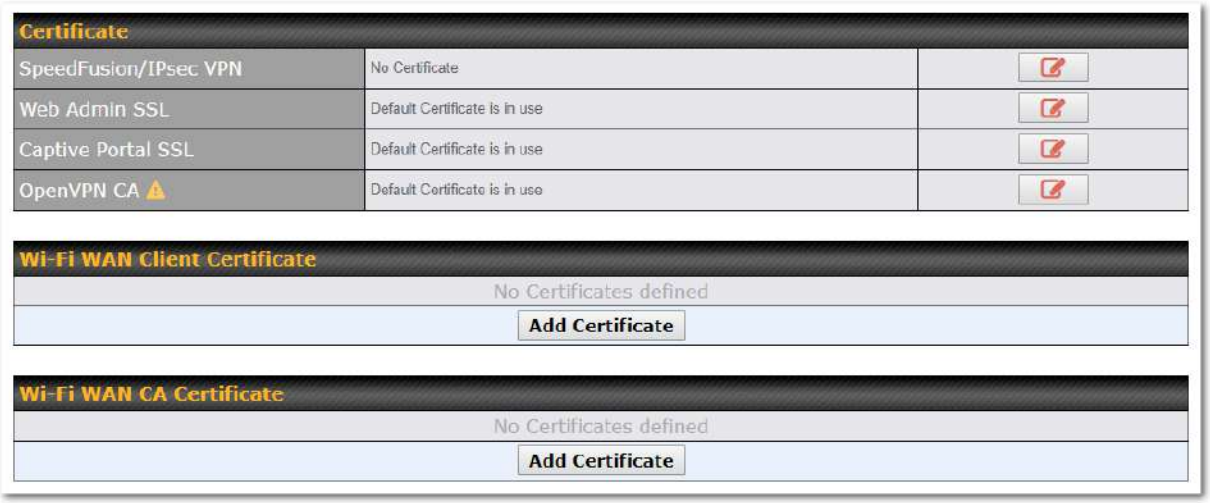
In drop-in mode, no other configuration needs to be set.

 Copyright @ 2021 Peplink



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



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.

 Copyright @ 2021 Peplink

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**.

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.

 Copyright @ 2021 Peplink

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.

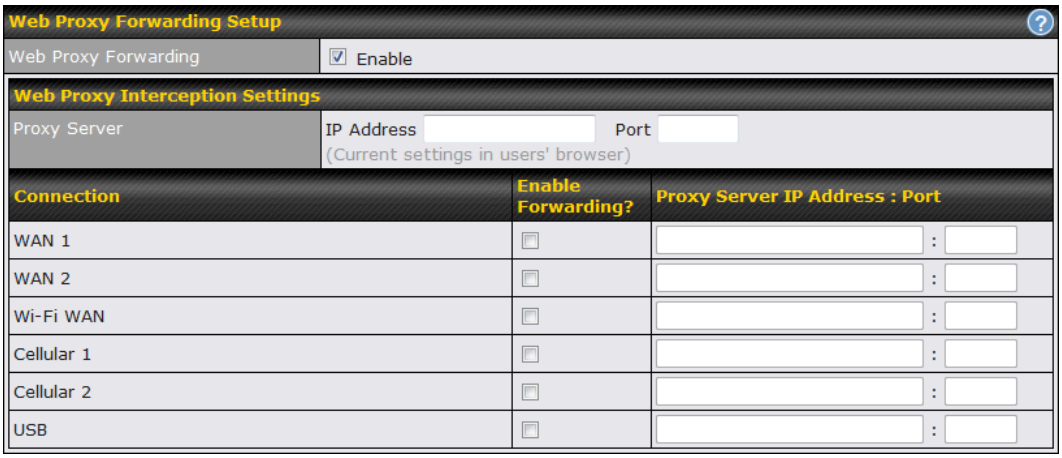
To enable the feature, select **Enable** under **SMTP Forwarding Setup**. Check **Enable Forwarding** for the WAN connection(s) that needs forwarding. Under **SMTP Server**, enter the ISP's e-mail server host name or IP address. Under **SMTP Port**, enter the TCP port number for each WAN.

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



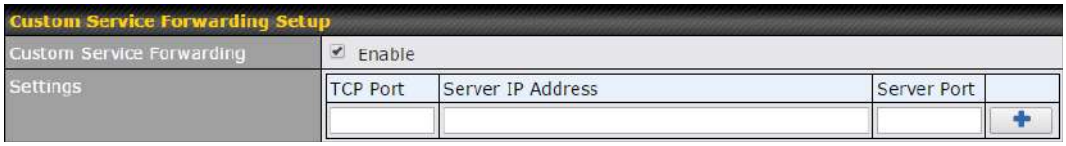
 Copyright @ 2021 Peplink

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

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

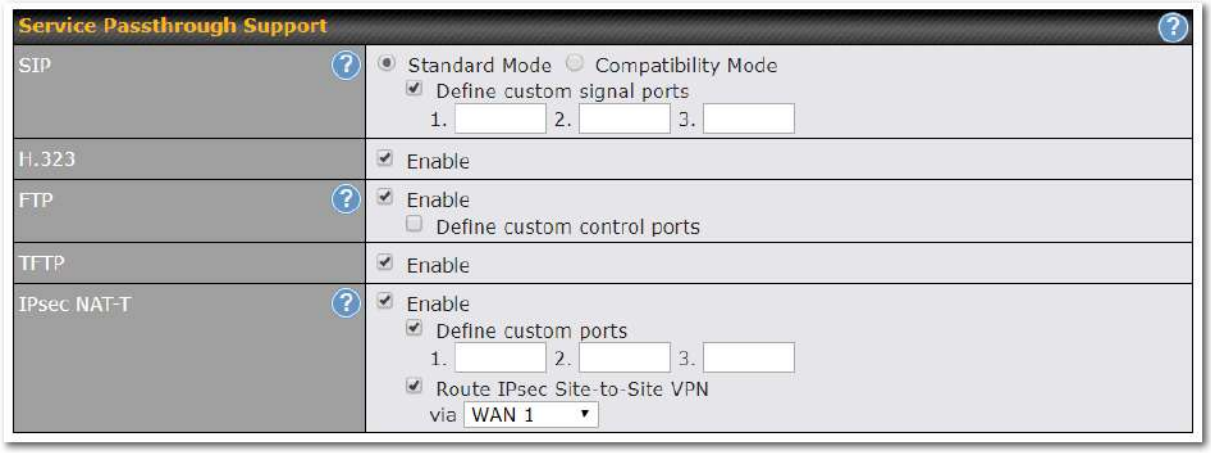


After clicking the **enable** checkbox, enter your TCP port for traffic heading to the router, and then specify the IP Address and Port of the server you wish to forward to the service to.

 Copyright @ 2021 Peplink

24.4 Service Passthrough

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



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.

 Copyright @ 2021 Peplink