



MAX Series

User Manual

Peplink Products:

BR2 Pro DX

Peplink Firmware 8.5.2

May 2025

COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice.

Copyright © 2021 Peplink Pepwave Ltd. All Rights Reserved. Pepwave and the Pepwave logo are trademarks of Peplink International Ltd. Other brands or products mentioned may be trademarks or registered trademarks of their respective owners.

Table of Contents

Introduction and Scope	6
Glossary	8
1 Product Features	9
1.1 Supported Network Features	9
1.2 Other Supported Features	12
2 MAX BR2 Pro DX Overview	13
2.1 Panel Appearance	13
3 Advanced Feature Summary	14
3.1 Drop-in Mode and LAN Bypass: Transparent Deployment	14
3.2 QoS: Clearer VoIP	14
3.3 Per-User Bandwidth Control	15
3.4 High Availability via VRRP	15
3.5 USB Modem and Android Tethering	16
3.6 Built-In Remote User VPN Support	16
3.7 SIM-card USSD support	17
3.8 KVM Virtualization	17
3.9 DPI Engine	18
3.10 NetFlow	18
3.11 Wi-Fi Air Monitoring	18
3.12 SP Default Configuration	18
3.13 Peplink Relay	19
3.14 DNS over HTTPS (DoH)	19
3.15 Peplink InTouch	19
3.16 Synergy Mode	19
3.17 Virtual WAN on VLAN	20
4 Installation	21
4.1 Preparation	21
4.2 Constructing the Network	21
4.3 Configuring the Network Environment	22
5 Connecting to the Web Admin Interface	23
6 SpeedFusion Connect Protect	25
6.1 Activate SpeedFusion Connect Protect	25
6.2 Enable SpeedFusion Connect Protect	26
6.3 Route by Cloud Application	31

6.4 Route by Wi-Fi SSID	32
6.5 Route by LAN Client	33
7 Configuring the LAN Interface(s)	35
7.1 Basic Settings	35
7.2 Port Settings	44
7.3 Captive Portal	45
8 Configuring the WAN Interface(s)	49
8.1 Ethernet WAN	52
8.2 Cellular WAN	60
8.3 Wi-Fi WAN	66
8.4 WAN Connection Settings (Common)	70
8.5 WAN Health Check	71
8.6 Bandwidth Allowance Monitoring	74
8.7 Additional Public IP address	75
8.8 Dynamic DNS Settings	75
9 SpeedFusion VPN	77
9.1 SpeedFusion VPN	78
10 IPsec VPN	88
10.1 IPsec VPN Settings	88
10.2 GRE Tunnel	92
11 OpenVPN	94
12 Outbound Policy	95
12.1 Adding Rules for Outbound Policy	95
13 Port Forwarding	105
13.1 UPnP / NAT-PMP Settings	107
14 NAT Mappings	108
15 Media Fast	110
15.1 Setting Up MediaFast Content Caching	110
15.2 Viewing MediaFast Statistics	112
15.3 Prefetch Schedule	113
16 Edge Computing	115
16.1 Configuring the ContentHub	115
16.2 Configure a website for ContentHub	115
16.3 Configure an application for ContentHub	117
17 Docker	120
18 KVM	121
19 QoS	122

19.1 User Groups	122
19.2 Bandwidth Control	123
19.3 Application Queue	123
19.4 Application	124
20 Firewall	126
20.1 Access Rules	127
20.2 Content Blocking	135
21 Routing Protocols	137
21.1 OSPF & RIPv2	137
21.2 BGP	139
22 Remote User Access	144
23 Miscellaneous Settings	147
23.1 High Availability	147
23.2 RADIUS Server	151
23.3 Certificate Manager	153
23.4 Service Forwarding	154
23.5 Service Passthrough	157
23.6 UART	158
23.7 GPS Forwarding	160
23.8 Ignition Sensing	161
Ignition Sensing installation	161
GPIO Menu	163
23.9 NTP Server	164
23.10 Grouped Networks	165
23.11 Remote SIM Management	166
23.12 SIM Toolkit	168
23.13 UDP Relay	170
24 AP	171
24.1 AP Controller	171
24.2 Wireless SSID	171
24.3 Wireless Mesh	177
24.4 Settings	178
25 AP Controller Status	185
25.1 Info	185
25.2 Access Point	187
25.3 Wireless SSID	190
25.4 Wireless Client	191

25.5 Mesh / WDS	192
25.6 Nearby Device	193
25.7 Event Log	193
26 Toolbox	194
27 System	195
27.1 Admin Security	195
27.2 Firmware	200
27.3 Time	202
27.4 Schedule	203
27.5 Email Notification	204
27.6 Event Log	207
27.7 SNMP	208
27.8 SMS Control	210
27.9 InControl	211
27.10 Configuration	212
27.11 Feature Add-ons	213
27.12 Reboot	213
28 Tools	214
28.1 Ping	214
28.2 Traceroute Test	215
28.3 Wake-on-LAN	215
28.4 WAN Analysis	216
28.5 CLI (Command Line Interface Support)	219
29 Status	220
29.1 Device	220
29.2 GPS Data	222
29.3 Active Sessions	223
29.4 Client List	225
29.5 UPnP / NAT-PMP	226
29.6 OSPF & RIPv2	227
29.7 BGP	227
29.8 SpeedFusion VPN	227
29.9 Event Log	232
30 WAN Quality	234
31 Usage Reports	235
31.1 Real-Time	235
31.2 Hourly	236

31.3 Daily	237
31.4 Monthly	238
Appendix A: Restoration of Factory Defaults	240
Appendix B: FusionSIM Manual	241
Appendix C: Overview of ports used by Peplink SD-WAN routers and other Peplink services	253
Appendix D: Declaration	255

Introduction and Scope

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

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

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

Tips

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



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

Glossary

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

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

1 Product Features

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

Our MAX HD series wireless routers are embedded with multiple 4G LTE modems, and allow simultaneous wireless Internet connections through multiple wireless networks. The wireless Internet connections can be bonded together using our SpeedFusion technology. This allows better reliability, larger bandwidth, and increased wireless coverage 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](https://DNS-O-Matic.com))
- Ping, DNS lookup, and HTTP-based health check

1.1.2 LAN

- Wi-Fi AP
- Ethernet LAN ports
- DHCP server on LAN

- Extended DHCP option support
- Static routing rules
- VLAN on LAN support

1.1.3 VPN

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

1.1.4 Firewall

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

1.1.5 Captive Portal

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

1.1.6 Outbound Policy

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

1.1.7 AP Controller

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

1.1.8 QoS

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

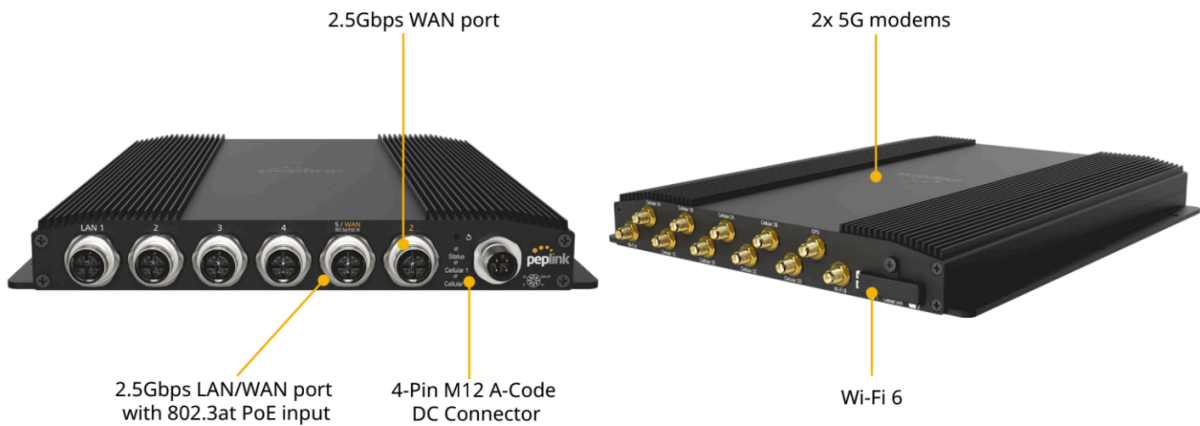
1.2 Other Supported Features

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

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

2 MAX BR2 Pro DX Overview

2.1 Panel Appearance



2.1.1 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)

3 Advanced Feature Summary

3.1 Drop-in Mode and LAN Bypass: Transparent Deployment



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

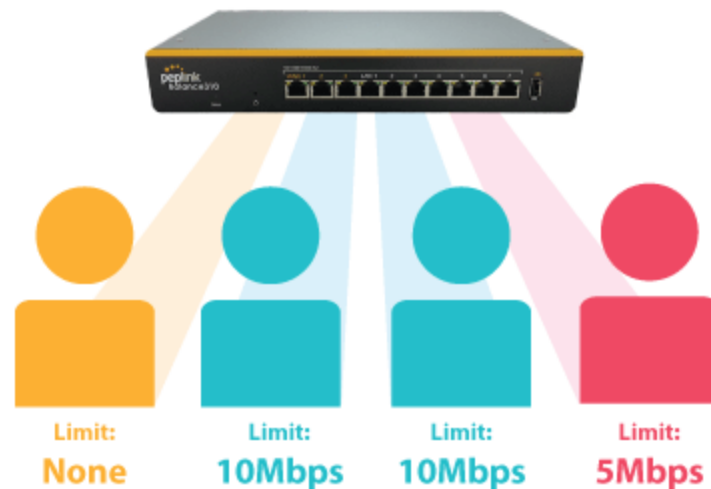
Note: Drop-in mode is compatible for All MAX models except MAX BR1 IP67

3.2 QoS: Clearer VoIP



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

3.3 Per-User Bandwidth Control



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

3.4 High Availability via VRRP



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

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

3.5 USB Modem and Android Tethering



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

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

3.6 Built-In Remote User VPN Support



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

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

[Click here for the full instructions on setting up OpenVPN connections](#)

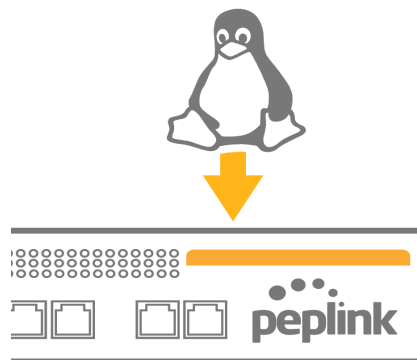
3.7 SIM-card USSD support



Cellular-enabled routers can now use USSD to check their SIM card's balance, process pre-paid cards, and configure carrier-specific services.

[Click here for full instructions on using USSD](#)

3.8 KVM Virtualization



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

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

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

3.9 DPI Engine

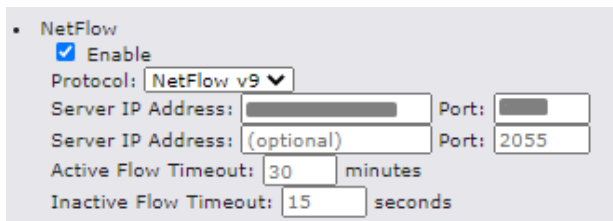
The DPI report written in the updated KB article will show further information on InControl2 through breaking down application categories into subcategories.

<https://forum.peplink.com/t/ic2-deep-packet-inspection-dpi-reports-and-everything-you-need-to-know-about-it/10151/>

3.10 NetFlow

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

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



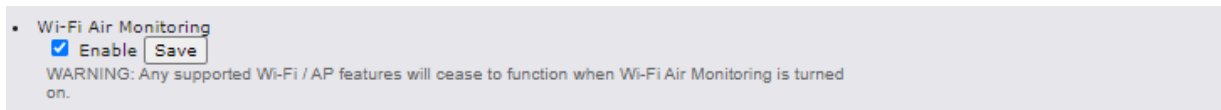
NetFlow configuration interface showing the following options:

- ☒ Enable
- Protocol: **NetFlow v9** (dropdown menu)
- Server IP Address: [text input] Port: [text input]
- Server IP Address: (optional) [text input] Port: 2055
- Active Flow Timeout: 30 minutes
- Inactive Flow Timeout: 15 seconds

3.11 Wi-Fi Air Monitoring

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



Wi-Fi Air Monitoring configuration interface showing the following options:

- ☒ Enable **Save** (button)
- WARNING: Any supported Wi-Fi / AP features will cease to function when Wi-Fi Air Monitoring is turned on.

3.12 SP Default Configuration

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

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

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>

3.16 Synergy Mode

Synergy mode is a cascade multiple devices and combine the number of WANs to a single device virtually. All the WANs on the Synergized Device will appear as native WAN interfaces at the Synergy Controller and it can be managed like the built-in WAN interfaces.

[https://forum.peplink.com/t/synergy-mode-\(firmware-8.3.0\)/639be7d8af8c71a6f3050323/](https://forum.peplink.com/t/synergy-mode-(firmware-8.3.0)/639be7d8af8c71a6f3050323/)

3.17 Virtual WAN on VLAN

The Virtual WAN Activation License allows you to create 1 x virtual WAN on a particular VLAN, on either WAN or LAN interface. This means that you can create a virtual WAN on VLAN for a WAN port, or a virtual WAN on VLAN for a LAN port.

<https://forum.peplink.com/t/b20x-virtual-wan-activation-license-faq/6204bac7d90b9e6355e96e8d/1>

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
- 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. Connect either another Ethernet cable or a USB modem to one of the WAN ports or USB ports respectively, or connect to Wi-Fi as WAN on the Pepwave router. Repeat the same process for any additional WAN ports.
3. Connect the power adapter to the power connector on the rear panel of the Pepwave router, and then plug it into a power outlet.

4.3 Configuring the Network Environment

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

- LAN configuration

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

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

- WAN configuration

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

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

5 Connecting to the Web Admin Interface

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

http://192.168.50.1

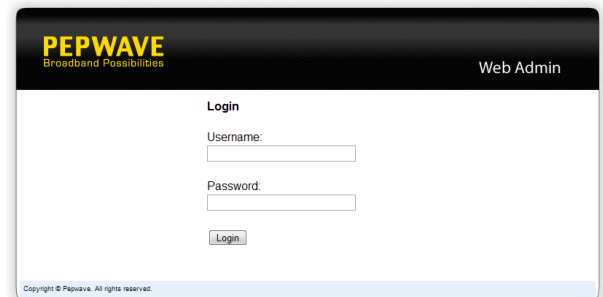
(This is the default LAN IP address for Pepwave routers.)

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

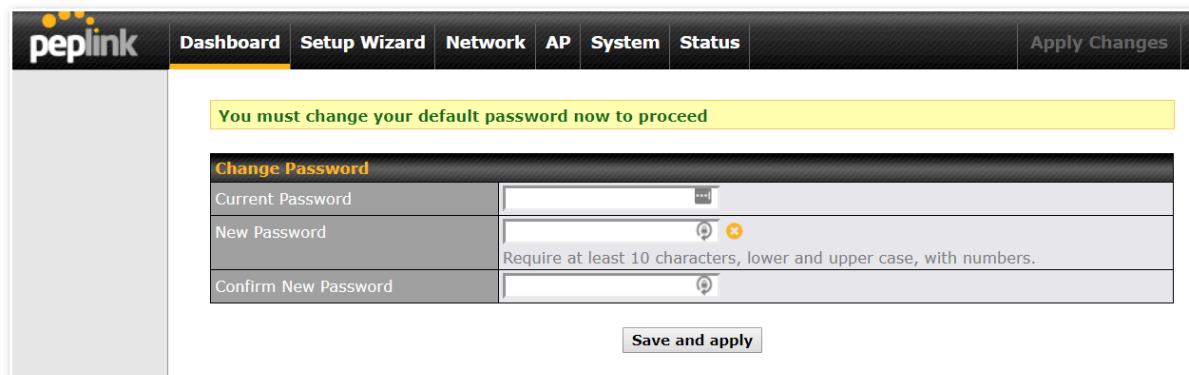
Username: admin

Password: admin

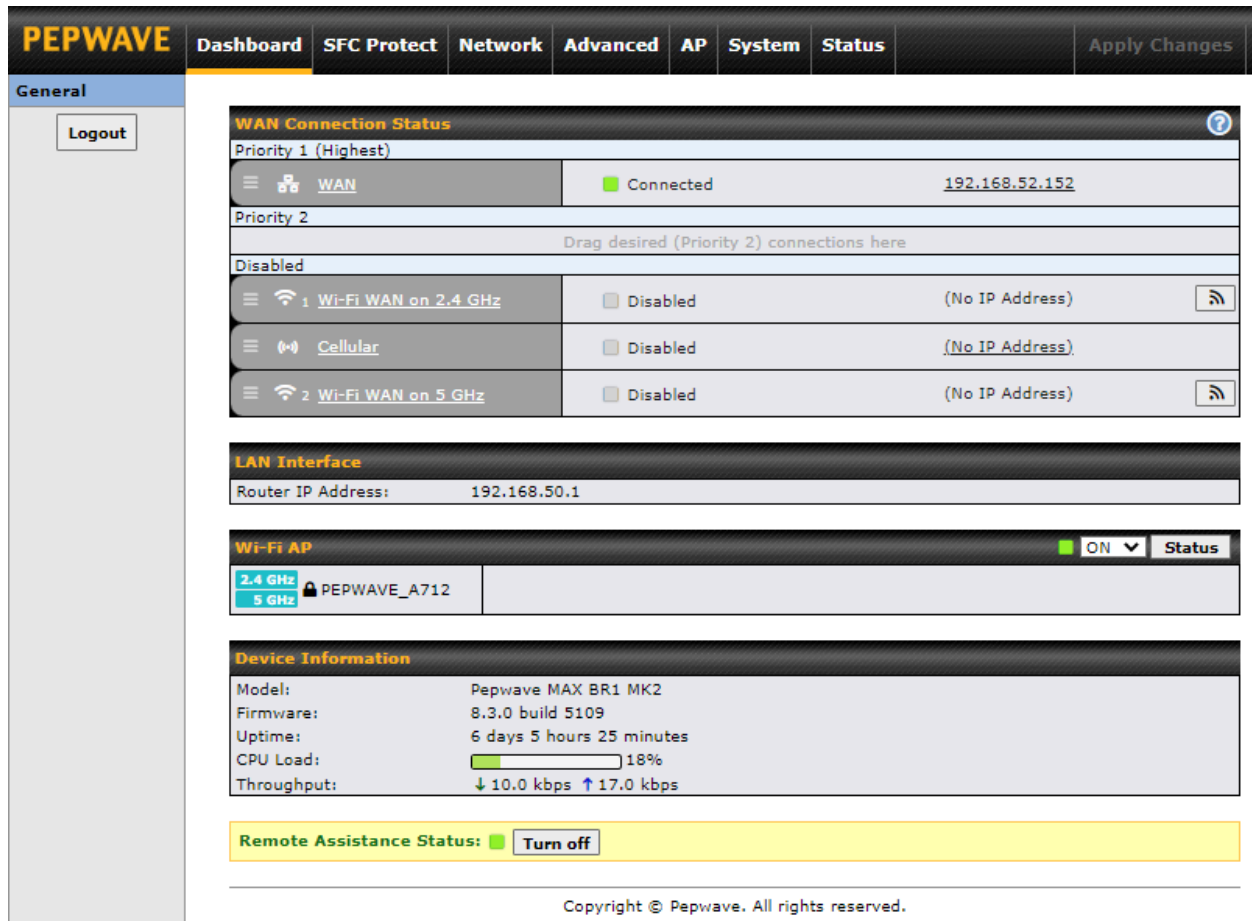
(This is the default username and password for Pepwave routers).



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



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



The screenshot shows the Peplink PEPWAVE web admin interface. The top navigation bar includes tabs for Dashboard, SFC Protect, Network, Advanced, AP, System, and Status, along with an 'Apply Changes' button. The left sidebar has a 'General' section with a 'Logout' button. The main content area displays several sections:

- WAN Connection Status:** A table showing connection priorities. Priority 1 (Highest) is 'WAN' with a status of 'Connected' and IP address '192.168.52.152'. Priority 2 is disabled with a prompt to 'Drag desired (Priority 2) connections here'. Below this, three other connections are listed as 'Disabled': 'Wi-Fi WAN on 2.4 GHz', 'Cellular', and 'Wi-Fi WAN on 5 GHz', all with '(No IP Address)'.
- LAN Interface:** Shows the 'Router IP Address' as '192.168.50.1'.
- Wi-Fi AP:** Shows the status as 'ON' with a dropdown menu and a 'Status' button. Below it, two frequencies are listed: '2.4 GHz' and '5 GHz', both with a lock icon and the name 'PEPWAVE_A712'.
- Device Information:** A table showing device details:

Model:	Pepwave MAX BR1 MK2
Firmware:	8.3.0 build 5109
Uptime:	6 days 5 hours 25 minutes
CPU Load:	18%
Throughput:	↓ 10.0 kbps ↑ 17.0 kbps
- Remote Assistance Status:** A yellow bar showing the status as 'Turn off'.

At the bottom of the dashboard, there is a copyright notice: 'Copyright © Pepwave. All rights reserved.'

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

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

Important Note

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

6 SpeedFusion Connect Protect

With Pepwave products, your device is able to connect to SpeedFusion Connect Protect 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.*



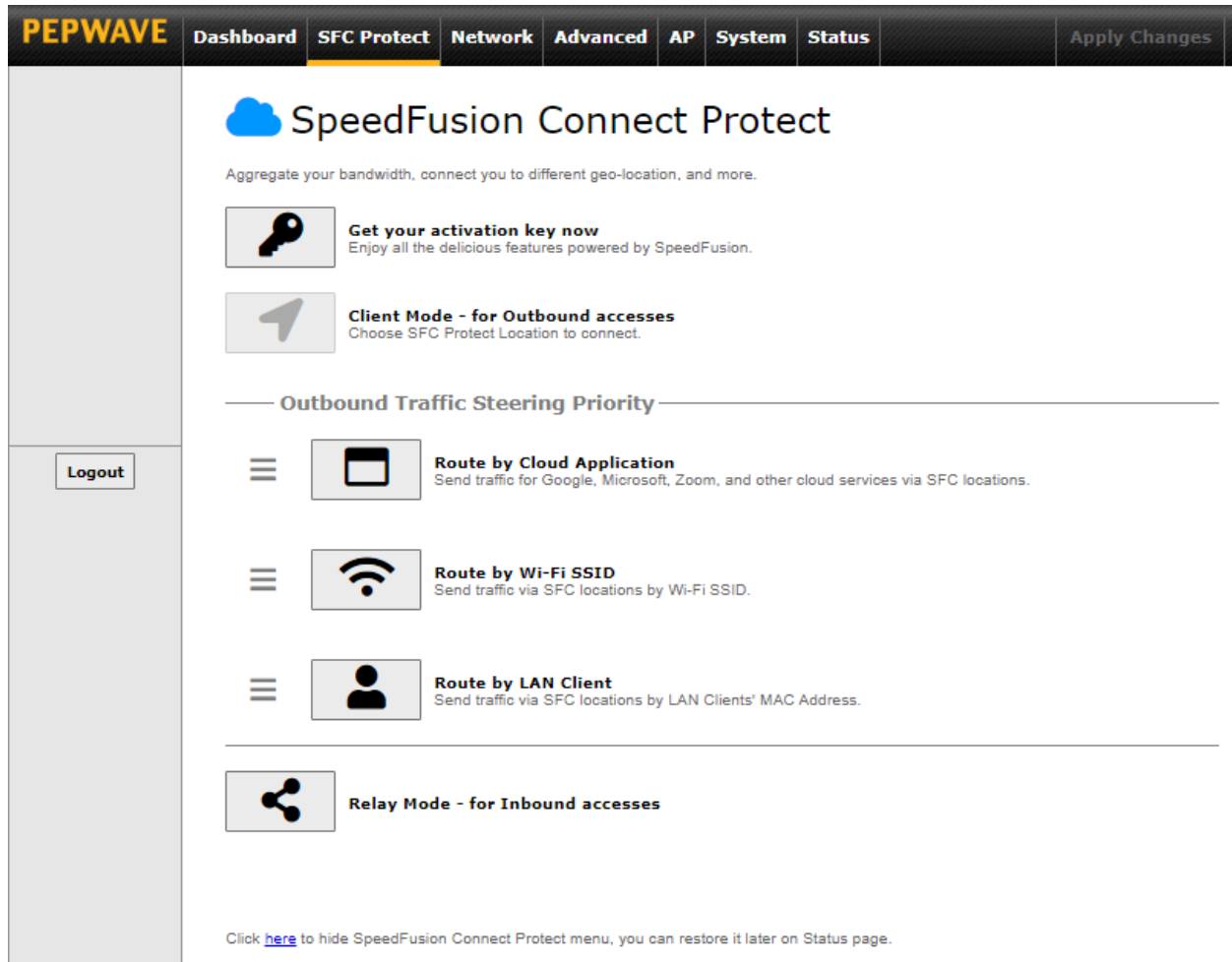
*SpeedFusion Connect Protect is supported in firmware version 8.1.0 and above. SpeedFusion Connect is a subscription basis. SpeedFusion Connect Protect license can be purchased at <https://estore.peplink.com/> > **SpeedFusion Service** > **SpeedFusion Connect Protect**.

6.1 Activate SpeedFusion Connect Protect

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

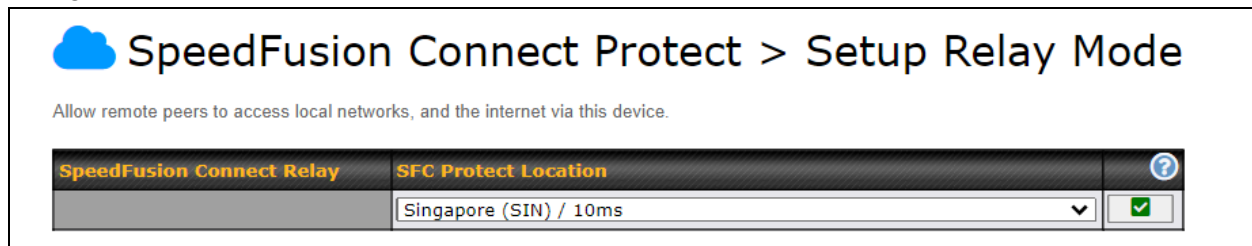
6.2 Enable SpeedFusion Connect Protect

Access the Web Admin of the device you want to create as the Peplink Relay Server, navigating to the “**SFC Protect**” tab.



The screenshot shows the Peplink Web Admin interface. The top navigation bar includes tabs for Dashboard, **SFC Protect**, Network, Advanced, AP, System, and Status. The **SFC Protect** tab is active. The main content area is titled "SpeedFusion Connect Protect" and includes a sub-header "Aggregate your bandwidth, connect you to different geo-location, and more." Below this, there are three main sections: "Get your activation key now" (with a key icon), "Client Mode - for Outbound accesses" (with a location pin icon), and "Outbound Traffic Steering Priority". Under "Outbound Traffic Steering Priority", there are three options: "Route by Cloud Application" (with a cloud icon), "Route by Wi-Fi SSID" (with a Wi-Fi icon), and "Route by LAN Client" (with a person icon). At the bottom, there is a "Relay Mode - for Inbound accesses" section (with a share icon). A "Logout" button is visible in the left sidebar. A footer note states: "Click [here](#) to hide SpeedFusion Connect Protect menu, you can restore it later on Status page."

To setup a Peplink Relay Mode, select “**Relay Mode - for Inbound accesses**” > Choose the **SFC Protect Location** you wish to connect to > Click on the **Green tick button** to confirm the change.



The screenshot shows the "SpeedFusion Connect Protect > Setup Relay Mode" configuration page. It includes a sub-header "Allow remote peers to access local networks, and the internet via this device." Below this, there is a table with two columns: "SpeedFusion Connect Relay" and "SFC Protect Location". The "SFC Protect Location" column contains a dropdown menu with "Singapore (SIN) / 10ms" selected. To the right of the dropdown is a green checkmark button. A help icon (?) is visible in the top right corner of the table.

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



SpeedFusion Connect Protect > Setup Relay Mode

Allow remote peers to access local networks, and the internet via this device.

SpeedFusion Connect Relay	SFC Protect Location	
SFC-RELAY-SERVER-HKG	Relay Sharing Code: 7848-8886-6627-6299	

To connect to SpeedFusion Connect Protect, you can select a **SFC Protect Location** of your choice, or simply and **Automatic** then the device will establish connection to the neareset SFC Protect server.

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



SpeedFusion Connect Protect > Choose SFC Protect Location

You can connect up to 3 different sfc protect locations.

SpeedFusion Connect Protect	SFC Protect Location	
	Automatic	

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.



SpeedFusion Connect Protect > Choose SFC Protect Location

You can connect up to 3 different sfc protect locations.

SpeedFusion Connect Protect	SFC Protect Location	
	[Relay Sharing] e.g. 1234-5678-1234-5678	

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

PEPWAVE Dashboard **SFC Protect** Network Advanced AP System Status **Apply Changes**

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

SpeedFusion Connect Protect > Choose SFC Protect Location

SpeedFusion Connect Protect	SFC Protect Location	
SFC	Automatic	

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

Wi-Fi AP ON Status

No Wi-Fi AP

SpeedFusion Connect Protect

SFC	Established
-----	--------------------------

Data usage allowance:

If you are running a latency sensitive service like video streaming or VOIP, a WAN Smoothing sub-tunnel can be created. Navigate to **SFC Protect > Client Mode - for Outbound accesses > SFC**.

SpeedFusion Connect Protect > Choose SFC Protect Location

SpeedFusion Connect Protect	SFC Protect Location	
SFC	Automatic	

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

SpeedFusion Connect Protect Profile

Enable	☒
SFC Protect Location	Automatic

1 2 - WAN Smoo... **+**

Tunnel Options

Local / Remote Tunnel ID	2	
Tunnel Name	WAN Smoothing	
Data Port	☒ Auto ☐ Custom	
Bandwidth Limit	☐	
TCP Ramp Up	☐	
WAN Smoothing	Overall Redundancy Level	Normal
	Maximum Level on the Same Link	Normal
Forward Error Correction	Off	
Receive Buffer	0 ms	
Packet Fragmentation	☒ Always ☐ Use DF Flag	

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

Wi-Fi AP ON Status

No Wi-Fi AP

SpeedFusion Connect Protect

SFC (1)	■ Established
SFC (2 - WAN Smoothing)	■ Established

Data usage allowance:

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

PEPWAVE Dashboard SFC Protect Network **Advanced** AP System Status Apply Changes

Advanced

- SpeedFusion VPN
- IPsec VPN
- GRE Tunnel
- OpenVPN
- Outbound Policy**
- Port Forwarding

NAT Mappings

QoS

- User Groups
- Bandwidth Control
- Application Queue
- Application

Firewall

- Access Rules
- Content Blocking

Routing Protocols

- OSPF & RIPv2
- BGP

Remote User Access

Add a New Custom Rule

Service Name:

Enable: ☒

Source: Any

Destination: IP Network Mask: 255.255.255.0 (/24)

Protocol: Any :: Protocol Selection ::

Algorithm: Priority

Priority Order: Highest Priority Not In Use

- ☒ SFC Protect: SFC
- ☐ WAN: WAN
- ☐ WAN: Cellular
- ☐ WAN: Wi-Fi WAN on 2.4 GHz
- ☐ WAN: Wi-Fi WAN on 5 GHz
- ☐ Lowest Priority

When No Connections are Available: Drop the Traffic

Terminate Sessions on Connection Recovery: ☐ Enable

Save Cancel

Outbound Policy

Custom

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

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

Expert Mode

Enabled

6.3 Route by Cloud Application

Optimize Cloud Application allows you to route Internet traffic through SpeedFusion Connect Protect based on the application. Go to **SFC Protect > Route by Cloud Application**.



SpeedFusion Connect Protect

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



Client Mode - for Outbound accesses
Choose SFC Protect Location to connect.

Outbound Traffic Steering Priority





Route by Cloud Application
Send traffic for Google, Microsoft, Zoom, and other cloud services via SFC locations.

Select a Cloud application to route through SpeedFusion Connect Protect from the drop down list > Click  > Save > Apply Changes.

Click the  to remove a selected Cloud application from routing through SpeedFusion Connect Protect.



SpeedFusion Connect Protect > Optimize Cloud Application

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

Automatic	
SFC (1)	Cloud Application --- Google Workspace Zoom Lifesize Salesforce WebEx Dropbox Microsoft Services Microsoft Office 365 Exchange Online SharePoint and OneDrive Skype for Business and Microsoft Teams +
SFC (2 - WAN Smoothing)	--- +

6.4 Route by Wi-Fi SSID

SpeedFusion Connect Protect provides a convenient way to route the Wi-Fi client to the cloud from **SFC Protect > Route by Wi-Fi SSID**.



SpeedFusion Connect Protect

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



Client Mode - for Outbound accesses
 Choose SFC Protect Location to connect.

Outbound Traffic Steering Priority




Route by Cloud Application
 Send traffic for Google, Microsoft, Zoom, and other cloud services via SFC locations.




Route by Wi-Fi SSID
 Send traffic via SFC locations by Wi-Fi SSID.

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



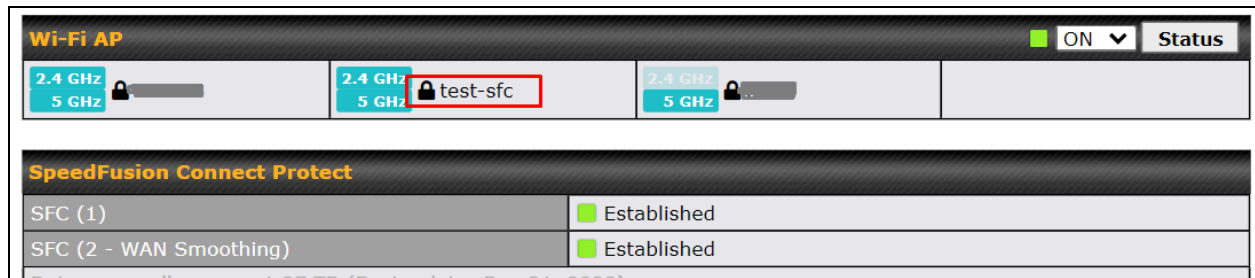
SpeedFusion Connect Protect > Link Wi-Fi to SFC Protect

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

Automatic			
SFC (1)	Reference SSID	SSID for SFC Protect	
	test-sfc	test-sfc (Automatic)	
	---		
SFC (2 - WAN Smoothing)	Reference SSID	SSID for SFC Protect	
	---		

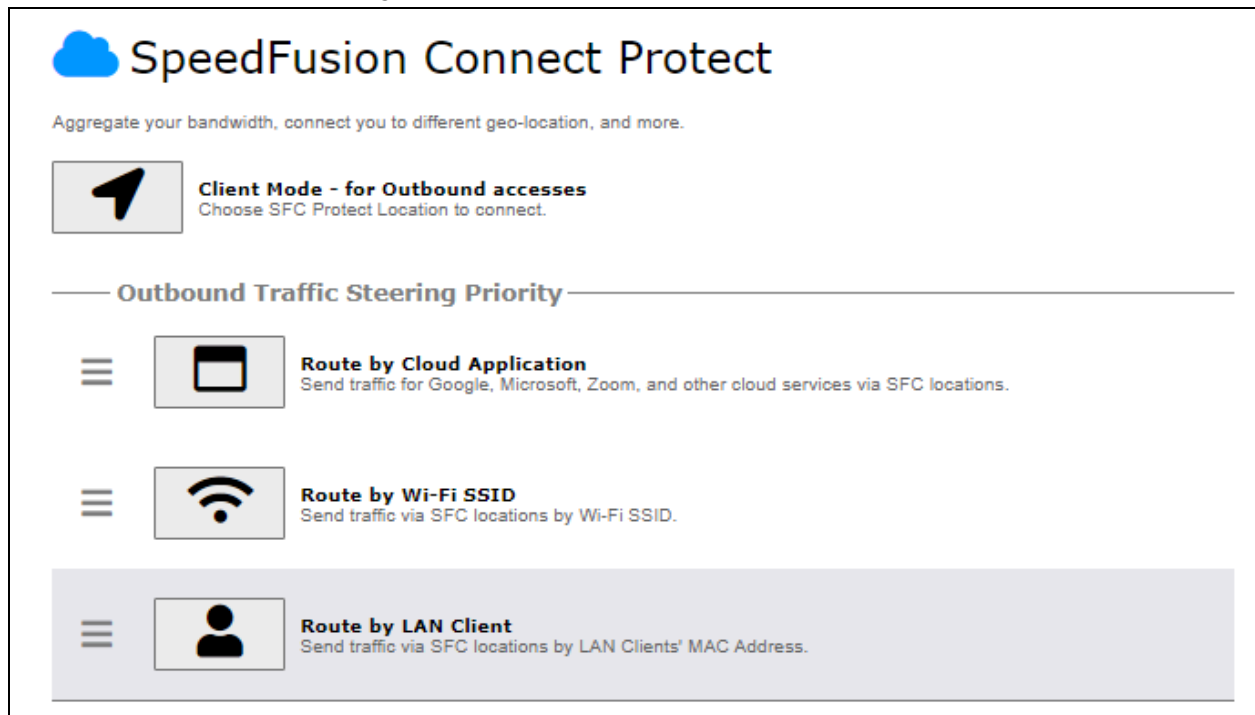
Save

SFC Protect SSID will be shown on **Dashboard**.



6.5 Route by LAN Client

SpeedFusion Connect Protect provides a convenient way to route the LAN client to the cloud from **SFC Protect > Route by LAN Client**.



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

SpeedFusion Connect Protect > Connect Clients to SFC Protect

Traffic from the selected clients will be redirected to the assigned SFC protect.

Automatic			
SFC (1)	Client	IP Address	
			+
SFC (2 - WAN Smoothing)	Client	IP Address	
			+

Save

7 Configuring the LAN Interface(s)

7.1 Basic Settings

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

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

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	255.255.255.0 (/24) ▼

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

Network Settings	
Name	
VLAN ID	
Inter-VLAN routing	☒

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

Layer 2 SpeedFusion VPN Bridging		?
SpeedFusion VPN Profiles to Bridge	? No profile is available	Help Close If you want to enable DHCP Option 82 Injection, please click here . This allow the device to inject Option 82 with Device Name information before forwarding the DHCP Request packet to SpeedFusion VPN peer, such that the DHCP Server can identify where does this request come from.
Spanning Tree Protocol	☐	
DHCP Option 82 Injection	☒	
Override IP Address when bridge connected	☒ Do not override ☐ Static ☐ By DHCP ☐ As None	

Layer 2 SpeedFusion VPN Bridging	
SpeedFusion VPN Profiles to Bridge	The remote network of the selected SpeedFusion VPN profiles will be bridged with this local LAN, creating a Layer 2 SpeedFusion VPN, they will be connected and operate like a single LAN, and any broadcast or multicast packets will be sent over the VPN.
Spanning Tree Protocol	Click the box will enable STP for this layer 2 profile bridge.
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 SpeedFusion VPN peer, such that the DHCP Server can identify where the request originates from.
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 SpeedFusion VPN 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 Server											
DHCP Server	? ☒ Enable										
DHCP Server Logging	☐										
IP Range	- 255.255.255.0 (/24) v										
Lease Time	Days Hours Mins										
DNS Servers	☒ Assign DNS server automatically										
BOOTP	☐										
Extended DHCP Option	<table border="1"> <thead> <tr> <th>Option</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td colspan="2">No Extended DHCP Option</td> </tr> <tr> <td colspan="2"> Add </td> </tr> </tbody> </table>	Option	Value	No Extended DHCP Option		Add					
Option	Value										
No Extended DHCP Option											
Add											
DHCP Reservation	? <table border="1"> <thead> <tr> <th>Name</th> <th>MAC Address</th> <th>Static IP</th> <th></th> </tr> </thead> <tbody> <tr> <td> </td> <td>00:00:00:00:00:00</td> <td> </td> <td> + </td> </tr> </tbody> </table>	Name	MAC Address	Static IP			00:00:00:00:00:00		+		
Name	MAC Address	Static IP									
	00:00:00:00:00:00		+								

DHCP Server Settings	
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.
DHCP Server Logging	Enable logging of DHCP events in the eventlog by selecting the checkbox.
IP Range	These settings allocate a range of IP addresses that will be assigned to LAN computers by the Pepwave router's DHCP server.
Lease Time	This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of Lease Time , the assigned IP address will no longer be valid and the IP address assignment must be renewed.
DNS Servers	This option allows you to input the DNS server addresses to be offered to DHCP clients. If Assign DNS server automatically is selected, the Pepwave router's built-in DNS server address (i.e., LAN IP address) will be offered.
BOOTP	Check this box to enable BOOTP on older networks that still require it.
Extended DHCP Option	In addition to standard DHCP options (e.g. DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts. To define an extended DHCP option, click the Add button, choose the option to define, and then enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only.
DHCP Reservation	This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses. The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses. Name (an optional field) allows you to specify a name to represent the device. MAC addresses should be in the format of 00:AA:BB:CC:DD:EE. Press  to create a new record. Press  to remove a record. Reserved clients information can be imported from the Client List, located at Status>Client List. For more details, please refer to Section 22.3.

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

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

DHCP Relay Settings	
Enable	Check this box to turn on DHCP relay. Click the  icon to disable DHCP relay.
DHCP Server IP Address	Enter the IP addresses of one or two DHCP servers in the provided fields. The DHCP servers entered here will receive relayed DHCP requests from the LAN. For active-passive DHCP server configurations, enter active and passive DHCP server relay IP addresses in DHCP Server 1 and DHCP Server 2 .
DHCP Option 82	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.
DHCP Relay Logging	Enable logging of DHCP Relay events in the eventlog by selecting the checkbox.

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

Static Route Settings 			
Static Route	Destination Network	Subnet Mask	Gateway
		255.255.255.0 (/24) ▼	
			

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

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

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

In case of a network address conflict with remote peers (i.e. SpeedFusion VPN / 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.

DNS Proxy Settings ?			
Enable	☒		
DNS Caching ?	☐		
Include Google Public DNS Servers ?	☐		
Local DNS Records ?	Host Name	IP Address	TTL
			3600 +
Domain Lookup Policy ?	Domain	Connection	
		v	+
DNS Resolvers ?	☐ WAN		192.168.52.1
	☐ Cellular		
	☐ Wi-Fi WAN on 2.4 GHz		
	☐ Wi-Fi WAN on 5 GHz		
	☐ SFC		
	☐ Untagged LAN		
Preferred connections are shown with ☒			
Save			

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 x to remove a record.
Domain Lookup Policy	DNS Proxy will lookup the domain names defined in this table using the specified connections only.

DNS Resolvers ^A

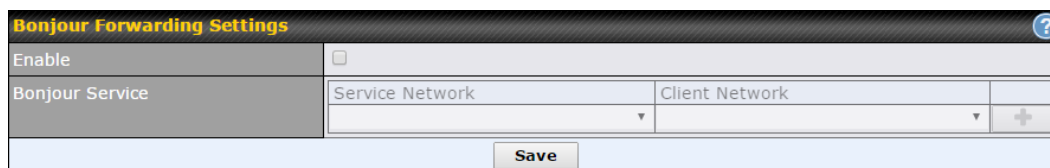
This field specifies which DNS servers can receive forwarded DNS requests. If no DNS server is selected, then all of them will be selected by default.

If you wish to select a SpeedFusion VPN peer, enter the IP address(es) of the VPN peer's DNS server.

Incoming queries will be forwarded to one of the selected servers. If none of the selected servers can be reached, then the router will forward incoming queries to all servers with healthy WAN connections.

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

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



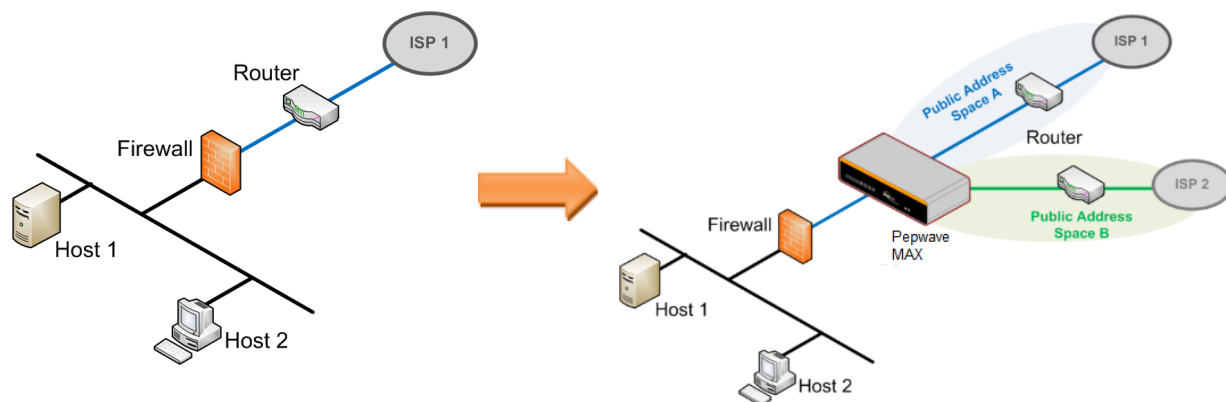
Bonjour Forwarding Settings		
Enable	☐	
Bonjour Service	Service Network	Client Network
Save		

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

Drop-In Mode

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

The following diagram illustrates drop-in mode setup:



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

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

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

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

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

Drop-in Mode Settings	
Enable	Drop-in mode eases the installation of the Pepwave MAX on a live network between the existing firewall and router, such that no configuration changes are required on existing equipment. Check the box to enable the drop-in mode feature.
WAN for Drop-In Mode	Select the WAN port to be used for drop-in mode. If WAN is selected, the high availability feature will be disabled automatically.
Shared Drop-In IP^A	When this option is enabled, the passthrough IP address will be used to connect to WAN hosts (email notification, remote syslog, etc.). The MAX will listen for this IP address when WAN hosts access services provided by the MAX (web admin access from the WAN, DNS server requests, etc.). To connect to hosts on the LAN (email notification, remote syslog, etc.), the default gateway address will be used. The MAX will listen for this IP address when LAN hosts access services provided by the MAX (web admin access from the WAN, DNS proxy, etc.).

Shared IP Address^A	Access to this IP address will be passed through to the LAN port if this device is not serving the service being accessed. The shared IP address will be used in connecting to hosts on the WAN (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.

7.2 Port Settings

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

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

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

7.3 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

General Settings

Name			
Enable	☒ Untagged LAN		
Hostname		<button>Default</button>	
Access Mode	☒ Open Access ☐ User Authentication ☐ External Server		

Portal Access Settings

Access Quota	30	mins (0: Unlimited)
	0	MB (0: Unlimited)
Quota Reset Time	☒ Daily at 00 :00 ☐ 1440 minutes after quota reached	
Inactive Timeout	0	minutes (0: No Timeout)
Allowed Networks	Domain Name / IP Address / Network +	
Allowed Clients	MAC / IP Address / Host Identifier +	
Splash Page	☒ Built-in ☐ External, URL: http://	
Popup Handling	☐ Bypass Popup (Redirection only takes place on normal browser) ☐ Automatically show splash page on Safari for Apple (iOS / macOS) devices	
Logout Hostname	(Not configured)	

Click [here](#) to preview / customize built-in splash page

Save

Cancel

Captive Portal Settings	
Name	Enter the name for the Captive Portal.
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.

Select **External Server** to use the Captive Portal with a HotSpot system.

As described in the following knowledgebase article:

<https://forum.peplink.com/t/using-hotspotsystem-wi-fi-on-pepwave-max-routers/>

Authentication

When selecting the “**User Authentication**” in the Access Mode field, you will see the available option for the Authentication via drop-down list:

- RADIUS Server

Access Mode	☐ Open Access ☒ User Authentication ☐ External Server	
Authentication	RADIUS Server ▼	

RADIUS Settings		
	Primary	Secondary
Authentication Protocol	PAP ▼	
	You may click here to define RADIUS Server Authentication profile, or you may go to RADIUS Server page to define multiple profiles	
Authentication Host		
Authentication Port	1812	1812
Authentication Secret	☒ Hide Characters	☒ Hide Characters
	You may click here to define RADIUS Server Accounting profile, or you may go to RADIUS Server page to define multiple profiles	
Accounting Host		
Accounting Port	1813	1813
Accounting Secret	☒ Hide Characters	☒ Hide Characters
CoA-DM	☐	
Accounting Interim Interval	?	
NAS-Identifier	?	

- LDAP Server

Access Mode	☐ Open Access ☒ User Authentication ☐ External Server	
Authentication	LDAP Server ▼	

LDAP Settings		
LDAP Server		Port Default
	☐ Use DN/Password to bind to LDAP Server	
Base DN		
Base Filter		

Fill in the necessary information to complete your connection to the server and enable authentication.

External Server

When selecting the “**External Server**” in the Access Mode field, you will see the available option for the Service Type via drop-down list:

- CoovaChilli

	Access Mode ☐ Open Access ☐ User Authentication ☒ External Server Server Type ? CoovaChilli CoovaChilli Settings UAM Secret ☒ Hide Characters HotspotSystem Access Mode ☐ Open Access ☐ User Authentication ☒ External Server Server Type ? HotspotSystem HotspotSystem Settings Operator Username Location ID Splash Page Domain ? customer.hotspotsystem.com
	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.
Inactive Timeout	Clients will get disconnected when the inactive the configured time is reached. Default 0: no timeout
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.
Popup Handling	Configurable options for popup handling: - Bypass Popup (Redirection only takes place on normal browser) - Automatically show splash page on Safari for Apple (iOS / macOS) devices
Logout Hostname	A hostname that can be used to logout captive portal when being accessed on browser.
Customize splash page	Click on the provided link in the Captive portal profile to customize the splash page. A new browser tab is opened with a WYSIWYG editor of the splash page o edit the content, click on the corresponding element after switching Edit Mode to ON.

Captive Portal



☐ Use uploaded Logo Image
☒ Use default Logo Image
☐ Choose File No file chosen

NOTE: Size max 512KB. Supported images types: JPEG, PNG and GIF.

EMPTY STRING

☒ I have read and agree to the [terms and conditions](#) ?

You must accept the terms and conditions before you can proceed

Agree

Powered by Pepwave.

Portal Configuration

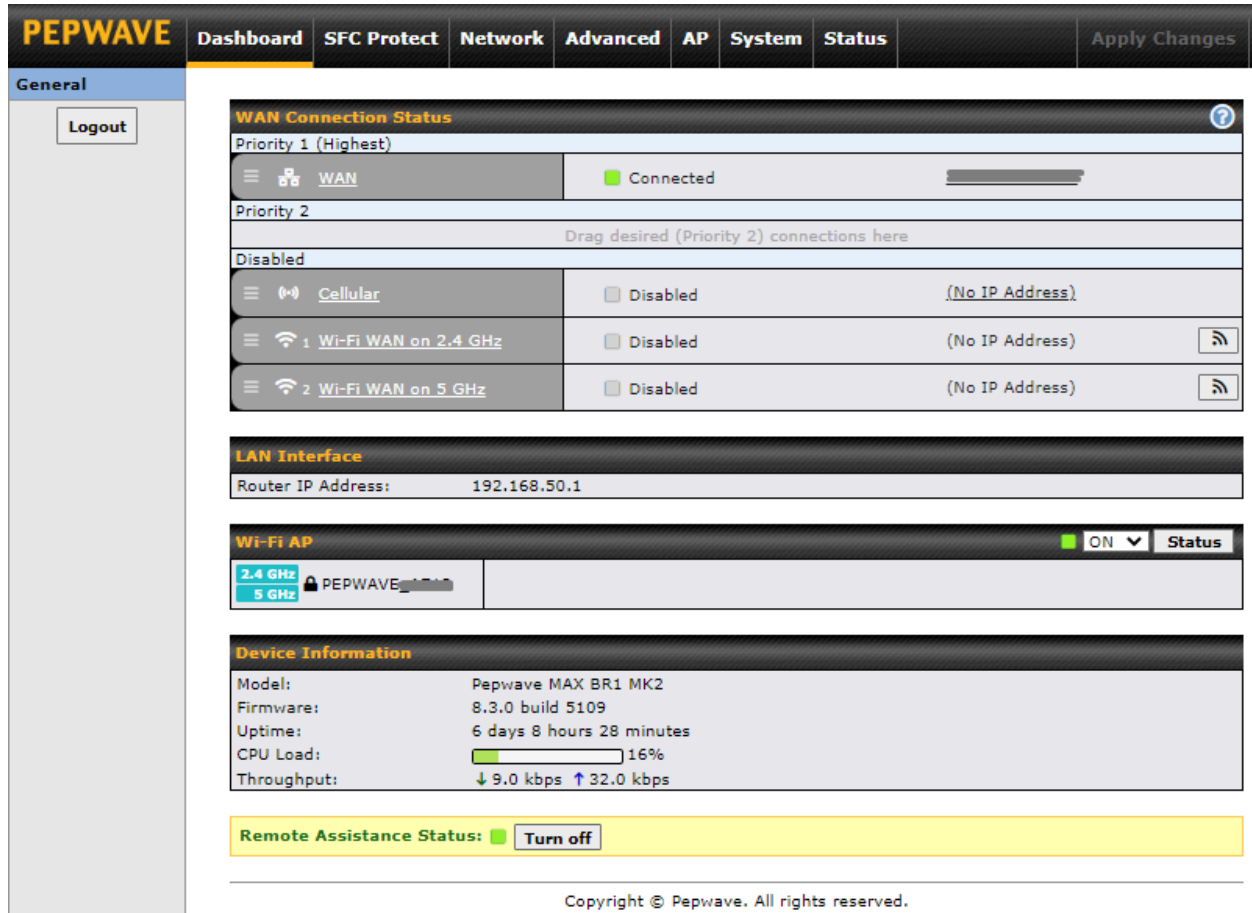
Show Quota Status	☒
Custom Landing Page	☐

Page: Login ▼ Edit mode ON ON ?

Save

8 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.



The screenshot displays the Peplink PEPWAVE web interface. The top navigation bar includes tabs for Dashboard, SFC Protect, Network, Advanced, AP, System, and Status, with an 'Apply Changes' button on the right. The left sidebar shows a 'General' section with a 'Logout' button. The main content area is divided into several sections:

- WAN Connection Status:** This section shows the status of WAN connections. It has a 'Priority 1 (Highest)' row with a 'WAN' connection that is 'Connected'. Below it, a 'Priority 2' row is labeled 'Drag desired (Priority 2) connections here'. Underneath, there are three 'Disabled' connections: 'Cellular', 'Wi-Fi WAN on 2.4 GHz', and 'Wi-Fi WAN on 5 GHz'. Each disabled connection has a 'Disabled' status and '(No IP Address)'.
- LAN Interface:** This section shows the 'Router IP Address' as '192.168.50.1'.
- Wi-Fi AP:** This section shows the status of the Wi-Fi Access Point. It is currently 'ON' and has a 'Status' button next to it. Below the status, there are two rows for '2.4 GHz' and '5 GHz' bands, both showing 'PEPWAVE' as the SSID.
- Device Information:** This section provides details about the device:
 - Model: Pepwave MAX BR1 MK2
 - Firmware: 8.3.0 build 5109
 - Uptime: 6 days 8 hours 28 minutes
 - CPU Load: 16% (indicated by a green progress bar)
 - Throughput: 9.0 kbps (down) and 32.0 kbps (up)
- Remote Assistance Status:** This section shows the status of remote assistance, which is currently 'Turn off'.

At the bottom of the interface, there is a copyright notice: 'Copyright © Pepwave. All rights reserved.'

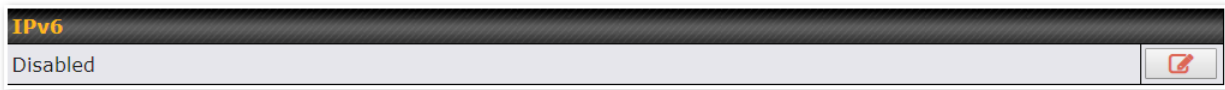
To enable a particular WAN connection, drag on the appropriate WAN by holding the left mouse button, move it to the **Disabled** row, and drop it by releasing the mouse button.

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

Important Note

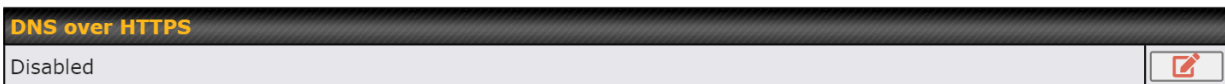
Connection details will be changed and become effective immediately after clicking the **Save and Apply** button.

IPv6

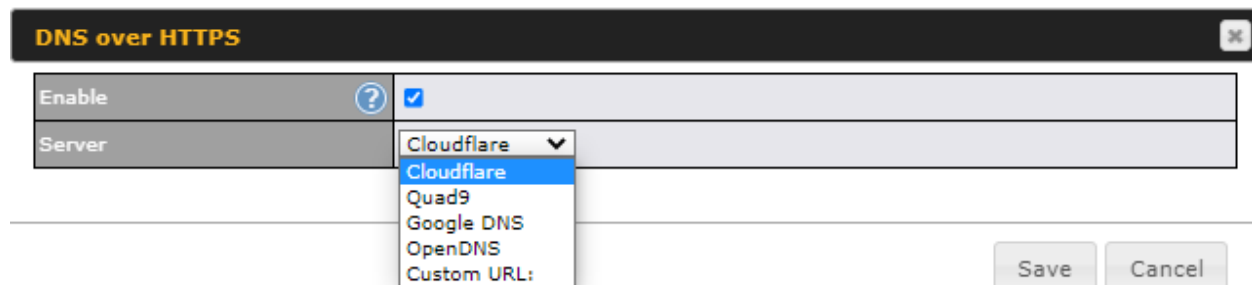


You can also enable IPv6 support in this section.

DNS over HTTPS (DoH)



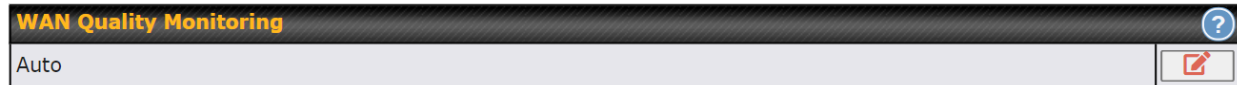
You can enable DoH (DNS over HTTPS) support in this section.



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.

WAN Quality Monitoring

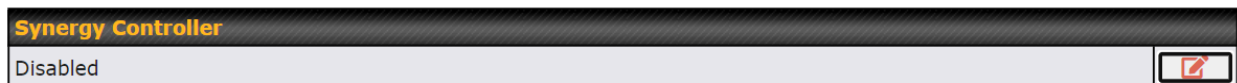
This settings advice how WAN Quality information is being gathered.



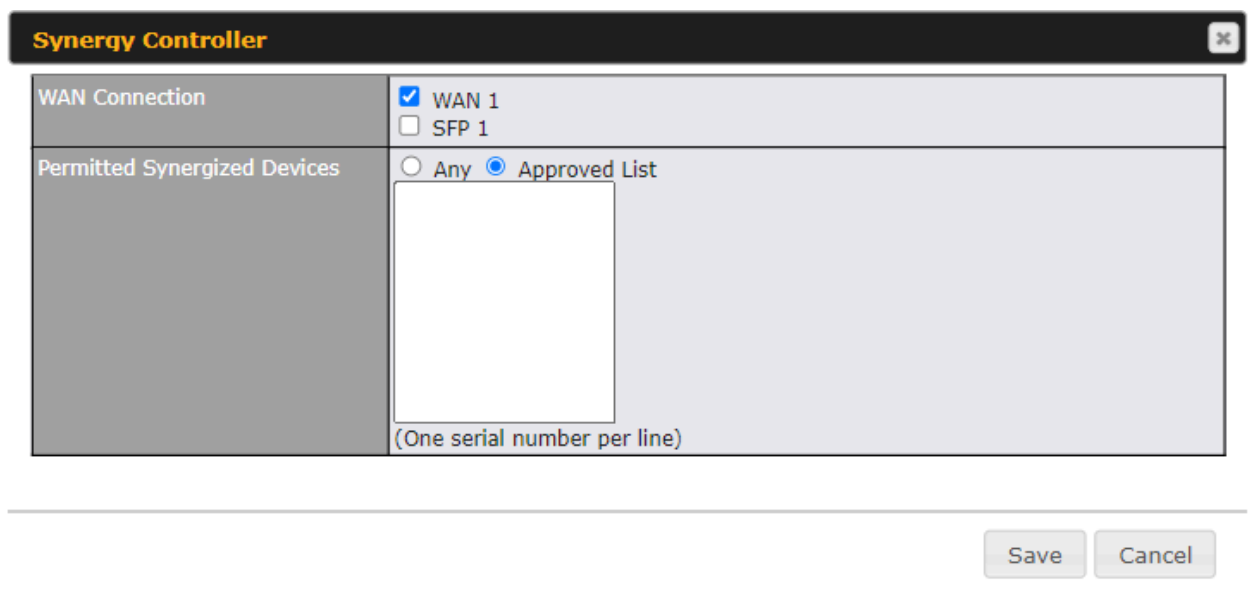
By default, WAN Quality will always be observed and gathered automatically. With customized choice of WAN connections, the device will always observe WAN Quality of those selected WAN connections. Other WAN connections may stop observing WAN Quality information if it is not necessary for the underlying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

Synergy Mode

You can enable the Synergy Controller in this section.



You may click this  to enable the Synergy Controller. By default, the setting is disabled.



WAN Connection	☒ WAN 1 ☐ SFP 1
Permitted Synergized Devices	☐ Any ☒ Approved List (One serial number per line)

You may select the WAN connection to use as a Synergy Link which will connect to synergized devices.

8.1 Ethernet WAN

There are four possible connection methods for the Ethernet WAN connection:

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

8.1.1 DHCP Connection

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

WAN Connection Settings	
WAN Connection Name	WAN
Enable	☒
Connection Priority	☒ Always-on (Priority 1) ☐ Backup
Independent from Backup WANs	☐
Connection Method	DHCP
Routing Mode	☒ NAT ☐ IP Forwarding
Management IP Address	255.255.255.0 (/24)
Custom Hostname	☐
DNS Servers	☒ Obtain DNS server address automatically ☐ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
IP Passthrough	☐
Standby State	☒ Remain connected ☐ Disconnect
Reply to ICMP Ping	☒ Yes ☐ No
Upload Bandwidth	1 Gbps
Download Bandwidth	1 Gbps

DHCP Connection Settings	
WAN Connection Name	Enter a name to represent this WAN connection.
Enable	This setting enables the WAN connection. If schedules have been defined, you will be able to select a schedule to apply to the connection.

Connection Priority	This option allows you to configure the WAN connection whether for normal daily usage or as a backup connection only. If Always-on is chosen, the WAN connection will be kept on continuously, regardless of the priority of other WAN connections. If Backup is chosen, the WAN connection will depend on other WAN connections. It will not be used when one or more higher priority dependent WAN connections are connected.
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.
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.
Management IP Address	Management IP Address is available for configuration when you click here for other DHCP settings. This option allows you to configure the management IP address for the DHCP WAN connection.
Custom Hostname	If your service provider's DHCP server requires you to supply a hostname value upon acquiring an IP address, you may enter the value here. If your service provider does not provide you with the value, you can safely bypass this option.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting Obtain DNS server address automatically results in the DNS servers being assigned by the WAN DHCP server to be used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned from the DHCP server.) When Use the following DNS server address(es) is selected, you may enter custom DNS server addresses for this WAN connection into the DNS Server 1 and DNS Server 2 fields.

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.
Standby State	This option allows you to choose whether to remain connected when this WAN connection is no longer in the highest priority and has entered the standby state. When Remain connected is chosen, upon bringing up this WAN connection to active, it will be immediately available for use. If this WAN connection is charged by connection time, you may want to set this option to Disconnect so that connection will be made only when needed. SpeedFusion VPN 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.

8.1.2 Static IP Connection

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

Connection Method	 Static IP ▼
Routing Mode	 ☒ NAT ☐ IP Forwarding
IP Address	
Subnet Mask	255.255.255.0 (/24) ▼
Default Gateway	
DNS Servers	☒ Use the following DNS server address(es) DNS Server 1: DNS Server 2:

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.

8.1.3 PPPoE Connection

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

Connection Method	 PPPoE ▼
Routing Mode	 ☒ NAT ☐ IP Forwarding
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:

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 (Optional)	If your ISP provides a PPPoE IP address, enter it here. Note: Leave this field blank unless it is provided by your ISP.
Keep Alive Interval	This is the time interval between each Keep-Alive packet.
Keep-Alive Retry	This is the number of consecutive Keep-Alive check failures before treating PPPoE connection as down.
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.

8.1.4 L2TP Connection

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

Connection Method	 L2TP ▼
Routing Mode	 ☒ NAT ☐ IP Forwarding
L2TP User Name	
L2TP Password	
Confirm L2TP Password	
Server IP Address / Host	
Address Type	☒ Dynamic IP ☐ Static IP
DNS Servers	☒ Obtain DNS server address automatically ☐ Use the following DNS server address(es) DNS Server 1: DNS Server 2:

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.

8.1.5 GRE Connection

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

Connection Method	 GRE ▼
Routing Mode	 ☒ NAT ☐ IP Forwarding
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:

GRE 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

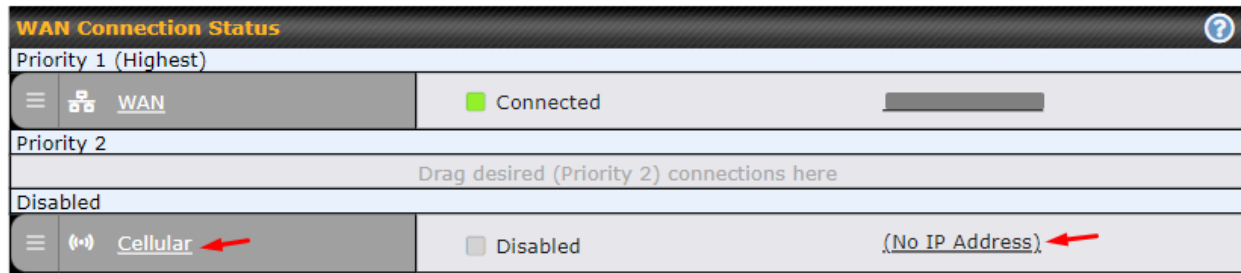
These settings allow you to specify the information required in order to communicate on the Internet via a fixed Internet IP address. The information is typically determined by and can be obtained from the ISP.

Remote GRE Host

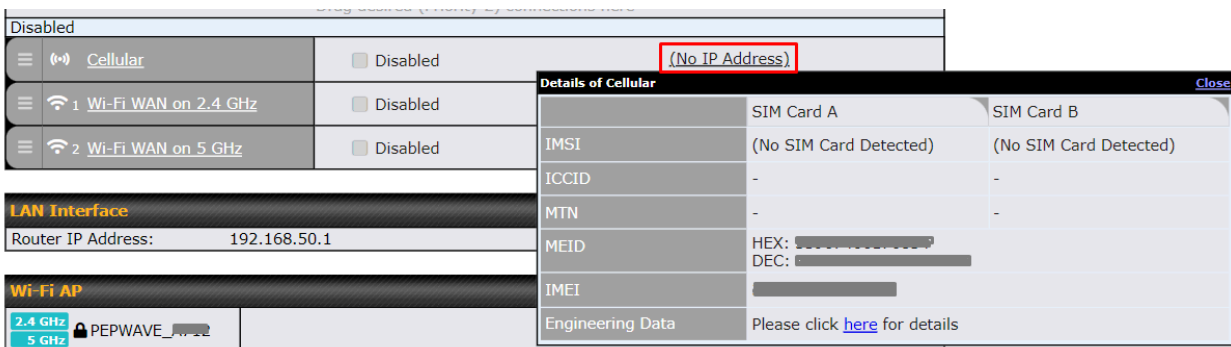
This field allows you to enter the IP address of the remote GRE.

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.
Outgoing NAT IP Address	This field is to enter the NAT IP address for outgoing via GRE tunnel.
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.

8.2 Cellular WAN



To access/configure the Cellular WAN settings, click **Network > Cellular Name**. You may click the “**No IP Address**” link to view the Cellular WAN details/status.



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.
MTN	This field is to display the mobile telephone number of the SIM card.
MEID	Some Pepwave routers support both HSPA and EV-DO. For Sprint or Verizon Wireless EV-DO users, a unique MEID identifier code (in hexadecimal format) is used by the carrier to associate the EV-DO device with the user. This information is presented in hex and decimal format.
IMEI	This is the unique ID for identifying the modem in GSM/HSPA mode.

WAN Connection Settings ?	
WAN Connection Name	Cellular
Enable	☒
Connection Priority	☒ Always-on (Priority 1) ☐ Backup
Independent from Backup WANs ?	☐
Routing Mode ?	☒ NAT
Management IP Address	255.255.255.0 (/24) ▼
DNS Servers	☒ Obtain DNS server address automatically ☐ Use the following DNS server address(es) DNS Server 1: DNS Server 2:
IP Passthrough ?	☐
Standby State ?	☒ Remain connected ☐ Disconnect
Idle Disconnect	☐
Reply to ICMP Ping ?	☒ Yes ☐ No

WAN Connection Settings	
WAN Connection Name	Indicate a name you wish to give this Cellular WAN connection
Enable	Click the checkbox to toggle the on and off state of this connection.
Connection Priority	This option allows you to configure the WAN connection whether for normal daily usage or as a backup connection only. If Always-on is chosen, the WAN connection will be kept on continuously, regardless of the priority of other WAN connections. If Backup is chosen, the WAN connection will depend on other WAN connections. It will not be used when one or more higher priority dependent WAN connections are connected.
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.
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 ?