



Pepwave MAX Adapter

User Manual

Pepwave Firmware 8.1.0

December 2020

Copyright & Trademarks

Specifications are subject to change without notice. Copyright © 2020 Pepwave Ltd. All Rights Reserved. Pepwave and the Pepwave logo are trademarks of Pepwave Ltd. Other brands or products mentioned may be trademarks or registered trademarks of their respective owners.

Table of Contents

Introduction and Scope	7
Glossary	8
Product Features	9
Supported Network Features	9
WAN	9
LAN	10
VPN	10
Firewall	10
Captive Portal	10
Outbound Policy	10
AP Controller	11
QoS	11
Other Supported Features	11
Overview	13
MAXAdapter	13
Drop-in Mode and LAN Bypass: Transparent Deployment	14
QoS: Clearer VoIP	14
Per-User Bandwidth Control	15
High Availability via VRRP	15
USB Modem and Android Tethering	16
Built-In Remote User VPN Support	16
SIM-card USSD support	17
DPI Engine	17
Installation	18
Preparation	18
Constructing the Network	18
Configuring the Network Environment	19
Connecting to the Web Admin Interface	19
SpeedFusion Cloud	22
Activate SpeedFusion Cloud Service	22
Enable SpeedFusion Cloud	24
Connect Clients to Cloud	31
Link Wi-Fi to Cloud	32

Configuring the LAN Interface(s)	34
Basic Settings	34
Port Settings	45
Captive Portal	45
Configuring the WAN Interface(s)	48
Ethernet WAN	49
DHCP Connection	52
Static IP Connection	53
PPPoE Connection	54
L2TP Connection	55
Cellular WAN	56
Wi-Fi WAN	63
Creating Wi-Fi Connection Profiles	69
WAN Health Check	70
Dynamic DNS Settings	72
Advanced Wi-Fi Settings	74
ContentHub Configuration	79
ContentHub	79
Configuring the ContentHub	79
Configure a website to be published from the ContentHub	80
Configure an application to be published from the ContentHub	81
MediaFast Configuration	83
Setting Up MediaFast Content Caching	84
Scheduling Content Prefetching	85
Viewing MediaFast Statistics	88
Bandwidth Bonding SpeedFusion™ / PepVPN	89
PepVPN	89
The Pepwave Router Behind a NAT Router	95
IPsec VPN	97
IPsec VPN Settings	97
Outbound Policy Management	101
Outbound Policy	101
Custom Rules for Outbound Policy	103
Algorithm: Weighted Balance	103
Algorithm: Persistence	104
Algorithm: Enforced	105

Algorithm: Priority	106
Algorithm: Overflow	106
Algorithm: Least Used	107
Algorithm: Lowest Latency	107
Expert Mode	108
Inbound Access	108
Port Forwarding Service	108
UPnP / NAT-PMP Settings	110
NAT Mappings	111
User Groups	113
Bandwidth Control	114
Application	114
Application Prioritization	114
Prioritization for Custom Applications	114
DSL/Cable Optimization	115
Firewall	115
Outbound and Inbound Firewall Rules	116
Access Rules	116
Apply Firewall Rules to PepVpn Traffic	120
Intrusion Detection and DoS Prevention	120
Content Blocking	122
Application Blocking	122
Web Blocking	122
Customized Domains	123
Exempted User Groups	123
Exempted Subnets	123
URL Logging	123
OSPF & RIPv2	123
BGP	127
Remote User Access	129
L2TP with IPsec	130
OpenVPN	130
PPTP	131
Authentication Methods	131
Miscellaneous Settings	133
High Availability	133
Certificate Manager	136

Service Forwarding	137
SMTP Forwarding	137
Web Proxy Forwarding	138
DNS Forwarding	139
Custom Service Forwarding	139
Service Passthrough	139
UART	141
GPS Forwarding	143
Ignition Sensing	143
Ignition Sensing installation	144
GPIO Menu	146
NTP Server	147
Grouped Networks	147
SIM Toolkit	148
AP - access point	151
AP Controller	151
Wireless SSID	151
Settings	156
AP Controller Status	162
Info	162
Access Point (Usage)	164
Wireless SSID	166
Wireless Client	167
Nearby Device	168
Event Log	169
Toolbox	170
System Settings	171
Admin Security	171
Firmware	174
Web admin interface : automatically check for updates	174
Web admin interface : install updates manually	175
The InControl method	176
Time	177
Schedule	177
Email Notification	178
Event Log	180
SNMP	181

SMS Control	183
InControl	184
Configuration	185
Feature Add-ons	186
Reboot	186
Tools	187
Ping	187
Traceroute Test	187
PepVPN Test	188
Wake-on-LAN	189
CLI (Command Line Interface Support)	189
Status	190
Device	190
GPS Data	191
Active Sessions	192
Client List	193
WINS Client	194
UPnP / NAT-PMP	194
OSPF & RIPv2	195
BGP	196
SpeedFusion Status	196
Event Log	198
WAN Quality	200
Usage Reports	200
Real-Time	201
Hourly	201
Daily	202
Monthly	203
Appendix A: Restoration of Factory Defaults	206
Appendix B: Declaration	206

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)
- Ping, DNS lookup, and HTTP-based health check

1.1.2 LAN

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

1.1.3 VPN

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

1.1.4 Firewall

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

1.1.5 Captive Portal

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

1.1.6 Outbound Policy

- Link load distribution per TCP/UDP service
- Persistent routing for specified source and/or destination IP addresses per TCP/UDP

service

- Traffic prioritization and DSL optimization
- Prioritize and route traffic to VPN tunnels with Priority and Enforced algorithms

1.1.7 AP Controller

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

1.1.8 QoS

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

1.2 Other Supported Features

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

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

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

2 Overview

2.1 MAXAdapter

2.1.1 Panel Appearance



2.1.2 LED Indicators

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

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

Advanced Feature Summary

2.2 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.

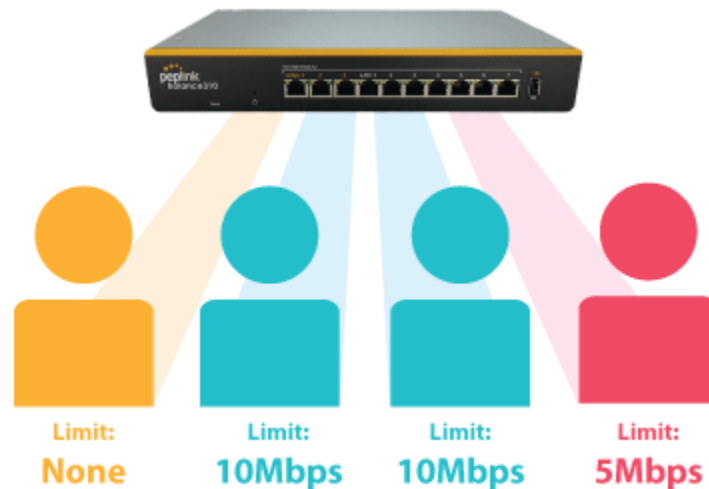
Note: Drop-in mode is compatible for All MAX models except MAX BR1 IP67

2.3 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.

2.4 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.

2.5 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)

2.6 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)

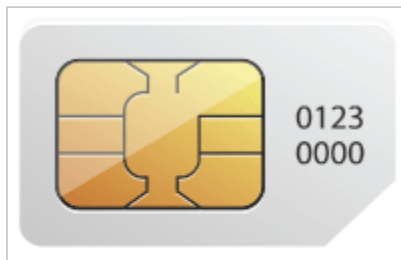
2.7 Built-In Remote User VPN Support



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](#)

2.8 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.](#)

2.9 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 Installation

The following section details connecting Pepwave routers to your network.

3.1 Preparation

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

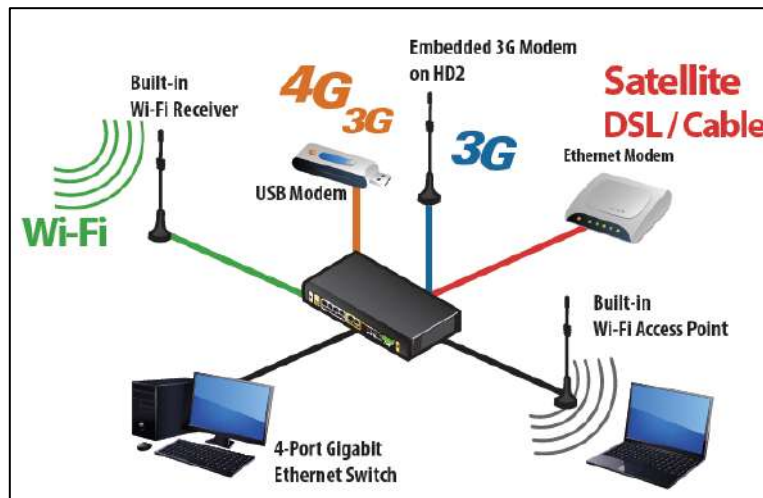
- At least one Internet/WAN access account and/or Wi-Fi access information
- Depending on network connection type(s), one or more of the following:
 - **Ethernet WAN:** A 10/100/1000BaseT UTP cable with RJ45 connector
 - **USB:** A USB modem
 - **Embedded modem:** A SIM card for GSM/HSPA service
 - **Wi-Fi WAN:** Wi-Fi antennas
 - **PC Card/Express Card WAN:** A PC Card/ExpressCard for the corresponding card slot
- A computer installed with the TCP/IP network protocol and a supported web browser. Supported browsers include Microsoft Internet Explorer 11 or above, Mozilla Firefox 24 or above, Apple Safari 7 or above, and Google Chrome 18 or above.

3.2 Constructing the Network

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

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

The following figure schematically illustrates the resulting configuration:



3.3 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**.

4 Connecting to the Web Admin Interface

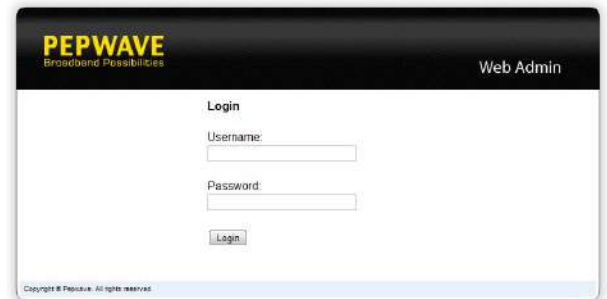
1. Start a web browser on a computer that is connected with the Pepwave router through the LAN.
2. To connect to the router's web admin interface, enter the following LAN IP address in the address field of the web browser:
`http://192.168.50.1`
(This is the default LAN IP address for Pepwave routers.)

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

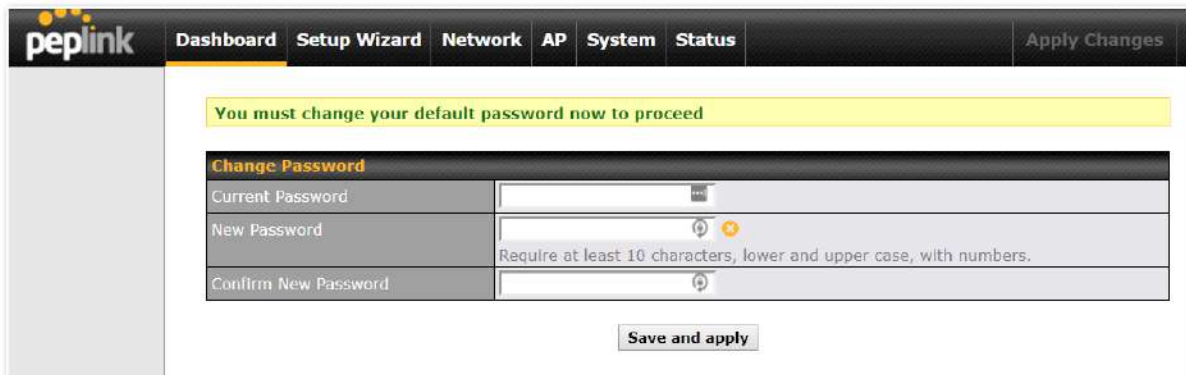
Username: admin

Password: admin

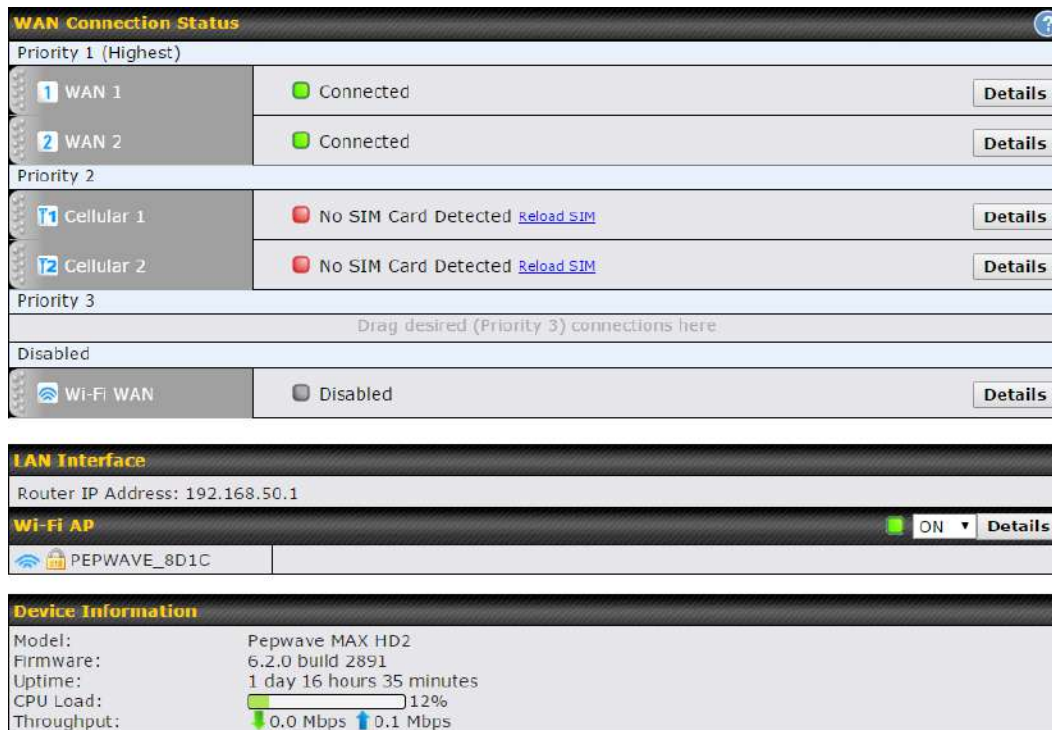
(This is the default username and password for Pepwave routers).



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



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



WAN Connection Status

Priority 1 (Highest)

1 WAN 1	Connected	Details
2 WAN 2	Connected	Details

Priority 2

1 Cellular 1	No SIM Card Detected Reload SIM	Details
2 Cellular 2	No SIM Card Detected Reload SIM	Details

Priority 3

Drag desired (Priority 3) connections here

Disabled

Wi-Fi WAN	Disabled	Details
-----------	----------	---------

LAN Interface

Router IP Address: 192.168.50.1

Wi-Fi AP ON [Details](#)

PEPWAVE_8D1C

Device Information

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

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

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

Important Note

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

5 SpeedFusion Cloud

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



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

5.1 Activate SpeedFusion Cloud Service

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

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

pavilion.peplink.com/speedfusioncloud/enrollment

peplink | PEPWAVE

SpeedFusion Cloud Device Entry

Please input the following details

Email *

receiver@abc.com

Device Serial number(s) *

191b-1d1d-0707

☐ I'm not a robot

Reset Submit

- **Step 1 - Update to Firmware 8.1.0 or above**
- **Step 2 - Enter Serial Numbers:** Enter the serial numbers of the devices you wish to enable the SpeedFusion Cloud service for. This page supports 200 devices maximum, so if you have more than that, please use multiple entries.
- **Step 3 - Receive Confirmation Email:** Once registration is complete, we will send you a confirmation email including license keys.
- **Step 4 - Apply SpeedFusion License:**
 - With InControl: InControl will then push the license automatically.
 - Without InControl: Apply the license keys from the WebUI by navigating to System > Feature Add-ons.
- **Step 5 - Assign Traffic:** Use Outbound Policy to define the traffic you want to protect using the SpeedFusion Cloud.

Please Note: The 90-day free period with 1000B of SpeedFusion traffic will begin once the SpeedFusion cloud service has been activated. Each device can only apply once.

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

PEPWAVE

Dashboard SpeedFusion Cloud Network Advanced AP System Status Apply Changes

System

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

Tools

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

Feature Activation

Activation Key

9629a523e54fe148f876e75cf95df776f248e248b618b618a6199b23e54fe148f876e75cf95df776f351e640e450b618b618a310ae10a711a219a6249c5af05ef747c958e346e248c95bf75df309a709a3199c7ae64cf34dd05ce540f947b66afa46e34db668f55dff5ff75dff46f809dd4cef09be18a619d16bbfa96c3083b48a7d337ade187a5ce2e4e1

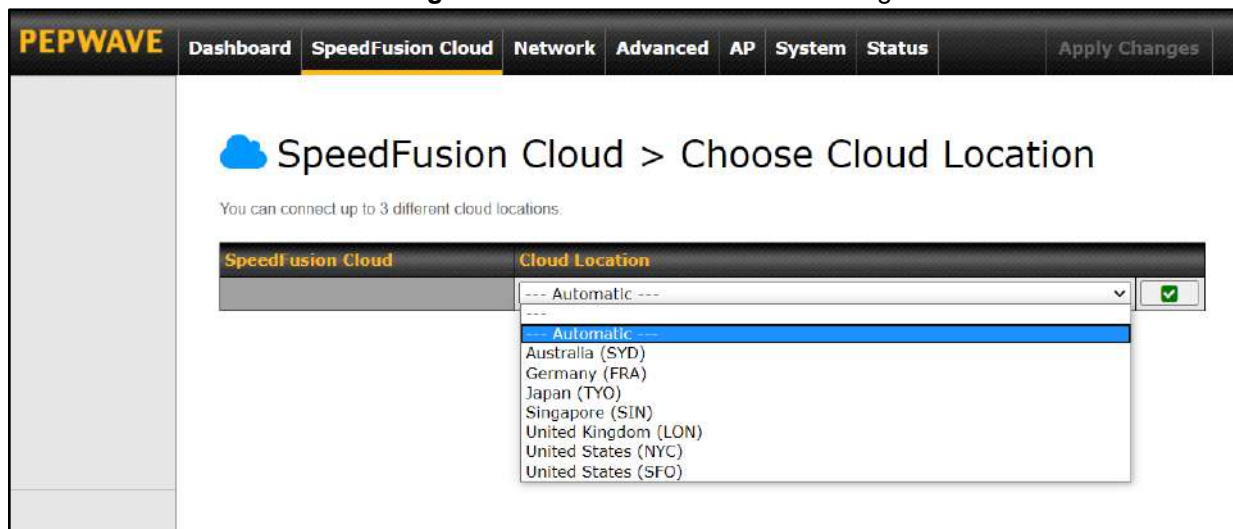
Activate

5.2 Enable SpeedFusion Cloud

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



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



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

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

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

SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

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

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

Changes applied successfully.

SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

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

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

PEPWAVE [Dashboard](#) [SpeedFusion Cloud](#) [Network](#) [Advanced](#) [AP](#) [System](#) [Status](#) [Apply Changes](#)

WAN Connection Status

Priority 1 (Highest)

Drag desired (Priority 1) connections here

Priority 2

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

Priority 3

Drag desired (Priority 3) connections here

Disabled

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

LAN Interface

Router IP Address: 192.168.50.1

Wi-Fi AP

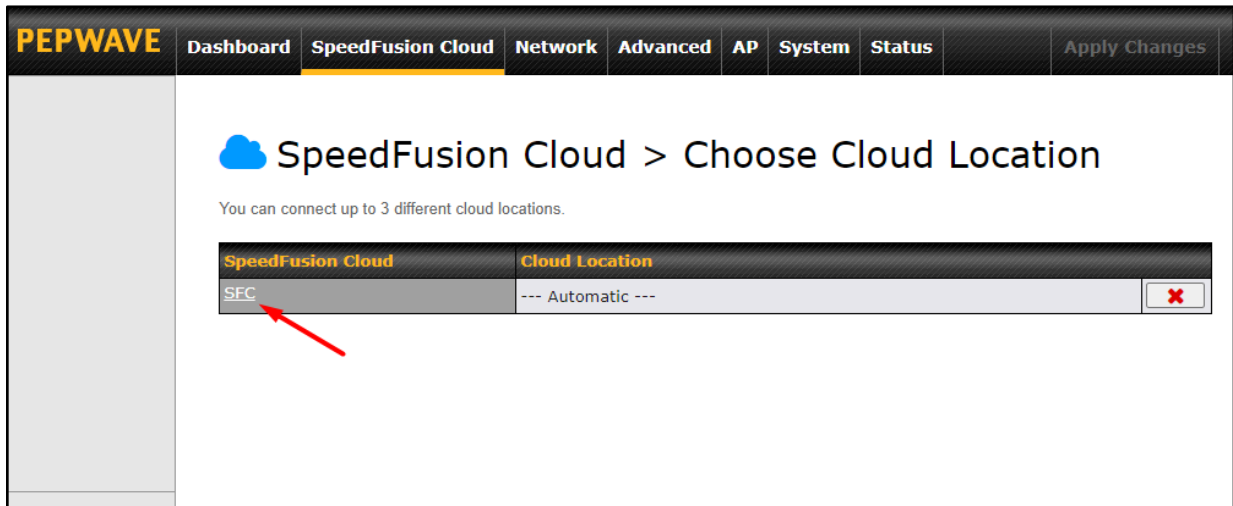
ON [Details](#)

PEPWAVE_EBB4

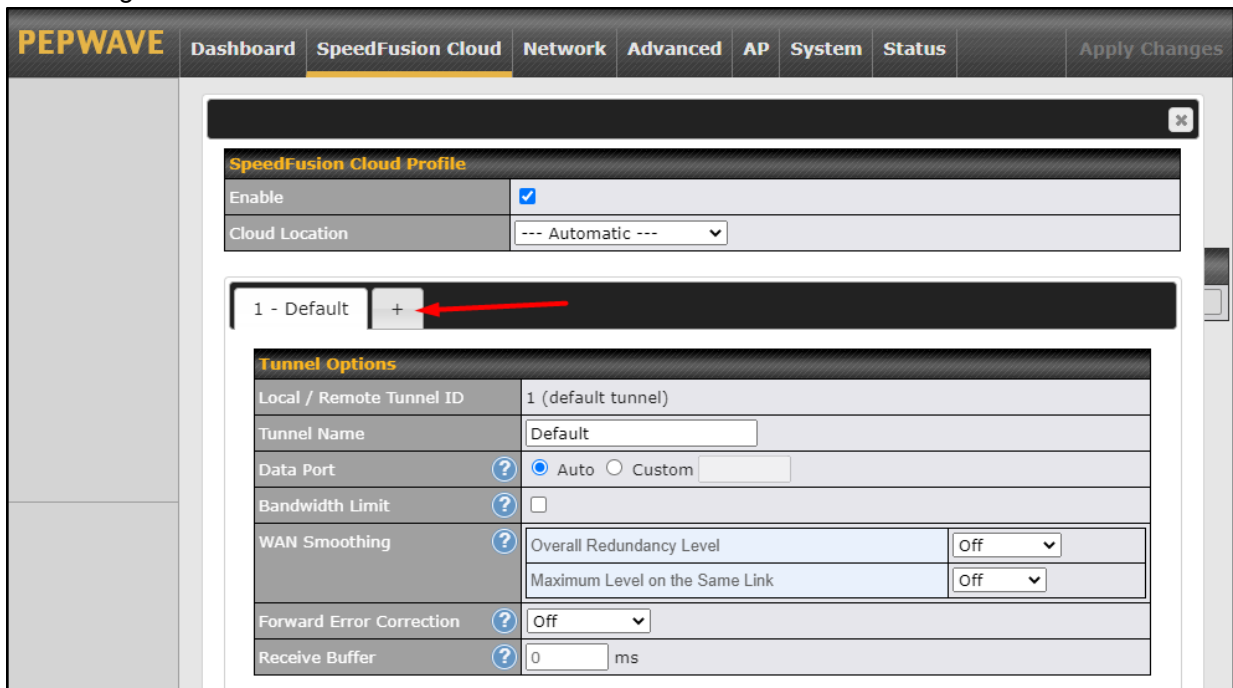
SpeedFusion Cloud

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

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



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



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

SpeedFusion Cloud Profile

Enable	☒
Cloud Location	--- Automatic ---

1 - Default 2 - WAN Smoo... +

Tunnel Options

Local / Remote Tunnel ID	2		
Tunnel Name	WAN Smoothing 		
Data Port	☒ Auto ☐ Custom		
Bandwidth Limit	☐		
WAN Smoothing	Overall Redundancy Level	Normal	
	Maximum Level on the Same Link	Normal	
Forward Error Correction	☐ Off		
Receive Buffer	0	ms	

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

PEPWAVE
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
Apply Changes

WAN Connection Status

Priority 1 (Highest)

Drag desired (Priority 1) connections here

Priority 2

Cellular 1

Connected to MY MAXIS **LTE-A**

Details

Cellular 2

Connected to MY MAXIS **LTE-A**

Details

Priority 3

Drag desired (Priority 3) connections here

Disabled

WAN 1

Disabled

Details

WAN 2

Disabled

Details

Cellular 3

Disabled

Details

Cellular 4

Disabled

Details

Wi-Fi WAN

Disabled

Details

LAN 1 as WAN

Disabled

Details

LAN 2 as WAN

Disabled

Details

LAN 3 as WAN

Disabled

Details

LAN Interface

Router IP Address: 192.168.50.1

Wi-Fi AP

ON

Details

PEPWAVE_EBB4

SpeedFusion Cloud

SFC (1 - Default)

Established

SFC (2 - WAN Smoothing)

Established

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

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

PEPWAVE

DashboardSpeedFusion CloudNetworkAdvancedAPSystemStatus

Apply Changes

Advanced

SpeedFusion

IPsec VPN

GRE Tunnel

Outbound Policy

Port Forwarding

NAT Mappings

QoS

User Groups

Bandwidth Control

Application

Firewall

Access Rules

Content Blocking

Routing Protocols

OSPF & RIPv2

BGP

Remote User Access

Misc. Settings

High Availability

RADIUS Server

Certificate Manager

Service Forwarding

Service Passthrough

GPS Forwarding

NTP Server

Grouped Networks

Outbound Policy

Custom

Add a New Custom Rule

Service Name

to_internet

Enable

☒

Source

IP Address

192.168.50.10

Destination

Any

Protocol

Any

:: Protocol Selection ::

Algorithm

Priority

Priority Order

Highest Priority

Cloud: SFC (1 - Defau...

Cloud: SFC (2 - WAN ...

WAN: WAN 1

WAN: WAN 2

WAN: Cellular 1

WAN: Cellular 2

WAN: Cellular 3

WAN: Cellular 4

WAN: USB

WAN: Wi-Fi WAN

WAN: LAN 1 as WAN

WAN: LAN 2 as WAN

WAN: LAN 3 as WAN

Lowest Priority

Not In Use

When No Connections are Available

Drop the Traffic

Terminate Sessions on Connection Recovery

☐ Enable

Save

Cancel

Outbound Policy

Custom

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

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

Expert Mode

Enabled

5.3 Connect Clients to Cloud

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

Dashboard
SpeedFusion Cloud
Network
AP
System
Status
Apply Changes

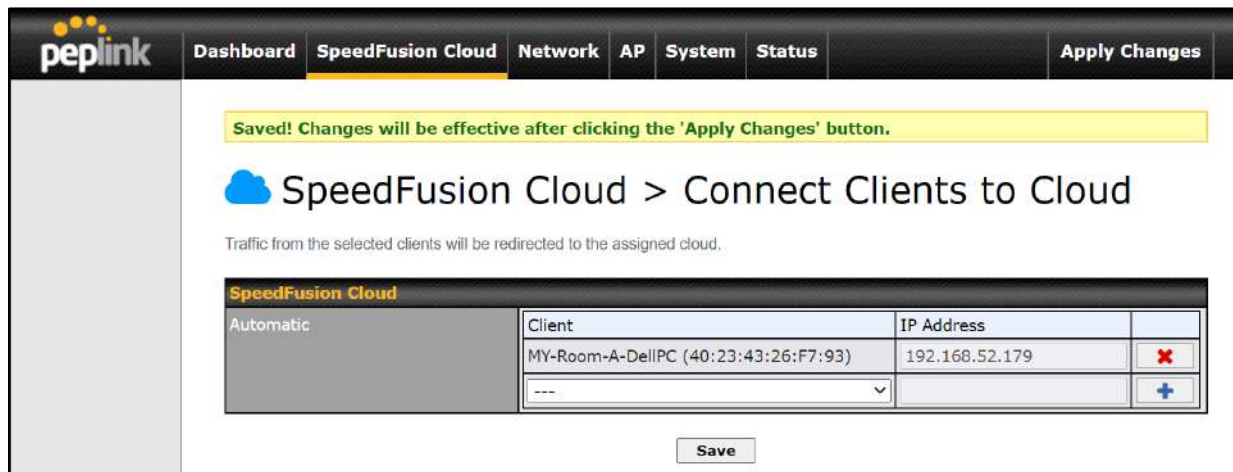
SpeedFusion Cloud

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

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

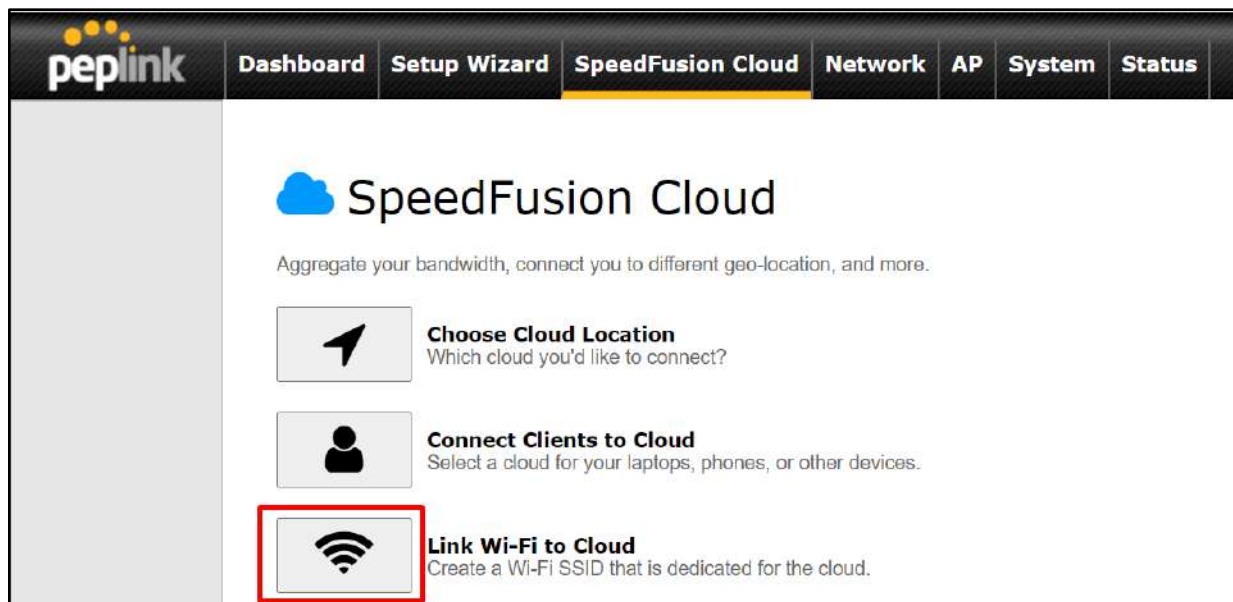
Connect Clients to Cloud
Select a cloud for your laptops, phones, or other devices.

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



5.4 Link Wi-Fi to Cloud

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



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



SpeedFusion Cloud > Link Wi-Fi to Cloud

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

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

Save

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



LAN Interface

Router IP Address: 192.168.54.1

Wi-Fi AP ON Details

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

6 Configuring the LAN Interface(s)

6.1 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 grey “X” means that the VLAN is used in other settings and cannot be deleted. You can find which settings are using the VLAN by hovering over the grey “X”.

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

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

IP Settings	
IP Address	255.255.255.0 (/24) ▼

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

Network Settings	
Name	
VLAN ID	
Inter-VLAN routing	☒

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

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

Layer 2 PepVPN Bridging	
PepVPN Profiles to Bridge	The remote network of the selected PepVPN profiles will be bridged with this local LAN, creating a Layer 2 PepVPN, they will be connected and operate like a single LAN, and any broadcast or multicast packets will be sent over the VPN.
Remote Network Isolation	Enable this option if you want to block network traffic between the remote networks, this will not affect the connectivity between them and this local LAN.
Spanning Tree Protocol	Click the box will enable STP for this layer 2 profile bridge.
Override IP Address when bridge	Select "Do not override" if the LAN IP address and local DHCP server should remain unchanged after the Layer 2 PepVPN is up. If you choose to override IP address when the VPN is connected, the device will not

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

DHCP Server											
DHCP Server		☒ Enable									
DHCP Server Logging		☐									
IP Range		- 255.255.255.0 (/24) ▼									
Lease Time		1 Days 0 Hours 0 Mins									
DNS Servers		☒ Assign DNS server automatically									
WINS Servers		☐ Assign WINS server									
BOOTP		☐									
Extended DHCP Option		<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" style="text-align: center;">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 style="text-align: center;">+</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 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 pass additional configuration information to LAN hosts. To define an extended DHCP option, click the Add button, choose the option to define and enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only.
DHCP Reservation	This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses. The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC addresses, and fixed IP addresses. Name (an optional field) allows you to specify a name to represent the device. MAC addresses should be in the format of 00:AA:BB:CC:DD:EE. Press  to create a new record. Press  to remove a record. Reserved client information can be imported from the Client List, located at Status>Client List. For more details, please refer to Section 22.3.

LAN Physical Settings	
Speed	Auto ▼

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

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

Static Route Settings

Static Route

This table is for defining static routing rules for the LAN segment. A static route consists of the network address, subnet mask, and gateway address. The address and subnet mask values are in w.x.y.z format.

The local LAN subnet and subnets behind the LAN will be advertised to the VPN. Remote routes sent over the VPN will also be accepted. Any VPN member will be able to route to the local subnets. Press  to create a new route. Press  to remove a route.

WINS Server Settings

Enable

☐

WINS Server Settings

Enable

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

DNS Proxy Settings

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

Preferred connections are shown with 

DNS Proxy Settings

Enable

To enable the DNS proxy feature, check this box, and then set up the feature at **Network>LAN>DNS Proxy Settings**. A DNS proxy server can be enabled to serve DNS requests originating from LAN/PPTP/SpeedFusion™ peers. Requests are forwarded to the **DNS servers/resolvers** defined for each WAN connection.

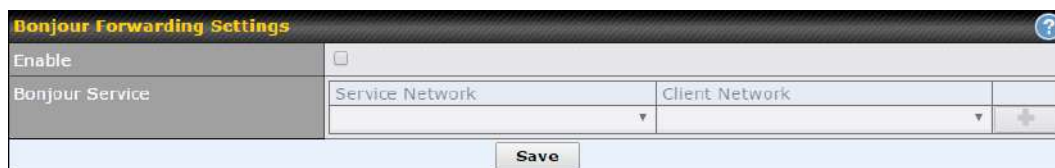
DNS Caching

This field is to enable DNS caching on the built-in DNS proxy server. When

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

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

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

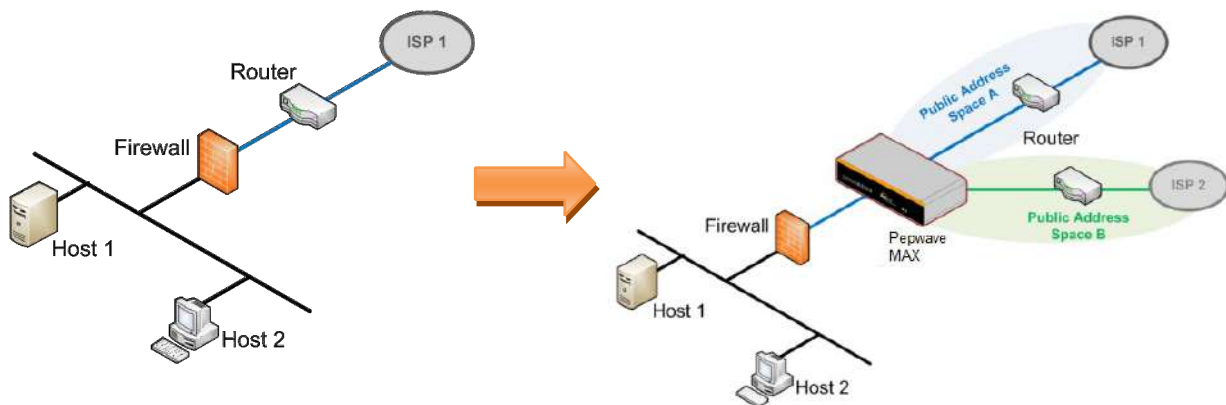


Bonjour Forwarding Settings	
Enable	Check this box to turn on Bonjour forwarding.
Bonjour Service	Choose Service and Client networks from the drop-down menus, and then click  to add the networks. To delete an existing Bonjour listing, click  .

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 - ↓ ×						
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.

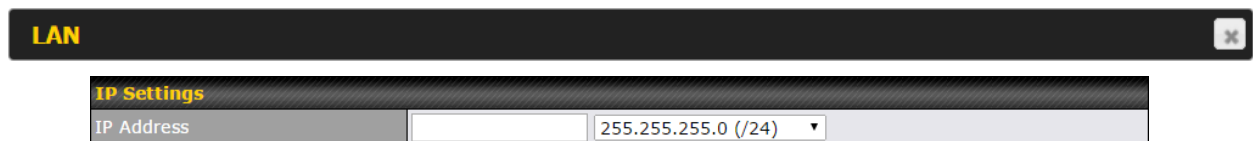
To enable VLAN configuration, click the  button in the **IP Settings** section.



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



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



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

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

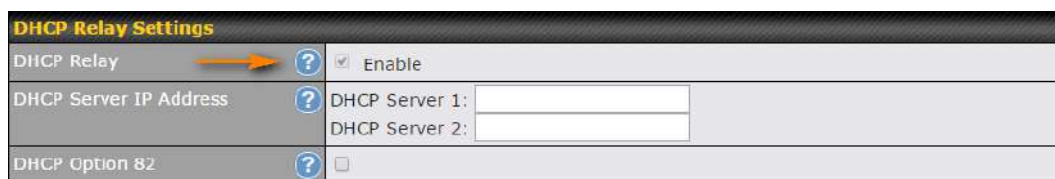
Network Settings	
Name	Enter a name for the LAN.
VLAN ID	Enter a number for the LAN.
Inter-VLAN routing	Check this box to enable routing between virtual LANs.
Captive Portal	Check this box to turn on captive portals.

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

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

DNS Servers	This option allows you to input the DNS server addresses to be offered to DHCP clients. If Assign DNS server automatically is selected, the Pepwave router's built-in DNS server address (i.e., LAN IP address) will be offered.
WINS Servers	This option allows you to specify the Windows Internet Name Service (WINS) server. You may choose to use the built-in WINS server or external WINS servers. When this unit is connected using SpeedFusion™, 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.



The screenshot shows the 'DHCP Relay Settings' form. It has three rows: 'DHCP Relay' with an 'Enable' checkbox and a help icon; 'DHCP Server IP Address' with two input fields for 'DHCP Server 1' and 'DHCP Server 2', and a help icon; and 'DHCP Option 82' with a checkbox and a help icon. An orange arrow points to the help icon in the first row.

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

Address	active-passive DHCP server configurations, enter active and passive DHCP server relay IP addresses in DHCP Server 1 and DHCP Server 2 .
DHCP Option 82	DHCP Option 82 includes device information as relay agent for the attached client when forwarding DHCP requests from client to server. This option also embeds the device's MAC address and network name in circuit and remote IDs. Check this box to enable DHCP Option 82.

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

6.2 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.

6.3 Captive Portal

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

Captive Portal Settings	
Enable	☒ Untagged LAN
Hostname	captive-portal.peplink.com Default
Access Mode	☒ Open Access ☐ User Authentication
Access Quota	30 mins (0: Unlimited) 0 MB (0: Unlimited)
Quota Reset Time	☒ Daily at 00 :00 ☐ 1440 minutes after quota reached
Allowed Networks	Domain Name / IP Address +
Allowed Clients	MAC / IP Address +
Splash Page	☒ Built-in ☐ External, URL: http://

Captive Portal Settings																						
Enable	Check Enable and then, optionally, select the LANs/VLANs that will use the captive portal.																					
Hostname	To customize the portal's form submission and redirection URL, enter a new URL in this field. To reset the URL to factory settings, click Default .																					
Access Mode	Click Open Access to allow clients to freely access your router. Click User Authentication to force your clients to authenticate before accessing your router.																					
RADIUS Server	This authenticates your clients through a RADIUS server. After selecting this option, you will see the following fields: <table border="1"> <tbody> <tr> <td>Authentication</td> <td colspan="2">RADIUS Server</td> </tr> <tr> <td>Auth Server</td> <td> </td> <td>Port 1812 Default</td> </tr> <tr> <td>Auth Server Secret</td> <td> </td> <td>☒ Hide Characters</td> </tr> <tr> <td>CoA-DM</td> <td colspan="2">☐</td> </tr> <tr> <td>Accounting Server</td> <td> </td> <td>Port 1813 Default</td> </tr> <tr> <td>Accounting Server Secret</td> <td> </td> <td>☒ Hide Characters</td> </tr> <tr> <td>Accounting Interim Interval</td> <td> </td> <td>seconds</td> </tr> </tbody> </table> Fill in the necessary information to complete your connection to the server and enable authentication.	Authentication	RADIUS Server		Auth Server		Port 1812 Default	Auth Server Secret		☒ Hide Characters	CoA-DM	☐		Accounting Server		Port 1813 Default	Accounting Server Secret		☒ Hide Characters	Accounting Interim Interval		seconds
Authentication	RADIUS Server																					
Auth Server		Port 1812 Default																				
Auth Server Secret		☒ Hide Characters																				
CoA-DM	☐																					
Accounting Server		Port 1813 Default																				
Accounting Server Secret		☒ Hide Characters																				
Accounting Interim Interval		seconds																				
LDAP Server	This authenticates your clients through a LDAP server. Upon selecting this option, you will see the following fields: <table border="1"> <tbody> <tr> <td>Authentication</td> <td colspan="2">LDAP Server</td> </tr> <tr> <td>LDAP Server</td> <td> </td> <td>Port 389 Default</td> </tr> <tr> <td></td> <td colspan="2">☐ Use DN/Password to bind to LDAP Server</td> </tr> <tr> <td>Base DN</td> <td colspan="2"> </td> </tr> <tr> <td>Base Filter</td> <td colspan="2"> </td> </tr> </tbody> </table>	Authentication	LDAP Server		LDAP Server		Port 389 Default		☐ Use DN/Password to bind to LDAP Server		Base DN			Base Filter								
Authentication	LDAP Server																					
LDAP Server		Port 389 Default																				
	☐ Use DN/Password to bind to LDAP Server																					
Base DN																						
Base Filter																						

	Fill in the necessary information to complete your connection to the server and enable authentication.
Access Quota	Set a time and data cap to each user's Internet usage.
Quota Reset Time	This menu determines how your usage quota resets. Setting it to Daily will reset it at a specified time every day. Setting a number of minutes after quota reached establish a timer for each user that begins after the quota has been reached.
Allowed Networks	Add networks that can bypass the captive Portal in this field. To whitelist a network, enter the domain name / IP address here and click  . To delete an existing network from the list of allowed networks, click the  button next to the listing.
Allowed Clients	Add MAC address and /or IP addresses for client devices that are allowed to bypass the Captive Portal. Clients accessing these domains and IP addresses will not be redirected to the splash page.
Splash Page	Here, you can choose between using the Pepwave router's built-in captive portal and redirecting clients to a URL you define.

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

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

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

7 Configuring the WAN Interface(s)

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

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

IPv6
Disabled Edit

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

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

Important Note

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

7.1 Ethernet WAN

Health Check Settings	
Health Check Method	PING
PING Hosts	Host 1: 8.8.8.8 Host 2: ☐ Use first two DNS servers as PING Hosts
Timeout	5 second(s)
Health Check Interval	5 second(s)
Health Check Retries	3
Recovery Retries	3

Health Check Settings

Health Check Method

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

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

	be treated as down for any IP routing errors. • PING - ICMP PING packets will be issued to test connectivity with configurable target IP addresses or host names. • DNS Lookup - DNS lookups will be issued to test the connectivity with configurable target DNS server IP addresses. • HTTP - HTTP connections will be issued to test the connectivity with configurable URLs and strings to match. Default: DNS Lookup
PING Hosts	These fields are for specifying the target IP addresses or host names where ICMP Ping packets will be sent to for health check. If the box Use first two DNS servers as PING Hosts is checked, the first two DNS servers will be the ping targets for checking the connection healthiness. If the box is not checked, the field Host 1 must be filled and the field Host 2 is optional. The connection is considered to be up if ping responses are received from any one of the ping hosts.
Timeout	If a health check test cannot be completed within the specified amount of time, the test will be treated as failed.
Health Check Interval	This is the time interval between each health check test.
Health Check Retries	This is the number of consecutive check failures before treating a connection as down.
Recovery Retries	This is the number of responses required after a health check failure before treating a connection as up again.

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

Bandwidth Allowance Monitor Settings

Bandwidth Allowance Monitor	Check the box <i>Enable</i> to enable bandwidth usage monitoring on this WAN connection for each billing cycle. When this option is not enabled, bandwidth usage of each month is still being tracked but no action will be taken.
Action	If Email Notification is enabled, you will receive an email notification when usage hits 75% and 95% of the monthly allowance. If the box Disconnect when usage hits 100% of monthly allowance is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume unless this option has been turned off or the usage has been reset when a new billing cycle starts.
Start Day	This option allows you to select which day of the month a billing cycle starts.
Monthly Allowance	This field is to specify the bandwidth allowance for each billing cycle.

Additional Public IP Settings

Additional Public IP Address	IP Address	
	Subnet Mask	255.255.255.0 (/24)
		Delete

Additional Public IP Settings

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

Dynamic DNS Settings

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

Dynamic DNS Settings

Dynamic DNS Service Provider	This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers: • changeip.com • dyndns.org • no-ip.org • tzo.com • DNS-O-Matic
-------------------------------------	---

Select **Disabled** to disable this feature. See **Section 9.5** for configuration details.

7.1.1 DHCP Connection

There are four possible connection methods:

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

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

Connection Method	 DHCP ▼
Routing Mode	 ☒ NAT
IP Address	10.88.3.158
Subnet Mask	255.255.255.0
Default Gateway	10.88.3.253
Hostname (Optional)	☐ Use custom hostname
DNS Servers	☒ Obtain DNS server address automatically 10.88.3.1 ☐ Use the following DNS server address(es) DNS Server 1: DNS Server 2:

DHCP Connection Settings	
Routing Mode	NAT allows substituting the real address in a packet with a mapped address that is routable on the destination network. By clicking the help icon in this field, you can display the IP Forwarding option, if your network requires it.
IP Address/ Subnet Mask/ Default Gateway	This information is obtained from the ISP automatically.
Hostname (Optional)	If your service provider's DHCP server requires you to supply a hostname value upon acquiring an IP address, you may enter the value here. If your service provider does not provide you with the value, you can safely bypass this option.
DNS Servers	Each ISP may provide a set of DNS servers for DNS lookups. This setting specifies the DNS (Domain Name System) servers to be used when a DNS lookup is routed through this connection. Selecting Obtain DNS server address automatically results in the DNS servers being assigned by the WAN DHCP server to be used for outbound DNS lookups over the connection. (The DNS servers are obtained along with the WAN IP address assigned from the DHCP server.)

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

7.1.2 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 Address	10.88.3.158
Subnet Mask	255.255.255.0
Default Gateway	10.88.3.253
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.

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.

7.2 Cellular WAN



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

Connection Details

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

Cellular Status

IMSI

This is the International Mobile Subscriber Identity which uniquely identifies the SIM card. This is applicable to 3G modems only.

MEID	Some Pepwave routers support both HSPA and EV-DO. For Sprint or Verizon Wireless EV-DO users, a unique MEID identifier code (in hexadecimal format) is used by the carrier to associate the EV-DO device with the user. This information is presented in hex and decimal format.
ESN	This serves the same purpose as MEID HEX but uses an older format.
IMEI	This is the unique ID for identifying the modem in GSM/HSPA mode.

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

Connection Settings	
WAN Connection Name	Indicate a name you wish to give this WAN connection
Enable	Click the checkbox to toggle the on and off state of this 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.
Subnet Selection	Choose Auto: The subnet mask will be set automatically. Force /31 Subnet: The subnet mask will be set as 255.255.255.254(/31), and the

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

Cellular Settings		
SIM Card	☒ Both SIMs ☐ SIM A Only ☐ SIM B Only	
Preferred SIM Card	☒ No Preference ☐ SIM A ☐ SIM B	
	SIM Card A	SIM Card B
Network Selection	☒ Auto ☐ Manual	☒ Auto ☐ Manual
LTE/3G	LTE Only ▾	LTE Only ▾
Optimal Network Discovery	☐	☐
Band Selection	Auto ▾	Auto ▾
Data Roaming	☐	☐
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	☒ Receive email notification ☐ Reserve for management traffic when usage hits 100% ☐ Disconnect when usage hits 100%	☒ Receive email notification ☐ Reserve for management traffic when usage hits 100% ☐ Disconnect when usage hits 100%
Start Day	On 26th ▾ of each month	On 21st ▾ of each month
Monthly Allowance	4 GB ▾	22 GB ▾

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

	bands (frequencies) When set to Manual, you can manually select the bands (frequencies) the SIM will connect to.
Data Roaming	This checkbox enables data roaming on this particular SIM card. When data roaming is enabled this option allows you to select in which countries the SIM has a data connection. The option is configured by using MMC (country) codes. Please check your service provider's data roaming policy before proceeding.
Authentication	Choose from PAP Only or CHAP Only to use those authentication methods exclusively. Select Auto to automatically choose an authentication method.
Operator Settings	This setting allows you to configure the APN settings of your connection. If Auto is selected, the mobile operator should be detected automatically. The connected device will be configured and connection will be made automatically. If there is any difficulty in making connection, you may select Custom to enter your carrier's APN , Login , Password , and Dial Number settings manually. The correct values can be obtained from your carrier. The default and recommended setting is Auto .
APN / Login / Password / SIM PIN	When Auto is selected, the information in these fields will be filled automatically. Select Custom to customize these parameters. The parameter values are determined by and can be obtained from the ISP.
Bandwidth Allowance Monitor	Check the box Enable to enable bandwidth usage monitoring on this WAN connection for each billing cycle. When this option is not enabled, bandwidth usage of each month is still being tracked but no action will be taken.
Action	If email notification is enabled, you will be notified by email when usage hits 75% and 95% of the monthly allowance. If Disconnect when usage hits 100% of monthly allowance is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume connection unless this option has been turned off or the usage has been reset when a new billing cycle starts.
Start Day	This option allows you to define which day of the month each billing cycle begins.
Monthly Allowance	This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

Signal Threshold Settings



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

The following values are used by the threshold scale:

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

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

Signal Threshold Settings ?			
LTE	RSRP:	n/a	dBm (Recovery: n/a dBm)
	SINR:	n/a	dB (Recovery: n/a dB)
3G	RSSI:	n/a	dBm (Recovery: n/a dBm)

General Settings	
Independent from Backup WANs	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available.
Standby State	This option allows you to choose whether to remain connected or disconnected when this WAN connection is no longer in the highest priority and has entered the standby state. When Remain connected is chosen, bringing up this WAN connection to active makes it immediately available for use.
Idle Disconnect	When Internet traffic is not detected within the user-specified timeframe, the modem will automatically disconnect. Once the traffic is resumed by the LAN host, the connection will be re-activated.

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

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

Dynamic DNS Settings

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

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

MTU

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

7.3 Wi-Fi WAN

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

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

WAN Connection Settings	
WAN Connection Name	Enter a name to represent this WAN connection.
Operating Schedule	Click the drop-down menu to apply a time schedule to this interface.
Independent from Backup WANs	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available.
Standby State	This setting specifies the state of the WAN connection while in standby. The available options are Remain Connected (hot standby) and Disconnect (cold standby).
MTU	This setting specifies the maximum transmission unit. By default, MTU is set to Custom 1440 . You may adjust the MTU value by editing the text field. Click Default to restore the default MTU value. Select Auto and the appropriate MTU value will be automatically detected. The auto-detection will run each time the WAN connection establishes
Reply to ICMP PING	If this setting is disabled, the WAN connection will not respond to ICMP ping requests. By default, this setting is enabled.

Wi-Fi WAN Settings	
Channel Width	20 MHz
Channel Selection	☒ Auto ☐ Custom
Data Rate	☒ Auto ☐ Fixed
Output Power	Max ☐ Boost
Roaming	☐
Connect to Any Open Mode AP	☐ Yes ☒ No
Beacon Miss Counter	5

Wi-Fi WAN Settings	
Channel Width	Select the channel width for this Wi-Fi WAN. 20MHz will have greater support for older devices using 2.4Ghz, while 40MHz is appropriate for networks with newer devices that connect using 5Ghz
Channel Selection	Determine whether the channel will be automatically selected. If you select custom, the following table will appear: Scan Channels Clear All 2.4GHz: ☒ 1 ☒ 2 ☒ 3 ☒ 4 ☒ 5 ☒ 6 ☒ 7 ☒ 8 ☒ 9 ☒ 10 ☒ 11 OK Cancel
Data Rate	Selecting Auto will enable the router to automatically determine the best data rate, while manually selecting a rate will force devices to connect using the fixed rate.
Output Power	If you are setting up a network with many Wi-Fi devices in close proximity, then you can configure the output power here. Click the “boost” button for additional power. However, with that option ticked, output power may exceed local regulatory limits.
Roaming	Checking this box will enable Wi-Fi roaming. Click the  icon for additional options.
Connect to Any Open Mode AP	This option is to specify whether the Wi-Fi WAN will connect to any open mode access points it finds.
Beacon Miss Counter	This sets the threshold for the number of missed beacons.

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

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

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

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

Health Check Settings	
Health Check Method	? Disabled

Health Check disabled. Network problem cannot be detected.

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

Health Check Method: PING

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

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

PING Hosts

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

Health Check Method: DNS Lookup

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

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

Health Check DNS Servers

This field allows you to specify two DNS hosts' IP addresses with which connectivity is to be tested via DNS Lookup.

If **Use first two DNS servers as Health Check DNS Servers** is checked, the first two DNS servers will be the DNS lookup targets for checking a connection's health. If the box is not checked, **Host 1** must be filled, while a value for **Host 2** is optional. If **Include public DNS servers** is selected and no response is received from all specified DNS servers, DNS lookups will also be issued to some public DNS servers. A WAN connection will be treated as down only if there is also no response received from the public DNS servers.

Connections will be considered as up if DNS responses are received from any one of the health check DNS servers, regardless of a positive or negative result. By default, the first two DNS servers of the WAN connection are used as the health check DNS servers.

Health Check Method: HTTP

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

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

URL 1 **WAN Settings>WAN Edit>Health Check Settings>URL1**
 The URL will be retrieved when performing an HTTP health check. When **String to Match** is left blank, a health check will pass if the HTTP return code is between 200 and 299 (Note: HTTP redirection codes 301 or 302 are treated as failures). When **String to Match** is filled, a health check will pass if the HTTP return code is between 200 and 299 and if the HTTP response content contains the string.

URL 2 **WAN Settings>WAN Edit>Health Check Settings>URL2**
 If **URL2** is also provided, a health check will pass if either one of the tests passed.

Other Health Check Settings

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

Timeout This setting specifies the timeout in seconds for ping/DNS lookup requests. The default timeout is **5 seconds**.

Health Check Interval This setting specifies the time interval in seconds between ping or DNS lookup requests. The default health check interval is **5 seconds**.

Health Check Retries This setting specifies the number of consecutive ping/DNS lookup timeouts after which the Peplink Balance will treat the corresponding WAN connection as down. Default health retries is set to **3**. Using the default **Health Retries** setting of **3**, the corresponding WAN connection will be treated as down after three consecutive timeouts.

Recovery Retries This setting specifies the number of consecutive successful ping/DNS lookup responses that must be received before the Peplink Balance treats a previously down WAN connection as up again. By default, **Recover Retries** is set to **3**. Using the default setting, a WAN connection that is treated as down will be considered as up again upon receiving three consecutive successful ping/DNS lookup responses.

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

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

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

7.3.1 Creating Wi-Fi Connection Profiles

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



This will open a window similar to the one shown below



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

7.4 WAN Health Check

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

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

two DNS servers will be the DNS lookup targets for checking a connection's health. If the box is not checked, **Host 1** must be filled, while a value for **Host 2** is optional. If **Include public DNS servers** is selected and no response is received from all specified DNS servers, DNS lookups will also be issued to some public DNS servers. A WAN connection will be treated as down only if there is also no response received from the public DNS servers.

Connections will be considered as up if DNS responses are received from any one of the health check DNS servers, regardless of a positive or negative result. By default, the first two DNS servers of the WAN connection are used as the health check DNS servers.

Health Check Method: HTTP

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

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

URL1

WAN Settings>WAN Edit>Health Check Settings>URL1

The URL will be retrieved when performing an HTTP health check. When **String to Match** is left blank, a health check will pass if the HTTP return code is between 200 and 299 (Note: HTTP redirection codes 301 or 302 are treated as failures). When **String to Match** is filled, a health check will pass if the HTTP return code is between 200 and 299 and if the HTTP response content contains the string.

URL 2

WAN Settings>WAN Edit>Health Check Settings>URL2

If **URL2** is also provided, a health check will pass if either one of the tests passed.

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

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

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

7.5 Dynamic DNS Settings

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

If the WAN connection's IP address is a reserved private IP address (i.e., behind a NAT router), the public IP of each WAN will be automatically reported to the DNS service provider.

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

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

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

Dynamic DNS Settings	
Dynamic DNS	This setting specifies the dynamic DNS service provider to be used for the WAN based on supported dynamic DNS service providers: • changeip.com • dyndns.org • no-ip.org • tzo.com • DNS-O-Matic • Others...
Account Name / Email Address	Support custom Dynamic DNS servers by entering its URL. Works with any service compatible with DynDNS API. Select Disabled to disable this feature.
Password / TZO Key	This setting specifies the registered user name for the dynamic DNS service.
Hosts / Domain	This setting specifies the password for the dynamic DNS service. 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.

8 Advanced Wi-Fi Settings

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

AP Settings	
SSID	☒ 2.4 GHz ☒ 5 GHz Integrated AP supports 2.4 GHz only. Testing
Operating Country	United States ▼
Preferred Frequency	☒ 2.4 GHz ☐ 5 GHz Integrated AP supports 2.4 GHz only.

AP Settings	
SSID	You can select the wireless networks for 2.4 GHz or 5 GHz separately for each SSID.
Operating Country	This drop-down menu specifies the national/regional regulations which the Wi-Fi radio should follow. • If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW). • If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW). NOTE: Users are required to choose an option suitable to local laws and regulations.
Preferred Frequency	Indicate the preferred frequency to use for clients to connect.

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

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

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

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

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

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

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

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

Web Administration Settings (on External AP)	
Enable	☒
Web Access Protocol	☐ HTTP ☒ HTTPS
Management Port	443
HTTP to HTTPS Redirection	☒
Admin Username	admin
Admin Password	601202b1afc6 Generate

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

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

Wi-Fi WAN Settings	
Channel Width	20/40 MHz
Bit Rate	Auto
Output Power	Max ☐ Boost

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

9 ContentHub Configuration

9.1 ContentHub

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

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

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

9.2 Configuring the ContentHub

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

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

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

ContentHub						
Enable		☒				
<button>Save</button>						
Schedule						
Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions
No Schedule						
<button>New Website</button>						

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

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

9.3 Configure a website to be published from the ContentHub

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

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

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

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

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

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

Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions
http://mytest.com						+ [edit] [delete]
/(root)	ftp://10.8.76.254/web...	-	-	-	[download icon]	[upload icon] [edit] [delete]

New Website

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

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

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

Websites	Source	Next Update	Last Updated	Elapsed Time	Status	Actions
http://mytest.com						+ [edit] [delete]
/(root)	ftp://10.8.76.254/web...	-	05-23 03:41	00:00:11	[checkmark]	[upload icon] [download icon] [edit] [delete]

New Website

Status details [Close](#)

Completed
+1 / 0 / -0 files

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

9.4 Configure an application to be published from the ContentHub

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

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

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

The screenshot shows the Peplink web interface. The top navigation bar includes links for Dashboard, Setup Wizard, Network, AP, System (selected), and Status. On the right of the navigation bar is an 'Apply Changes' button. The left sidebar contains a 'System' menu with options like Admin Security, Firmware, Time, Schedule, Email Notification, Event Log, SNMP, InControl, Configuration, Feature Add-ons, and Reboot. Below this is a 'Tools' menu with Ping, Traceroute, Wake-on-LAN, Storage Manager, and Package Manager (highlighted). A 'Logout' button is at the bottom of the sidebar. The main content area shows the 'System' status with a timestamp '(Last Update: Tue May 23 04:02:36 UTC 2017)'. Below this is the 'Package List' section, which has an 'Update All' button. The package list contains three entries: Node.js (Version: 6.9.2, Size: 8.99 MB, Date: Fri Feb 24 07:45:28 UTC 2017), Python (Version: 2.7.12, Size: 20.29 MB, Date: Fri Feb 24 07:45:28 UTC 2017), and Ruby (Version: 2.3.3, Size: 31.44 MB, Date: Fri Feb 24 07:45:30 UTC 2017). Each entry has a green download icon to its right.

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

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

Schedule

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

Save & Apply Now

Cancel

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

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

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

10 MediaFast Configuration

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

10.1 Setting Up MediaFast Content Caching

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

MediaFast

Enable ☐

Domains / IP Addresses ? ☐ Cache all ☐ Whitelist ☒ Blacklist

Source IP Subnet ? ☒ Any ☐ Custom

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

Secure Content Caching

Enable ? ☐ Note: Please enable MediaFast for Secure Content Caching

Domains / IP Addresses ? ☐ Cache all ☒ Whitelist ☐ Blacklist

googlevideo.com
youtube.com

Source IP Subnet ? ☒ Any ☐ Custom

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

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

Cache Control					
Content Type	☒ Video ☒ Audio ☒ Images ☒ OS / Application Updates				
Cache Lifetime Settings	<table border="1"> <thead> <tr> <th>File Extension</th> <th>Lifetime (days)</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table>	File Extension	Lifetime (days)		
File Extension	Lifetime (days)				

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

10.2 Scheduling Content Prefetching

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

Prefetch Schedule							
Name	Status	Next Run Time	Last Run Time	Last Duration	Result	Last Download	Actions
▶ Course Progress	Downloading	04-11 06:00	04-09 02:03	-		0 B	
▶ National Geog	Ready	04-11 00:00	04-09 00:00	00:01		4.98 kB	
▶ Syllabus	Downloading	04-11 06:00	04-09 06:00	-		0 B	
▶ Vimeo	Ready	04-11 00:00	04-09 02:03	00:01		115.91 kB	
▶ ted	Ready	04-11 00:00	04-09 00:00	00:01		62.26 kB	
New Schedule							
Tools							
Clear Web Cache Clear Statistics							

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

MediaFast Schedule

Name (optional)			
Active	☒		
URL	+		
Depth	2 ▾ levels	Default	
Time Period	From 00 ▾ : 00 ▾ to 01 ▾ : 00 ▾		
Repeat	Everyday ▾		
Bandwidth Limit	0	Gbps ▾	(0: Unlimited)

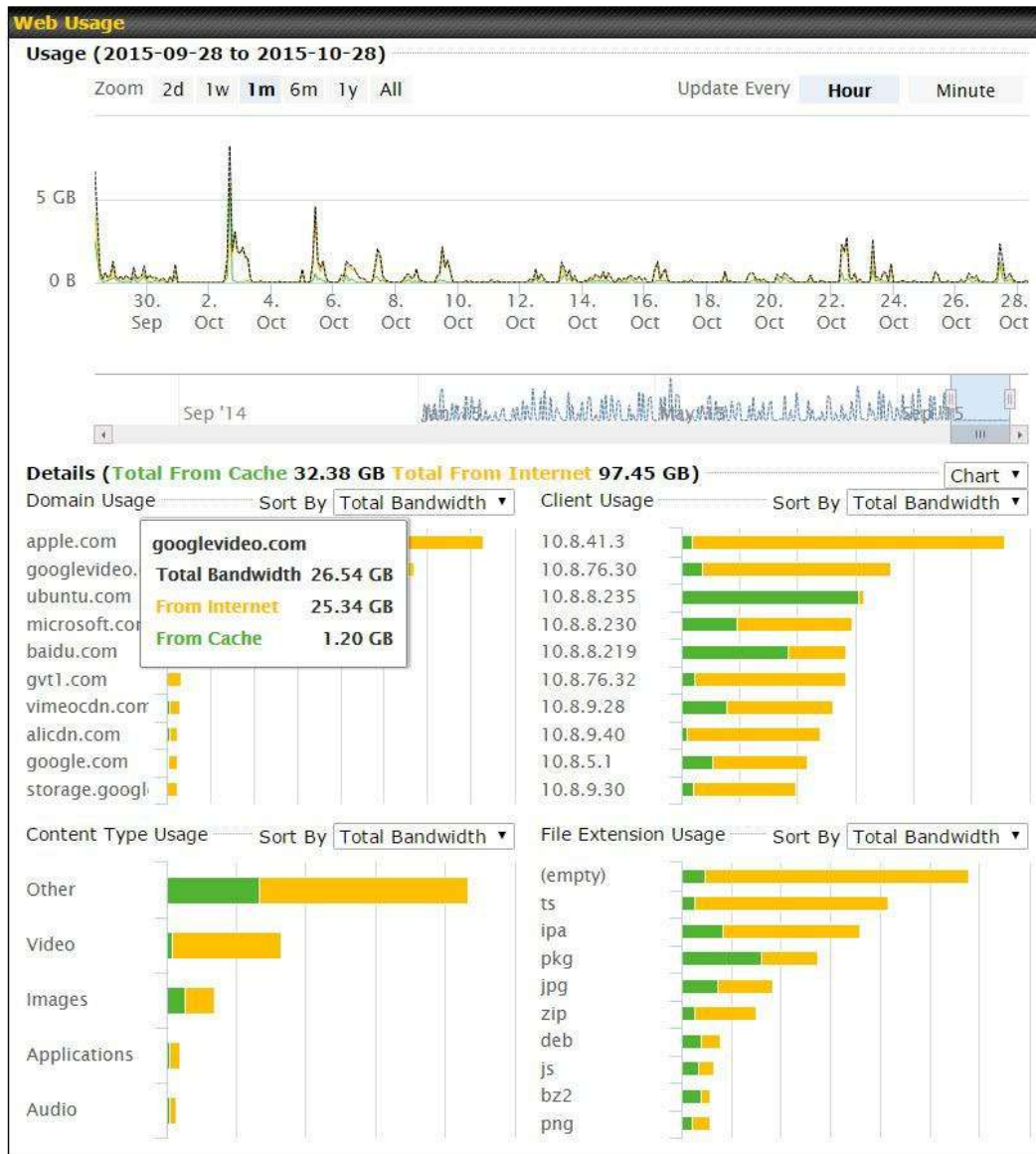
Simply provide the requested information to create your schedule.

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.

10.3 Viewing MediaFast Statistics

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



11 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.

11.1 PepVPN

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

PepVPN with SpeedFusion™



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

Profile	Remote ID	Remote Address(es)	
 FL Office	8345-5F7A-DE97		 
New Profile			

Send All Traffic To
No PepVPN profile selected 

PepVPN
Local ID  MAX_HD2_DEF1 

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

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

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

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

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

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

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

ID/Remote Certificate	Balance's VPN authentication method, as explained above. To authenticate VPN connections using X.509 certificates, copy and paste certificate details into these fields. To get more information on a listed X.509 certificate, click the Show Details link below the field.
Allow Shared Remote ID	When this option is enabled, the router will allow multiple peers to run using the same remote ID.
NAT Mode	Check this box to allow the local DHCP server to assign an IP address to the remote peer. When NAT Mode is enabled, all remote traffic over the VPN will be tagged with the assigned IP address using network address translation.
Remote IP Address / Host Names (Optional)	If NAT Mode is not enabled, you can enter a remote peer's WAN IP address or hostname(s) here. If the remote uses more than one address, enter only one of them here. Multiple hostnames are allowed and can be separated by a space character or carriage return. Dynamic-DNS host names are also accepted. This field is optional. With this field filled, the Peplink MAX will initiate connection to each of the remote IP addresses until it succeeds in making a connection. If the field is empty, the Peplink MAX will wait for connection from the remote peer. Therefore, at least one of the two VPN peers must specify this value. Otherwise, VPN connections cannot be established.
Cost	Define path cost for this profile. OSPF will determine the best route through the network using the assigned cost. Default: 10
Data Port	This field is used to specify a UDP port number for transporting outgoing VPN data. If Default is selected, UDP port 4500 will be used. Port 32015 will be used if the remote unit uses Firmware prior to version 5.4 or if port 4500 is unavailable. If Custom is selected, enter an outgoing port number from 1 to 65535. Click the  icon to configure data stream using TCP protocol [EXPERIMENTAL]. In the case TCP protocol is used, the exposed TCP session option can be authorised to work with TCP accelerated WAN link.
Bandwidth Limit	Define maximum download and upload speed to each individual peer. This functionality requires the peer to use PepVPN version 4.0.0 or above.
Cost	Define path cost for this profile. OSPF will determine the best route through the network using the assigned cost. Default: 10
WAN Smoothing^A	Select the degree to which WAN Smoothing will be implemented across your WAN links.
Use IP ToS	Checking this button enables the use of IP ToS header field.
Latency Difference Cutoff	Traffic will be stopped for links that exceed the specified millisecond value with respect to the lowest latency link. (e.g. Lowest latency is 100ms, a value of 500ms means links with latency 600ms or more will not be used)

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

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

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

WAN Connection Priority

WAN Connection Priority

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

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

Send All Traffic To

No PepVPN profile selected 

Send All Traffic To

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



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

Outbound Policy/PepVPN Outbound Custom Rules

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

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

The screenshot shows the 'PepVPN Local ID' configuration window. It has a label 'Local ID' followed by a text field containing 'MAX_HD2_8D1C' and an edit icon.

PepVPN Local ID

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

The screenshot shows the 'PepVPN Settings' configuration window. It contains three sections: 'Handshake Port' with radio buttons for 'Default' (selected) and 'Custom' (with an empty text field); 'Backward Compatibility' with radio buttons for 'High (firmware 5.3+)' (selected) and 'Latest (firmware 6.2+)'; and 'Link Failure Detection Time' with radio buttons for 'Recommended (Approx. 15 secs)' (selected), 'Fast (Approx. 6 secs)', 'Faster (Approx. 2 secs)', and 'Extreme (Under 1 sec)'. A note at the bottom states: 'Shorter detection time incurs more health checks and higher bandwidth overhead'.

PepVPN Settings

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

expected detection time is six seconds.

When **Faster** is selected, a health check packet is sent every second, and the expected detection time is two seconds.

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

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

Important Note

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

Tip

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



<http://youtu.be/TLQgdpPSY88>

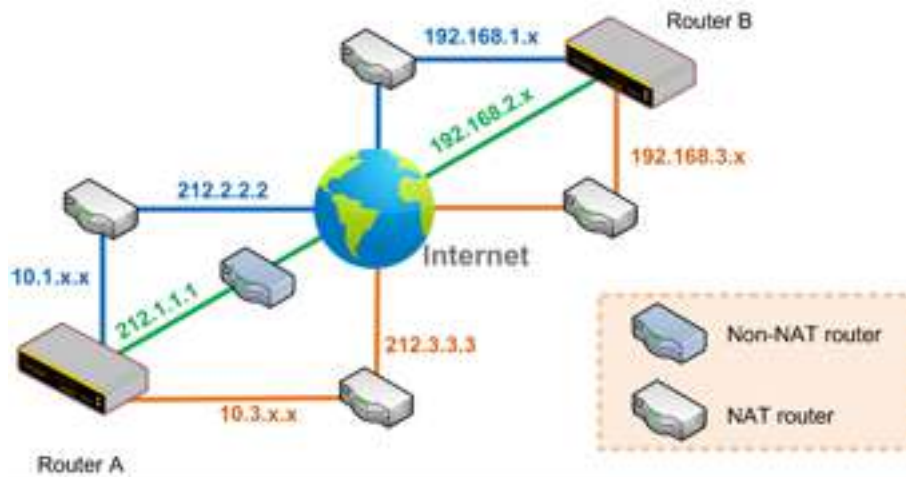
11.2 The Pepwave Router Behind a NAT Router

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.

11.3 SpeedFusion™ Status

SpeedFusion™ 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.

12 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.

12.1 IPsec VPN Settings

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



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



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

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

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

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.

13 Outbound Policy Management

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

Important Note

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

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

Outbound Policy

Custom

Rules (Drag and drop rows to change rule order)

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

13.1 Outbound Policy

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

There are three main selections for the outbound traffic policy:

- High Application Compatibility
- Normal Application Compatibility
- Custom

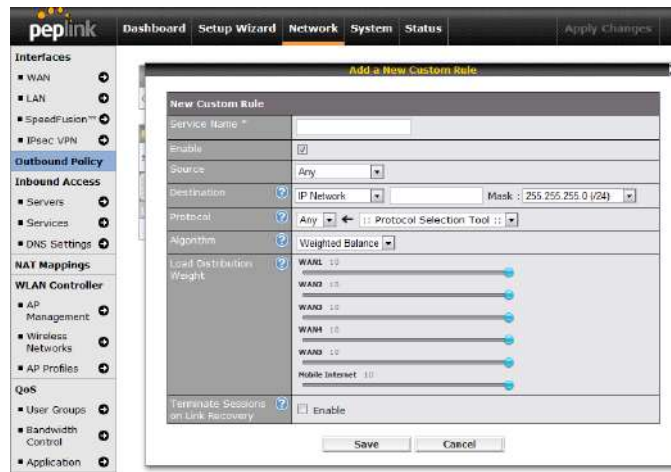
Note that some Pepwave routers provide only the **Send All Traffic To** setting here. See **Section 12.1** for details.

Outbound Policy Settings	
High 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!



http://youtu.be/rKH4AS_bQnE

13.2 Custom Rules for Outbound Policy

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

Outbound Policy
?

Custom


Rules ⚡ Drag and drop rows to change rule order
?

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

Expert Mode
?

Enabled


13.2.1 Algorithm: Weighted Balance

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

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

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

For example, with the following weight settings:

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

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

Matching traffic distributed to Ethernet WAN1 is $16.7\% = (10 / 60 \times 100\%)$.

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

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

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

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

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

13.2.2 Algorithm: Persistence

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

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

Pepwave routers can be configured to distribute data traffic across multiple WAN connections.

Also, the Internet IP depends on the WAN connections over which communication actually takes place. As a result, a LAN client computer behind the Pepwave router may communicate using multiple Internet IP addresses. For example, a LAN client computer behind a Pepwave router with three WAN connections may communicate on the Internet using three different IP addresses.

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

Algorithm	Persistence
Persistence Mode	☒ By Source ☐ By Destination
Load Distribution	☐ Auto ☒ Custom
Load Distribution Weight	WAN 1 10 WAN 2 10 Wi-Fi WAN 10 Cellular 1 10 Cellular 2 10 USB 10

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

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

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

13.2.3 Algorithm: Enforced

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

Algorithm	?	Enforced
Enforced Connection	?	WAN: WAN 1 WAN: WAN 1 WAN: WAN 2 WAN: Wi-Fi WAN WAN: Cellular 1 WAN: Cellular 2 WAN: USB VPN: Connection 1
		Save Cancel

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.

13.2.4 Algorithm: Priority

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

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

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

Tip

Configure multiple distribution rules to accommodate different kinds of services.

13.2.5 Algorithm: Overflow

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

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

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

13.2.6 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.

13.2.7 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.

13.2.8 Expert Mode

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

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

above the bar to override the SpeedFusion™ routes.

Help

Close

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

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

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

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

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

14 Inbound Access

14.1 Port Forwarding Service

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

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

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

Enable	☒ Yes ☐ No																												
Service Name	Service_1																												
IP Protocol	? TCP ← :: Protocol Selection Tool :: ↓																												
Port	? Any Port ↓																												
Inbound IP Address(es) (Require at least one IP address)	? <table> <tr> <th colspan="2">Connection / IP Address(es)</th><th>All</th><th>Clear</th></tr> <tr> <td>☒ WAN 1</td><td>☒ 10.88.3.158 (Interface IP)</td><td></td><td></td></tr> <tr> <td>☐ WAN 2</td><td></td><td></td><td></td></tr> <tr> <td>☐ Wi-Fi WAN</td><td></td><td></td><td></td></tr> <tr> <td>☐ Cellular 1</td><td></td><td></td><td></td></tr> <tr> <td>☐ Cellular 2</td><td></td><td></td><td></td></tr> <tr> <td>☐ USB</td><td></td><td></td><td></td></tr> </table>	Connection / IP Address(es)		All	Clear	☒ WAN 1	☒ 10.88.3.158 (Interface IP)			☐ WAN 2				☐ Wi-Fi WAN				☐ Cellular 1				☐ Cellular 2				☐ USB			
Connection / IP Address(es)		All	Clear																										
☒ WAN 1	☒ 10.88.3.158 (Interface IP)																												
☐ WAN 2																													
☐ Wi-Fi WAN																													
☐ Cellular 1																													
☐ Cellular 2																													
☐ USB																													
Server IP Address	? 120.78.95.7																												

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

Port

The **Port** setting specifies the port(s) that correspond to the service, and can be configured to behave in one of the following manners:

Any Port, Single Port, Port Range, Port Map, and Range Mapping

Port	?	Any Port
------	---	----------

Any Port: all traffic that is received by the Pepwave router via the specified protocol is forwarded to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Any Port**, all TCP traffic is forwarded to the configured servers.

Port	?	Single Port	Service Port: 80
------	---	-------------	------------------

Single Port: traffic that is received by the Pepwave router via the specified protocol at the specified port is forwarded via the same port to the servers specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Single Port** and **Service Port** 80, TCP traffic received on port 80 is forwarded to the configured servers via port 80.

Port	?	Port Range	Service Ports: 80 - 88
------	---	------------	------------------------

Port Range: traffic that is received by the Pepwave router via the specified protocol at the specified port range is forwarded via the same respective ports to the LAN hosts specified by the **Servers** setting. For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Range** and **Service Ports** 80-88, TCP traffic received on ports 80 through 88 is forwarded to the configured servers via the respective ports.

Port	?	Port Mapping	Service Port: 80	Map to Port: 88
------	---	--------------	------------------	-----------------

Port Mapping: traffic that is received by Pepwave router via the specified protocol at the specified port is forwarded via a different port to the servers specified by the **Servers** setting.

For example, with **IP Protocol** set to **TCP**, and **Port** set to **Port Mapping**, **Service Port** 80, and **Map to Port** 88, TCP traffic on port 80 is forwarded to the configured servers via port 88.

(Please see below for details on the **Servers** setting.)

Port	?	Range Mapping	Service Ports: 80 - 88	Map to Ports: 88 - 96
------	---	---------------	------------------------	-----------------------

Range Mapping: traffic that is received by the Pepwave router via the specified protocol at the specified port range is forwarded via a different port to the servers specified by the **Servers** setting.

Inbound IP Address(es)

This setting specifies the WAN connections and Internet IP address(es) from which the service can be accessed.

Server IP Address

This setting specifies the LAN IP address of the server that handles the requests for the service.

14.1.1 UPnP / NAT-PMP Settings

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

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

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

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

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

15 NAT Mappings

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

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

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

LAN Client(s)	? IP Address ▾												
Address	?												
Inbound Mappings	? Connection / Inbound IP Address(es) ☐ WAN 1 ☐ WAN 2 ☐ Wi-Fi WAN ☐ Cellular 1 ☐ Cellular 2 ☐ USB												
Outbound Mappings	? Connection / Outbound IP Address <table border="1"> <tbody> <tr> <td>WAN 1</td> <td>10.88.3.158 (Interface IP) ▾</td> </tr> <tr> <td>WAN 2</td> <td>Interface IP ▾</td> </tr> <tr> <td>Wi-Fi WAN</td> <td>Interface IP ▾</td> </tr> <tr> <td>Cellular 1</td> <td>Interface IP ▾</td> </tr> <tr> <td>Cellular 2</td> <td>Interface IP ▾</td> </tr> <tr> <td>USB</td> <td>Interface IP ▾</td> </tr> </tbody> </table>	WAN 1	10.88.3.158 (Interface IP) ▾	WAN 2	Interface IP ▾	Wi-Fi WAN	Interface IP ▾	Cellular 1	Interface IP ▾	Cellular 2	Interface IP ▾	USB	Interface IP ▾
WAN 1	10.88.3.158 (Interface IP) ▾												
WAN 2	Interface IP ▾												
Wi-Fi WAN	Interface IP ▾												
Cellular 1	Interface IP ▾												
Cellular 2	Interface IP ▾												
USB	Interface IP ▾												

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

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

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

Important Note

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

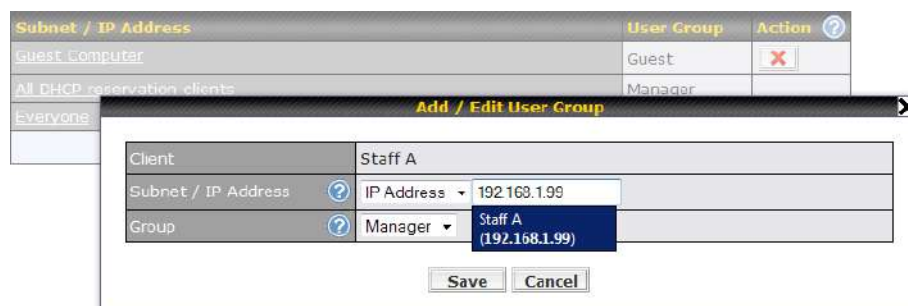
16

16.1 User Groups

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

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

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



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

Add / Edit User Group

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

Save Cancel

Add / Edit User Group	
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.

16.2 Bandwidth Control

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

Group Bandwidth Reservation				
Enable		☒		
	Manager	Staff	Guest	
Bandwidth %	50%	30%	20%	
WAN 1	500.0M/500.0M	300.0M/300.0M	200.0M/200.0M	
WAN 2	500.0M/500.0M	300.0M/300.0M	200.0M/200.0M	

16.3 Application

16.3.1 Application Prioritization

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

Application Prioritization	
☒ Apply same settings to all users	
☐ Customize	

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

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

16.3.2 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.

16.3.3 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.

17 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.

Outbound Firewall Rules (Drag and drop rows by the left to change rule order)					
Rule	Protocol	Source	Destination	Action	
Default	Any	Any	Any	✓	
Add Rule					

Inbound Firewall Rules (Drag and drop rows by the left to change rule order)					
Rule	Protocol	WAN	Source	Destination	Action
Default	Any	Any	Any	Any	✓
Add Rule					

Internal Network Firewall Rules (Drag and drop rows by the left to change rule order)					
Rule	Protocol	Source	Destination	Action	
Default	Any	Any	Any	✓	
Add Rule					

Intrusion Detection and DoS Prevention					
Disabled					

Local Service Firewall Rules (Drag and drop rows by the left to change rule order)					
Rule	Service	WAN	Source	Action	
Default	Any	Any	Any	✓	
Add Rule					

17.1 Outbound and Inbound Firewall Rules

17.1.1 Access Rules

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

Outbound Firewall Rules (Drag and drop rows by the left to change rule order)					
Rule	Protocol	Source	Destination	Action	
test	Any	Any	Any	✓	✗
Default	Any	Any	Any	✓	
Add Rule					

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

Add a New Outbound Firewall Rule

New Firewall Rule

Rule Name	
Enable	☒ Always on
Protocol	Any Protocol Selection Tool
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	☒ Allow ☐ Deny
Event Logging	☐ Enable

Save
Cancel

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

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

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

Add Rule

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

Add a New Inbound Firewall Rule

New Firewall Rule

Rule Name	
Enable	☒
WAN Connection	Any
Protocol	Any Protocol Selection Tool
Source IP & Port	Any Address
Destination IP & Port	Any Address
Action	☒ Allow ☐ Deny
Event Logging	☐ Enable

Save
Cancel

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

Internal Network Firewall Rules (Drag and drop rows by the left to change rule order)					
Rule	Protocol	Source	Destination	Action	
test	Any	Any	Any		
Default	Any	Any	Any		
Add Rule					

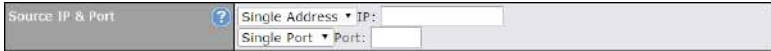
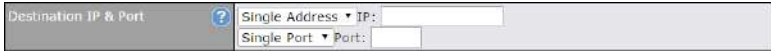
Click **Add Rule** to display the following window:

Add a New Internal Network Firewall Rule

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

Save
Cancel

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: - TCP - UDP - ICMP - 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 that matches the both of the following: • Source IP & port • Destination IP & port With the value of Allow for the Action setting, the matching traffic passes through the router (to be routed to the destination). If the value of the Action setting is set to Deny, the matching traffic does not pass through the router (and is discarded).
Event Logging	This setting specifies whether or not to log matched firewall events. The logged messages are shown on the page Status>Event Log. A sample message is as follows: Aug 13 23:47:44 Denied CONN=Ethernet WAN SRC=20.3.2.1 DST=192.168.1.20 LEN=48 PROTO=TCP SPT=2260 DPT=80 • CONN: The connection where the log entry refers to • SRC: Source IP address • DST: Destination IP address • LEN: Packet length • PROTO: Protocol • SPT: Source port • DPT: Destination port

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

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

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

Outbound Firewall Rules (Drag and drop rows to change rule order)					
Rule	Protocol	Source IP Port	Destination IP Port	Policy	
No web access	TCP	Any Any	Any 80	Deny	
No FTP access	TCP	Any Any	Any 21	Deny	
Default	Any	Any	Any	Allow	
Add Rule					

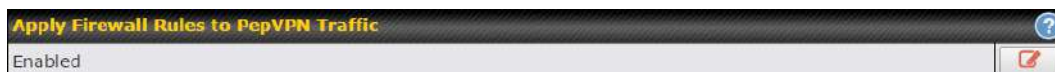
To remove a rule, click the  button.

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

Tip

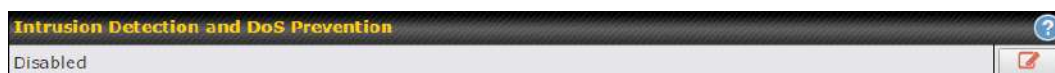
If the default inbound rule is set to **Allow** for NAT-enabled WANs, no inbound Allow firewall rules will be required for inbound port forwarding and inbound NAT mapping rules. However, if the default inbound rule is set as **Deny**, a corresponding Allow firewall rule will be required.

17.1.2 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.

17.1.3 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

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

17.2 Content Blocking

Application Blocking
?

Please Select Application...
+

Web Blocking
?

Preset Category

☐ High
☐ Moderate
☐ Low
☒ Custom

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

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

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

Customized Domains

cbs.com
+

Exempted Domains from Web Blocking
+

Exempted User Groups
?

Manager
☐ Exempt

Staff
☐ Exempt

Guest
☐ Exempt

Exempted Subnets
?

Network
Subnet Mask

+

URL Logging

Enable
☐

Log Server Host
Port:

17.2.1 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.

17.2.2 Web Blocking

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

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

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

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

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

17.2.3 Customized Domains

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

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

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

17.2.4 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.

17.2.5 Exempted Subnets

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

17.2.6 URL Logging

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

18 OSPF & RIP v2

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

RIPv2 item on the sidebar to reach the following menu:

OSPF		
Router ID	LAN IP Address	
Area	Interfaces	
0.0.0.0	PepVPN	
Add		

PepVPN OSPF Area	
0.0.0.0	

RIPv2	
No RIPv2 Defined.	
	

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

OSPF settings

Area ID	0.0.0.0
Link Type	☒ Broadcast ☐ Point-to-Point
Authentication	None ▾
Interfaces	☐ Untagged LAN ☐ V167 (192.168.167.1/24) ☐ WAN 1 ☐ WAN 2 ☐ WAN 3 ☐ WAN 4 ☐ WAN 5 ☒ PepVPN

Save

Cancel

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

To access RIPv2 settings, click .

RIPv2 settings

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

Save

Cancel

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

OSPF & RIPv2 Route Advertisement

PepVPN Route Isolation	☐ Enable						
Network Advertising	--- All LAN/VLAN networks will be advertised when no network advertising is chosen. +						
Static Route Advertising	☒ Enable <table> <tr> <th>Excluded Networks</th><th>Subnet Mask</th><th></th></tr> <tr> <td></td><td>255.255.255.0 (/24) ▾</td><td>+</td></tr> </table>	Excluded Networks	Subnet Mask			255.255.255.0 (/24) ▾	+
Excluded Networks	Subnet Mask						
	255.255.255.0 (/24) ▾	+					

Save

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	Enable this option to advertise LAN static routes over OSPF & RIPv2. Static routes that match the Excluded Networks table will not be advertised.

19 BGP

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

BGP	AS	Neighbors	
Uplink	64520	172.16.51.1	
Add			

Click "x" to delete a BGP profile

Click "Add" to add a new BGP profile

BGP Profile						
Profile Name						
Enable	☒					
Interface	WAN 1					
Router ID	☒ LAN IP Address ☐ Custom:					
Autonomous System						
Neighbor	IP Address	Autonomous System	Multihop / TTL	Password	AS-Path Prepending	
			disable			
Hold Time	 240					

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

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

Route Advertisement			
Network Advertising	?	---	+
Static Route Advertising	?	☒ Enable	
		Excluded Networks	Subnet Mask
			255.255.255.0 (/24) +
Advertise OSPF Route	?	☐	

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

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

Filter Mode	This option selects the route import filter mode. 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	This specifies the network in the "route import" entry

Networks

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

Route Export

Export to other BGP Profile


☐

Export to OSPF


☐

Export to other BGP Profile

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

Export to OSPF

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

20 Remote User Access

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

20.1 L2TP with IPsec

Remote User Access Settings	
Enable	☒
VPN Type	☒ L2TP with IPsec ☐ PPTP ☐ OpenVPN
Preshared Key	☒ Hide Characters

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

Continue to configure the authentication method.

20.2 OpenVPN

Remote User Access Settings	
Enable	☒
VPN Type	☐ L2TP with IPsec ☐ PPTP ☒ OpenVPN You can obtain the OpenVPN client profile from the status page .

Select OpenVPN and continue to configure the authentication method.

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

OpenVPN Client Profile	 Route all traffic Split tunnel
------------------------	--

You have a choice between 2 different OpenVPN Client profiles.

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

20.3 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.

20.4 Authentication Methods

Connect to Network	<input <="" lan="" td="" type="button" untagged="" value="?" ▼=""/>		
Authentication	Local User Accounts ▼		
User Accounts	<input <="" td="" type="button" username="" value="?"/> <td>Password</td> <td> + </td>	Password	+

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

User accounts:

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

Note:

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

The password must be between 8 and 12 characters long.

LDAP Server:

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

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

Radius Server:

Authentication	RADIUS Server ▼
Auth Protocol	MS-CHAP v2 ▼
Auth Server	Port 1812 Default
Auth Server Secret	☒ Hide Characters
Accounting Server	Port 1813 Default
Accounting Server Secret	☒ Hide Characters

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

Active Directory:

Connect to Network	 Untagged LAN ▼
Authentication	Active Directory ▼
Server Hostname	
Domain	
Admin Username	
Admin Password	☒ Hide Characters

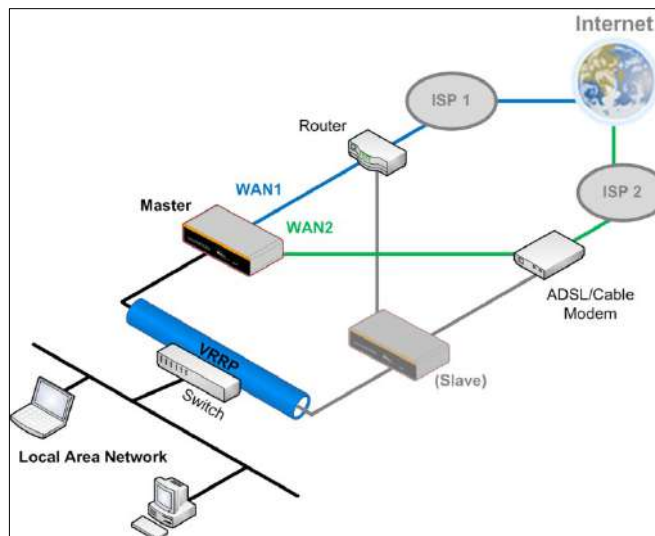
Enter the matching Active Directory details to allow for Active Directory server authentication.

21 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).

21.1 High Availability

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



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

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

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

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

Interface for Master Router

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

Interface for Slave Router

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

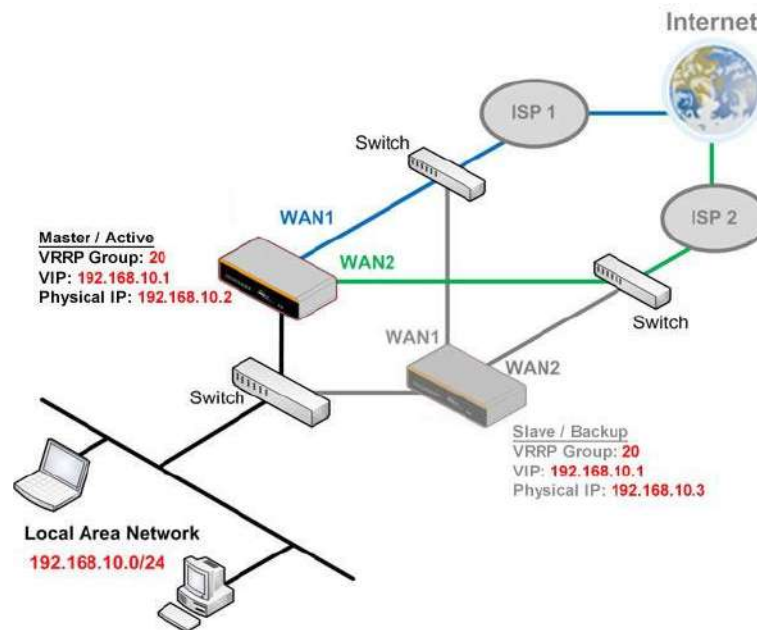
High Availability	
Enable	Checking this box specifies that the Pepwave router is part of a high availability configuration.
Group Number	This number identifies a pair of Pepwave routers operating in a high availability configuration. The two Pepwave routers in the pair must have the same Group Number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

IP

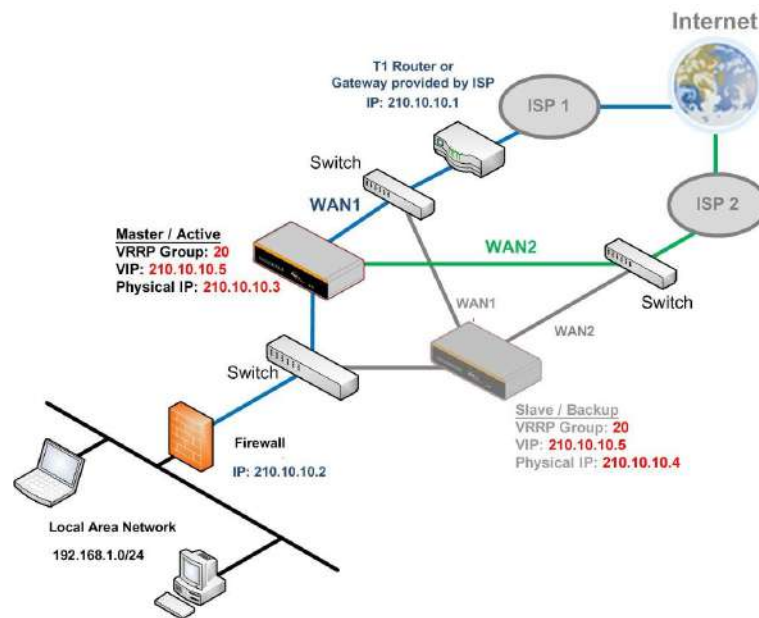
Subnet Mask This setting specifies the subnet mask of the LAN.

Important Note

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



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



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

21.2 Certificate Manager

Certificate		
SpeedFusion/IPsec VPN	No Certificate	
Web Admin SSL	Default Certificate is in use	
Captive Portal SSL	Default Certificate is in use	
OpenVPN CA ⚠	Default Certificate is in use	
Wi-Fi WAN Client Certificate		
No Certificates defined		
<button>Add Certificate</button>		
Wi-Fi WAN CA Certificate		
No Certificates defined		
<button>Add Certificate</button>		

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

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

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

21.3 Service Forwarding

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

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

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

All checkboxes are currently unchecked.

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.

21.3.1 SMTP Forwarding

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

WAN connection to the WAN's corresponding SMTP server.



SMTP Forwarding Setup

SMTP Forwarding ☒ Enable

Connection	Enable Forwarding?	SMTP Server	SMTP Port
WAN 1	☐		
WAN 2	☐		
Wi-Fi WAN	☐		
Cellular 1	☐		
Cellular 2	☐		
USB	☐		

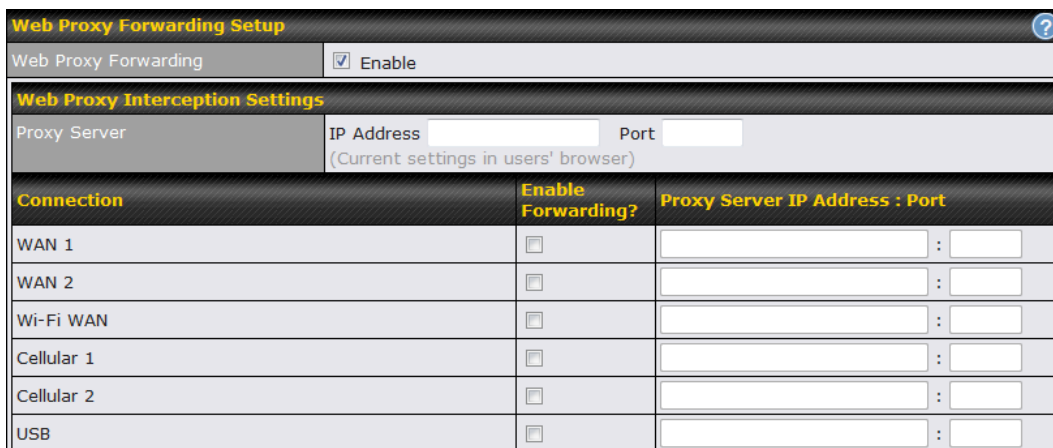
To enable the feature, select **Enable** under **SMTP Forwarding Setup**. Check **Enable Forwarding** for the WAN connection(s) that needs forwarding. Under **SMTP Server**, enter the ISP's e-mail server host name or IP address. Under **SMTP Port**, enter the TCP port number for each WAN.

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

Note

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

21.3.2 Web Proxy Forwarding



Web Proxy Forwarding Setup

Web Proxy Forwarding ☒ Enable

Web Proxy Interception Settings

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

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

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

to the connection's original destination.

21.3.3 DNS Forwarding

DNS Forwarding Setup	
Forward Outgoing DNS Requests to Local DNS Proxy	☒ Enable

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

21.3.4 Custom Service Forwarding

Custom Service Forwarding Setup			
Custom Service Forwarding	☒ Enable		
Settings	TCP Port	Server IP Address	Server Port
			+

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

21.4 Service Passthrough

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

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

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

Service Passthrough Support

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

21.5 UART

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

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

Serial to Network	
Enable	☒
Allowed Source IP Subnets	☒ Any ☐ Allows access from the following IP subnets only
Web Console	☐

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

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

Data Packing	
Packing Length	0 byte(s)
Delimiter	☐
Delimiter process	Do Nothing ▼
Force Transmit	0 ms

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

DB-9 Pepwave MAX Terminal Block

Pin 1 –

Pin 2 Rx (rated -+25V)

Pin 3 Tx (rated -+12V)

Pin 4 –

Pin 5 –

Pin 6 –

Pin 7 RTS

Pin 8 CTS

Pin 9 –

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

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

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

21.6 GPS Forwarding

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

GPS Forwarding				
Enable	☒			
Server	Server IP Address / Host Name	Port	Protocol	Report Interval (s)
			UDP	1 +
GPS Report Format	☒ NMEA ☐ TAIP			
NMEA Sentence Type	☒ GPRMC ☐ GPGGA ☐ GPVTG ☐ GPGSA ☐ GPGSV			
Vehicle ID	?			

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

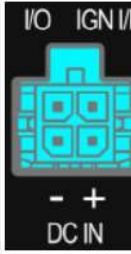
21.7 Ignition Sensing

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

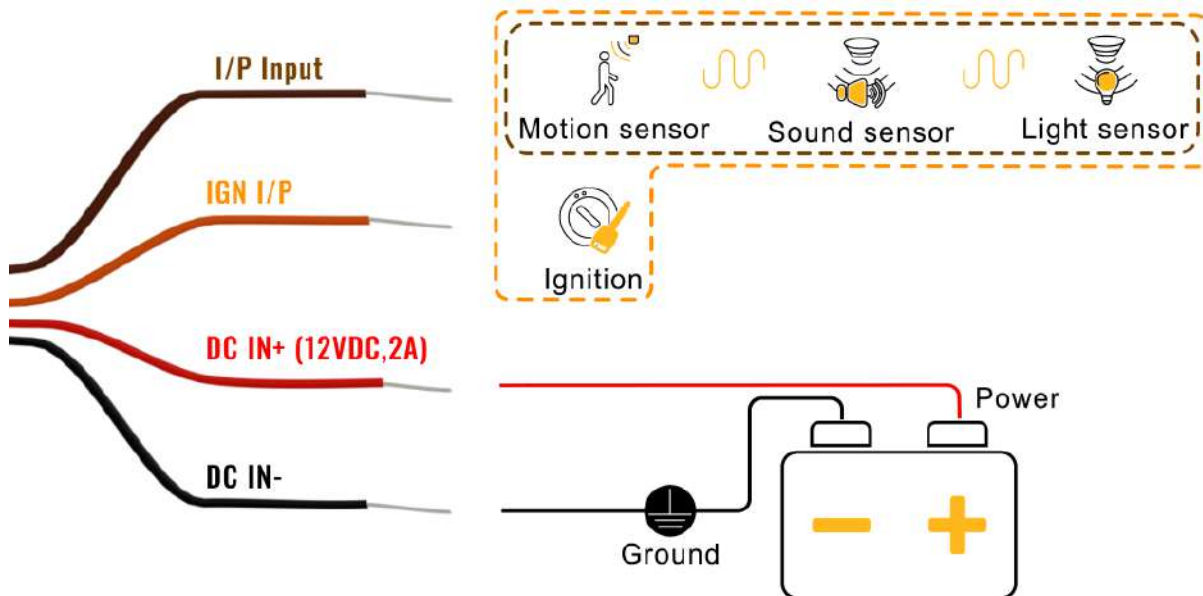
This feature allows the cellular router to start up or shut down when the engine of that vehicle is started or turned off.

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

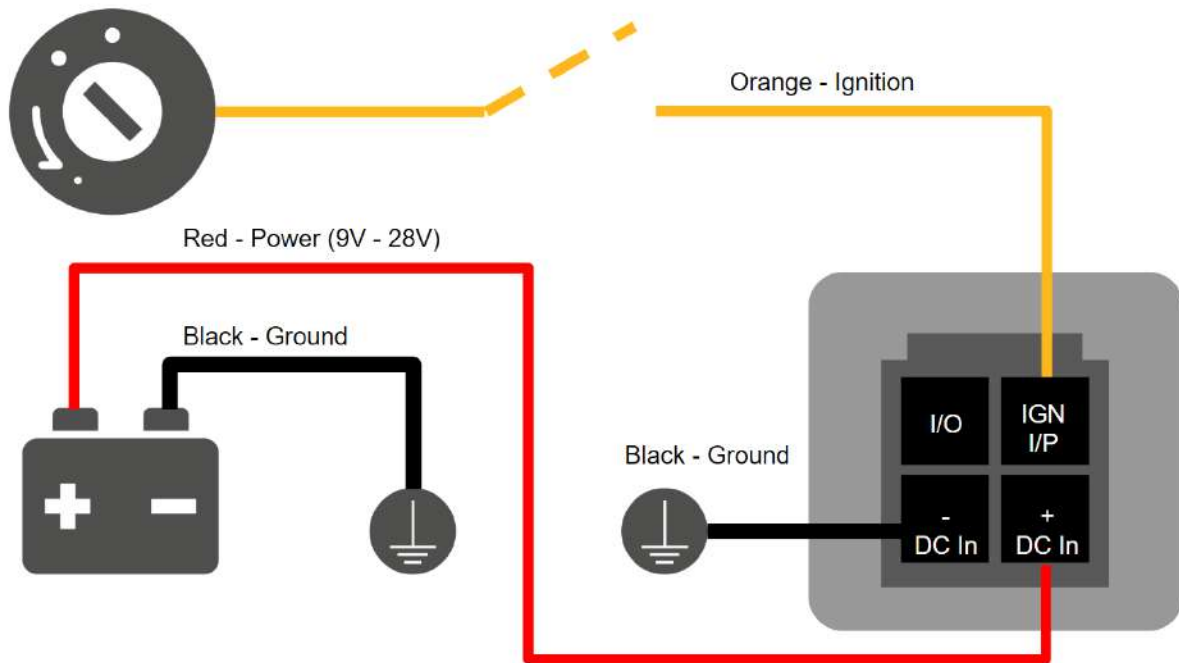
Ignition Sensing installation

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

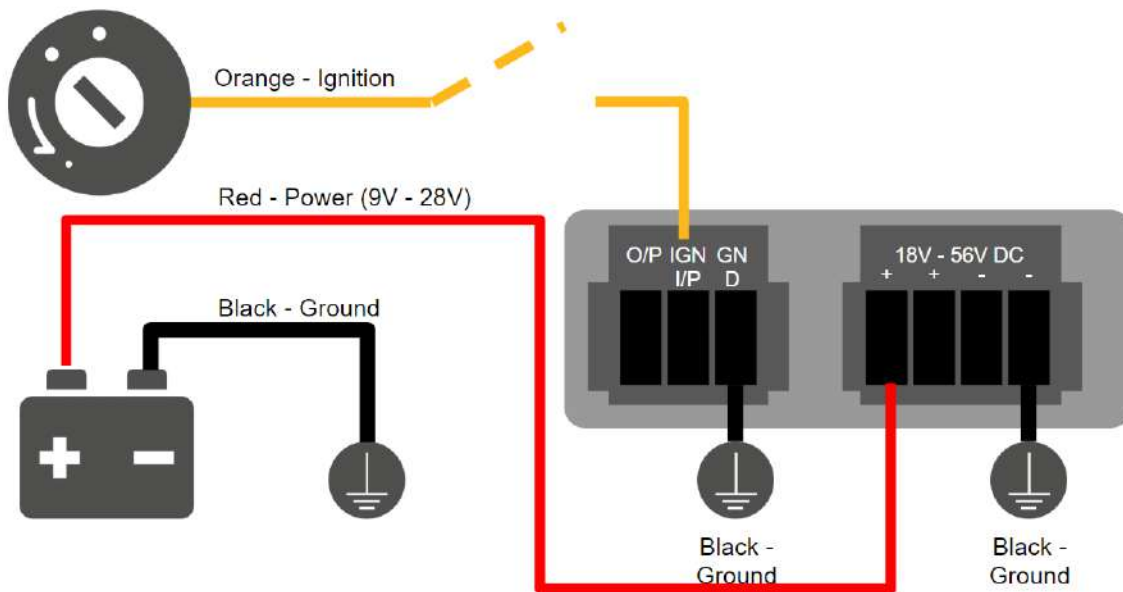
* Currently not functional; will be used for additional features in future firmware



Connectivity diagram for devices with 4-pin connector



Connectivity diagram for devices with terminal block connection



GPIO Menu

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

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

IGN I/P	
Enable	☒
Type	Digital Input ▼
Mode	Ignition Sensing ▼
Delay	seconds

Still under development:

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

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

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

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

O/P	
Enable	☒
Type	Digital Output ▼
Mode	WAN Status ▼

21.8 NTP Server

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

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

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

NTP Server	
Enable	☐
Save	

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

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

21.9 Grouped Networks

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

Grouped Networks		
Name	Networks	
Example	192.168.1.71/28	X
Add Group		

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

Grouped Networks		
Name	Example	
Networks	Network	Subnet Mask
	192.168.1.71	255.255.255.240 (/28) ✖
		255.255.255.255 (/32) +
Save Cancel		

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

21.10 SIM Toolkit

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

USSD

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

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

USSD	
USSD Code	Submit

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

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

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

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

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

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

SMS

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

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

SMS		Refresh
Jun 21, 2017 18:00	Info Hi! Welcome to your new account! You can change this when you first login at www.peplink.com	✖
May 06, 2017 12:23	Info Hi! Your new email is ready to use. Go to your My2 account on your desktop or on a mobile phone click here http://m2.peplink.com/activate	✖
Mar 15, 2017 10:03	From: Steve Hi! There is planned maintenance in the database this week. If your service is affected, you can get updates from http://m2.peplink.com	✖
Mar 06, 2017 14:50	Info Hi! Your new email is ready to use. Go to your My2 account on your desktop or on a mobile phone click here http://m2.peplink.com/activate	✖
Dec 28, 2016 09:53	From: Steve Hi, we hope you're enjoying our 1 month trial offer. As we remind you, this offer applied to your first 100k. Your 100k trial offer will expire by February 1st. Thank you!	✖
Dec 06, 2016 13:09	Info Hi! Your new email is ready to use. Go to your My2 account on your desktop or on a mobile phone click here http://m2.peplink.com/activate	✖
Nov 08, 2016 11:29	From: Steve Hi! There is planned maintenance in the database this week. If your service is affected, you can get updates from http://m2.peplink.com	✖
Sep 07, 2016 17:05	From: Steve Hi! We're sorry to hear that you're having trouble with your account. We'll get it fixed for you as soon as possible. Thank you!	✖

22 AP - access point

23 AP Controller

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

AP Controller	
AP Management	☒ Integrated AP ☒ External AP
Sync. Method	As soon as possible ▼
Permitted AP	☒ Any ☐ Approved List

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

23.1 Wireless SSID

SSID	Security Policy
No SSID Defined	
Add	

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



SSID

SSID Settings

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

Security Settings

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

Access Control Settings

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

Save Cancel

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

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

^A - Advanced feature. Click the  button on the top right-hand corner to activate.

Security Settings	
Security Policy	WPA2 - Personal ▼
Encryption	AES:CCMP
Shared Key	 ☒ Hide Characters

Security Settings	
Security Policy	This setting configures the wireless authentication and encryption methods. Available options : • Open (No Encryption)

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

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

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

NOTE:

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

Access Control Settings	
Restricted Mode	Deny all except listed ▼
MAC Address List	?

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

RADIUS Server Settings	Primary Server	Secondary Server
Host		
Secret	 ☒ Hide Characters	 ☒ Hide Characters
Authentication Port	1812 Default	1812 Default
Accounting Port	1813 Default	1813 Default
NAS-Identifier	Device Name	

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

23.2 Settings

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

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

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

	should follow. • If a North American region is selected, RF channels 1 to 11 will be available and the maximum transmission power will be 26 dBm (400 mW). • If European region is selected, RF channels 1 to 13 will be available. The maximum transmission power will be 20 dBm (100 mW). NOTE: Users are required to choose an option suitable to local laws and regulations. Per FCC regulation, the country selection is not available on all models marketed in the US. All US models are fixed to US channels only.
Preferred Frequency	These buttons determine the frequency at which access points will attempt to broadcast. This feature will only work for APs that can transmit at both 5.4GHz and 5GHz frequencies.
Protocol	This section displays the 2.4 GHz protocols your APs are using.
Channel Width	There are three options: 20 MHz, 20/40 MHz, and 40 MHz. With this feature enabled, the Wi-Fi system can use two channels at once. Using two channels improves the performance of the Wi-Fi connection.
Channel	This drop-down menu selects the 802.11 channel to be utilized. Available options are from 1 to 11 and from 1 to 13 for the North America region and Europe region, respectively. (Channel 14 is only available when the country is selected as Japan with protocol 802.11b.) If Auto is set, the system will perform channel scanning based on the scheduled time set and choose the most suitable channel automatically.
Auto Channel Update	Indicate the time of day at which update automatic channel selection.
Output Power^A	This drop-down menu determines the power at which the AP under this profile will broadcast. When fixed settings are selected, the AP will broadcast at the specified power level, regardless of context. When Dynamic settings are selected, the AP will adjust its power level based on its surrounding APs in order to maximize performance. The Dynamic: Auto setting will set the AP to do this automatically. Otherwise, the Dynamic: Manual setting will set the AP to dynamically adjust only if instructed to do so. If you have set Dynamic:Manual, you can go to AP>Toolbox>Auto Power Adj. to give your AP further instructions. If you click the Boost checkbox, the AP under this profile will transmit using additional power. Please note that using this option with several APs in close proximity will lead to increased interference.
Client Signal Strength Threshold^A	This field determines that maximum signal strength each individual client will receive. The measurement unit is megawatts.
Max number of Clients^A	This field determines the maximum clients that can be connected to APs under this profile.

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

^A - Advanced feature. Click the  button on the top right-hand corner to activate.

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

Web Administration Settings

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

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

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

Wi-Fi Radio Settings	
Operating Country	United States ▼
Wi-Fi Antenna	☐ Internal ☒ External

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

Wi-Fi Radio Settings

Operating Country

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

Wi-Fi Antenna

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

Important Note

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

Wi-Fi AP Settings

Protocol

This option allows you to specify whether 802.11b and/or 802.11g client association requests will be accepted. Available options are **802.11ng** and **802.11na**. By default, **802.11ng** is selected.

Channel

This option allows you to select which 802.11 RF channel will be used. **Channel 1 (2.412 GHz)** is selected by default.

Channel Width

Auto (20/40 MHz) and **20 MHz** are available. The default setting is **Auto (20/40 MHz)**, which allows both widths to be used simultaneously.

Output Power

This option is for specifying the transmission output power for the Wi-Fi AP. There are 4 relative power levels available – **Max**, **High**, **Mid**, and **Low**. The actual output power will be bound by the regulatory limits of the selected country.

Beacon Rate^A

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

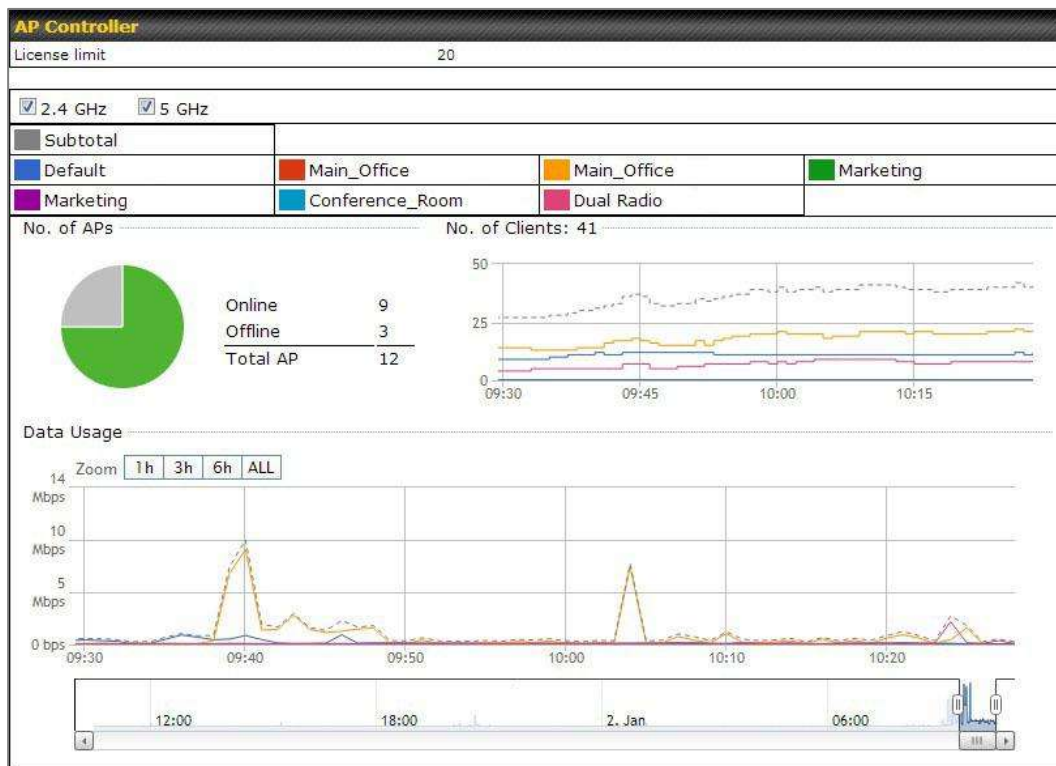
Beacon Interval^A	This option is for setting the time interval between each beacon. By default, 100ms is selected.
DTIM^A	This field allows you to set the frequency for the beacon to include a delivery traffic indication message. The interval is measured in milliseconds. The default value is set to 1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

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

24 AP Controller Status

24.1 Info

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



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

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

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

Events

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

24.2 Access Point (Usage)

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

Search Filter	
AP Name / Serial Number / SSID	All
	☐ Include Offline APs
Search Result	

Managed APs							Expand	Collapse
Name	IP Address	MAC	Location	Firmware Pack ID	Configuration			
▼ Default (8/9 online)								
☐ J200-AMT-1000	10.8.82.11	00:1A:DD:BD:73:E0	-	3.5.2	None	✓	-	

Usage																																																																																					
AP Name/Serial Number	This field enables you to quickly find your device if you know its name or serial number. Fill in the field to begin searching. Partial names and serial numbers are supported.																																																																																				
Online Status	This button toggles whether your search will include offline devices.																																																																																				
Managed Wireless Devices	This table shows the detailed information on each AP, including channel, number of clients, upload traffic, and download traffic. Click the blue arrows at the left of the table to expand and collapse information on each device group. You could also expand and collapse all groups by using the Expand Collapse buttons. On the right of the table, you will see the following icons:   . Click the  icon to see a usage table for each client: <table border="1"> <thead> <tr> <th>MAC Address</th> <th>IP Address</th> <th>Type</th> <th>Signal</th> <th>SSID</th> <th>Upload</th> <th>Download</th> </tr> </thead> <tbody> <tr> <td>90:56:f2:98:75:ff</td> <td>10.9.2.7</td> <td>802.11ng</td> <td>Excellent (37)</td> <td>Balance</td> <td>56.26 MB</td> <td>36.26 MB</td> </tr> <tr> <td>c4:5a:b7:b7:d7:15</td> <td>10.9.2.123</td> <td>802.11ng</td> <td>Excellent (42)</td> <td>Balance</td> <td>5.65 MB</td> <td>2.26 MB</td> </tr> <tr> <td>70:56:81:1d:87:f3</td> <td>10.9.2.102</td> <td>802.11ng</td> <td>Good (23)</td> <td>Balance</td> <td>1.86 MB</td> <td>606.63 KB</td> </tr> <tr> <td>e0:63:e5:83:45:c8</td> <td>10.9.2.101</td> <td>802.11ng</td> <td>Excellent (39)</td> <td>Balance</td> <td>3.42 MB</td> <td>474.52 KB</td> </tr> <tr> <td>18:00:2d:3d:4e:7f</td> <td>10.9.2.66</td> <td>802.11ng</td> <td>Excellent (25)</td> <td>Balance</td> <td>540.29 KB</td> <td>443.57 KB</td> </tr> <tr> <td>14:5a:05:80:4f:40</td> <td>10.9.2.76</td> <td>802.11ng</td> <td>Excellent (29)</td> <td>Balance</td> <td>2.24 KB</td> <td>3.57 KB</td> </tr> <tr> <td>00:1a:dd:c5:4e:24</td> <td>10.8.9.84</td> <td>802.11ng</td> <td>Excellent (26)</td> <td>Wireless</td> <td>9.86 MB</td> <td>9.75 MB</td> </tr> <tr> <td>00:1a:dd:bb:29:ac</td> <td>10.8.9.73</td> <td>802.11ng</td> <td>Excellent (25)</td> <td>Wireless</td> <td>9.36 MB</td> <td>11.14 MB</td> </tr> <tr> <td>40:b0:fa:c3:26:2c</td> <td>10.8.9.18</td> <td>802.11ng</td> <td>Good (23)</td> <td>Wireless</td> <td>118.05 MB</td> <td>7.92 MB</td> </tr> <tr> <td>e4:25:e7:8a:d3:12</td> <td>10.10.11.23</td> <td>802.11ng</td> <td>Excellent (35)</td> <td>Marketing</td> <td>74.78 MB</td> <td>4.58 MB</td> </tr> <tr> <td>04:f7:e4:ef:63:05</td> <td>10.10.11.71</td> <td>802.11ng</td> <td>Poor (12)</td> <td>Marketing</td> <td>84.84 KB</td> <td>119.32 KB</td> </tr> </tbody> </table> Click the  icon to configure each client	MAC Address	IP Address	Type	Signal	SSID	Upload	Download	90:56:f2:98:75:ff	10.9.2.7	802.11ng	Excellent (37)	Balance	56.26 MB	36.26 MB	c4:5a:b7:b7:d7:15	10.9.2.123	802.11ng	Excellent (42)	Balance	5.65 MB	2.26 MB	70:56:81:1d:87:f3	10.9.2.102	802.11ng	Good (23)	Balance	1.86 MB	606.63 KB	e0:63:e5:83:45:c8	10.9.2.101	802.11ng	Excellent (39)	Balance	3.42 MB	474.52 KB	18:00:2d:3d:4e:7f	10.9.2.66	802.11ng	Excellent (25)	Balance	540.29 KB	443.57 KB	14:5a:05:80:4f:40	10.9.2.76	802.11ng	Excellent (29)	Balance	2.24 KB	3.57 KB	00:1a:dd:c5:4e:24	10.8.9.84	802.11ng	Excellent (26)	Wireless	9.86 MB	9.75 MB	00:1a:dd:bb:29:ac	10.8.9.73	802.11ng	Excellent (25)	Wireless	9.36 MB	11.14 MB	40:b0:fa:c3:26:2c	10.8.9.18	802.11ng	Good (23)	Wireless	118.05 MB	7.92 MB	e4:25:e7:8a:d3:12	10.10.11.23	802.11ng	Excellent (35)	Marketing	74.78 MB	4.58 MB	04:f7:e4:ef:63:05	10.10.11.71	802.11ng	Poor (12)	Marketing	84.84 KB	119.32 KB
MAC Address	IP Address	Type	Signal	SSID	Upload	Download																																																																															
90:56:f2:98:75:ff	10.9.2.7	802.11ng	Excellent (37)	Balance	56.26 MB	36.26 MB																																																																															
c4:5a:b7:b7:d7:15	10.9.2.123	802.11ng	Excellent (42)	Balance	5.65 MB	2.26 MB																																																																															
70:56:81:1d:87:f3	10.9.2.102	802.11ng	Good (23)	Balance	1.86 MB	606.63 KB																																																																															
e0:63:e5:83:45:c8	10.9.2.101	802.11ng	Excellent (39)	Balance	3.42 MB	474.52 KB																																																																															
18:00:2d:3d:4e:7f	10.9.2.66	802.11ng	Excellent (25)	Balance	540.29 KB	443.57 KB																																																																															
14:5a:05:80:4f:40	10.9.2.76	802.11ng	Excellent (29)	Balance	2.24 KB	3.57 KB																																																																															
00:1a:dd:c5:4e:24	10.8.9.84	802.11ng	Excellent (26)	Wireless	9.86 MB	9.75 MB																																																																															
00:1a:dd:bb:29:ac	10.8.9.73	802.11ng	Excellent (25)	Wireless	9.36 MB	11.14 MB																																																																															
40:b0:fa:c3:26:2c	10.8.9.18	802.11ng	Good (23)	Wireless	118.05 MB	7.92 MB																																																																															
e4:25:e7:8a:d3:12	10.10.11.23	802.11ng	Excellent (35)	Marketing	74.78 MB	4.58 MB																																																																															
04:f7:e4:ef:63:05	10.10.11.71	802.11ng	Poor (12)	Marketing	84.84 KB	119.32 KB																																																																															

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

Close

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

Click the  icon to see a graph displaying usage:

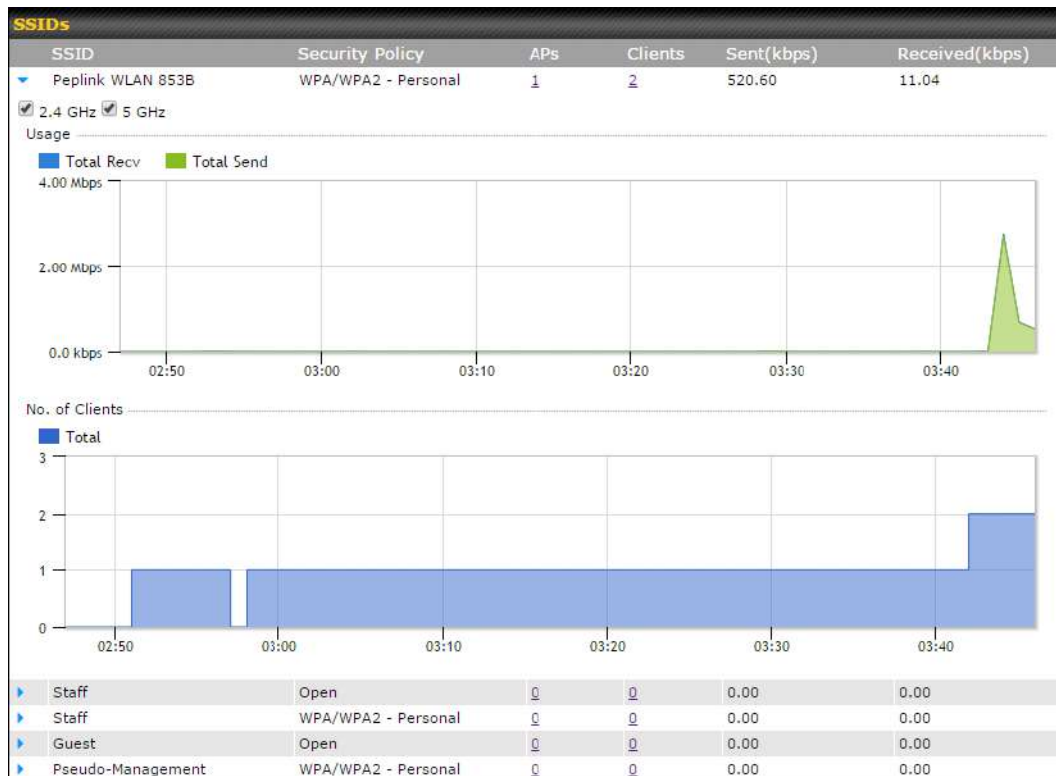


Click any point in the graphs to display detailed usage and client information for that device, using that SSID, at that point in time. On the **Data Usage by** menu, you can display the information by SSID or by AP send/receive rate. Click the **Event** tab next to **Wireless Usage** to view a detailed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

Event Information	
Events	
Jan 2 11:53:39	Client 00:26:8B:08:AC:FD associated with Wireless_11a
Jan 2 11:59:31	Client 60:57:20:24:B6:4C disassociated from Marketing_11a
Jan 2 11:18:55	Client A8:8B:CF:E1:0F:1E disassociated from Balance_11a
Jan 2 11:11:54	Client A8:8B:CF:E1:0F:1E associated with Balance_11a
Jan 2 11:10:45	Client 60:57:20:24:B6:4C associated with Marketing_11a
Jan 2 11:00:36	Client 00:21:6A:35:59:A4 associated with Balance_11a
Jan 2 11:00:20	Client 60:57:20:24:B6:4C disassociated from Marketing_11a
Jan 2 10:59:09	Client 00:21:6A:35:59:A4 disassociated from Balance_11a
Jan 2 10:42:28	Client F4:D7:E2:15:35:E9 associated with Balance_11a
Jan 2 10:29:12	Client 84:7A:86:78:1E:4B associated with Balance_11a
Jan 2 10:24:27	Client 90:89:31:0D:11:EC disassociated from Marketing_11a
Jan 2 10:24:27	Client 90:89:31:0D:11:EC roamed to Marketing_11a at 2830-BFC9-D230
Jan 2 10:13:22	Client E8:9D:28:A8:43:93 associated with Balance_11a
Jan 2 10:13:22	Client E8:9D:28:A8:43:93 roamed to Balance_11a from 2830-BF7F-594C
Jan 2 10:07:52	Client CC:3A:61:89:07:F3 associated with Wireless_11a
Jan 2 10:04:35	Client 60:57:20:24:B6:4C associated with Marketing_11a
Jan 2 10:03:38	Client 60:57:20:24:B6:4C disassociated from Marketing_11a
Jan 2 09:58:27	Client 00:26:8B:08:AC:FD disassociated from Wireless_11a
Jan 2 09:52:46	Client 00:26:8B:08:AC:FD associated with Wireless_11a
Jan 2 09:20:26	Client 8C:13A:E3:3F:17:62 associated with Balance_11a
More...	
Close	

24.3 Wireless SSID

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



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

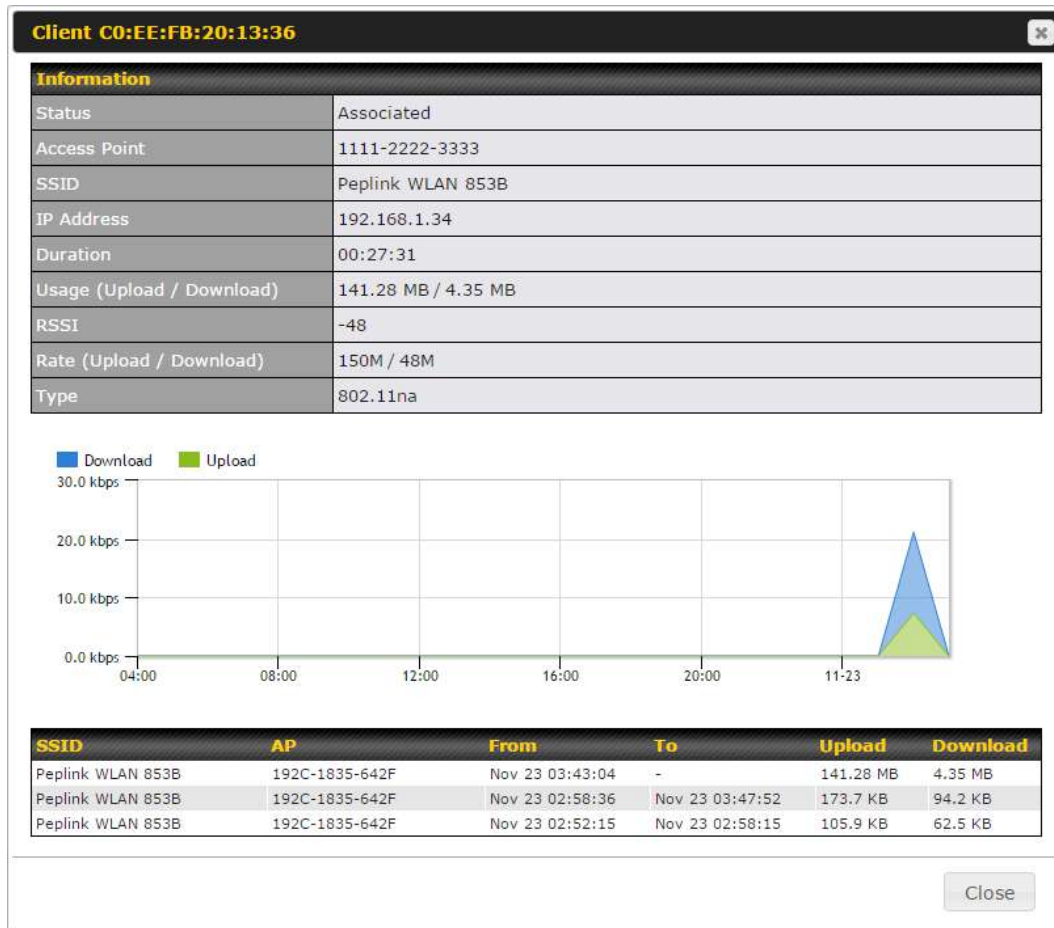
24.4 Wireless Client

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

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

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

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



24.5 Nearby Device

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