



# Pepwave Surf SOHO

## User Manual

**Peplink Products:**  
Surf SOHO

Pepwave Firmware 8.2.1  
December 2022

### COPYRIGHT & TRADEMARKS

Specifications are subject to change without notice.

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

# Table of Contents

<b>Introduction and Scope</b>	<b>6</b>
<b>Glossary</b>	<b>7</b>
<b>Product Features</b>	<b>8</b>
LAN	8
VPN	8
Firewall	9
Outbound Policy	9
QoS	9
Other Supported Features	9
<b>Pepwave Surf SOHO Router Overview</b>	<b>10</b>
Panel Appearance	10
LED Indicators	12
<b>Advanced Feature Summary</b>	<b>13</b>
Drop-in Mode and LAN Bypass: Transparent Deployment	13
QoS: Clearer VoIP	13
USB Modem	14
Built-In Remote User VPN Support	14
DPI Engine	14
Wi-Fi Air Monitoring	15
SP Default Configuration	15
Peplink Relay	15
DNS over HTTPS (DoH)	15
Peplink InTouch	15
<b>Installation</b>	<b>16</b>
Preparation	16
Constructing the Network	16
<b>Connecting to the Web Admin Interface</b>	<b>16</b>
<b>SpeedFusion Connect</b>	<b>19</b>
Activate SpeedFusion Connect Service	19
Enable SpeedFusion Connect	19
Connect Clients to Cloud	26
Link Wi-Fi to Cloud	27
Optimize Cloud Application	29
<b>Configuring the LAN Interface(s)</b>	<b>31</b>

Network Settings	31
Port Settings	38
<b>Configuring the WAN interface</b>	<b>39</b>
WAN > WAN Quality Monitoring	40
WAN > Ethernet WAN	41
WAN > Physical Interface Settings	42
WAN > Health Check Settings	43
WAN > Bandwidth Allowance Monitor	44
WAN > Additional IP Address Settings	45
WAN > Dynamic DNS Settings	45
Wi-Fi WAN and USB WiFi Network connection	46
WAN > WiFi Connection Profiles	48
WAN > Signal threshold settings	50
<b>PepVPN</b>	<b>52</b>
PepVPN > Send ALL traffic	57
Outbound Policy Management	59
<b>Port Forwarding</b>	<b>62</b>
UPnP / NAT-PMP Settings	64
<b>NAT Mappings</b>	<b>65</b>
<b>QoS</b>	<b>67</b>
User Group	67
Bandwidth Control	67
Application Prioritization	68
<b>Firewall</b>	<b>71</b>
Outbound and Inbound Firewall Rules	72
Intrusion Detection and DoS Prevention	75
Content Blocking	76
<b>Routing Protocols</b>	<b>77</b>
OSPF & RIPv2	77
BGP	80
<b>Remote User Access</b>	<b>84</b>
L2TP with IPsec	84
OpenVPN	85
PPTP	85
Authentication Methods	86
<b>Miscellaneous Settings</b>	<b>88</b>
RADIUS Server	88

Certificate Manager	90
Service Forwarding	90
Service Passthrough	93
Grouped Networks	94
SIM Toolkit	95
<b>AP</b>	<b>99</b>
Wireless SSID	99
Settings	105
<b>AP &gt; Status</b>	<b>108</b>
Access Point	108
Wireless SSID	111
Wireless Client	112
Mesh / WDS	114
Nearby Device	115
Event Log	116
<b>System Settings</b>	<b>117</b>
Admin Security	117
Firmware	120
Time	121
Schedule	122
Email Notification	123
Event Log	127
SNMP	128
InControl	130
Configuration	131
Feature Add-ons	132
Reboot	132
<b>Tools</b>	<b>133</b>
Ping	133
Traceroute Test	134
Wake-on-LAN	134
WAN Analysis	135
<b>Status</b>	<b>138</b>
Device	139
Active Sessions	141
Client List	143
OSPF & RIPv2a	144
BGP	144

PepVPN Status	144
Event Log	147
WAN Quality	148
Usage Reports	149
<b>Appendix A: Restoration of Factory Defaults</b>	<b>153</b>
<b>Appendix B: Overview of ports used by Peplink SD-WAN routers and other Peplink services</b>	<b>154</b>
<b>Appendix C: Declaration</b>	<b>156</b>

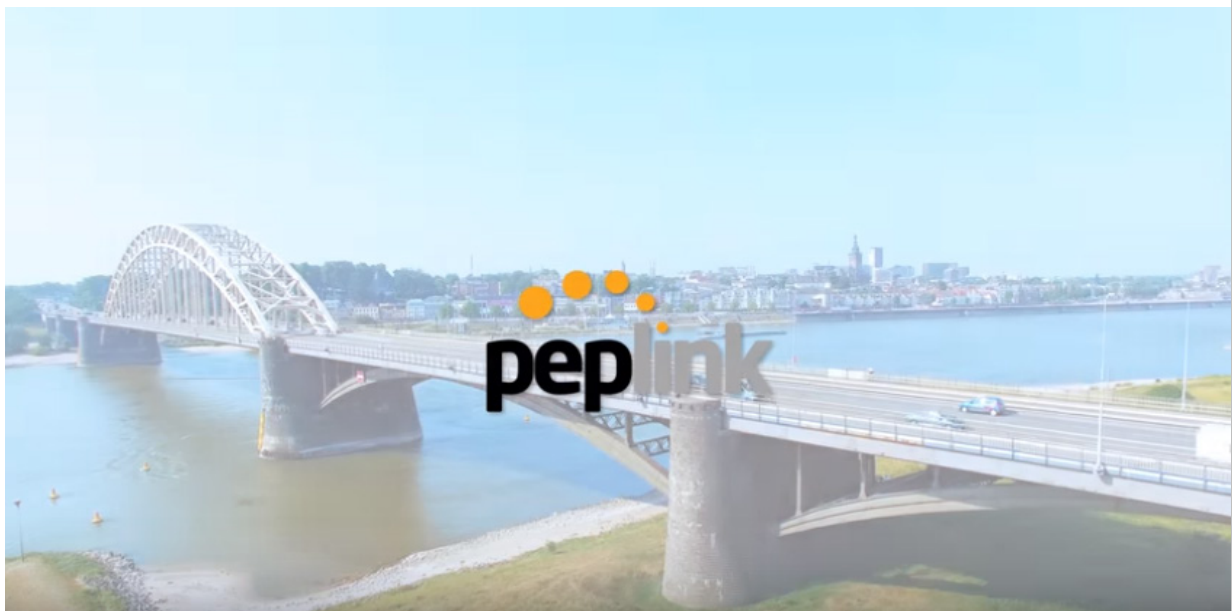
## Introduction and Scope

The Surf SOHO is a professional-grade router that is secure, reliable, and easy to use.

With the Surf SOHO, you can connect to the Internet using a USB cellular modem, Ethernet, or Wi-Fi. Hook the Surf SOHO up to Ethernet and Cellular connections, and it will automatically fail over from one to the other as needed. That way, you can stay connected even when a connection breaks.

This manual covers setting up a Surf SOHO router 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](#).

## 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

## Product Features

PepwaveSurf SOHO routers enable all LAN users to share broadband Internet connections, and they provide advanced features to enhance Internet access. Our Surf SOHO routers support one Ethernet, one USB 4G LTE/3G WAN, and Wi-Fi as WAN for failover

It also includes three SMA dual-band antennas that allows better reliability, larger bandwidth, and increased wireless coverage.

Below is a list of supported features on Pepwave routers. Features vary by model.

For more information, please visit [our website](#).

### WAN

- Ethernet WAN connection in full/half duplex
- Static IP support for PPPoE
- 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 pass through
- Intelligent Failover
- MAC address clone and passthrough
- Customizable MTU and MSS values
- WAN connection health check
- Dynamic DNS
- Ping, DNS lookup, and HTTP-based health check

### LAN

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

### VPN

- Site-to-Site VPN
- 256-bit AES Encryption
- Dynamic Routing
- Pre-shared key authentication
- PPTP/L2TP/Open VPN - VPN server



## 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

## 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

## 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

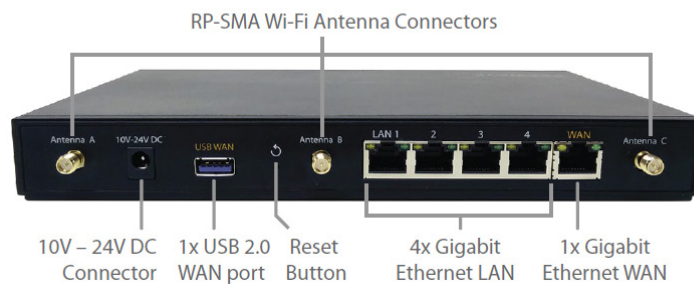
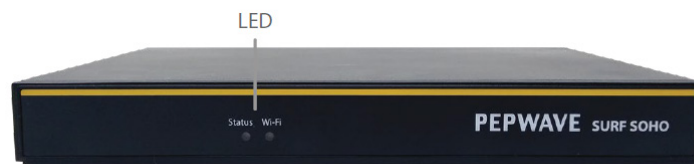
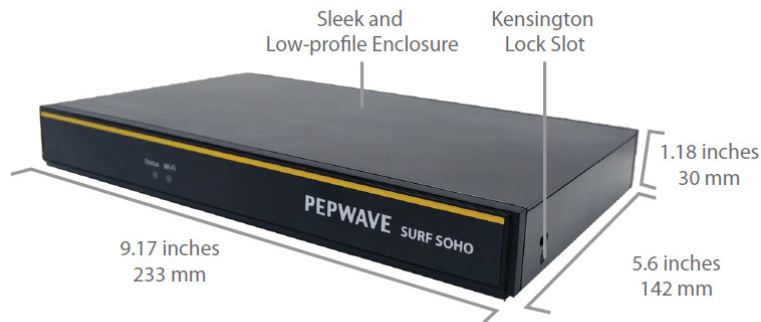
## Other Supported Features

- User-friendly web-based administration interface
- HTTP and HTTPS support for web admin interface
- 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
- Syslog
- SIP passthrough
- PPTP packet pass through
- Event log
- Active sessions

- Client list
- UPnP / NAT-PMP
- Real-time, hourly, daily, and monthly bandwidth usage reports and charts

## Pepwave Surf SOHO Router Overview

### Panel Appearance



Specifications	
<b>WAN Interface</b>	1x 100/1000M Ethernet Port 1x USB 2.0 Interface Wi-Fi as WAN
<b>LAN Interface</b>	4x 100/1000M Ethernet Ports Simultaneous Dual-Band 11ac Wi-Fi AP
<b>Wi-Fi AP Operating Frequency</b>	2412 – 2472 MHz and 5180 - 5825 MHz
<b>Wi-Fi Antenna</b>	3x External Wi-Fi Antenna
<b>Recommended Users</b>	1-25
<b>Router Throughput</b>	120Mbps
<b>Number of PPTP VPN Users</b>	3
<b>Number of PPTP VPN Users</b>	2
<b>Power Input</b>	DC Jack: 10V – 24VDC AC Adapter: AC Input 100V – 240V, DC Output 12V, 1.5A
<b>Power Consumption</b>	26W (max) with USB WAN 22W (max) without USB WAN
<b>Dimensions</b>	9.17 x 5.6 x 1.18 inch 233 x 142 x 30 mm
<b>Weight</b>	0.86 pounds 388 grams
<b>Operating Temperature</b>	-14° to 113°F -10° to 45°C
<b>Humidity</b>	15% – 95% (non-condensing)
<b>Certifications</b>	FCC, CE, RoHS
<b>Warranty</b>	1-Year Limited Warranty

## LED Indicators

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

Wi-Fi and Status Indicators		
<b>Wi-Fi</b>	OFF	Disabled Intermittent
	Blinking	Enabled but no client connected
	ON	Client(s) connected to wireless network
	Continuous blinking	Transferring data to wireless network
<b>Status</b>	OFF	System initializing
	Red	Booting up or busy
	Green	Ready state

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

Wi-Fi Signal	
Off	No connection
<b>Signal strength</b>	Wi-Fi signal strength (low, medium, and high)

## Advanced Feature Summary

### 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.

### 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.

## USB Modem



For increased WAN diversity, plug in a USB LTE modem as a backup. Peplink routers are compatible with over [250 modem types](#).

## 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](#)

## DPI Engine

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

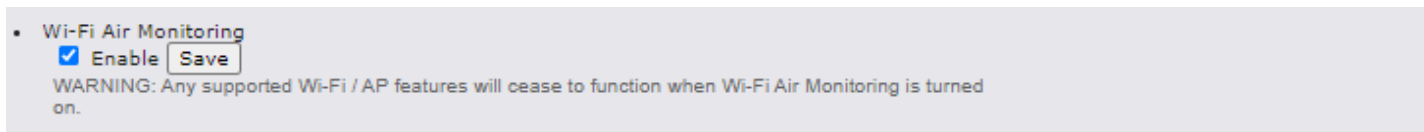
sscs

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

## Wi-Fi Air Monitoring

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

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



## SP Default Configuration

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

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

## Peplink Relay

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

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

## DNS over HTTPS (DoH)

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

## Peplink InTouch

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

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

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

## Installation

The following section details connecting Pepwave routers to your network.

### 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:** An ethernet cable with RJ45 connector
- **USB:** A USB modem
- **Wi-Fi WAN:** Wi-Fi antennasA computer with the TCP/IP network protocol and a web browser installed. 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.

### Constructing the Network

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/, connect to one of the WAN ports on the Pepwave router. Repeat the same procedure for other WAN ports.

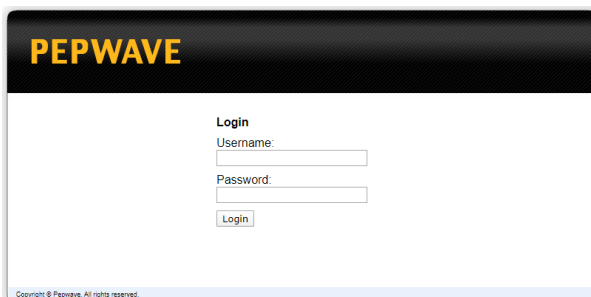
Connect the power adapter to the power connector on the rear panel of the Pepwave router, and then plug it into a power outlet.

## Connecting to the Web Admin Interface

Start a web browser on a computer that is connected with the Pepwave Surf SOHO through the LAN.

To connect to the web admin of the Pepwave Surf SOHO, enter the following LAN IP address in the address field of the web browser: **https://192.168.50.1**

(This is the default LAN IP address of the Pepwave Surf SOHO.) Enter the following to access the web admin interface.



**Username:** admin

**Password:** admin

(This is the default admin user login of the Pepwave



Surf SOHO.)

You must change the default password on the first successful logon.

Password requirements are: A minimum of 10 lower AND upper case characters, including at least 1 number.

When HTTP is selected, the URL will be redirected to HTTPS by default.

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

You must change your default password now to proceed

**Change Password**

Current Password	<input type="password"/>
New Password	<input type="password"/>
Require at least 10 characters, lower and upper case, with numbers.	
Confirm New Password	<input type="password"/>

Save and apply

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

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

**WAN Connection Status**

Priority 1 (Highest)

Wi-Fi WAN on 2.4 ...	Connected to <input type="text"/>	Wireless Networks Details
Wi-Fi WAN on 5 GHz	Connected to <input type="text"/>	Wireless Networks Details

Priority 2

Drag desired (Priority 2) connections here

Disabled

WAN	<input type="checkbox"/> Disabled	Details
OpenVPN WAN 1	<input type="checkbox"/> Disabled	Details

**LAN Interface**

Router IP Address: 192.168.50.1

**Wi-Fi AP** OFF Details

Wi-Fi AP has been disabled

(No Wi-Fi AP)

**Device Information**

Model:	Pepwave Surf SOHO MK3
Firmware:	8.2.0b01 build 5054
Uptime:	0 days 1 hour 51 minutes
CPU Load:	31%
Throughput:	↓ 52.0 kbps ↑ 67.0 kbps

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.

**Device Information** displays details about the device, including model name, firmware version, CPU Load, throughput and uptime.

#### 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.

## SpeedFusion Connect

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

### Activate SpeedFusion Connect Service

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

### Enable SpeedFusion Connect

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

here to hide SpeedFusion Connect menu, you can restore it later on Status page.'" data-bbox="117 131 915 575"/&gt;

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



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

## SpeedFusion Connect > Setup Relay Mode

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

SpeedFusion Connect	Cloud Location
SFH-SHARE-SIN	Relay Sharing Code: <input type="text"/> COPY <input type="button" value="X"/>

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

## SpeedFusion Connect > Choose Cloud Location

You can connect up to 3 different cloud locations.

SpeedFusion Connect	Cloud Location
	<div style="border: 1px solid gray; padding: 5px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span>---</span> <span>▼</span> </div> <div style="background-color: #e0e0e0; padding: 2px;">---</div> <div style="padding: 2px;"> <p>[Automatic]</p> <p>[Home Sharing]</p> <p><b>Suggested Built-in Cloud Location</b></p> <p>Singapore (SIN) / 38ms</p> <p>India, Bangalore (BLR) / 53ms</p> <p>Australia, Sydney (SYD) / 103ms</p> <p><b>Built-in Cloud Location</b></p> <p>Australia, Sydney (SYD)</p> <p>Brazil, Sao Paulo (SAO)</p> <p>Canada, Toronto (YTO)</p> <p>Finland, Helsinki (HEL)</p> <p>France, Paris (PAR)</p> <p>Germany, Frankfurt (FRA)</p> <p>Hong Kong (HKG)</p> <p>India, Bangalore (BLR)</p> <p>Israel, Tel Aviv (TLV)</p> <p>Japan, Tokyo (TYO)</p> <p>Netherlands, Amsterdam (AMS)</p> <p>New Zealand, Invercargill (IVC)</p> </div> </div>

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

**SpeedFusion Connect > Choose Cloud Location**

You can connect up to 3 different cloud locations.

SpeedFusion Connect	Cloud Location	
	---	<input checked="" type="checkbox"/>

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

**SpeedFusion Connect > Choose Cloud Location**

You can connect up to 3 different cloud locations.

SpeedFusion Connect	Cloud Location	
	[Home Sharing]	<input checked="" type="checkbox"/>
	e.g. 1234-5678-1234-5678	

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

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

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

SpeedFusion Connect > Choose Cloud Location

SpeedFusion Connect	Cloud Location	
SFC	[Automatic]	<input type="checkbox"/>
	---	<input checked="" type="checkbox"/>

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

Changes applied successfully.

SpeedFusion Connect > Choose Cloud Location

SpeedFusion Connect	Cloud Location	
SFC	[Automatic]	<input type="checkbox"/>
	---	<input checked="" type="checkbox"/>

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

The screenshot shows the PEPWAVE dashboard with the following sections:

- WAN Connection Status:**
  - Priority 1 (Highest):
    - WAN: No Cable Detected
    - Wi-Fi WAN: Connected to [Network Name]
  - Priority 2: Drag desired (Priority 2) connections here
  - Disabled: Cellular (Disabled)
- LAN Interface:** Router IP Address: 192.168.50.1
- Wi-Fi AP:** OFF
- SpeedFusion Connect:** SFC Established. Data usage allowance: 200.00 GB (Expiry date: [Date]).

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

The screenshot shows the SFC configuration page with the following settings:

- SpeedFusion Connect Profile:**
  - Enable:
  - Cloud Location: [Automatic]
- Tunnel Options:**
  - Local / Remote Tunnel ID: 1 (default tunnel)
  - Tunnel Name: Default
  - Data Port:  Auto  Custom
  - Bandwidth Limit:
  - WAN Smoothing:
    - Overall Redundancy Level: Off
    - Maximum Level on the Same Link: Off
  - Forward Error Correction: Off
  - Receive Buffer: 0 ms
  - Packet Fragmentation:  Always  Use DF Flag



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 +

**Tunnel Options**

Local / Remote Tunnel ID 1 (default tunnel)

Tunnel Name Default

Data Port  Auto  Custom

Bandwidth Limit

WAN Smoothing

Overall Redundancy Level Off

Maximum Level on the Same Link Off

Forward Error Correction Off

Receive Buffer 0 ms

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

**SFC**

**SpeedFusion Connect Profile**

Enable

Cloud Location [Automatic]

1 - Default 2 - WAN Smoo... x +

**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

Packet Fragmentation  Always  Use DF Flag

Logout

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

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.

Service	Algorithm	Source	Destination	Protocol / Port
to-Internet	Priority VPN: SFC (1 - Def...	IP Address 192.168.50.11	Any	Any
Default	(Auto)			

## Connect Clients to Cloud

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

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

Automatic			
SFC	Client	IP Address	
	LAPTOP-TIRBRFPU ( )	192.168.50.20	+

## Link Wi-Fi to Cloud

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

## SpeedFusion Connect

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



### Setup Relay Mode

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



### Choose Cloud Location

Which cloud you'd like to connect?

### Traffic Steering Priority



### Connect Clients to Cloud

Select a cloud for your laptops, phones, or other devices.




### Link Wi-Fi to Cloud

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

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

## SpeedFusion Connect > Link Wi-Fi to Cloud

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

Automatic			
SFC	Reference SSID	SSID for Cloud	
	test	test-SSID-SFC	

Save

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

**LAN Interface**

Router IP Address: 192.168.50.1

**Wi-Fi AP** ■ ON ▾ Details

test	test-SSID-SFC	
------	---------------	--

## Optimize Cloud Application

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

### SpeedFusion Connect

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

**Setup Relay Mode**  
Allow remote peers to access local networks, and the internet via this device.

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



---


**Traffic Steering Priority**

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

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

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

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



## SpeedFusion Connect > Optimize Cloud Application

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

Automatic	
SFC	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="background-color: #e6f2ff; padding: 2px;">Cloud Application</div> <div style="border-bottom: 1px solid #ccc; padding: 2px;">---</div> <div style="background-color: #007bff; color: #fff; padding: 2px;">---</div> <div style="padding: 2px;">Google Workspace</div> <div style="padding: 2px;">Microsoft Office 365</div> <div style="padding: 2px;">Zoom</div> <div style="padding: 2px;">Lifesize</div> <div style="padding: 2px;">Salesforce</div> </div> <div style="float: right; text-align: center; border-left: 1px solid #ccc; border-right: 1px solid #ccc; padding: 2px 5px;">+</div>

# Configuring the LAN Interface(s)

## Network Settings

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

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

[New LAN](#)

This represents the LAN interfaces that are active on your router (including VLAN). A gray “X” means that the VLAN is used in other settings and cannot be deleted.

You can find which settings are using the VLAN by hovering over the gray “X”.

Alternatively, a red “X” means that there are no settings using the VLAN.

You can delete that VLAN by clicking the red “X”

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

**IP Settings**

IP Address  ▼

**IP Settings**

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

**Network Settings** ?

Name	<input type="text"/>	<b>Help</b>	<a href="#">Close</a>
VLAN ID	<input type="text"/>	To define a layer-2 bridging based PepVPN, please click <a href="#">here</a> .	
Inter-VLAN routing	<input checked="" type="checkbox"/>		

**Network Settings**

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

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



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



DHCP Server									
DHCP Server <span>?</span>	<input checked="" type="checkbox"/> Enable								
DHCP Server Logging	<input type="checkbox"/>								
IP Range	<input type="text" value="255.255.255.0"/> (/24)								
Lease Time	<input type="text" value="0"/> Mins								
DNS Servers	<input checked="" type="checkbox"/> Assign DNS server automatically								
BOOTP	<input type="checkbox"/>								
Extended DHCP Option	<table border="1"> <thead> <tr> <th>Option</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center;">No Extended DHCP Option</td> </tr> <tr> <td colspan="2" style="text-align: center;"><b>Add</b></td> </tr> </tbody> </table>	Option	Value	No Extended DHCP Option		<b>Add</b>			
Option	Value								
No Extended DHCP Option									
<b>Add</b>									
DHCP Reservation <span>?</span>	<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		+						

**Help** Close

Check the *Enable* box to enable the built-in DHCP server which serves DHCP requests on the LAN.  
If you want to enable DHCP relay server, click [here](#).



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

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

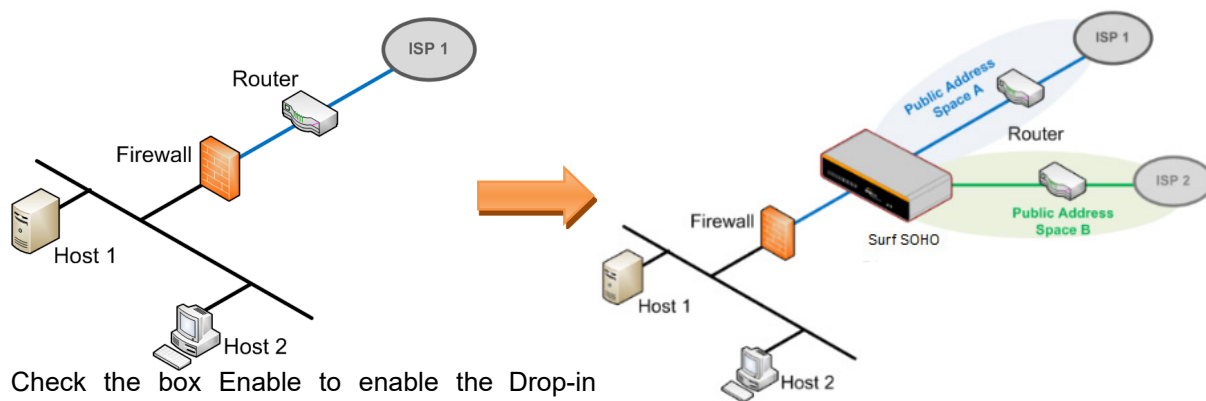
DHCP Relay Settings	
<b>DHCP Relay</b>	Enter the address of the DHCP server here. DHCP requests will be relayed to it.

<b>DHCP Server IP Address</b>	DHCP requests from the LAN are relayed to the entered DHCP server. For active-passive DHCP server configurations, enter active and passive DHCP server IPs into the <b>DHCP Server 1</b> and <b>DHCP Server 2</b> fields.
<b>DHCP Option 82</b>	This feature includes device information as relay agent for the attached client when forwarding DHCP requests from a DHCP client to a DHCP server. Device MAC address and network name are embedded to circuit ID and Remote ID in option 82.
<b>DHCP Relay Logging</b>	Check this box to log DHCP relay activity.

## Drop-In Mode

Drop-in mode (or transparent bridging mode) eases the installation of the Surf SOHO 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 **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 Surf SOHO as part of the network using drop-in mode, it will, depending on model, support one or more WAN connections. Some SOHO 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 <span style="float: right;">?</span>	
Enable	<input checked="" type="checkbox"/>
WAN for Drop-In Mode <span>?</span>	WAN <span>▼</span> <input checked="" type="checkbox"/> Apply NAT on VLAN networks outgoing Internet traffic VLAN network(s) may route their outgoing Internet traffic to this unit. When this checkbox is checked their traffic will be NAT'd before forwarding out of this WAN. Leave this checkbox checked if you are not sure.
Share Drop-In IP <span>?</span>	<input checked="" type="checkbox"/>
Shared IP Address <span>?</span>	<input type="text"/> 255.255.255.0 (/24) <span>▼</span>
Static Route	Destination Network
	Subnet Mask
	<input type="text"/> 255.255.255.0 (/24) <span>▼</span> <span>+</span>
WAN Default Gateway <span>?</span>	<input type="text"/> <input checked="" type="checkbox"/> I have other host(s) on WAN segment IP Address <input type="text"/> - <input type="text"/> <div style="text-align: center;">↓</div> <input type="text"/> <span>✕</span>
WAN DNS Servers <span>?</span>	DNS server 1: <input type="text"/> DNS server 2: <input type="text"/>
<p>NOTE: The DHCP Server Settings will be overwritten.</p> <p>The following WAN settings will be overwritten: Connection Method, MTU, Health Check, Additional Public IP, and Dynamic DNS Settings.</p> <p>The PPTP Server will be disabled.</p> <p>Tip: please review the DNS Forwarding setting under the Service Forwarding section.</p>	



Drop-in Mode Settings	
<b>Enable</b>	Drop-in mode eases the installation of the Surf SOHO on a live network between the existing firewall and router, such that no configuration changes are required on existing equipment. Check the box to enable the drop-in mode feature.
<b>WAN for Drop-In Mode</b>	Select the WAN port to be used for drop-in mode. If <b>WAN</b> is selected, the high availability feature will be disabled automatically.
<b>Shared Drop-In IP<sup>A</sup></b>	<p>When this option is enabled, the passthrough IP address will be used to connect to WAN hosts (email notification, remote syslog, etc.). The SOHO will listen for this IP address when WAN hosts access services provided by the SOHO (web admin access from the WAN, DNS server requests, etc.).</p> <p>To connect to hosts on the LAN (email notification, remote syslog, etc.), the default gateway address will be used. The SOHO will listen for this IP address when LAN hosts access services provided by the SOHO(web admin access from the WAN, DNS proxy, etc.).</p>
<b>Shared IP Address<sup>A</sup></b>	Access to this IP address will be passed through to the LAN port if this device is not serving the service being accessed. The shared IP address will be used in connecting to hosts on the WAN (e.g., email notification, remote syslog, etc.) The device will also listen on the IP address when hosts on the WAN access services served on this device (e.g., web admin accesses from WAN, DNS server, etc.)

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








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

### 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.

Entries in this list will allow traffic to route to a different subnet that is connected to the LAN interface. Any traffic destined for a network/mask pair will be directed to the corresponding gateway instead of routed through WANs.

Virtual Network Mapping <span style="float: right;"></span>			
One-to-One NAT <span style="float: right;"></span>		Local Network	Virtual Network <span style="float: right;"></span>
Many-to-One NAT <span style="float: right;"></span>		Local Network	Virtual IP Address <span style="float: right;"></span>

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

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

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


### Virtual Network Mapping

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

DNS Proxy Settings <span style="float: right;">?</span>		
Enable	<input checked="" type="checkbox"/>	
DNS Caching <span>?</span>	<input type="checkbox"/>	
Include Google Public DNS Servers <span>?</span>	<input type="checkbox"/>	
Local DNS Records <span>?</span>	Host Name	IP Address <span>+</span>
Domain Lookup Policy <span>?</span>	Domain	Connection <span>+</span>
DNS Resolvers <span>?</span>	WAN Connection	DNS Servers
	<input type="checkbox"/> WAN 1	1.1.1.1 1.0.0.1
	<input type="checkbox"/> WAN 2	
	<input type="checkbox"/> WAN 3	
	<input type="checkbox"/> WAN 4	8.8.8.8 8.8.4.4
	<input type="checkbox"/> WAN 5	
	<input type="checkbox"/> Mobile Internet	
	LAN Connection	DNS Servers
<input type="checkbox"/> Untagged LAN		
Preferred connections are shown with <input checked="" type="checkbox"/>		

DNS Proxy Settings	
<b>Enable</b>	<p>To enable the DNS proxy feature, check this box, and then set up the feature at <b>Network&gt;LAN&gt;DNS Proxy Settings</b>.</p> <p>A DNS proxy server can be enabled to serve DNS requests originating from LAN/PPTP/SpeedFusion™ peers. Requests are forwarded to the <b>DNS servers/resolvers</b> defined for each WAN connection.</p>
<b>DNS Caching</b>	<p>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 improve DNS response time by storing all received DNS results for faster DNS lookup. However, it cannot return the most updated result for frequently updated DNS records. By default, <b>DNS Caching</b> is disabled.</p>
<b>Include Google Public DNS Servers</b>	<p>When this option is enabled, the DNS proxy server will 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.</p>
<b>Local DNS Records</b>	<p>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 Surf SOHO, the corresponding IP address will be returned. To display the option to set TTL manually, click <span>?</span>.</p> <p>Click <span>+</span> to create a new record. Click <span>×</span> to remove a record.</p>

<b>Domain Lookup Policy</b>	DNS proxy will look up the domain names defined here using only the specified connections.
<b>DNS Resolvers<sup>A</sup></b>	<p>Check the box to enable the WINS server. A list of WINS clients will be displayed at <b>Network&gt;LAN&gt;DNS Proxy Settings&gt;DNS Resolvers</b>.</p> <p>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.</p> <p>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.</p>

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

## Port Settings

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

Port Settings				
	Name	Enable	Speed	Advertise Speed
1	LAN Port 1	<input checked="" type="checkbox"/>		
2	LAN Port 2	<input checked="" type="checkbox"/>		
3	LAN Port 3	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
4	LAN Port 4	<input checked="" type="checkbox"/>		

On this screen, you can enable specific ports, name the LAN ports, as well as determine the speed of the LAN ports.

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

## Configuring the WAN interface

WAN Interface settings are located at **Network>WAN**.

The router supports wan connections supplied by a USB 2.0 Interface USB cellular modem, Ethernet, or Wi-Fi.

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

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

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

### DNS over HTTPS (DoH)

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

**DNS over HTTPS** ✕

Enable	?	<input checked="" type="checkbox"/>	
Server			<div style="border: 1px solid gray; padding: 2px;"> <span style="background-color: #f0f0f0; padding: 2px;">Cloudflare</span> ▾           <ul style="list-style-type: none"> <li style="background-color: #e0e0e0; padding: 2px;">Cloudflare</li> <li style="padding: 2px;">Quad9</li> <li style="padding: 2px;">Google DNS</li> <li style="padding: 2px;">OpenDNS</li> <li style="padding: 2px;">Custom URL:</li> </ul> </div>

DNS over HTTPS	
<b>Enable</b>	When this option is enabled, the DNS proxy server will use HTTPS connections to forward DNS requests to the DoH resolver; it will not fallback to traditional UDP DNS options.
<b>Server</b>	<p>The options to configure DoH with a predefined server are:</p> <ul style="list-style-type: none"> <li>Cloudflare - The DNS server IP addresses for <b>Cloudflare</b> will be using 1.1.1.1, which is unfiltered.</li> <li>Quad9 - The DNS server IP addresses for <b>Quad9</b> will be using 9.9.9.9 and 142.112.112.112, which is malware blocking and DNSSEC.</li> <li>Google DNS - The DNS server IP addresses for <b>Google DNS</b> will be using 8.8.8.8 and 8.8.4.4, which is RFC8484 standard.</li> <li>OpenDNS - The DNS server IP addresses for <b>OpenDNS</b> will be using 208.67.222.222 and 208.67.220.220, which is standard DNS.</li> <li>Custom URL - You may select <b>Custom URL:</b>, and enter the <b>resolver URL</b> and <b>IP address</b>.</li> </ul>

## WAN > WAN Quality Monitoring

This setting advice how WAN Quality information is being gathered.

By default, WAN Quality information will always be collected automatically for all WAN connections.

With a customized choice of WAN connections, the router will only collect the WAN Quality information of those selected WAN connections.

### Important Note

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




## WAN > Ethernet WAN

WAN connection details need to be configured to connect the router to the internet or another WAN

To start configuring the WAN connection choose **Network>WAN** from the menu and choose a WAN connection and then click **Details**.

WAN Connection Settings	
WAN Connection Name	<input type="text"/> <span>Default</span>
Connection Method <span>?</span>	DHCP ▾
Routing Mode <span>?</span>	<input checked="" type="radio"/> NAT
Hostname (Optional)	<input type="text"/> <input type="checkbox"/> Use custom hostname
DNS Servers	<input checked="" type="checkbox"/> Obtain DNS server address automatically <input type="checkbox"/> Use the following DNS server address(es) DNS Server 1: <input type="text"/> DNS Server 2: <input type="text"/>
IP Passthrough <span>?</span>	<input type="checkbox"/>
Independent from Backup WANs <span>?</span>	<input type="checkbox"/>
Standby State <span>?</span>	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnect
Reply to ICMP Ping <span>?</span>	<input checked="" type="radio"/> Yes <input type="radio"/> No
Upload Bandwidth <span>?</span>	10 <input type="text"/> Mbps ▾
Download Bandwidth <span>?</span>	110 <input type="text"/> Mbps ▾

WAN Connection Settings	
<b>WAN Connection Name</b>	Enter a name to represent this WAN connection.
<b>Schedule</b>	Click the drop-down menu to apply a time schedule to this interface (only visible if Schedules have been created in <b>System &gt; Schedule</b> )
<b>Connection Method</b>	<p>There are five possible connection methods for Ethernet WAN:</p> <ul style="list-style-type: none"> <li>• DHCP</li> <li>• Static IP</li> <li>• PPPoE</li> <li>• L2TP</li> <li>• GRE</li> </ul> <p>The connection method and details are determined by, and can be obtained from the ISP.</p>
<b>Routing Mode</b>	This field shows that <b>NAT</b> (network address translation) will be applied to the traffic routed over

	this WAN connection. <b>IP Forwarding</b> is available when you click the link in the help text.
<b>Hostname (Optional)</b>	Provide a hostname for this WAN port if requested by the ISP
<b>Management IP Address</b>	<p><b>Management IP Address</b> is available for configuration when you click the link in the help icon via the Hostname. </p> <p>This option allows you to configure the management IP address for the DHCP WAN connection.</p>
<b>DNS Servers</b>	Select a DNS server for this port to use. This port can either be automatically selected or manually designated.
<b>Ip Passthrough</b>	When this IP Passthrough option is active, after the ethernet WAN connection is up, the router's DHCP server will offer the connection's IP address to one LAN client. All incoming or outgoing traffic will be routed without NAT.
<b>Independent from Backup WANs</b>	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available
<b>Standby State</b>	This option allows you to choose whether to remain the connection connected or disconnect it when this WAN connection is no longer in the highest priority and has entered the standby state.
<b>Reply to ICMP Ping</b>	If No is selected, this option is disabled and the system will not reply to any ICMP ping echo requests to the WAN IP addresses of this WAN connection(Default option is "Yes")
<b>Upload Bandwidth</b>	<p>This field refers to the maximum upload speed.</p> <p>This value is referenced when default weight is chosen for outbound traffic and traffic prioritization. A correct value can result in effective traffic prioritization and efficient use of upstream bandwidth.</p>
<b>Download Bandwidth</b>	<p>This field refers to the maximum download speed.</p> <p>Default weight control for outbound traffic will be adjusted according to this value.</p>

## WAN > Physical Interface Settings

Physical Interface Settings	
<b>Port Speed</b>	This setting specifies port speed and duplex configurations of the WAN port. By default, <b>Auto</b> is selected and the appropriate data speed is automatically detected by the Pepwave router. In the event of negotiation issues, the port speed can be manually specified. You can also choose whether or not to advertise the speed to the peer by selecting the <b>Advertise Speed</b> checkbox.
<b>MTU</b>	This setting specifies the maximum transmission unit. By default, MTU is set to <b>Custom 1440</b> . You may adjust the MTU value by editing the text field. Click <b>Default</b> to restore the default MTU value. Select <b>Auto</b> and the appropriate MTU value will be automatically detected. Auto-detection will run

	each time the WAN connection establishes.
<b>MSS</b>	This setting should be configured based on the maximum payload size that the local system can handle. The MSS (maximum segment size) is computed from the MTU minus 40 bytes for TCP over IPv4. If the MTU is set to <b>Auto</b> , the MSS will also be set automatically. By default, MSS is set to <b>Auto</b> .

Physical Interface Settings	
<b>MAC Address Clone</b>	Some service providers (e.g., cable providers) identify the client's MAC address and require the client to always use the same MAC address to connect to the network. In such cases, change the WAN interface's MAC address to the original client PC's MAC address via this field. The default MAC address is a unique value assigned at the factory. In most cases, the default value is sufficient. Clicking <b>Default</b> restores the MAC address to the default value.
<b>VLAN</b>	Click the square if you wish to enable VLAN functionality for the WAN connection and enable multiple broadcast domains. Once you enable VLAN, you will be able to enter a name for your network.

## WAN > Health Check Settings

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.

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

## Health Check Methods

**PING:** The router will send an ICMP/PING packet to the specified IP address (or host name) to test WAN connectivity.

**DNS Lookup:** The router will perform a DNS lookup to the specified DNS server.

**HTTP:** The router will perform an HTTP request to the specified URLs. Optional with strings to match.

**SmartCheck:** Available in Cellular/USB WAN only, SmartCheck initiates when outbound traffic goes unresponded for 10 seconds. When SmartCheck initiates, it will run an ICMP health check.

## Health Check Parameters

**Timeout:** During any health check, the router will send a health check packet. The router will wait the specified number of seconds for a response before the health check is considered as failed.

**Health Check Interval:** This number specifies the period between each health check.

**Health Check Retries:** This number specified the number of health check attempts the router will make. Upon reaching this number, the link will be considered as failed

**Recovery Retries:** This specified the number of successful health checks a failed links needs before the link is considered as up again.

## WAN > Bandwidth Allowance Monitor

The Bandwidth Allowance Monitor helps to keep track of your network usage.

To enable this function, connect to the Web Admin Interface and go to **Network > WAN**.

Check the box **Enable** next to Bandwidth Allowance Monitor and you can see the following:

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

**Action:** If the feature **Email Notification** is enabled, you will be notified through email when usage hits 75% and 95% of the monthly allowance.

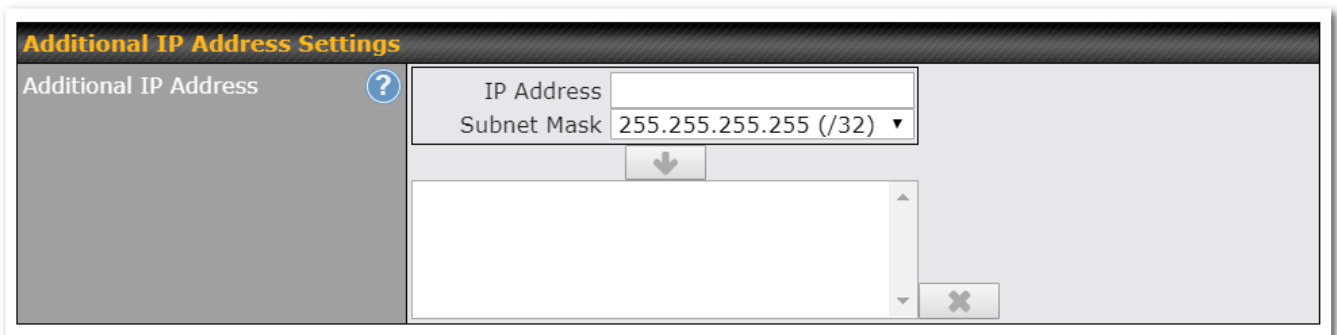
If the box **Disconnect when usage hits 100% of monthly allowance** is checked, this WAN connection will be disconnected automatically when the usage hits the monthly allowance. It will not resume connection unless this option has been turned off or the usage has been reset when a new billing cycle starts.

**Start Day:** This option allows you to define which day in the month each billing cycle begins.

**Monthly Allowance:** This field is for defining the maximum bandwidth usage allowed for the WAN connection each month.

## WAN > Additional IP Address Settings

The **IP Address** list represents the list of fixed Internet IP addresses assigned by the ISP, in the event that more than one Internet IP address is assigned to this WAN connection.



Enter the subnet IP Address and Subnet Mask, press the down arrow button, and the list will be populated by the IP addresses of the specified subnet. You should delete the WAN connection's primary IP address and the gateway address from the list by pressing the *Delete* button after selecting them in the list.

These additional IP addresses can be assigned to a device on the LAN using NAT Mappings

## WAN > Dynamic DNS Settings

Pepwave Surf SOHO routers allow registering 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 hostname.

With dynamic DNS service enabled for a WAN connection, you can connect to your WAN's IP address externally 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 Surf SOHO will connect to the dynamic DNS service provider to update the provider's IP address records.

Dynamic DNS Settings	
Dynamic DNS Service Provider ?	Others... URL: members.dyndns.org/nic/update
Username	Disabled
Password	changeip.com
Confirm Password	dyndns.org
Hosts	no-ip.org
	DNS-O-Matic
	Others...

If your desired provider is not listed, you may check with **DNS-O-Matic**. This service supports updating 30 other dynamic DNS service providers. (Note: Peplink is not affiliated with DNS-O-Matic.)


## Wi-Fi WAN and USB WiFi Network connection

To access Wi-Fi WAN settings, click **Network>WAN>Wireless network connection**.

The WiFi-WAN and USB WiFi Network connection configuration is similar to the Ethernet WAN configuration, but has a few unique options that are shown in this section.

The options that are the same as the ethernet WAN connection configuration are shown in the Ethernet WAN section.

Wi-Fi WAN Settings	
Channel Width	20/40 MHz
Channel	<input type="radio"/> Auto <input checked="" type="radio"/> Custom <input type="button" value="Edit"/> Channels:
Output Power	Max <input type="checkbox"/> Boost
Data Rate	<input checked="" type="radio"/> Auto <input type="radio"/> Fixed
Roaming	<input checked="" type="checkbox"/> Enable
Roaming Algorithm	<input checked="" type="radio"/> Normal <input type="radio"/> Advanced
Roaming Signal Level Threshold	-75 dBm
Roaming Signal Level Gain	5 dBm
Roaming Check Interval	30 seconds
Connect to Any Open Mode AP ?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Beacon Miss Counter	5
Channel Scan Interval	50 ms

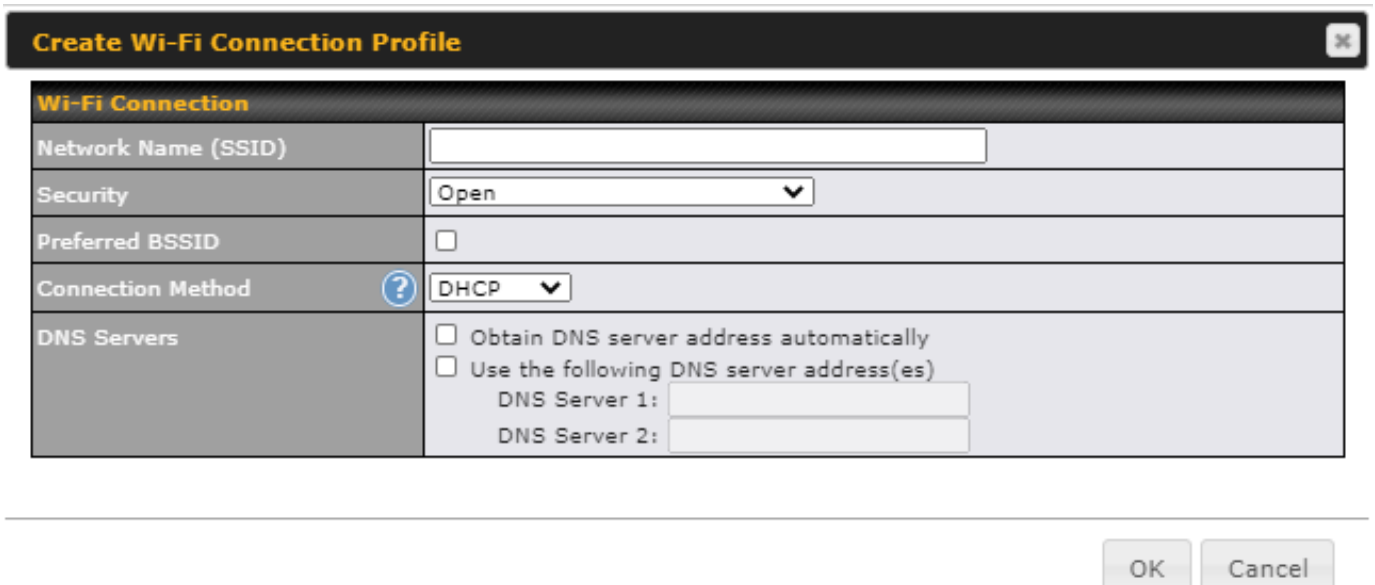
Wi-Fi WAN Settings																																				
<b>Channel Width</b>	choose between the available options 20 Mhz, 20/40Mhz, 20/40/80 Mhz																																			
<b>Channel Selection</b>	<p>Determine whether the channel will be automatically selected. If you select custom, the following table will appear:</p> <div data-bbox="548 499 1367 787" style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <div style="background-color: #333; color: white; padding: 2px; display: flex; justify-content: space-between; align-items: center;"> <span><b>Edit auto channel</b></span> <span>✕</span> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="background-color: #eee;">Scan Channels</td> <td style="text-align: center;">Clear</td> <td style="text-align: center;">All</td> <td colspan="4"></td> </tr> <tr> <td></td> <td colspan="5">2.4 GHz:</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"><input checked="" type="checkbox"/> 1</td> <td style="text-align: center;"><input checked="" type="checkbox"/> 2</td> <td style="text-align: center;"><input checked="" type="checkbox"/> 3</td> <td style="text-align: center;"><input checked="" type="checkbox"/> 4</td> <td style="text-align: center;"><input checked="" type="checkbox"/> 5</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"><input checked="" type="checkbox"/> 6</td> <td style="text-align: center;"><input checked="" type="checkbox"/> 7</td> <td style="text-align: center;"><input checked="" type="checkbox"/> 8</td> <td style="text-align: center;"><input checked="" type="checkbox"/> 9</td> <td style="text-align: center;"><input checked="" type="checkbox"/> 10</td> <td></td> </tr> <tr> <td></td> <td style="text-align: center;"><input checked="" type="checkbox"/> 11</td> <td colspan="4"></td> <td></td> </tr> </table> <div style="text-align: right; margin-top: 10px;"> <input type="button" value="OK"/> <input type="button" value="Cancel"/> </div> </div>	Scan Channels	Clear	All						2.4 GHz:							<input checked="" type="checkbox"/> 1	<input checked="" type="checkbox"/> 2	<input checked="" type="checkbox"/> 3	<input checked="" type="checkbox"/> 4	<input checked="" type="checkbox"/> 5			<input checked="" type="checkbox"/> 6	<input checked="" type="checkbox"/> 7	<input checked="" type="checkbox"/> 8	<input checked="" type="checkbox"/> 9	<input checked="" type="checkbox"/> 10			<input checked="" type="checkbox"/> 11					
Scan Channels	Clear	All																																		
	2.4 GHz:																																			
	<input checked="" type="checkbox"/> 1	<input checked="" type="checkbox"/> 2	<input checked="" type="checkbox"/> 3	<input checked="" type="checkbox"/> 4	<input checked="" type="checkbox"/> 5																															
	<input checked="" type="checkbox"/> 6	<input checked="" type="checkbox"/> 7	<input checked="" type="checkbox"/> 8	<input checked="" type="checkbox"/> 9	<input checked="" type="checkbox"/> 10																															
	<input checked="" type="checkbox"/> 11																																			
<b>Output Power</b>	<p>Low, Medium, High, Max (boost options for tickbox).            Max is the Maximum transmit power supported for that country / Maximum power supported of that device (the smaller value).            High, Medium, Low is having -3dBm each from the previous level.            Transmit power of 2.4Ghz is generally approximately 20dBm.</p>																																			
<b>Data Rate</b>	One of the available advanced options is the ability to configure the Data rate according to the MCS Index (see <a href="http://mcsindex.com/">http://mcsindex.com/</a> )																																			
<b>Roaming</b>	Checking this box will enable Wi-Fi roaming. Click the  icon for additional options.																																			
<b>Roaming Algorithm</b>	select Normal (default) pr Advanced (enables Intensive Scan options)																																			
<b>Roaming Signal Level Threshold</b>	Configure the Roaming Signal Level Threshold in dBm																																			
<b>Roaming Signal Level Gain</b>	Configure the Roaming Signal Level Gain in dBm																																			
<b>Roaming Check Interval</b>	Configure the Roaming Check Interval in Seconds																																			
<b>Connect to Any Open Mode AP</b>	This option is to specify whether the Wi-Fi WAN will connect to any open mode access points it finds.																																			
<b>Beacon Miss Counter</b>	Client devices will disconnect from the AP when this amount of beacons is missed																																			
<b>Channel Scan Interval</b>	Configure Channel Scan Interval in ms.																																			

## WAN > WiFi Connection Profiles

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



This will open a window similar to the one shown below:



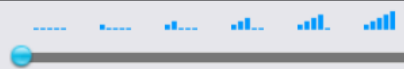


Wi-Fi Connection Profile Settings																																									
<b>Network Name (SSID)</b>	Enter a name to represent this Wi-Fi connection.																																								
<b>Security</b>	<p>This option allows you to select which security policy is used for this wireless network. Available options:</p> <ul style="list-style-type: none"> <li> <b>Open</b> <table border="1"> <tr> <td>Security</td> <td>Open</td> </tr> </table> </li> <li> <b>WEP</b> <table border="1"> <tr> <td>Security</td> <td>WEP</td> </tr> <tr> <td>Encryption Key</td> <td><input type="text"/></td> </tr> <tr> <td></td> <td><input checked="" type="checkbox"/> Hide Characters</td> </tr> </table> </li> <li> <b>WPA/WPA2 – Personal</b> <table border="1"> <tr> <td>Security</td> <td>WPA/WPA2-Personal</td> </tr> <tr> <td>Shared Key</td> <td><input type="text"/></td> </tr> <tr> <td></td> <td><input checked="" type="checkbox"/> Hide Characters</td> </tr> </table> </li> <li> <b>WPA/WPA2 – Enterprise</b> <table border="1"> <tr> <td>Security</td> <td>WPA/WPA2-Enterprise</td> </tr> <tr> <td>Login ID</td> <td><input type="text"/></td> </tr> <tr> <td>Password</td> <td><input type="text"/></td> </tr> <tr> <td>Confirm Password</td> <td><input type="text"/></td> </tr> <tr> <td>EAP Method</td> <td>PEAP</td> </tr> <tr> <td>EAP Phase 2 Method</td> <td>EAP/CHAP</td> </tr> <tr> <td>EAP outer authentication identity</td> <td> <input checked="" type="radio"/> Anonymous  <input type="radio"/> User Credentials  <input type="radio"/> Other: <input type="text"/> </td> </tr> </table> </li> <li> <b>WPA3 – Personal</b> <table border="1"> <tr> <td>Security</td> <td>WPA3-Personal</td> </tr> <tr> <td>Shared Key</td> <td><input type="text"/></td> </tr> <tr> <td></td> <td><input checked="" type="checkbox"/> Hide Characters</td> </tr> </table> </li> <li> <b>WPA2/WPA3 – Personal</b> <table border="1"> <tr> <td>Security</td> <td>WPA2/WPA3-Personal</td> </tr> <tr> <td>Shared Key</td> <td><input type="text"/></td> </tr> <tr> <td></td> <td><input checked="" type="checkbox"/> Hide Characters</td> </tr> </table> </li> <li> <b>802.1x with dynamic WEP key</b> </li> </ul>	Security	Open	Security	WEP	Encryption Key	<input type="text"/>		<input checked="" type="checkbox"/> Hide Characters	Security	WPA/WPA2-Personal	Shared Key	<input type="text"/>		<input checked="" type="checkbox"/> Hide Characters	Security	WPA/WPA2-Enterprise	Login ID	<input type="text"/>	Password	<input type="text"/>	Confirm Password	<input type="text"/>	EAP Method	PEAP	EAP Phase 2 Method	EAP/CHAP	EAP outer authentication identity	<input checked="" type="radio"/> Anonymous <input type="radio"/> User Credentials <input type="radio"/> Other: <input type="text"/>	Security	WPA3-Personal	Shared Key	<input type="text"/>		<input checked="" type="checkbox"/> Hide Characters	Security	WPA2/WPA3-Personal	Shared Key	<input type="text"/>		<input checked="" type="checkbox"/> Hide Characters
Security	Open																																								
Security	WEP																																								
Encryption Key	<input type="text"/>																																								
	<input checked="" type="checkbox"/> Hide Characters																																								
Security	WPA/WPA2-Personal																																								
Shared Key	<input type="text"/>																																								
	<input checked="" type="checkbox"/> Hide Characters																																								
Security	WPA/WPA2-Enterprise																																								
Login ID	<input type="text"/>																																								
Password	<input type="text"/>																																								
Confirm Password	<input type="text"/>																																								
EAP Method	PEAP																																								
EAP Phase 2 Method	EAP/CHAP																																								
EAP outer authentication identity	<input checked="" type="radio"/> Anonymous <input type="radio"/> User Credentials <input type="radio"/> Other: <input type="text"/>																																								
Security	WPA3-Personal																																								
Shared Key	<input type="text"/>																																								
	<input checked="" type="checkbox"/> Hide Characters																																								
Security	WPA2/WPA3-Personal																																								
Shared Key	<input type="text"/>																																								
	<input checked="" type="checkbox"/> Hide Characters																																								

	<table border="1"> <tr> <td>Security</td> <td>802.1x with dynamic WEP key ▼</td> </tr> <tr> <td>EAP Method</td> <td>PEAP ▼</td> </tr> <tr> <td>EAP Phase 2 Method</td> <td>EAP/CHAP ▼</td> </tr> <tr> <td>Login ID</td> <td><input type="text"/></td> </tr> <tr> <td>Password</td> <td><input type="text"/></td> </tr> <tr> <td>Confirm Password</td> <td><input type="text"/></td> </tr> <tr> <td>EAP outer authentication identity</td> <td> <input checked="" type="radio"/> Anonymous  <input type="radio"/> User Credentials  <input type="radio"/> Other: <input type="text"/> </td> </tr> </table>	Security	802.1x with dynamic WEP key ▼	EAP Method	PEAP ▼	EAP Phase 2 Method	EAP/CHAP ▼	Login ID	<input type="text"/>	Password	<input type="text"/>	Confirm Password	<input type="text"/>	EAP outer authentication identity	<input checked="" type="radio"/> Anonymous <input type="radio"/> User Credentials <input type="radio"/> Other: <input type="text"/>
Security	802.1x with dynamic WEP key ▼														
EAP Method	PEAP ▼														
EAP Phase 2 Method	EAP/CHAP ▼														
Login ID	<input type="text"/>														
Password	<input type="text"/>														
Confirm Password	<input type="text"/>														
EAP outer authentication identity	<input checked="" type="radio"/> Anonymous <input type="radio"/> User Credentials <input type="radio"/> Other: <input type="text"/>														
<b>Preferred BSSID</b>	Configure the BSSID; the BSSID is the MAC address of the wireless access point (WAP)														
<b>Connection Method</b>	Choose DHCP or Static IP														
<b>DNS servers</b>	Configure the DNS servers that this WAN connection should use														

## WAN > Signal threshold settings

**Signal Threshold Settings** ?

Acceptable Level 

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

The signal threshold can also be configured using values (this option can be enabled after selecting the question mark)

**Signal Threshold Settings** ?

Signal Strength RSSI:  dBm (Recovery:  dBm)

### Indication of WiFi strength values:

Signal Strength	Quality indication
-30 dBm	Maximum signal strength
-50 dBm	Excellent signal strength
-60 dBm	Good, reliable signal strength

<b>-67 dBm</b>	Minimum signal strength for applications that require very reliable, timely delivery of data packets.
<b>-70 dBm</b>	Not strong; goof for soet internet browsing and email
<b>-80 dBm</b>	Unreliable
<b>-90 dBm</b>	Unusable

## PepVPN

PepVPN is the core engine of Peplink site-to-site VPN technology.

It is ideal for establishing a secure tunnel over any WAN link.

On top of all the benefits of IPsec and other conventional VPN technologies, the PepVPN engine also offers:

**Long-distance Ethernet cable** – PepVPN allows a secure and seamless Ethernet tunnel over any IP connection (Layer 2 over Layer 3). It virtually provides a long-distance Ethernet cable over any WAN link.

**Works in any dynamic IP environment** – PepVPN is fully compatible with any dynamic IP environment and NAT, allowing you to establish a VPN behind a NAT gateway or firewall without worrying about static IP addresses (one public IP address is needed to establish a PeVPN Connection).

To start, navigate to Network > VPN > SpeedFusion and enter a Local ID and click save.

This device will be identified by other SpeedFusion Peers by this local ID

When a PepVPN connection is established between sites, 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. Each profile specifies the settings for creating a VPN connection with one remote Pepwave or Peplink device.

The Pepwave Surf Soho supports 2 PepVPN remote peers per device (5 with upgrade license).

PEPWAVE
Dashboard
SpeedFusion Cloud
Network
Advanced
AP
System
Status
Apply Changes

**Advanced**

- PepVPN
- GRE Tunnel
- Port Forwarding

**NAT Mappings**

**QoS**

- Bandwidth Control
- Application

**Firewall**

- Access Rules
- Content Blocking

**Routing Protocols**

- OSPF & RIPv2
- BGP

**Remote User Access**

**Misc. Settings**

- RADIUS Server
- Certificate Manager
- Service Forwarding
- Service Passthrough
- Grouped Networks
- SIM Toolkit

Logout

## PepVPN

AES 256

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

Profile	Remote ID	Remote Address(es)	?
No VPN Connection Defined			
<span style="border: 1px solid #ccc; padding: 5px 20px;">New Profile</span>			

**Send All Traffic To**

No PepVPN profile selected ✎

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

Service	Algorithm	Source	Destination	Protocol / Port	
(Auto)					
<span style="border: 1px solid #ccc; padding: 5px 20px;">Add Rule</span>					

**PepVPN Local ID**

Local ID	?	SURF_SOHO_8F18	✎
----------	---	----------------	---


**PepVPN Settings** ?

Link Failure Detection Time	?	<input checked="" type="radio"/> Recommended (Approx. 15 secs) <input type="radio"/> Fast (Approx. 6 secs) <input type="radio"/> Faster (Approx. 2 secs) <input type="radio"/> Extreme (Under 1 sec) <small>Shorter detection time incurs more health checks and higher bandwidth overhead</small>
<span style="border: 1px solid #ccc; padding: 5px 20px;">Save</span>		

To configure PepVPN, navigate to **Advanced > PepVPN** and select **New Profile**.

The example below had allPepVPN advanced features enabled.

PepVPN Profile <span style="float: right;">?</span>					
Name	<input type="text"/>				
Enable	<input checked="" type="checkbox"/>				
Encryption	<input checked="" type="radio"/> 256-bit AES <input type="radio"/> OFF				
Authentication	<input checked="" type="radio"/> Remote ID / Pre-shared Key				
Remote ID / Pre-shared Key	<table border="1"> <thead> <tr> <th>Remote ID</th> <th>Pre-shared Key</th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> </tr> </tbody> </table>	Remote ID	Pre-shared Key	<input type="text"/>	<input type="text"/>
Remote ID	Pre-shared Key				
<input type="text"/>	<input type="text"/>				
NAT Mode	<input type="checkbox"/>				
Remote IP Address / Host Names (Optional)	<input type="text"/> <small>If this field is empty, this field on the remote unit must be filled</small>				
Cost	<input type="text" value="10"/>				
Data Port	<input type="text" value="UDP"/> <input checked="" type="radio"/> Auto <input type="radio"/> Custom <input type="text"/>				
Bandwidth Limit	<input type="checkbox"/>				
Receive Buffer	<input type="text" value="0"/> ms				
Packet Fragmentation	<input checked="" type="radio"/> Always <input type="radio"/> Use DF Flag				
Use IP ToS	<input type="checkbox"/>				
Latency Difference Cutoff	<input type="text" value="500"/> ms				

PepVPN Profile Settings	
<b>Name</b>	This field is for specifying a name to represent this profile. The name can be any combination of alphanumeric characters (0-9, A-Z, a-z), underscores ( _ ), dashes ( - ), and/or non-leading/trailing spaces ( ).
<b>Active</b>	When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled.
<b>Encryption</b>	By default, VPN traffic is encrypted with <b>256-bit AES</b> . If <b>Off</b> is selected on both sides of a VPN connection, no encryption will be applied.
<b>Authentication</b>	Select from <b>By Remote ID Only</b> , <b>Preshared Key</b> . When selecting <b>By Remote ID Only</b> , be sure to enter a unique peer ID number in the <b>Remote ID</b> field.
<b>Remote ID / Pre-shared Key</b>	This optional field becomes available when <b>Remote ID / Pre-shared Key</b> is selected as the Pepwave Surf SOHO's VPN <b>Authentication</b> method, as explained above. <b>Pre-shared Key</b> defines the pre-shared key used for this particular VPN connection. The VPN connection's session key will be further protected by the pre-shared key. The connection will be up only if the pre-shared keys on each side match. When the peer is running firmware 5.0+, this setting will be ignored.
<b>NAT Mode</b>	Check this box to allow the local DHCP server to assign an IP address to the remote peer. When <b>NAT Mode</b> is enabled, all remote traffic over the VPN will be tagged with the assigned IP address using network address translation.
<b>Remote IP Address / Host Names (Optional)</b>	<p>If <b>NAT Mode</b> is not enabled, you can enter a remote peer's WAN IP address or hostname(s) here. If the remote uses more than one address, enter only one of them here. Multiple hostnames are allowed and can be separated by a space character or carriage return. Dynamic-DNS host names are also accepted.</p> <p>This field is optional. With this field filled, the Pepwave Surf SOHO will initiate connection to each of the remote IP addresses until it succeeds in making a connection. If the field is empty, the Pepwave Surf SOHO will wait for connection from the remote peer. Therefore, at least one of the two VPN peers must specify this value. Otherwise, VPN connections cannot be established.</p> <p>Click the  icon to configure data stream using TCP protocol [EXPERIMENTAL]. In the case TCP protocol is used, the exposed TCP session option can be authorised to work with TCP accelerated WAN link.</p>
<b>Cost</b>	<p>Define path cost for this profile.</p> <p>OSPF will determine the best route through the network using the assigned cost.</p> <p>Default: 10</p>
<b>Data Port</b>	This field is used to specify a UDP or TCP port number for transporting outgoing VPN data. If <b>Default</b> is selected, UDP port 4500 will be used. Port 32015 will be used if port 4500 is unavailable. If <b>Custom</b> is selected, enter an outgoing port number from 1 to 65535.
<b>Bandwidth Limit</b>	Define maximum download and upload speed to each individual peer. This functionality requires the peer to use PepVPN version 4.0.0 or above.

<b>Receive Buffer</b>	Receive Buffer can help to reduce out-of-order packets and jitter, but will introduce extra latency to the tunnel. Default is 0 ms, which disable the buffer, and maximum buffer size is 2000 ms.
<b>Packet Fragmentation</b>	<p>If the packet size is larger than the tunnel's MTU, it will be fragmented inside the tunnel in order to pass through.</p> <p>Select Always to fragment any packets that are too large to send, or Use DF Flag to only fragment packets with Don't Fragment bit cleared. This can be useful if your application does Path MTU Discovery, usually sending large packets with DF bit set, if allowing them to go through by fragmentation, the MTU will not be detected correctly.</p>
<b>Use IP ToS<sup>A</sup></b>	If Use IP ToS is enabled, the ToS value of the data packets will be copied to the PepVPN header during encapsulation.
<b>Latency Difference Cutoff<sup>A</sup></b>	Traffic will be stopped for links that exceed the specified millisecond value with respect to the lowest latency link. (e.g. Lowest latency is 100ms, a value of 500ms means links with latency 600ms or more will not be used)
<b>Multiple PepVPN profiles between the same 2 sites<sup>A</sup></b>	<p>Enable this advanced feature to create up to 5 PepVPN tunnels from your router to the same remote location, each with different behavior.</p> <p>See: <a href="https://forum.peplink.com/t/outbound-policies-within-a-pepvpn-or-speedfusion-tunnel/">https://forum.peplink.com/t/outbound-policies-within-a-pepvpn-or-speedfusion-tunnel/</a></p>

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

To enable Layer 2 Bridging between PepVPN profiles, navigate to **Network>LAN>Basic Settings>\*LAN Profile Name\***.

Traffic Distribution	
Policy	Bonding ▼

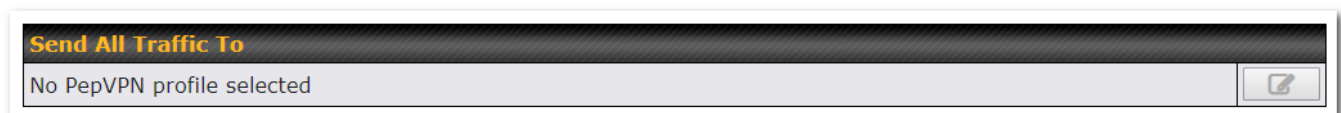
Traffic Distribution	
Policy	Dynamic Weighted Bonding ▼
Congestion Latency Level	Default ▼
Ignore Packet Loss Event	<input type="checkbox"/>
Disable Bufferbloat Handling	<input type="checkbox"/>
Disable TCP ACK Optimization	<input type="checkbox"/>
Packet Jitter Buffer	150 ms


Traffic Distribution	
<b>Policy</b>	<p>This option allows you to select the desired out-bound traffic distribution policy:</p> <ul style="list-style-type: none"> <li>Bonding - Aggregate multiple WAN-to-WAN links into a single higher</li> </ul>

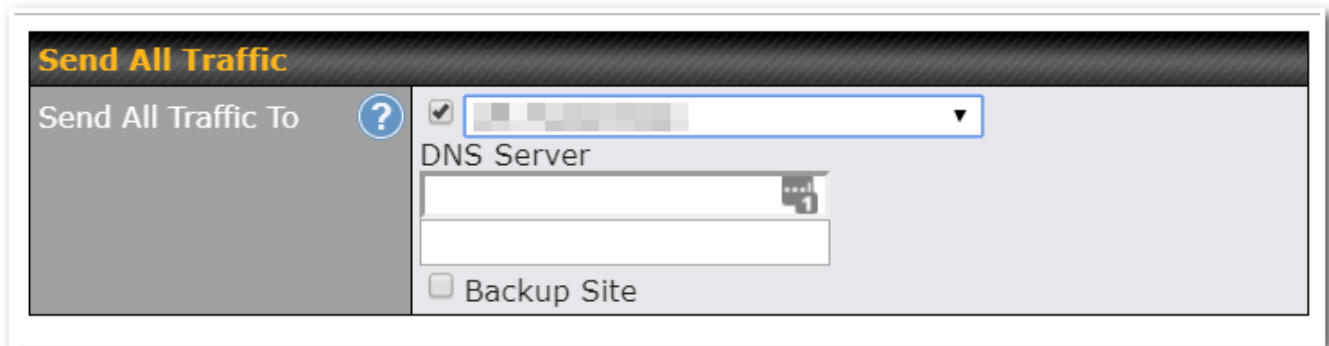


	<p>throughput tunnel.</p> <ul style="list-style-type: none"> <li>Dynamic Weighted Bonding - Aggregates WAN-to-WAN links with similar latencies.</li> </ul> <p>By default, Bonding is selected as a traffic distribution policy.</p>
<b>Congestion Latency Level</b>	<p>For most WANs, especially on cellular networks, the latency will increase when the link becomes more congested.</p> <p>Setting the <b>Congestion Latency Level</b> to <b>Low</b> will treat the link as congested more aggressively.</p> <p>Setting it to <b>High</b> will allow the latency to increase more before treating it as congested.</p>
<b>Ignore Packet Loss Event</b>	<p>By default when there is packet loss, it's considered as congestion event. If this is not the case, select this option to ignore the packet loss event.</p>
<b>Disable Bufferbloat Handling</b>	<p>Bufferbloat is a phenomenon on the WAN side when it is congested. The latency can become very high due to buffering on the uplink. By default, the Dynamic Weighted Bonding policy will try its best to mitigate bufferbloat by reducing TCP throughput when the WAN is congested. However, as a side effect, the tunnel might not achieve maximum bandwidth.</p> <p>Selecting this option will <b>disable</b> the bufferbloat handling mentioned above.</p>
<b>Disable TCP ACK Optimization</b>	<p>By default, TCP ACK will be forwarded to remote peers as fast as possible. This will consume more bandwidth, but may help to improve TCP performance as well.</p> <p>Selecting this option will <b>disable</b> the TCP ACK optimization mentioned above.</p>
<b>Packet Jitter Buffer</b>	<p>The default jitter buffer is 150ms, and can be modified from 0ms to 500ms. The jitter buffer may increase the tunnel latency. If you want to keep the latency as low as possible, you can set it to 0ms to disable the buffer.</p> <p><b>Note:</b> If the Receive Buffer is set, the Packet Jitter Buffer will be automatically disabled.</p>

## PepVPN > Send ALL traffic

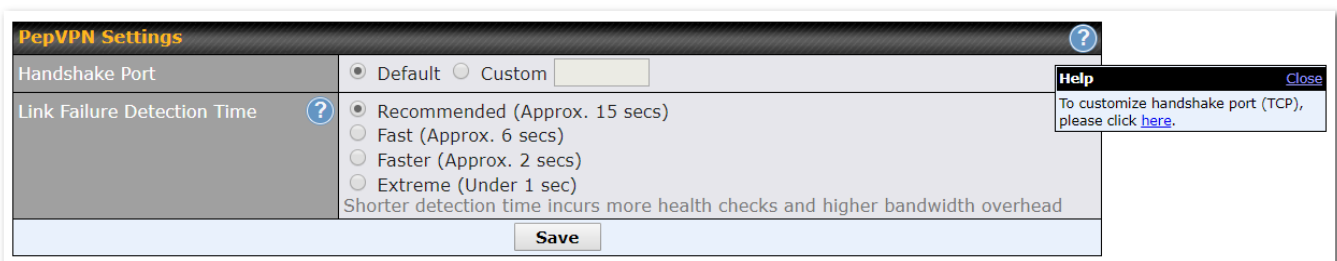


This feature allows you to redirect all traffic to a specified PepVPN connection. Click the  button to select your connection and the following menu will appear:




You can (optionally) 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.

### Handshake Port and Link Failure Detection Time



#### Handshake Port

Click the  icon to customize the handshake port (TCP) used to initialize the PepVPN connection. The handshake uses TCP port 32015 by default.

#### 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.

## Outbound Policy Management

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

### Important Note

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

The settings for managing and load balancing outbound traffic are located at **Advanced > PepVPN**

The screenshot below shows the Outbound Policy window with Expert mode enabled.

Rules (👉 Drag and drop rows by the left to change rule order) ?					
Service	Algorithm	Source	Destination	Protocol / Port	
PepVPN / OSPF / BGP / RIPv2 Routes					
HTTPS Persistence	Enforced WAN: WAN	Any	Any	TCP 443	✖
<input type="button" value="Add Rule"/>					

The bottom-most rule HTTPS\_Persistence is **Default**. This rule manages the device's default manner of controlling outbound traffic for all connections that do not match any of the rules above it.

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

Under Expert Mode, a special rule is displayed on the Custom Rules table which is "PepVPN Routes". It presents all PepVPN routes learned from remote VPN peers. By default, this bar is on the top of all custom rules. That means traffic for remote VPN subnets will be routed to its corresponding VPN peer. You can create custom Priority or Enforced rules and move them above the bar to override the PepVPN Routes.

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

## Adding new Custom Outbound Policies

To add new custom rules (Outbound Policies) select Add Rule.

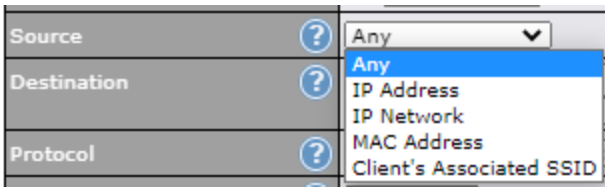
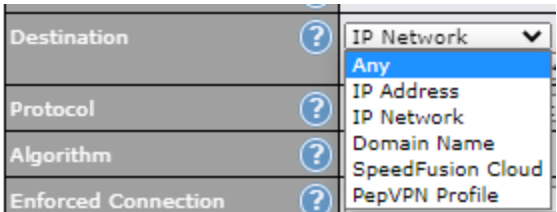
The Pepwave Surf SOHO supports 2 algorithms for the Outbound Policies, Enforced and Priority.

The options for Outbound policies are:

**Add a New Custom Rule**
✕

<b>Service Name</b>	<input style="width: 90%;" type="text"/>		
<b>Enable</b>	<input checked="" type="checkbox"/>		
<b>Source</b>	<input type="text" value="Any"/>		
<b>Destination</b>	<input type="text" value="IP Network"/> ?	<input style="width: 100px;" type="text"/>	Mask: <input type="text" value="255.255.255.0 (/24)"/>
<b>Protocol</b>	<input type="text" value="Any"/> ?	<input type="text" value="← :: Protocol Selection ::"/>	
<b>Algorithm</b>	<input type="text" value="Enforced"/> ?		
<b>Enforced Connection</b>	<input type="text" value=""/> ?		

### Default Outbound Policy Settings

<b>Service Name</b>	This field is for specifying a name to represent this profile. The name can be any combination of alphanumeric characters (0-9, A-Z, a-z), underscores (_), dashes (-), and/or non-leading/trailing spaces ( ).
<b>Enable</b>	When this box is checked, this outbound policy will be enabled. Otherwise, it will be disabled.
<b>Source</b>	<p>This setting specifies the source IP address, IP network, MAC address or Client's Associated SSID for traffic that matches the rule.</p> 
<b>Destination</b>	<p>This setting specifies the destination IP address, IP network, Domain name, SpeedFusion Cloud, PepVPN Profile or Grouped network for traffic that matches the rule.</p> 
<b>Protocol</b>	This setting specifies the IP protocol and port of traffic that matches this rule. Via a drop-down menu, the following protocols can be specified:

	<ul style="list-style-type: none"> <li>• Any</li> <li>• TCP</li> <li>• UDP</li> <li>• IP</li> <li>• DSCP</li> </ul> <p>Alternatively, the <b>Protocol Selection Tool</b> drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.) After selecting an item from the <b>Protocol Selection Tool</b> drop-down menu, the protocol and port number remains manually modifiable.</p>
<b>Algorithm</b>	<p>This setting specifies the behavior of the Pepwave router for the custom rule.</p> <p>One of the following values can be selected:</p> <ul style="list-style-type: none"> <li>• Enforced : Enforce traffic matching this rule through a selected WAN or VPN connection.</li> <li>• Priority: Prioritise traffic matching this rule through selected WAN or VPN connection(s)</li> </ul>
<b>Enforced Connection</b>	<p>Specify the WAN or VPN connection to be used for routing traffic regardless of the connection's health status.</p>
<b>When No Connections are Available</b>	<p>This field allows you to configure the default action when all the selected Connections are not available.</p> <ul style="list-style-type: none"> <li>• Drop the Traffic - Traffic will be discarded.</li> <li>• Use Any Available Connections - Traffic will be routed to any available Connection, even it is not selected in the list.</li> <li>• Fall-through to Next Rule - Traffic will continue to match next Outbound Policy rule just like this rule is inactive.</li> </ul>
<b>Terminate Sessions on Connection Recovery</b>	<p>In the case when the highest priority connection is unavailable, matching sessions may routed through a lower priority connection or skipped to next matching rule (Fall-through to Next Rule). By checking this option, those sessions will be terminated upon connection recovery of any higher priority connections. Terminated sessions will go through all the rules again to determine the outgoing connection.</p> <p>When Source is a MAC address, this option will be disabled automatically.</p> <p>Default: Disable</p>

## Port Forwarding

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

Service	IP Address(es)	Server	Protocol
No Services Defined			
<input type="button" value="Add Service"/>			

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

**Port Forwarding** ✕

Enable	<input checked="" type="checkbox"/>										
Service Name	<input type="text"/>										
Protocol	TCP ▾ ◀ :: Protocol Selection :: ▾										
Port	Any Port ▾										
Inbound IP Address(es) (Require at least one IP address)	<div style="border: 1px solid black; padding: 2px;"> <div style="background-color: #333; color: white; padding: 2px;"><b>Connection / IP Address(es)</b> <span style="float: right;">All Clear</span></div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td><input type="checkbox"/></td><td><input type="text"/></td></tr> <tr><td><input type="checkbox"/></td><td><input type="text"/></td></tr> <tr><td><input type="checkbox"/></td><td><input type="text"/></td></tr> <tr><td><input type="checkbox"/></td><td><input type="text"/></td></tr> <tr><td><input type="checkbox"/></td><td><input type="text"/></td></tr> </table> </div>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>	<input type="text"/>
<input type="checkbox"/>	<input type="text"/>										
<input type="checkbox"/>	<input type="text"/>										
<input type="checkbox"/>	<input type="text"/>										
<input type="checkbox"/>	<input type="text"/>										
<input type="checkbox"/>	<input type="text"/>										
Server IP Address	<input type="text"/>										

Port Forwarding Settings	
<b>Enable</b>	This setting specifies whether the inbound service takes effect. When <b>Enable</b> is checked, the inbound service takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When this setting is disabled, the inbound service does not take effect: the Pepwave router disregards the other parameters of the rule.
<b>Service Name</b>	This setting identifies the service to the system administrator. Valid values for this setting consist of only alphanumeric and underscore “_” characters.
<b>Protocol</b>	The <b>Protocol</b> setting, along with the <b>Port</b> setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Traffic that is received by the Pepwave router via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the <b>Servers</b> setting. Please see below for details on the <b>Port</b> and

**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.

## UPnP / NAT-PMP Settings

UPnP and NAT-PMP are network protocols which allow a computer connected to a LAN port or WiFi AP 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 a LAN port or WiFi AP.

UPnP / NAT-PMP Settings	
UPnP	<input type="checkbox"/> Enable
NAT-PMP	<input type="checkbox"/> Enable
<input type="button" value="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**.

Forwarded Ports						
External	Internal	Internal Address	UPnP / NAT-PMP	Protocol	Description	
8080	8080	192.168.1.10	UPnP	TCP	Test8080	<input type="button" value="X"/>

In the example above, the UPnP device is running. When the UPnP device is disconnected, the router will suspend the service and incoming traffic will be dropped (without error/notification message). The UPnP rule will remain for an interval after the UPnP device is disconnected before being removed.



## 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 <i>Interface IP</i> only	
<input type="button" value="Add NAT Rule"/>			

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

LAN Client(s)	IP Address	
Address	<input type="text"/>	
Inbound Mappings	<b>Connection / Inbound IP Address(es)</b>	
	<input type="checkbox"/> WAN 1	
	<input type="checkbox"/> WAN 2	
	<input type="checkbox"/> Wi-Fi WAN	
	<input type="checkbox"/> Cellular 1	
	<input type="checkbox"/> Cellular 2	
Outbound Mappings	<b>Connection / Outbound IP Address</b>	
	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	
<b>LAN Client(s)</b>	NAT mapping rules can be defined for a single LAN <b>IP Address</b> , an <b>IP Range</b> , or an <b>IP Network</b> .
<b>Address</b>	This refers to the LAN host's private IP address. The system maps this address to a number of public IP addresses (specified below) in order to facilitate inbound and outbound traffic. This option is only available when <b>IP Address</b> is selected.
<b>Range</b>	The IP range is a contiguous group of private IP addresses used by the LAN host. The system maps these addresses to a number of public IP addresses (specified below) to facilitate outbound traffic. This option is only available when <b>IP Range</b> is selected.

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

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

#### Important Note

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

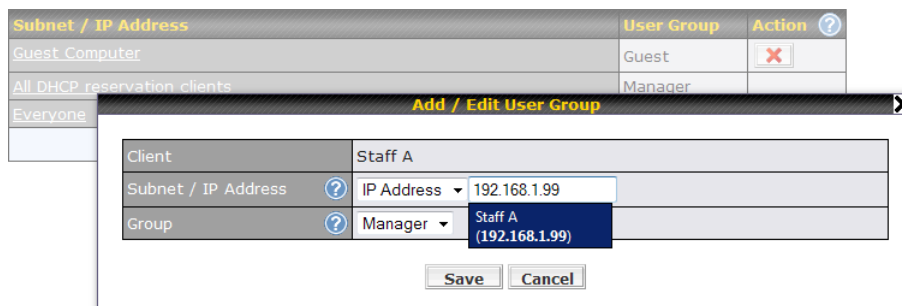
# QoS

## User Group

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

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

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





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

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

## Bandwidth Control

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

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

Group Bandwidth Reservation			
Enable	<input checked="" type="checkbox"/>		
			
	<b>Manager</b>	<b>Staff</b>	<b>Guest</b>
<b>Bandwidth %</b>	<b>50%</b>	<b>30%</b>	<b>20%</b>
USB	500.00 Mbps 500.00 Mbps	300.00 Mbps 300.00 Mbps	200.00 Mbps 200.00 Mbps
Wi-Fi WAN on 2.4 GHz	10.00 Mbps 10.00 Mbps	6.00 Mbps 6.00 Mbps	4.00 Mbps 4.00 Mbps
Wi-Fi WAN on 5 GHz	10.00 Mbps 10.00 Mbps	6.00 Mbps 6.00 Mbps	4.00 Mbps 4.00 Mbps

The default download and upload limits are set to unlimited (set as 0). This can be changed as necessary to restrict the speeds to individual devices connected to the router, either wired or wireless. Note, this limit is applied to all devices..


Individual Bandwidth Limit			
Enable	<input checked="" type="checkbox"/>		
User Bandwidth Limit		Download	Upload
	Manager	Unlimited	Unlimited
	Staff	0 <input type="text"/> Mbps <input type="button" value="v"/>	0 <input type="text"/> Mbps <input type="button" value="v"/> (0: Unlimited)
	Guest	0 <input type="text"/> Mbps <input type="button" value="v"/>	0 <input type="text"/> Mbps <input type="button" value="v"/> (0: Unlimited)

## Application Prioritization

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	
	↑ High <input type="button" value="v"/>	<input type="button" value="x"/>
	↑ High <input type="button" value="v"/>	<input type="button" value="x"/>
	↑ High <input type="button" value="v"/>	<input type="button" value="x"/>
	↑ High <input type="button" value="v"/>	<input type="button" value="x"/>
<input type="button" value="Add"/>		

## Prioritization for Custom Applications

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

When **Supported Applications** is selected, the Pepwave router will inspect network traffic and prioritize the selected applications. Alternatively, you can select **Custom Applications** and define the application by providing the protocol, scope, port number, and DSCP value.

**Add / Edit Application**
✕

Type <span style="float: right;">?</span>	<input checked="" type="radio"/> Supported Applications <input type="radio"/> Custom Applications
Category <span style="float: right;">?</span>	Audio Video Streaming ▼
Application	1Kxun ▼

**Add / Edit Application**
✕

Type <span style="float: right;">?</span>	<input type="radio"/> Supported Applications <input checked="" type="radio"/> Custom Applications
Application Name	<input style="width: 90%;" type="text"/>
Scope / Protocol	TCP ▼
Port	Single Port ▼ <input style="width: 50px;" type="text"/>

## DSL/Cable Optimization


DSL/cable-based WAN connections have lower upload bandwidth and higher download bandwidth. When a DSL/cable circuit's uplink is congested, the download bandwidth will be affected. Users will not be able to download data at full speed until the uplink becomes less congested. **DSL/Cable Optimization** can relieve such an issue. When it is enabled, the download speed will become less affected by the upload traffic. By default, this feature is enabled.

**DSL/Cable Optimization**
?

Enable	<input checked="" type="checkbox"/>
--------	-------------------------------------

## PepVPN Traffic Optimization

Enable this option to grant PepVPN traffic the highest priority when WAN is congested.

PepVPN Traffic Optimization 	
Enable	<input checked="" type="checkbox"/>

# 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

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

**Advanced**

- PepVPN
- GRE Tunnel
- Port Forwarding

**NAT Mappings**

**QoS**

- Bandwidth Control
- Application

**Firewall**

- **Access Rules**
- Content Blocking

**Routing Protocols**

- OSPF & RIPv2
- BGP

**Remote User Access**

**Misc. Settings**

- RADIUS Server
- Certificate Manager
- Service Forwarding
- Service Passthrough
- Grouped Networks
- SIM Toolkit

---

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

Rule	Protocol	Source	Destination	Action	
Default	Any	Any	Any	✓	

---

**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	✓	

---

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

Rule	Protocol	Source	Destination	Action	
Default	Any	Any	Any	✓	

---

**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	✓	

## Outbound and Inbound Firewall Rules

The outbound and inbound firewall settings are located at **Advanced>Firewall>Access 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	<input type="text"/>
Enable	<input checked="" type="checkbox"/> Always on ▾
Protocol	<input type="text" value="Any"/> ▾ ← :: Protocol Selection :: ▾
Source	<input type="text" value="Any Address"/> ▾
Destination	<input type="text" value="Any Address"/> ▾
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Event Logging	<input type="checkbox"/> Enable

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

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

**Add Rule**



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

**Add a New Inbound Firewall Rule** ✕

---

**New Firewall Rule**

Rule Name	<input type="text"/>
Enable	<input checked="" type="checkbox"/> Always on ▾
WAN Connection	<input type="text" value="Any"/> ▾
Protocol	<input type="text" value="Any"/> ▾ ← :: Protocol Selection :: ▾
Source	<input type="text" value="Any Address"/> ▾
Destination	<input type="text" value="Any Address"/> ▾
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Event Logging	<input type="checkbox"/> Enable

---

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

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

Rule	Protocol	Source	Destination	Action	
<input type="text" value="test"/>	Any	Any	Any	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="text" value="Default"/>	Any	Any	Any	<input checked="" type="checkbox"/>	

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

**Add a New Internal Network Firewall Rule** ✕

---

**New Firewall Rule**

Rule Name	<input type="text"/>
Enable	<input checked="" type="checkbox"/> Always on ▾
Protocol	<input type="text" value="Any"/> ▾ ← :: Protocol Selection :: ▾
Source	<input type="text" value="Any Address"/> ▾
Destination	<input type="text" value="Any Address"/> ▾
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny
Event Logging	<input type="checkbox"/> Enable

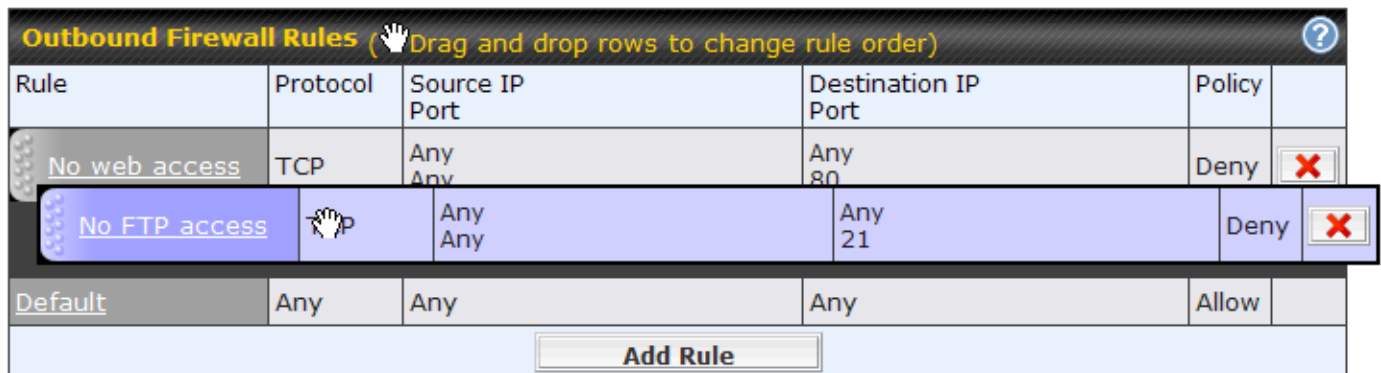
---

Inbound / Outbound / Internal Network Firewall Settings	
<b>Rule Name</b>	This setting specifies a name for the firewall rule.
<b>Enable</b>	<p>This setting specifies whether the firewall rule should take effect. If the box is checked, the firewall rule takes effect. If the traffic matches the specified protocol/IP/port, actions will be taken by the Pepwave router based on the other parameters of the rule. If the box is not checked, the firewall rule does not take effect. The Pepwave router will disregard the other parameters of the rule.</p> <p>Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule.</p>
<b>WAN Connection (Inbound)</b>	Select the WAN connection that this firewall rule should apply to.
<b>Protocol</b>	<p>This setting specifies the protocol to be matched. Via a drop-down menu, the following protocols can be specified:</p> <ul style="list-style-type: none"> <li>• Any</li> <li>• TCP</li> <li>• UDP</li> <li>• ICMP</li> <li>• DSCP</li> <li>• IP</li> </ul> <p>Alternatively, the <b>Protocol Selection Tool</b> drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.)</p> <p>After selecting an item from the <b>Protocol Selection Tool</b> drop-down menu, the protocol and port number remains manually modifiable.</p>
<b>Source IP &amp; Port</b>	This specifies the source IP address(es) and port number(s) to be matched for the firewall rule. A single address, Network, MAC Address or Grouped Network can be specified as the <b>Source</b> setting.
<b>Destination IP &amp; Port</b>	This specifies the destination IP address(es) and port number(s) to be matched for the firewall rule. A single address, Network, MAC Address or a Grouped Network, can be specified as the <b>Destination</b> setting.
<b>Action</b>	This option allows you to define whether to allow or deny an IP session matching this Firewall Rule
<b>Event Logging</b>	<p>This setting specifies whether or not to log matched firewall events. The logged messages are shown on the page <b>Status&gt;Event Log</b>. A sample message is as follows:</p> <p>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</p> <ul style="list-style-type: none"> <li>• <b>CONN:</b> The connection where the log entry refers to</li> <li>• <b>SRC:</b> Source IP address</li> <li>• <b>DST:</b> Destination IP address</li> <li>• <b>LEN:</b> Packet length</li> <li>• <b>PROTO:</b> Protocol</li> <li>• <b>SPT:</b> Source port</li> <li>• <b>DPT:</b> Destination port</li> </ul>

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

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

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



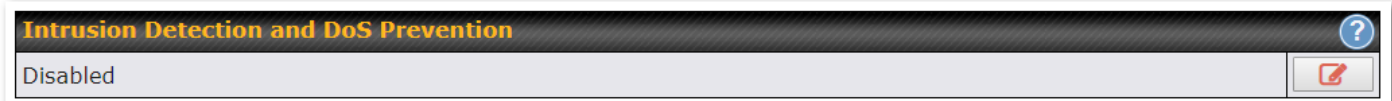
To remove a rule, click the button.

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

### 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.

## Intrusion Detection and DoS Prevention



Pepwave routers can detect and prevent intrusions and denial-of-service (DoS) attacks from the Internet.

To turn on this feature, click , check the **Enable** check box, and press the **Save** button.

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

- Port scan
  - NMAP FIN/URG/PSH

- Xmas tree
- Another Xmas tree
- Null scan
- SYN/RST
- SYN/FIN
- SYN flood prevention
- Ping flood attack prevention

## Content Blocking

**Application Blocking** ?

Please Select Application... +

**Web Blocking** ?

Preset Category
 

High  
 Moderate  
 Low  
 Custom

Adware  
 P2P/File sharing

Audio-Video  
 Pornography

File Hosting  
 Update Sites

Content Filtering Database Auto Update ?

Customized Domains ?  
 +

Exempted Domains from Web Blocking ?  
 +

**Exempted Subnets** ?

Network	Subnet Mask	
<input style="width: 95%;" type="text"/>	255.255.255.0 (/24) <span style="float: right;">▼</span>	+

**URL Logging**

Enable

Log Server Host  Port: 514

### Application Blocking

Choose applications to be blocked from LAN/PPTP/PepVPN peer clients' access, except for those on the Exempted Subnets defined in that particular section on the same page.

## Web Blocking

Defines website domain names to be blocked from LAN/PPTP/PepVPN peer clients' access except for those on the Exempted Subnets defined in that particular section on the same page.

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.

## Exempted Subnets

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

## URL Logging

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

# Routing Protocols

The Pepwave Surf SOHO supports OSPF ,RIPv2 and BGP dynamic routing protocols.

## OSPF & RIPv2

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	No interface is selected	
<input type="button" value="Add"/>		

RIPv2
No RIPv2 Defined.

OSPF & RIPv2 Route Advertisement		
PepVPN Route Isolation		<input type="checkbox"/> Enable
Network Advertising		<div style="border: 1px solid #ccc; padding: 2px;">---</div> <div style="font-size: 8px; margin-top: 2px;">All LAN/VLAN networks will be advertised when no network advertising is chosen.</div> <div style="text-align: right;"></div>
Static Route Advertising		<input checked="" type="checkbox"/> Enable
	Excluded Networks	Subnet Mask
	<div style="border: 1px solid #ccc; height: 15px;"></div>	255.255.255.0 (/24)
<input type="button" value="Save"/>		

### OSPF


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

#### OSPF settings

Area ID	<div style="border: 1px solid #ccc; height: 20px;"></div>
Link Type	<input checked="" type="radio"/> Broadcast <input type="radio"/> Point-to-Point
Authentication	None
Interfaces	<div style="font-size: 8px; margin-bottom: 5px;">? <input type="checkbox"/> [blurred]</div> <div style="font-size: 8px; margin-bottom: 5px;">? <input type="checkbox"/> [blurred]</div>

Help Close  
 Click [here](#) to customize interface cost

OSPF Settings	
<b>Area ID</b>	Determine the name of your <b>Area ID</b> to apply to this group. Machines linked to this group will send and receive related OSPF packets, while unlinked machines will ignore it.
<b>Link Type</b>	Choose the network type that this area will use.
<b>Authentication</b>	Choose an authentication method, if one is used, from this drop-down menu. Available options are <b>MD5</b> and <b>Text</b> . Enter the authentication key next to the drop-down menu.
<b>Interfaces</b>	Determine which interfaces this area will use to listen to and deliver OSPF packets
<b>Interface Cost</b>	Enable the advanced option (question mark) to be able to configure a custom cost for each interface.

To access RIPv2 settings, click  .

**RIPv2 settings** ✕

Authentication	None ▼
Interfaces	<input type="checkbox"/> <span style="background-color: #eee; padding: 2px;">[blurred]</span> <input type="checkbox"/> <span style="background-color: #eee; padding: 2px;">[blurred]</span>

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

**OSPF & RIPv2 Route Advertisement**

PepVPN Route Isolation	?	<input type="checkbox"/> Enable
Network Advertising	?	<div style="border: 1px solid #ccc; padding: 2px; display: flex; align-items: center;"> <span style="background-color: #eee; padding: 2px;">---</span> <span style="margin-left: 5px;">▼</span> <span style="margin-left: 5px; border: 1px solid #ccc; padding: 2px;">+</span> </div> <small>All LAN/VLAN networks will be advertised when no network advertising is chosen.</small>
Static Route Advertising	?	<input type="checkbox"/> Enable

### OSPF & RIPv2 Route Advertisement

<b>PepVPN Route Isolation</b>	<p>Enable this option if you want to isolate PepVPN peers from each other. Received PepVPN routes will not be forwarded to other PepVPN peers to reduce bandwidth consumption.</p> <p>Note: This will only hide routing information between PepVPN peers, if you want to fully block inter-PepVPN traffics, you should configure Firewall rules instead.</p>
<b>Network Advertising</b>	<p>Selected networks will be advertised over OSPF &amp; RIPv2. If no network is selected, all LAN / VLAN networks will be advertised by default.</p> <p>All the networks belonging to interfaces that have OSPF or RIPv2 enabled will be advertised even if they are not selected in this table.</p>
<b>Static Route Advertising</b>	<p>Enable this option to advertise LAN static routes over OSPF &amp; RIPv2. Static routes that match the Excluded Networks table will not be advertised.</p>



## BGP

BGP (Border Gateway Protocol) is a protocol that manages how packets are routed across the internet through the exchange of routing and reachability information between edge routers. BGP directs packets between autonomous systems (AS) -- networks managed by a single enterprise or service provider.

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

BGP	AS	Neighbors
No BGP Profile Defined.		
<input type="button" value="Add"/>		

Click "x" to delete a BGP profile

Click "Add" to add a new BGP profile

BGP Profile						
Profile Name	<input type="text"/>					
Enable	<input checked="" type="checkbox"/>					
Interface	Untagged LAN <input type="button" value="v"/>					
Router ID	<input checked="" type="radio"/> LAN IP Address <input type="radio"/> Custom: <input type="text"/>					
Autonomous System	<input type="text"/>					
Neighbor	<input type="button" value="?"/>	IP Address	Autonomous System	Multihop / TTL	Password	AS-Path Prepending
		<input type="text"/>	<input type="text"/>	disable	<input type="text"/>	<input type="text"/>
Hold Time	<input type="button" value="?"/>	<input type="text" value="240"/>				
Next Hop Self	<input type="button" value="?"/>	<input type="checkbox"/>				
iBGP Local Preference	<input type="button" value="?"/>	<input type="text" value="100"/>				
BFD	<input type="button" value="?"/>	<input type="checkbox"/> Enable				



BGP Profile	
<b>Name</b>	This field is for specifying a name to represent this profile.
<b>Enable</b>	When this box is checked, this BGP profile will be enabled. If it is left unchecked, it will be disabled.
<b>Interface</b>	The interface in which the BGP neighbor is located.
<b>Autonomous System</b>	The Autonomous System Number (ASN) assigned to this profile.
<b>Neighbor</b>	BGP Neighbors and their details.
<b>IP address</b>	The IP address of the Neighbor.

<b>Autonomous System</b>	The Neighbor's ASN.
<b>Multihop/TTL</b>	This field determines the Time-to-live (TTL) of BGP packets. Leave this field blank if the BGP neighbor is directly connected, otherwise you must specify a TTL value. This option should be used if the configured Neighbor's IP address does not match the selected Interface's network subnets. The TTL value must be between 2 to 255.
<b>Password</b>	(Optional) Assign a password for MD5 authentication of BGP sessions.
<b>AS-Path Prepending:</b>	AS path to be prepended to the routes received from this Neighbor. Values must be ASN and separated by commas. For example: inputting "64530,64531" will prepend "64530, 64531" to received routes.
<b>Hold Time</b>	Wait time in seconds for a keepalive message from a Neighbor before considering the BGP connection as stalled. The value must be either 0 (infinite hold time) or between 3 and 65535 inclusively. Default: 240
<b>Next Hop Self</b>	Enable this option to advertise your own source address as the next hop when propagating routes.
<b>iBGP Local Preference</b>	This is the metric advertised to iBGP Neighbors to indicate the preference for external routes. The value must be between 0 to 4294967295 inclusively. Default: 100
<b>BFD</b>	Enable this option to add Bidirectional Forwarding Detection for path failure. All directly connected Neighbors that use the same physical interface share the same BFD settings. All multihop Neighbors share the same multihop BFD settings. You can configure BFD settings in the BGP profile listing page after this option is enabled.

Route Advertisement								
Network Advertising	?	---	+					
Static Route Advertising	?	<input type="checkbox"/> Enable						
Custom Route Advertising	?	<table border="1"> <thead> <tr> <th>Networks</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>	Networks	Subnet Mask			255.255.255.0 (/24)	+
Networks	Subnet Mask							
	255.255.255.0 (/24)	+						
Advertise OSPF Route	?	<input type="checkbox"/>						
Set Community	?	<table border="1"> <thead> <tr> <th>Community</th> <th>Route Prefix</th> <th></th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td>+</td> </tr> </tbody> </table>	Community	Route Prefix				+
Community	Route Prefix							
		+						

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

<b>Advertising</b>	
<b>Advertise OSPF Route</b>	When this box is checked, every learnt OSPF route will be advertised.
<b>Set Community</b>	<p>Assign a prefix to a Community</p> <p>Community: Two numbers in new-format. e.g. 65000:21344</p> <p>Well-known communities: no-export 65535:65281 no-advertise 65535:65282 no-export-subconfed 65535:65283 no-peer 65535:65284</p> <p>Route Prefix: Comma separated networks. e.g. 172.168.1.0/24,192.168.1.0/28</p>

Route Import			
Filter Mode		Reject ▼	
Blocked Networks	Network	Subnet Mask	Exact Match
		255.255.255.0 (/24) ▼	<input type="checkbox"/>
			

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

Route Export			
Filter Mode		Accept ▾	
Restricted Networks	Network	Subnet Mask	Exact Match
	<input type="text"/>	255.255.255.0 (/24) ▾	<input type="checkbox"/>
Export to other BGP Profile		<input type="checkbox"/>	
Export to OSPF		<input type="checkbox"/>	

<b>Filter Mode</b>	<p>This field allows for the selection of the filter mode for route export.</p> <p><b>None:</b> All BGP routes will be accepted.</p> <p><b>Accept:</b> Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected.</p> <p><b>Reject:</b> Routes in "Restricted Networks" will be rejected, routes not in the list will be accepted.</p>
<b>Restricted / Blocked Networks</b>	<p>This field specifies the network(s) in the "route export" entry.</p> <p><b>Exact Match:</b> When this box is checked, only routes with the same Network and Subnet Mask will be filtered. Otherwise, routes within the Networks and Subnets will be filtered.</p>
<b>Export to other BGP Profile</b>	When this box is checked, routes learnt from this BGP profile will be exported to other BGP profiles.
<b>Export to OSPF</b>	When this box is checked, routes learnt from this BGP profile will be exported to the OSPF routing protocol.

## 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.

### L2TP with IPsec

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

#### L2TP with IPsec Remote User Access Settings

**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.

<b>Listen On</b>	This setting is for specifying the WAN IP addresses that allow remote user access.
<b>Disable Weak Ciphers</b>	Click the  button to show and enable this option. When checked, weak ciphers such as 3DES will be disabled.

Continue to configure the authentication method.

## OpenVPN

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

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	 <a href="#">Route all traffic</a>   <a href="#">Split tunnel</a>
------------------------	--

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.

## PPTP



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

No additional configuration required.

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

Continue to configure authentication methods.

## Authentication Methods

Connect to Network	 Untagged LAN ▾		
Authentication	Local User Accounts ▾		
User Accounts	Username	Password	
	<input type="text"/>	<input type="password"/>	

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

### User accounts:

This setting allows you to define the Remote User Accounts.


Click Add to input username and password to create an account. After adding the user accounts, you can click on a username to edit the account password.

### Note:

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

The password must be between 8 and 12 characters long.

### LDAP Server:

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

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

**Radius Server:**

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

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

**Active Directory:**

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

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

## Miscellaneous Settings

### RADIUS Server

RADIUS Server settings are located at **Advanced>Misc. Settings>RADIUS Server**.

Authentication Server	Host	Port
No server profiles defined		
<a href="#">New Profile</a>		

Accounting Server	Host	Port
No server profiles defined		
<a href="#">New Profile</a>		

Click **New Profile** to display the following screen:

**Authentication Server**
✕

Name	<input type="text"/>
Host	<input type="text"/>
Port	<input type="text" value="1812"/>
Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters

Authentication Server	
<b>Name</b>	This field is for specifying a name to represent this profile.
<b>Host</b>	Specifies the IP address or hostname of the RADIUS server host.
<b>Authentication Port</b>	This setting specifies the UDP destination port for authentication requests. By default, the port number is 1812.
<b>Secret</b>	This field is for entering the secret key for communicating to the RADIUS server.
<b>Accounting Port</b>	This setting specifies the UDP destination port for accounting requests. By default, the port number is 1813.



**Accounting Server**
✕

Name	<input style="width: 90%;" type="text"/>
Host	<input style="width: 90%;" type="text"/>
Port	<input style="width: 90%;" type="text" value="1813"/>
Secret	<input style="width: 90%;" type="password"/> <input checked="" type="checkbox"/> Hide Characters

Accounting Server	
<b>Name</b>	This field is for specifying a name to represent this profile.
<b>Host</b>	Specifies the IP address or hostname of the RADIUS server host.
<b>Authentication Port</b>	This setting specifies the UDP destination port for authentication requests. By default, the port number is 1812.
<b>Secret</b>	This field is for entering the secret key for communicating to the RADIUS server.
<b>Accounting Port</b>	This setting specifies the UDP destination port for accounting requests. By default, the port number is 1813.

## Certificate Manager

Certificate		
PepVPN	No Certificate	
Web Admin SSL	Default Certificate is in use	
OpenVPN CA	Default Certificate is in use	

Wi-Fi WAN Client Certificate
No Certificates defined
<input type="button" value="Add Certificate"/>

Wi-Fi WAN CA Certificate
No Certificates defined
<input type="button" value="Add Certificate"/>

This section allows you to assign certificates for the local VPN, OpenVPN, Captive Portal, Mediafast, Contenthub, Wi-Fi WAN (Client and CA) and web admin SSL for extra security.

Read the following knowledgebase article for full instructions on how to create and import a self-signed certificate:

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

## Service Forwarding

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

SMTP Forwarding Setup				
SMTP Forwarding	<input type="checkbox"/> Enable			

Web Proxy Forwarding Setup				
Web Proxy Forwarding	<input type="checkbox"/> Enable			

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

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

## SMTP Forwarding

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

**SMTP Forwarding Setup** ?

SMTP Forwarding
 Enable

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

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 email server hostname 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.

## Web Proxy Forwarding

**Web Proxy Forwarding Setup** ?

Web Proxy Forwarding  Enable

**Web Proxy Interception Settings**

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

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

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

## 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.

## Custom Service Forwarding

**Custom Service Forwarding Setup**

Custom Service Forwarding  Enable

Settings	Source Network	TCP Port	Server IP Address	Server Port	
	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	+

After clicking the **enable** checkbox, enter your TCP port for traffic heading to the router, and then specify

the IP Address and Port of the server you wish to forward the service to.

## Service Passthrough

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

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

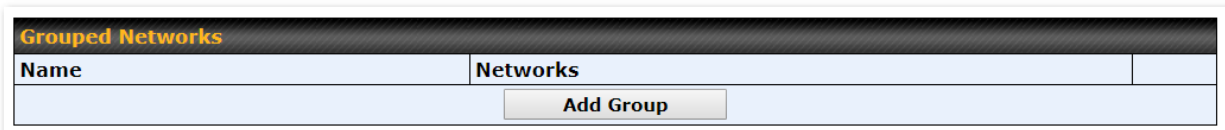
(Registered trademarks are copyrighted by their respective owner)

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

Service Passthrough Support	
<b>SIP</b>	Session initiation protocol, aka SIP, is a voice-over-IP protocol. The Pepwave router can act as a SIP application layer gateway (ALG) which binds connections for the same SIP session to the same WAN connection and translate IP address in the SIP packets correctly in <b>NAT mode</b> . Such passthrough support is always enabled, and there are two modes for selection: <b>Standard Mode</b> and <b>Compatibility Mode</b> . If your SIP server's signal port number is non-standard, you can check the box <b>Define custom signal ports</b> and input the port numbers to the text boxes.
<b>H.323</b>	With this option enabled, protocols that provide audio-visual communication sessions will be defined on any packet network and pass through the Pepwave router.
<b>FTP</b>	FTP sessions consist of two TCP connections; one for control and one for data. In a multi-WAN situation, they must be routed to the same WAN connection. Otherwise, problems will arise in transferring files. By default, the Pepwave router monitors TCP control connections on port 21 for any FTP connections and binds TCP connections of the same FTP session to the same WAN. If you have an FTP server listening on a port number other than 21, you can check <b>Define custom control ports</b> and enter the port numbers in the text boxes.
<b>TFTP</b>	The Pepwave router monitors outgoing TFTP connections and routes any incoming TFTP data packets back to the client. Select <b>Enable</b> if you want to enable TFTP passthrough support.

Service Passthrough Support	
<b>SIP</b>	Session initiation protocol, aka SIP, is a voice-over-IP protocol. The Pepwave router can act as a SIP application layer gateway (ALG) which binds connections for the same SIP session to the same WAN connection and translate IP address in the SIP packets correctly in NAT mode. Such passthrough support is always enabled, and there are two modes for selection: <b>Standard Mode</b> and <b>Compatibility Mode</b> . If your SIP server's signal port number is non-standard, you can check the box <b>Define custom signal ports</b> and input the port numbers to the text boxes.
<b>IPsec NAT-T</b>	This field is for enabling the support of IPsec NAT-T passthrough. UDP ports 500, 4500, and 10000 are monitored by default. You may add more custom data ports that your IPsec system uses by checking <b>Define custom ports</b> . If the VPN contains IPsec site-to-site VPN traffic, check <b>Route IPsec Site-to-Site VPN</b> and choose the WAN connection to route the traffic to.

## Grouped Networks

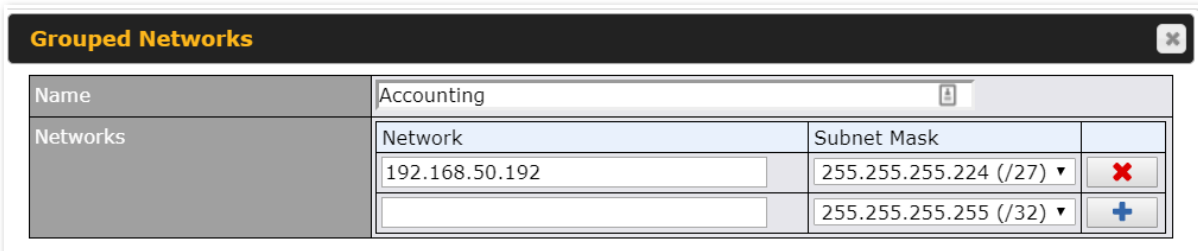


Using "Grouped Networks" you can group and name a range of IP addresses, which can then be used to define firewall rules or outbound policies.

Start by clicking on "add group" then fill in the appropriate fields.

In this example we'll create a group "accounting"

Click save when you have finished adding the required networks.



The grouped network "accounting" can now be used to configure a group policy or firewall rule.

## SIM Toolkit

The SIM Toolkit, accessible via **Advanced>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.

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	<input type="text" value="*138#"/> <input type="button" value="Submit"/>
Receive SMS	<input type="button" value="Get"/>



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

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

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

Received SMS		
May 27 20:02	<p><b>PCX</b>            As of May 27th            Account Balance: \$ 0.00            Amount Unbilled            Voice Calls: 0 minutes            Video Calls: 0 minutes            SMS (Roaming): 0            SMS (Within Network): 0            MMS (Roaming): 0            MMS (Within Network): 0            Data Usage: 7384KB            (For reference only, please refer to bill)</p>	<input type="button" value="✘"/>
Aug 8 , 2013 14:51	<p><b>PCX</b>            iPhone &amp; Android users need to make sure "PCX" is entered as the APN under "Settings" &gt; "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)</p>	<input type="button" value="✘"/>

## SMS

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

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



# AP

Use the controls on the AP tab to set the wireless SSID and AP settings.

## Wireless SSID

Wireless network settings, including the name of the network (SSID) and security policy can be defined and managed in this section.

SSID	Security Policy
	WPA2 - Personal

[New SSID](#)

Click **Add** to create a new network profile, or click the existing network profile to modify its settings.

SSID	<input type="text"/>
Enable	Always on ▼
VLAN	Untagged LAN ▼
Broadcast SSID	<input checked="" type="checkbox"/>
Data Rate	<input checked="" type="radio"/> Auto <input type="radio"/> Fixed
Multicast Filter	<input type="checkbox"/>
Multicast Rate	MCS16/MCS8/MCS0/6M ▼
IGMP Snooping	<input type="checkbox"/>
Layer 2 Isolation	<input type="checkbox"/>
Maximum number of clients	2.4 GHz: <input type="text" value="0"/> 5 GHz: <input type="text" value="0"/> (0: Unlimited)
Band Steering	<input type="button" value="?"/> Disable ▼

SSID Settings	
<b>SSID</b>	This setting specifies the Router SSID that Wi-Fi clients will see when scanning.

<b>Enable</b>	Click the drop-down menu to choose predefined schedules as your starting point. Please note that upon selection, previous changes on the schedule map will be deleted.
<b>VLAN</b>	Some service providers require the router to enable VLAN tagging for Internet traffic. If it is required by your service provider, you can enable this field and enter the VLAN ID that the provider requires.
<b>Broadcast SSID</b>	This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. Broadcast SSID is enabled by default.
<b>Data Rate</b>	Select Auto to allow your access point to set the data rate automatically, or select Fixed and choose a rate from the drop-down menu. Click the MCS Index link to display a reference table containing MCS and matching HT20 and HT40 values.
<b>Multicast Filter</b>	This setting enables the filtering of multicast network traffic to the wireless SSID.
<b>Multicast Rate</b>	This setting specifies the transmit rate to be used for sending multicast network traffic.
<b>IGMP Snooping</b>	To allow your access point to convert multicast traffic to unicast traffic for associated clients, select this option.
<b>Layer 2 Isolation</b>	<p>Layer 2 refers to the second layer in the ISO Open System Interconnect model.</p> <p>When this option is enabled, it will block communication between Wi-Fi clients within the same VLAN, SSID or subnet, as a security measure that best suits a company Guest/Visitor Wi-Fi access scenario.</p> <p>Do refer to this link  <a href="https://forum.peplink.com/t/lan-isolation-with-balance30-and-ap-one-ac-mini-help-needed/3914/3">https://forum.peplink.com/t/lan-isolation-with-balance30-and-ap-one-ac-mini-help-needed/3914/3</a>  for visual illustration of the feature. By default, the setting is disabled.</p>
<b>Maximum number of Clients</b>	Enter the maximum number of clients that can simultaneously connect to your SSID, or enter 0 to allow unlimited Wi-Fi clients.
<b>Band Steering</b>	<p>To reduce 2.4 GHz band overcrowding, AP with band steering steers clients capable of 5 GHz operation to 5 GHz frequency.</p> <p><b>Force</b> - Clients capable of 5 GHz operation are only offered with 5 GHz frequency.</p> <p><b>Prefer</b> - Clients capable of 5 GHz operation are encouraged to associate with 5 GHz frequency. If the clients insist to attempt on 2.4 GHz frequency, 2.4 GHz frequency will be offered.</p> <p>Default: <b>Disable</b></p>

Security Settings	
Security Policy	WPA2 - Personal ▼
Encryption	AES:CCMP
Shared Key <span style="float: right;">?</span>	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters
Management Frame Protection	Default (Disabled) ▼
Fast Transition <span style="float: right;">?</span>	<input type="checkbox"/>

Security Settings	
Security Policy	WPA2 - Enterprise ▼
Encryption	AES:CCMP
802.1X Version	<input checked="" type="radio"/> V1 <input type="radio"/> V2
Management Frame Protection	Default (Disabled) ▼
Fast Transition <span style="float: right;">?</span>	<input type="checkbox"/>

Security Settings	
<b>Security Policy</b>	<p>This setting configures the wireless authentication and encryption methods. Available options :</p> <ul style="list-style-type: none"> <li>• Open (No Encryption)</li> <li>• WPA3 -Personal (AES:CCMP)</li> <li>• WPA2/WPA3 -Personal (AES:CCMP)</li> <li>• WPA2 -Personal (AES:CCMP)</li> <li>• WPA2 – Enterprise</li> <li>• WPA/WPA2 - Personal (TKIP/AES: CCMP)</li> <li>• WPA/WPA2 – Enterprise</li> </ul> <p>When WPA/WPA2 - Enterprise is selected, RADIUS-based 802.1 x authentication is enabled. Under this configuration, the Shared Key option does not apply and is therefore hidden. 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.</p> <p>When WPA/WPA2 - Personal is selected, 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.</p> <p><b>NOTE:</b> 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.</p>
<b>Management Frame Protection</b>	<p>This feature protects stations against forged management frames spoofed from other devices. Frames that are protected include Disassociation, Deauthentication and QoS Action.</p>

Security Settings	
<b>Fast Transition</b>	When WPA2/WPA3 - (Personal / Enterprise) is selected, the Fast Transition option is the standard defined for 801.11r to reduce the association process when it roams from one Access Point to another Access Point.

Access Control Settings	
Restricted Mode	Deny all except listed ▼
MAC Address List <span style="float: right;">?</span>	<input type="text"/>

Access Control	
<b>Restricted Mode</b>	The settings allow administrators to control access using Mac address filtering. Available options are <b>None</b> , <b>Deny all except listed</b> , <b>Accept all except</b> and <b>RADIUS MAC Authentication</b> .
<b>MAC Address List</b>	Connections originating from the MAC addresses in this list will be either denied or accepted based on the option selected in the previous field.

RADIUS Settings	Primary Server	Secondary Server
	You may click <a href="#">here</a> to define RADIUS Server Authentication profile, or you may go to <a href="#">RADIUS Server</a> page to define multiple profiles	
Authentication Host	<input type="text"/>	<input type="text"/>
Authentication Port	1812	1812
Authentication Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters
	You may click <a href="#">here</a> to define RADIUS Server Accounting profile, or you may go to <a href="#">RADIUS Server</a> page to define multiple profiles	
Accounting Host	<input type="text"/>	<input type="text"/>
Accounting Port	1813	1813
Accounting Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters
NAS-Identifier	Device Name ▼	

## RADIUS Server

<b>Host</b>	Specifies the IP address or hostname of the RADIUS server host.
<b>Secret</b>	This field is for entering the secret key for communicating to the RADIUS server.
<b>Authentication Port</b>	This setting specifies the UDP destination port for authentication requests. By default, the port number is 1812.
<b>Accounting Port</b>	This setting specifies the UDP destination port for accounting requests. By default, the port number is 1813.
<b>NAS-Identifier</b>	The setting allows administrators to identify the client to the RADIUS server. Available options are <b>Device Name</b> , <b>LAN Mac Address</b> , <b>Device Serial Number</b> and <b>Custom Value</b> .

Guest Protect			
Block All Private IP	<input type="checkbox"/>		
Custom Subnet	Network	Subnet Mask	
	<input type="text"/>	255.255.255.0 (/24) ▼	<input type="button" value="+"/>
Block Exception	Network	Subnet Mask	
	<input type="text"/>	255.255.255.0 (/24) ▼	<input type="button" value="+"/>

RADIUS Server	
<b>Block All Private IP</b>	Check this box to deny all connection attempts by private IP addresses.
<b>Custom Subnet</b>	To create a custom subnet for guest access, enter the IP address and choose a subnet mask from the drop-down menu.
<b>Block Exception</b>	To block access from a particular subnet, enter the IP address and choose a subnet mask from the drop-down menu.

Firewall Settings			
Firewall Mode	Lockdown - Block all except... ▼		
Firewall Exceptions	Disable		
	Flexible - Allow all except... Lockdown - Block all except...		
	<table border="1"> <thead> <tr> <th>Item</th> </tr> </thead> <tbody> <tr> <td><input type="button" value="New Rule"/></td> </tr> </tbody> </table>	Item	<input type="button" value="New Rule"/>
Item			
<input type="button" value="New Rule"/>			

Firewall Settings	
<b>Firewall Mode</b>	The settings allow administrator to control access to the SSID based on Firewall Rules. Available options are <b>Disable, Lockdown - Block all except...</b> and <b>Flexible - Allow all except...</b>
<b>Firewall Exceptions</b>	Create Firewall Rules based on <b>Port, IP Network, MAC address</b> or <b>Domain Name</b>



## Settings

Navigating to **AP>Settings** displays a screen similar to the one shown below:

Wi-Fi Radio Settings	
Operating Country	United States ▼
SSID	2.4GHz 5GHz <input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>

Wi-Fi AP Settings	
Protocol	802.11ng ▼ 802.11ac ▼
Channel Width	20/40 MHz ▼ 80 MHz ▼
Channel	Auto ▼ <input type="button" value="Edit"/> Channels: 1 2 3 4 5 6 7 8 9 10 11
Auto Channel Update	Daily at <input type="button" value="Clear"/> <input type="button" value="All"/> <input type="checkbox"/> 00:00 <input type="checkbox"/> 01:00 <input type="checkbox"/> 02:00 <input checked="" type="checkbox"/> 03:00 <input type="checkbox"/> 04:00 <input type="checkbox"/> 05:00 <input type="checkbox"/> 06:00 <input type="checkbox"/> 07:00 <input type="checkbox"/> 08:00 <input type="checkbox"/> 09:00 <input type="checkbox"/> 10:00 <input type="checkbox"/> 11:00 <input type="checkbox"/> 12:00 <input type="checkbox"/> 13:00 <input type="checkbox"/> 14:00 <input type="checkbox"/> 15:00 <input type="checkbox"/> 16:00 <input type="checkbox"/> 17:00 <input type="checkbox"/> 18:00 <input type="checkbox"/> 19:00 <input type="checkbox"/> 20:00 <input type="checkbox"/> 21:00 <input type="checkbox"/> 22:00 <input type="checkbox"/> 23:00 <input checked="" type="checkbox"/> Wait until no active client associated
Output Power	Max ▼ <input type="checkbox"/> Boost
Client Signal Strength Threshold	0 -95 dBm (0: Unlimited)
Maximum number of clients	0 (0: Unlimited)
Beacon Rate	<input type="button" value="?"/> 1 Mbps ▼
Beacon Interval	<input type="button" value="?"/> 100 ms ▼
DTIM	<input type="button" value="?"/> 1 <input type="button" value="Default"/>
RTS Threshold	0 <input type="button" value="Default"/>
Fragmentation Threshold	0 (0: Disable) <input type="button" value="Default"/>
Distance / Time Converter	<input type="range"/> 4050 m Note: Input distance for recommended values
Slot Time	<input type="button" value="?"/> <input type="radio"/> Auto <input checked="" type="radio"/> Custom 9 <input type="button" value="Default"/> $\mu$ s
ACK Timeout	<input type="button" value="?"/> 48 <input type="button" value="Default"/> $\mu$ s
Frame Aggregation	<input type="checkbox"/>

Wi-Fi Radio Settings	
<b>Operating Country</b>	This option sets the country whose regulations the Pepwave router follows.
<b>SSID</b>	Select if an SSID is broadcasting on 2.4 Ghz, 5 Ghz or both bands

Wi-Fi AP Settings	
<b>Protocol</b>	This option allows you to specify which client association requests will be accepted. By default, <b>802.11ng</b> is selected.
<b>Channel Width</b>	Settings for 2.4 GHz AP and 5GHz AP can be configured here: <b>2.4 GHz: 40 MHz, 20/40 MHz and 20 MHz</b> are available. The default setting is <b>20/40 MHz</b> , which allows both widths to be used simultaneously. <b>80 MHz , 40 Mhz, 20 Mhz, and(20/40 MH)</b> are available. The default setting is <b>80 MHz</b> . Note: 802.11ng and 802.11na are not part of the 802.11 standard. It is simply a notation for indicating 802.11n use on the 2.4-GHz band (11ng) or 802.11n use on the 5-GHz band (11na).
<b>Channel</b>	This option allows you to select which 802.11 RF channel will be used.
<b>Auto Channel Update</b>	Indicate the time of day for updating the automatic channel selection.
<b>Output Power</b>	This option is for specifying the transmission output power for the Wi-Fi AP. There are 4 relative power levels available – <b>Max, High, Mid, and Low</b> . The actual output power will be bound by the regulatory limits of the selected country.
<b>Client Signal Strength Threshold<sup>A</sup></b>	This field determines that maximum signal strength each individual client will receive. The measurement unit is dBm.
<b>Maximum number of clients</b>	Enter the maximum number of clients that can simultaneously connect to the wireless network or enter 0 to allow an unlimited number of connections.
<b>Beacon Rate<sup>A</sup></b>	This option is for setting the transmit bit rate for sending a beacon. By default, <b>1Mbps</b> is selected.
<b>Beacon Interval<sup>A</sup></b>	This option is for setting the time interval between each beacon. By default, <b>100ms</b> is selected.
<b>DTIM<sup>A</sup></b>	This field allows you to set the frequency for the beacon to include a delivery traffic indication message. The interval is measured in milliseconds. The default value is set to <b>1 ms</b> .
<b>RTS Threshold</b>	Set the minimum packet size for your access point to send an RTS using the RTS/CTS handshake. Setting 0 disables this feature.
<b>Fragmentation Threshold<sup>A</sup></b>	Determines the maximum size (in bytes) that each packet fragment will be broken down into. Set 0 to disable fragmentation.

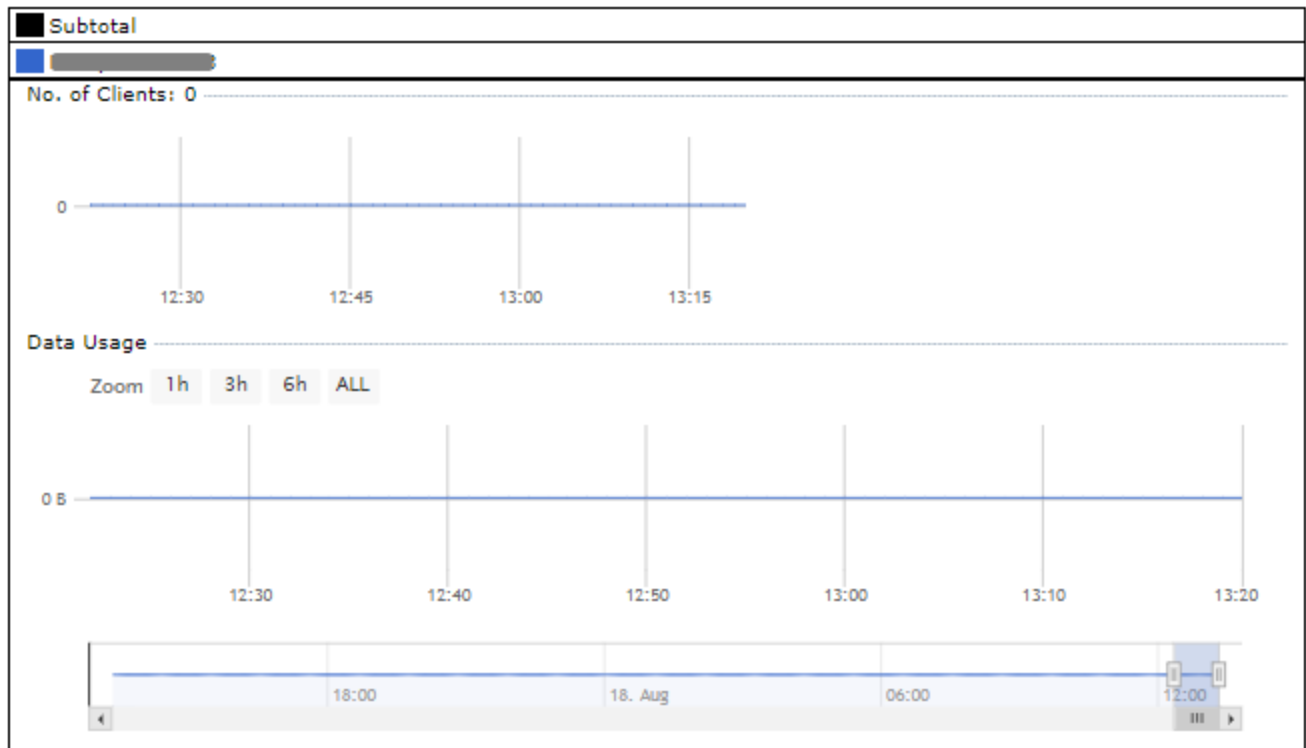
<b>Distance/Time Converter<sup>A</sup></b>	Select the distance you want your Wi-Fi to cover in order to adjust the below parameters. Default values are recommended.
<b>Slot Time<sup>A</sup></b>	This field is for specifying the wait time before the Surf SOHO transmits a packet. By default, this field is set to <b>9 μs</b> .
<b>ACK Timeout<sup>A</sup></b>	This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to <b>48 μs</b> .
<b>Frame Aggregation<sup>A</sup></b>	This option allows you to enable frame aggregation to increase transmission throughput.

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





## AP > Status

### Access Point

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




AP Status	
Name	IP Address
[Redacted]	(Local)

Access Point	
<b>AP Name/Serial Number</b>	This field allows you to quickly find your device if you know its name or serial number. Fill in the field to begin searching. Partial names and serial numbers are supported.
<b>AP Status</b>	<p>This table shows the detailed information of each AP, including channel, number of clients, upload traffic, and download traffic. On the right-hand side of the table, you will see the following icons:</p> <p>  </p> <p>Clicking on the  icon displays a table with a list of clients and their usage.</p>

Client List						
MAC Address	IP Address	Type	Signal	SSID	Upload	Download
80:56:f2:98:75:ff	10.9.2.7	802.11ng	Excellent (37)	Balance	66.26 MB	36.26 MB
c4:6a:b7:bf:d7:15	10.9.2.123	802.11ng	Excellent (42)	Balance	6.65 MB	2.26 MB
70:56:81:1d:87:f3	10.9.2.102	802.11ng	Good (23)	Balance	1.86 MB	606.63 KB
e0:63:e5:83:45:c8	10.9.2.101	802.11ng	Excellent (39)	Balance	3.42 MB	474.52 KB
18:00:2d:3d:4e:7f	10.9.2.66	802.11ng	Excellent (25)	Balance	640.29 KB	443.57 KB
14:5a:05:80:4f:40	10.9.2.76	802.11ng	Excellent (29)	Balance	2.24 KB	3.67 KB
00:1a:dd:c5:4e:24	10.8.9.84	802.11ng	Excellent (29)	Wireless	9.86 MB	9.76 MB
00:1a:dd:bb:29:ec	10.8.9.73	802.11ng	Excellent (25)	Wireless	9.36 MB	11.14 MB
40:b0:fa:c3:26:2c	10.8.9.18	802.11ng	Good (23)	Wireless	118.05 MB	7.92 MB
e4:25:e7:8a:d3:12	10.10.11.23	802.11ng	Excellent (35)	Marketing	74.78 MB	4.58 MB
04:f7:e4:ef:68:05	10.10.11.71	802.11ng	Poor (12)	Marketing	84.84 KB	119.32 KB

Close

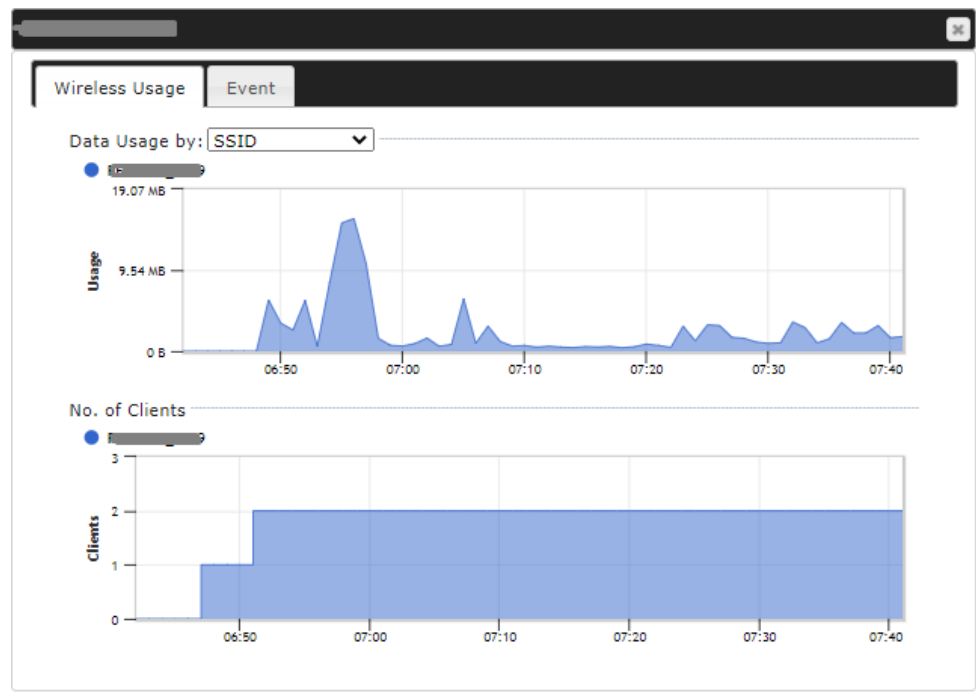
Clicking on the  icon allows you to configure the AP device's details.

AP Details	
Serial Number	1
MAC Address	A8:C0:EA:05:FC:80
Product Name	Pepwave Surf SOHO MK3
Firmware Version	8.1.3 build 5030
SSID List	2.4 GHz: PEPWAVE_ (A8:C0:EA:05:FC:85) PEPWAVE_ (A8:C0:EA:05:FC:85) 5 GHz: PEPWAVE_ (A8:C0:EA:05:FC:89) PEPWAVE_ (A8:C0:EA:05:FC:89)
Current Channel	2.4 GHz: 6 5 GHz: 36
Current Output Power	2.4 GHz: 20 dBm 5 GHz: 18 dBm

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) that this client will follow, as well as the channels that the client will broadcast on.

Clicking on the  icon displays usage in the form of graphs.



Close

Click on 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.

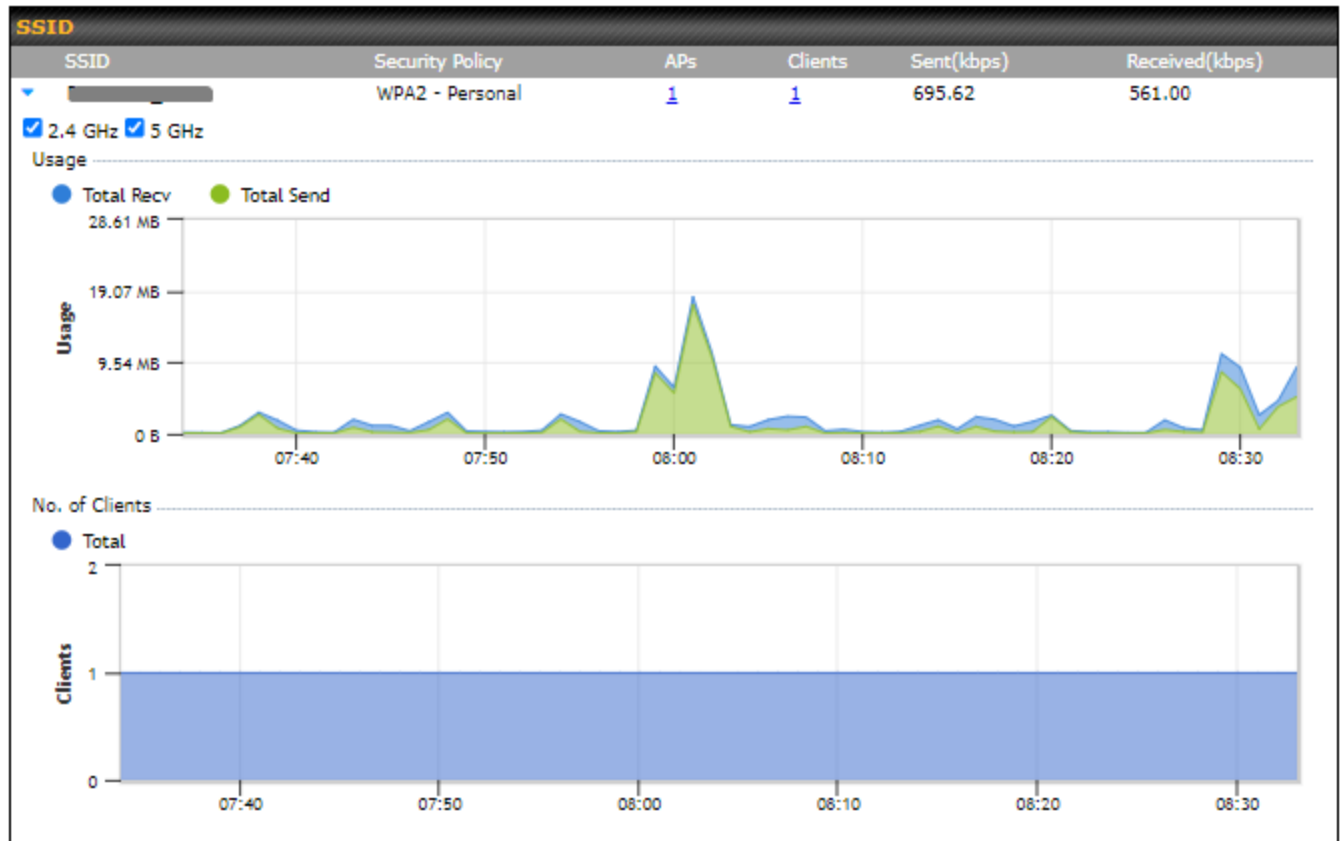
The figure shows the 'Event Log' tab with a list of events. The table contains the following data:

Timestamp	Event Description	Frequency
Aug 18 13:54:41	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with [redacted] (2.4 GHz)	2.4 GHz
Aug 18 13:54:41	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) disassociated from [redacted] (2.4 GHz)	2.4 GHz
Aug 18 13:52:14	Client G... (B2:AD:FF:A4:3F:FF) associated with [redacted] (2.4 GHz)	2.4 GHz
Aug 18 13:48:58	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with [redacted] (2.4 GHz)	2.4 GHz
Aug 18 12:12:33	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with [redacted] (5 GHz)	5 GHz
Aug 18 11:25:32	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) disassociated from [redacted] (2.4 GHz)	2.4 GHz
Aug 17 15:14:28	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with [redacted] (5 GHz)	5 GHz
Aug 17 15:14:27	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) disassociated from [redacted] (5 GHz)	5 GHz
Aug 17 15:14:11	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with [redacted] (5 GHz)	5 GHz
Aug 17 15:13:35	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) disassociated from [redacted] (5 GHz)	5 GHz
Aug 17 11:51:13	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with [redacted] (5 GHz)	5 GHz
Aug 17 11:51:13	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) disassociated from [redacted] (2.4 GHz)	2.4 GHz
Aug 17 09:00:05	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with [redacted] (2.4 GHz)	2.4 GHz
Aug 17 09:00:04	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) disassociated from [redacted] (2.4 GHz)	2.4 GHz
Aug 17 09:00:04	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with [redacted] (2.4 GHz)	2.4 GHz
Aug 16 09:42:15	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with [redacted] (2.4 GHz)	2.4 GHz
Aug 16 09:42:15	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) disassociated from [redacted] (5 GHz)	5 GHz
Aug 16 09:07:18	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with [redacted] (5 GHz)	5 GHz
Aug 13 09:03:53	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with [redacted] (5 GHz)	5 GHz
Aug 12 18:28:44	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) disassociated from [redacted] (5 GHz)	5 GHz

Close

## Wireless SSID

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



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

## Wireless Client

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

Search Filter	
Search Key	<input type="text" value="Client MAC Address / SSID"/>
Maximum Result (1-256)	<input type="text" value="50"/>
Show Associated Clients Only	<input type="checkbox"/>
Search Result	

Wireless Clients							
Name / MAC Address ▲	IP Address	Type	RSSI (dBm)	SSID	AP	Duration	
██████████/...	██████████	802.11ac	-54	██████████	██████████	02:26:42	☆   📊
B2:AD:FF:A4:3F:FF	-	802.11ng	-	-	-	-	☆   📊

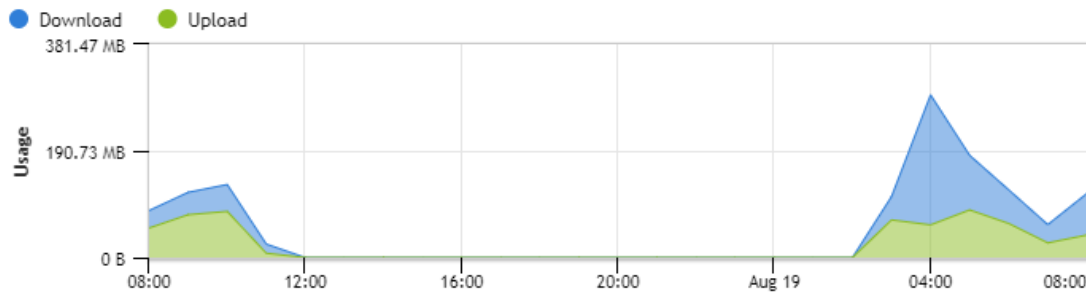
Top 10 Clients of last hour (Updated at 08:00)			
Client	Upload	Download	
██████████	26.29 MB	32.64 MB	☆   📊

Here, you will be able to see your network's heaviest users as well as search for specific users. Clicking on the ☆ icon bookmarks the specific user, and clicking on the 📊 icon displays additional details about the user.



Client C8:B2:9B:63:C2:CA

Information	
Status	Associated
Client	[REDACTED]
Access Point	[REDACTED]
SSID	[REDACTED]
IP Address	[REDACTED]
Duration	02:29:38
Usage (Download / Upload)	134.83 MB / 110.36 MB
RSSI	-55 dBm
Rate (Download / Upload)	780M / 702M
Type	802.11ac



SSID	AP	From	To	Download	Upload
[REDACTED]	[REDACTED]	Aug 19 06:13:53	-	134.81 MB	110.31 MB
[REDACTED]	[REDACTED]	Aug 19 03:29:59	Aug 19 06:13:53	403.89 MB	228.41 MB
[REDACTED]	[REDACTED]	Aug 19 03:29:36	Aug 19 03:29:55	287.5 KB	289.8 KB
[REDACTED]	[REDACTED]	Aug 19 03:29:20	Aug 19 03:29:36	783.5 KB	1.18 MB
[REDACTED]	[REDACTED]	Aug 18 06:54:41	Aug 18 11:09:59	184.06 MB	291.00 MB
[REDACTED]	[REDACTED]	Aug 18 06:48:58	Aug 18 06:54:41	11.06 MB	6.99 MB
[REDACTED]	[REDACTED]	Aug 18 05:12:33	-	-	-
[REDACTED]	[REDACTED]	Aug 18 05:12:33	-	87.37 MB	118.64 MB
[REDACTED]	[REDACTED]	Aug 18 02:53:47	Aug 18 04:25:32	238.13 MB	145.16 MB

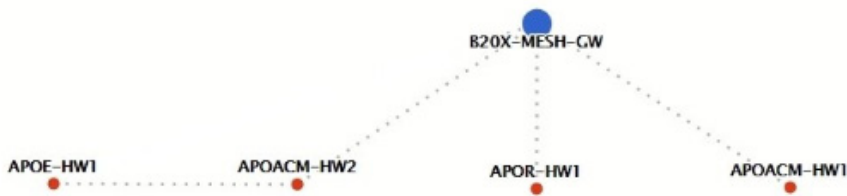
Close

## Mesh / WDS

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

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

Network Graph



## Nearby Device

A list of nearby devices can be accessed by navigating to **AP > Nearby Device**.

Search Filter	
Search Key	<input type="text" value="MAC Address / SSID"/>
Type	<input type="text" value="All"/>
Maximum Result (1-999)	<input type="text" value="200"/>
Time	From <input type="text"/> hh:mm to <input type="text"/> hh:mm
<input type="button" value="Search"/>	

Nearby Devices							
Mark	Type	MAC Address	SSID	Channel	Encryption	Last Seen	Mark as
	Station Probe	54:27:1E:71:24:3D	-	6		2 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Station Probe	F8:A7:63:99:1A:4B	-	6		2 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Station Probe	B4:69:21:67:77:E9	-	6		3 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Station Probe	F4:D1:08:C4:49:B0	-	36		3 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Station Probe	08:F8:BC:63:B4:28	-	6		4 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Station Probe	44:1C:A8:9C:2E:3B	-	6		5 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Station Probe	E8:5A:8B:F7:EF:9D	-	36		5 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Station Probe	C4:FE:5B:AC:44:9B	-	6		6 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Station Probe	80:30:49:3E:35:A1	-	36		7 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Station Probe	40:EC:99:5E:83:1E	-	6		8 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Station Probe	50:3D:C6:8C:2C:DA	-	36		9 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Station Probe	E4:F0:42:2E:FE:7A	-	36		10 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Station Probe	38:F9:D3:99:BE:5D	-	6		13 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Station Probe	94:90:34:FE:9E:61	-	6		16 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Station Probe	88:46:04:51:9B:31	-	6		17 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Station Probe	F4:60:E2:D8:B1:14	-	6		20 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Station Probe	B0:89:00:24:93:ED	-	6		23 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Station Probe	C8:F6:50:E2:03:00	-	6		26 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Station Probe	A4:77:33:57:A6:E2	-	6		30 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>
	Station Probe	68:3E:26:FC:F9:B3	-	6		32 minutes ago	<input checked="" type="checkbox"/> <input type="checkbox"/>

[Prev](#) 1-20  (79) [Next](#)

### Suspected Rogue Devices

Hovering over a device's MAC address will result in a popup with information on how the device was detected. Clicking on the   icons will mark the device and move them to the table of identified devices.

## Event Log

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

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

Event Log		<input checked="" type="checkbox"/> Auto refresh
Aug 23 11:24:23	Client LAPTOP-... associated with ...	
Aug 23 10:16:08	Client LAPTOP-... disassociated from ...	
Aug 23 09:40:33	Client LAPTOP-... associated with ...	
Aug 20 17:23:07	Client LAPTOP-... associated with ...	
Aug 20 17:23:07	Client LAPTOP-... disassociated from ...	
Aug 20 09:02:40	Client LAPTOP-T... associated with ...	
Aug 19 18:38:02	Client LAPTOP-T... associated with ...	
Aug 19 18:37:44	Client LAPTOP-... disassociated from ...	
Aug 19 18:19:46	Client LAPTOP-T... associated with ...	
Aug 19 17:52:37	Client LAPTOP-... disassociated from ...	
Aug 19 17:51:35	Client LAPTOP-... associated with ...	
Aug 19 17:43:05	Client LAPTOP-... disassociated from ...	
Aug 19 17:42:30	Client LAPTOP-T... associated with ...	
Aug 19 17:37:41	Client LAPTOP-... disassociated from ...	
Aug 19 17:36:37	Client LAPTOP-... associated with ...	
Aug 19 17:19:10	Client LAPTOP-T... disassociated from ...	
Aug 19 17:15:21	Client LAPTOP-... associated with ...	
Aug 19 17:13:16	Client LAPTOP-... disassociated from ...	
Aug 19 13:13:53	Client LAPTOP-T... associated with ...	
Aug 19 13:13:53	Client LAPTOP-T... disassociated from ...	

[More...](#)

### Events

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

## System Settings

The options on the System tab control login and security settings, firmware upgrades, SNMP settings, and other settings.

## Admin Security

The **Admin Security** section allows you to set up your access point's name, password, security settings, and other options

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

<b>Confirm User Password</b>	This field allows you to verify and confirm the new user password.																						
<b>Web Session Timeout</b>	This field specifies the number of hours and minutes that a web session can remain idle before the Pepwave router terminates its access to the web admin interface. By default, it is set to <b>4 hours</b> .																						
<b>Authentication Method</b>	<p>With this external authentication is selected, the web admin will authenticate using the corresponding external server. Authenticated users are treated as either "admin" with full read-write permission or "user" with read-only access. Local admin and user accounts will be disabled. However, when the device is not able to communicate with the external server, local accounts are enabled to allow emergency access. By default, it is set to Local Account.</p> <p>Available options:</p> <ul style="list-style-type: none"> <li>• Local Account</li> <li>• RADIUS</li> </ul> <table border="1" data-bbox="454 735 1567 1228"> <tr> <td>Authentication Method</td> <td><input type="radio"/> Local Account <input checked="" type="radio"/> RADIUS <input type="radio"/> TACACS+</td> </tr> <tr> <td>Authentication Protocol</td> <td>MS-CHAP v2 ▼</td> </tr> <tr> <td colspan="2">You may click <a href="#">here</a> to define RADIUS Server Authentication profile, or you may go to <a href="#">RADIUS Server</a> page to define multiple profiles</td> </tr> <tr> <td>Authentication Host</td> <td><input type="text"/></td> </tr> <tr> <td>Authentication Port</td> <td>1812</td> </tr> <tr> <td>Authentication Secret</td> <td><input type="text"/> <input checked="" type="checkbox"/> Hide Characters</td> </tr> <tr> <td colspan="2">You may click <a href="#">here</a> to define RADIUS Server Accounting profile, or you may go to <a href="#">RADIUS Server</a> page to define multiple profiles</td> </tr> <tr> <td>Accounting Host</td> <td><input type="text"/></td> </tr> <tr> <td>Accounting Port</td> <td>1813</td> </tr> <tr> <td>Accounting Secret</td> <td><input type="text"/> <input checked="" type="checkbox"/> Hide Characters</td> </tr> <tr> <td>Authentication Timeout</td> <td>3 seconds</td> </tr> </table>	Authentication Method	<input type="radio"/> Local Account <input checked="" type="radio"/> RADIUS <input type="radio"/> TACACS+	Authentication Protocol	MS-CHAP v2 ▼	You may click <a href="#">here</a> to define RADIUS Server Authentication profile, or you may go to <a href="#">RADIUS Server</a> page to define multiple profiles		Authentication Host	<input type="text"/>	Authentication Port	1812	Authentication Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters	You may click <a href="#">here</a> to define RADIUS Server Accounting profile, or you may go to <a href="#">RADIUS Server</a> page to define multiple profiles		Accounting Host	<input type="text"/>	Accounting Port	1813	Accounting Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters	Authentication Timeout	3 seconds
Authentication Method	<input type="radio"/> Local Account <input checked="" type="radio"/> RADIUS <input type="radio"/> TACACS+																						
Authentication Protocol	MS-CHAP v2 ▼																						
You may click <a href="#">here</a> to define RADIUS Server Authentication profile, or you may go to <a href="#">RADIUS Server</a> page to define multiple profiles																							
Authentication Host	<input type="text"/>																						
Authentication Port	1812																						
Authentication Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters																						
You may click <a href="#">here</a> to define RADIUS Server Accounting profile, or you may go to <a href="#">RADIUS Server</a> page to define multiple profiles																							
Accounting Host	<input type="text"/>																						
Accounting Port	1813																						
Accounting Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters																						
Authentication Timeout	3 seconds																						
<b>Authentication Protocol</b>	This specifies the authentication protocol used. Available options are <b>MS-CHAP v2</b> and <b>PAP</b> .																						
<b>Authentication Host</b>	This specifies the IP address or hostname of the RADIUS server host.																						
<b>Authentication Port</b>	This setting specifies the UDP destination port for authentication requests.																						
<b>Authentication Secret</b>	This field is for entering the secret key for accessing the RADIUS server.																						
<b>Accounting Host</b>	This specifies the IP address or hostname of the RADIUS server host.																						
<b>Accounting Port</b>	This setting specifies the UDP destination port for accounting requests.																						
<b>Accounting Secret</b>	This field is for entering the secret key for accessing the accounting server.																						
<b>Authentication</b>	This option specifies the time value for authentication timeout																						

<p><b>Timeout</b></p> <ul style="list-style-type: none"> <li>TACACS+</li> </ul> <table border="1"> <tr> <td>Authentication Method</td> <td><input type="radio"/> Local Account <input type="radio"/> RADIUS <input checked="" type="radio"/> TACACS+</td> </tr> <tr> <td>TACACS+ Server</td> <td><input type="text"/></td> </tr> <tr> <td>TACACS+ Server Secret</td> <td><input type="text"/> <input checked="" type="checkbox"/> Hide Characters</td> </tr> <tr> <td>TACACS+ Server Timeout</td> <td><input type="text" value="3"/> seconds</td> </tr> </table>		Authentication Method	<input type="radio"/> Local Account <input type="radio"/> RADIUS <input checked="" type="radio"/> TACACS+	TACACS+ Server	<input type="text"/>	TACACS+ Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters	TACACS+ Server Timeout	<input type="text" value="3"/> seconds
Authentication Method	<input type="radio"/> Local Account <input type="radio"/> RADIUS <input checked="" type="radio"/> TACACS+								
TACACS+ Server	<input type="text"/>								
TACACS+ Server Secret	<input type="text"/> <input checked="" type="checkbox"/> Hide Characters								
TACACS+ Server Timeout	<input type="text" value="3"/> seconds								
<b>TACACS+ Server</b>	This specifies the access address of the external TACACS+ server.								
<b>TACACS+ Server Secret</b>	This field is for entering the secret key for accessing the RADIUS server.								
<b>TACACS+ Server Timeout</b>	This option specifies the time value for TACACS+ timeout								
<b>CLI SSH &amp; Console</b>	The CLI (command line interface) can be accessed via SSH. This field enables CLI support. For additional information regarding CLI, please refer to <b>Section 30.5</b> .								
<b>CLI SSH Access</b>	This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only.								
<b>CLI SSH Port</b>	This field determines the port on which clients can access CLI SSH.								
<b>CLI SSH Access Public Key</b>	This field is for entering the Public Key for Admin Users and Read-only Users to access CLI SSH.								
<b>Security</b>	<p>This option is for specifying the protocol(s) through which the web admin interface can be accessed:</p> <ul style="list-style-type: none"> <li>HTTP</li> <li>HTTPS</li> <li>HTTP/HTTPS</li> </ul> <p>HTTP to HTTPS redirection is enabled by default to force HTTPS access to the web admin interface.</p>								
<b>Web Admin Access</b>	<p>This option is for specifying the network interfaces through which the web admin interface can be accessed:</p> <ul style="list-style-type: none"> <li>LAN only</li> <li>LAN/WAN</li> </ul> <p>If LAN/WAN is chosen, the <b>WAN Connection Access Settings</b> form will be displayed.</p>								
<b>Web Admin Port</b>	This field is for specifying the port number on which the web admin interface can be accessed.								

## Firmware

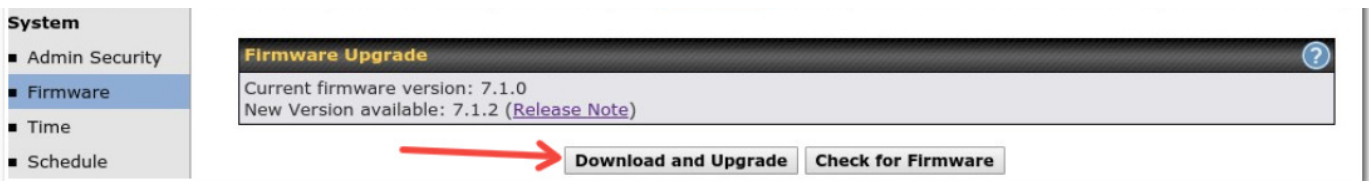
Upgrading firmware can be done in one of three ways.

Using the router's interface to automatically check for an update, using the router's interface to manually upgrade the firmware, or using InControl2 to push an upgrade to a router.

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

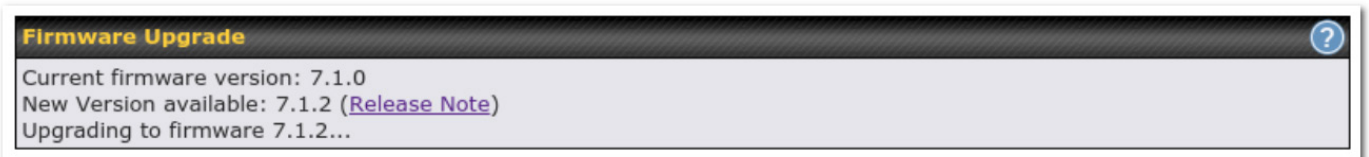


If an update is found the buttons will change to allow you to **Download and Update** the firmware.



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

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



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

### Firmware Upgrade

It may take up to 8 minutes.



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

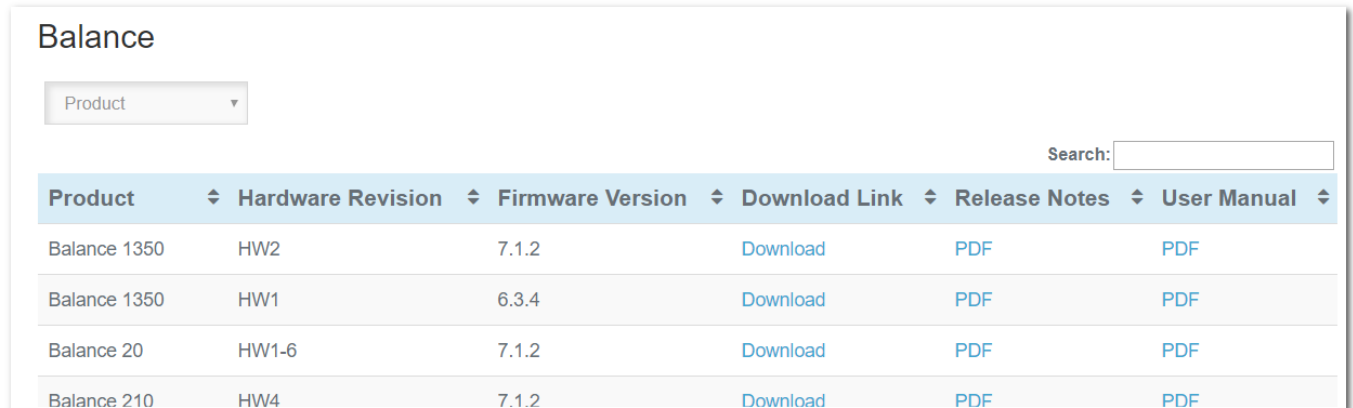
### Web admin interface : install updates manually

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



recommended or required for a couple of reasons.

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

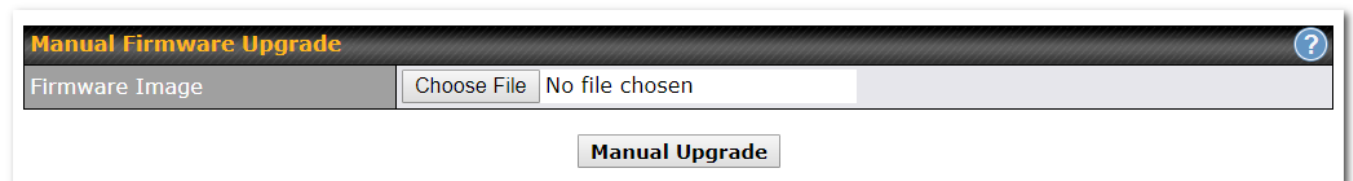


Product	Hardware Revision	Firmware Version	Download Link	Release Notes	User Manual
Balance 1350	HW2	7.1.2	<a href="#">Download</a>	<a href="#">PDF</a>	<a href="#">PDF</a>
Balance 1350	HW1	6.3.4	<a href="#">Download</a>	<a href="#">PDF</a>	<a href="#">PDF</a>
Balance 20	HW1-6	7.1.2	<a href="#">Download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

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

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

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



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

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

## The InControl method

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

## Time

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

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

Save

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

## Schedule

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

Name	Time	Used by
No schedule profile defined		
<span>New Schedule</span>		

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

**Edit schedule profile** ✕

**Schedule Settings**

Enable	<input checked="" type="checkbox"/> The schedule function of those associated features will be lost if profile is disabled.
Name	<input type="text"/>
Schedule	Always on ▾
Used by	


**Schedule Map**

	Midnight	4am	8am	Noon	4pm	8pm
Sunday	[Grid of 24 green checkmarks]					
Monday	[Grid of 24 green checkmarks]					
Tuesday	[Grid of 24 green checkmarks]					
Wednesday	[Grid of 24 green checkmarks]					
Thursday	[Grid of 24 green checkmarks]					
Friday	[Grid of 24 green checkmarks]					
Saturday	[Grid of 24 green checkmarks]					

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

## Email Notification

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

Email Notification Setup <span style="float: right;">?</span>	
Email Notification	<input checked="" type="checkbox"/> Enable
SMTP Server	smtp.mycompany.com <input checked="" type="checkbox"/> Require authentication
Connection Security	None ▾
SMTP Port	25
SMTP User Name	smtpuser
SMTP Password	••••
Confirm SMTP Password	••••
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com 

Email Notification Settings	
<b>Email Notification</b>	This setting specifies whether or not to enable email notification. If <b>Enable</b> is checked, the Pepwave router will send email messages to system administrators when the WAN status changes or when new firmware is available. If <b>Enable</b> is not checked, email notification is disabled and the Pepwave router will not send email messages.
<b>SMTP Server</b>	This setting specifies the SMTP server to be used for sending email. If the server requires authentication, check <b>Require authentication</b> .
<b>Connection Security</b>	This setting specifies via a drop-down menu one of the following valid connection security: <ul style="list-style-type: none"> <li>• None</li> <li>• STARTTLS</li> <li>• SSL/TTS</li> </ul> When connection security is selected, <b>SMTP Port</b> will set a default port number automatically.
<b>SMTP Port</b>	This field is for specifying the SMTP port number. By default, this is set to <b>25</b> ; when <b>STARTTLS</b> is selected, the default port number will be set to <b>587</b> . When <b>SSL/TTS</b> is selected, the default port number will be set to <b>465</b> . You may customize the port number by editing this field.
<b>SMTP User Name / Password</b>	This setting specifies the SMTP username and password while sending email. These options are shown only if <b>Require authentication</b> is checked in the <b>SMTP Server</b> setting.
<b>Confirm SMTP Password</b>	This field allows you to verify and confirm the new administrator password.
<b>Sender's Email Address</b>	This setting specifies the email address the Pepwave router will use to send reports.

### Email Notification Settings

**Recipient's Email Address** This setting specifies the email address(es) to which the Pepwave router will send email notifications. For multiple recipients, separate each email using the enter key.

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

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

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

**Test email sent.**  
 (NOTE: Settings are not saved. To confirm the update, click 'Save' button.)

Email Notification Setup <span style="float: right;">?</span>	
Email Notification	<input checked="" type="checkbox"/> Enable
SMTP Server	<input type="text"/> <input checked="" type="checkbox"/> Require authentication
Connection Security	SSL/TLS <span style="font-size: small;">(Note: any server certificate will be accepted)</span>
SMTP Port	<input type="text" value="465"/>
SMTP User Name	<input type="text"/>
SMTP Password	<input type="password"/>
Confirm SMTP Password	<input type="password"/>
Sender's Email Address	<input type="text"/>
Recipient's Email Address	<input type="text"/>

**Test Result**

```
[INFO] Try email through auto detected connection
[INFO] SMTP through SSL connected
[<-] 220 smtp.gmail.com ESMTP h11sm3907691pjjg.46 - gsmt
[>-] EHLO balance.peplink.com
[<-] 250-smtp.gmail.com at your service, [14.192.209.255]
[<-] 250-SIZE 35882577
[<-] 250-8BITMIME
[<-] 250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN OAUTHBEARER XOAUTH
[<-] 250-ENHANCEDSTATUSCODES
[<-] 250-PIPELINING
[<-] 250-CHUNKING
[<-] 250 SMTPUTF8
[>-] AUTH PLAIN AGdwc2djbjk0QGdtYWlsLmNvbQBwdnJ6bWF6cGhtYXJpanpp
```

## Event Log

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

Send Events to Remote Syslog Server <span style="float: right;">?</span>	
Remote Syslog	<input type="checkbox"/>
Remote Syslog Host	<input type="text"/>
Port:	<input type="text" value="514"/>

Push Events to Mobile Devices <span style="float: right;">?</span>	
Push Events	<input checked="" type="checkbox"/>

URL Logging	
Enable	<input checked="" type="checkbox"/>
Log Server Host	<input type="text"/>
Port:	<input type="text" value="514"/>

Session Logging	
Enable	<input checked="" type="checkbox"/>
Log Server Host	<input type="text"/>
Port:	<input type="text" value="514"/>

Save

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

**Session Logging Host** This setting specifies the IP address or hostname of the Session log server.

## SNMP

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

SNMP Settings	
SNMP Device Name	SURF_SOHO_8439
Location <span style="float: right;">?</span>	<input type="text"/>
SNMP Port	<input type="text" value="161"/> <span>Default</span>
SNMPv1	<input type="checkbox"/> Enable
SNMPv2c	<input type="checkbox"/> Enable
SNMPv3	<input type="checkbox"/> Enable
SNMP Trap	<input checked="" type="checkbox"/> Enable
SNMP Trap Community	<input type="text"/>
SNMP Trap Server	<input type="text"/>
SNMP Trap Port	<input type="text" value="162"/>
SNMP Trap Server Heartbeat	<input type="checkbox"/>
<input type="button" value="Save"/>	

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

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

SNMP Settings	
<b>SNMP Device Name</b>	This field shows the router name defined at <b>System&gt;Admin Security</b> .
<b>SNMP Port</b>	This option specifies the port which SNMP will use. The default port is <b>161</b> .
<b>SNMPv1</b>	This option allows you to enable SNMP version 1.



<b>SNMPv2</b>	This option allows you to enable SNMP version 2.
<b>SNMPv3</b>	This option allows you to enable SNMP version 3.
<b>SNMP Trap</b>	This option allows you to enable SNMP Trap. If enabled, the following entry fields will appear.
<b>SNMP Trap Community</b>	This setting specifies the SNMP Trap community name.
<b>SNMP Trap Server</b>	Enter the IP address of the SNMP Trap server.
<b>SNMP Trap Port</b>	This option specifies the port which the SNMP Trap server will use. The default port is <b>162</b> .
<b>SNMP Trap Server Heartbeat</b>	This option allows you to enable and configure the heartbeat interval for the SNMP Trap server.

To add an SNMP community, click the **Add SNMP Community** button in the **Community Name** table; the following screen will be displayed:

**SNMP Community** ✕

Community Name	<input style="width: 90%;" type="text"/>
Allowed Network	<input style="width: 20%;" type="text"/> / 255.255.255.0 (/24) ▼

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

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

**SNMPv3 User** ✕

User Name	<input style="width: 90%;" type="text"/>
Authentication	SHA ▾ <input style="width: 80%;" type="text"/>
Privacy	DES ▾ <input style="width: 80%;" type="text"/>

SNMPv3 User Settings	
<b>User Name</b>	This setting specifies a user name to be used in SNMPv3.
<b>Authentication Protocol</b>	This setting specifies via a drop-down menu one of the following valid authentication protocols: <ul style="list-style-type: none"> <li>NONE</li> <li>MD5</li> <li>SHA</li> </ul> When MD5 or SHA is selected, an entry field will appear for the password.
<b>Privacy Protocol</b>	This setting specifies via a drop-down menu one of the following valid privacy protocols: <ul style="list-style-type: none"> <li>None</li> <li>DES</li> <li>AES</li> </ul> When AES or DES is selected, an entry field will appear for the password.

## InControl

**Controller Management Settings**

Controller <span style="float: right;">?</span>	InControl ▾ <input type="checkbox"/> Restricted to Status Reporting Only
Privately Host InControl	<input checked="" type="checkbox"/>
InControl Host	<input style="width: 90%;" type="text"/> <input style="width: 90%;" type="text"/> <input type="checkbox"/> Fail over to InControl in the cloud.

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

When this checkbox is checked, the device's status information will be sent to the Peplink InControl

system. This device's usage data and configuration will be sent to the system if you enable the features in the system.

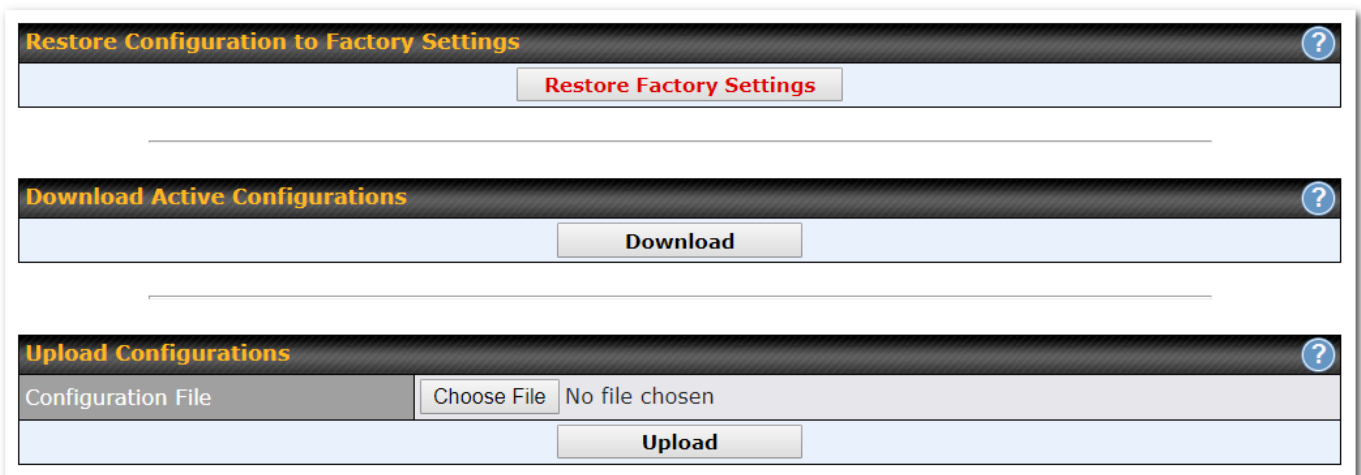
When the box **Restricted to Status Reporting Only** is ticked, the router will only report its status, but can't be managed or configured by InControl.

Alternatively, you can also privately host InControl. Simply check the "Privately Host InControl" box and enter the IP Address of your InControl Host. If you have multiple hosts, you may enter the primary and backup IP addresses for the InControl Host and tick the "Fail over to InControl in the cloud" box. The device will connect to either the primary InControl Host or the secondary/backup ICA/IC2.

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

## Configuration

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



Configuration	
<b>Restore Configuration to Factory Settings</b>	The <b>Restore Factory Settings</b> button is to reset the configuration to factory default settings. After clicking the button, you will need to click the <b>Apply Changes</b> button on the top right corner to make the settings effective.
<b>Download Active Configurations</b>	Click <b>Download</b> to backup the current active settings.
<b>Upload Configurations</b>	To restore or change settings based on a configuration file, click <b>Choose File</b> to locate the configuration file on the local computer, and then click <b>Upload</b> . The new settings can then be applied by clicking the <b>Apply Changes</b> button on the page header, or you can cancel the procedure by pressing <b>discard</b> on the main page of the web admin interface.

## Feature Add-ons

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

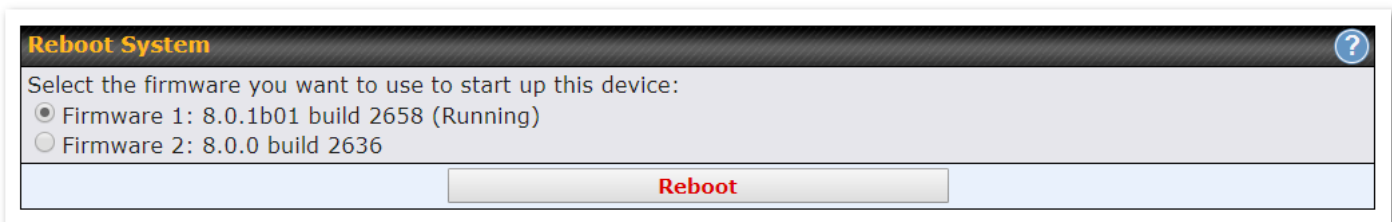


The screenshot shows a web interface titled "Feature Activation". It contains a label "Activation Key" on the left side of a large, empty text input field. Below the input field is a button labeled "Activate".

## Reboot

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

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



The screenshot shows a web interface titled "Reboot System" with a help icon (question mark) in the top right corner. Below the title is the instruction "Select the firmware you want to use to start up this device:". There are two radio button options: "Firmware 1: 8.0.1b01 build 2658 (Running)" and "Firmware 2: 8.0.0 build 2636". Below these options is a button labeled "Reboot".

# Tools

## Ping

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

**Ping**

Connection	WAN 1
Destination	8.8.8.8
Packet Size	56
Number of times	Times 5

**Results**

```

PING 8.8.8.8 (8.8.8.8) from 10.22.1.182 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_req=1 ttl=121 time=11.8 ms
64 bytes from 8.8.8.8: icmp_req=2 ttl=121 time=11.7 ms
64 bytes from 8.8.8.8: icmp_req=3 ttl=121 time=11.6 ms
64 bytes from 8.8.8.8: icmp_req=4 ttl=121 time=11.6 ms
64 bytes from 8.8.8.8: icmp_req=5 ttl=121 time=11.4 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 11.427/11.680/11.888/0.166 ms
          
```

### Tip

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

## Traceroute Test

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

**Traceroute**

Connection	WAN 1
Destination	64.233.189.99

**Results**

```

Traceroute to 64.233.189.99 (64.233.189.99), 30 hops max, 90 bytes packet
 0 10.0.1.1 [10.0.1.1] 0.700 ms 0.472 ms 0.267 ms
 1 10.0.0.254 [10.0.0.254] 0.010 ms 0.000 ms 0.000 ms
 2 10.0.0.1 [10.0.0.1] 0.070 ms 0.000 ms 0.000 ms
 3 10.0.0.2 [10.0.0.2] 0.002 ms 0.000 ms 0.000 ms
 4 108.143.88.254 [108.143.88.254] 0.204 ms 0.176.240.22 [0.176.240.22] 0.707 ms 108.143.88.254 [108.143.88.254] 0.472 ms
 5 192.75.48.129 [192.75.48.129] 0.000 ms 192.75.48.129 [192.75.48.129] 0.293 ms 0.293 ms
 6 209.85.243.30 [209.85.243.30] 0.000 ms 7.000 ms 7.000 ms
 7 209.85.243.30 [209.85.243.30] 0.000 ms 209.85.243.30 [209.85.243.30] 0.000 ms
 8 209.85.243.30 [209.85.243.30] 0.000 ms 209.85.243.30 [209.85.243.30] 0.000 ms
 9 209.85.243.30 [209.85.243.30] 0.000 ms 209.85.243.30 [209.85.243.30] 0.000 ms
 10 209.85.243.30 [209.85.243.30] 0.000 ms 209.85.243.30 [209.85.243.30] 0.000 ms
 11 209.85.243.30 [209.85.243.30] 0.000 ms 209.85.243.30 [209.85.243.30] 0.000 ms
 12 209.85.243.30 [209.85.243.30] 0.000 ms 209.85.243.30 [209.85.243.30] 0.000 ms
 13 209.85.243.30 [209.85.243.30] 0.000 ms 209.85.243.30 [209.85.243.30] 0.000 ms
 14 64.233.189.99 [64.233.189.99] 0.170 ms 0.144 ms 0.000 ms
          
```

**Tip**

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

## Wake-on-LAN

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

**Wake-on-LAN**

Wake-on-LAN Target	Custom MAC Address...	00:00:00:00:00:00	<input type="button" value="Send"/>
--------------------	-----------------------	-------------------	-------------------------------------

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

## WAN Analysis

The WAN Analysis feature allows you to run a WAN to WAN speed test between 2 Peplink devices . You can set a device up as a **Server** or a **Client**. One device must be set up as a server to run the speed tests and the server must have a public IP address.

**PEPWAVE** | Dashboard | SpeedFusion Cloud | Network | Advanced | AP | **System** | Status

**System**


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

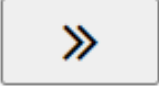
**Tools**

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

### WAN Performance Analysis

Check your point-to-point WAN performance with another peer

 **As a server**  
For the peer who has public IP addresses to accept connection.

 **As a client**  
For the peer to initiate connection.

The default port is 6000 and can be changed if required. The IP address of the WAN interface will be shown in the **WAN Connection Status** section.

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

- System**
  - Admin Security
  - Firmware
  - Time
  - Schedule
  - Email Notification
  - Event Log
  - SNMP
  - InControl
  - Configuration
  - Feature Add-ons
  - Reboot
- Tools**
  - Ping
  - Traceroute
  - Wake-on-LAN
  - WAN Analysis**

## WAN Performance Analysis

Check your point-to-point WAN performance with another peer

**Server Settings**

Status	<input checked="" type="checkbox"/> Listening (Control Port: 6000)
Control Port	<input type="text" value="6000"/>

**WAN Connection Status**

WAN	<input checked="" type="checkbox"/> <div style="width: 100px; height: 10px; background-color: #ccc;"></div>
USB	No Device Detected
Wi-Fi WAN on 2.4 GHz	<input type="checkbox"/> Disabled
Wi-Fi WAN on 5 GHz	<input type="checkbox"/> Disabled

The client side has a few more settings that can be changed. Make sure that the **Control Port** matches what's been entered on the server side. Select the WAN(s) that will be used for testing and enter the Servers WAN IP address. Once all of the options have been set, click the **Start Test** button.



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

**System**

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

**Tools**

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

Logout

## WAN Performance Analysis

Check your point-to-point WAN performance with another peer

**Client Settings**

Control Port	6000
Data Port	45232 - 45239
Type	<input checked="" type="radio"/> TCP <input type="radio"/> UDP
Direction	<input checked="" type="radio"/> Upload <input type="radio"/> Download
Duration	20 seconds (5 - 600)

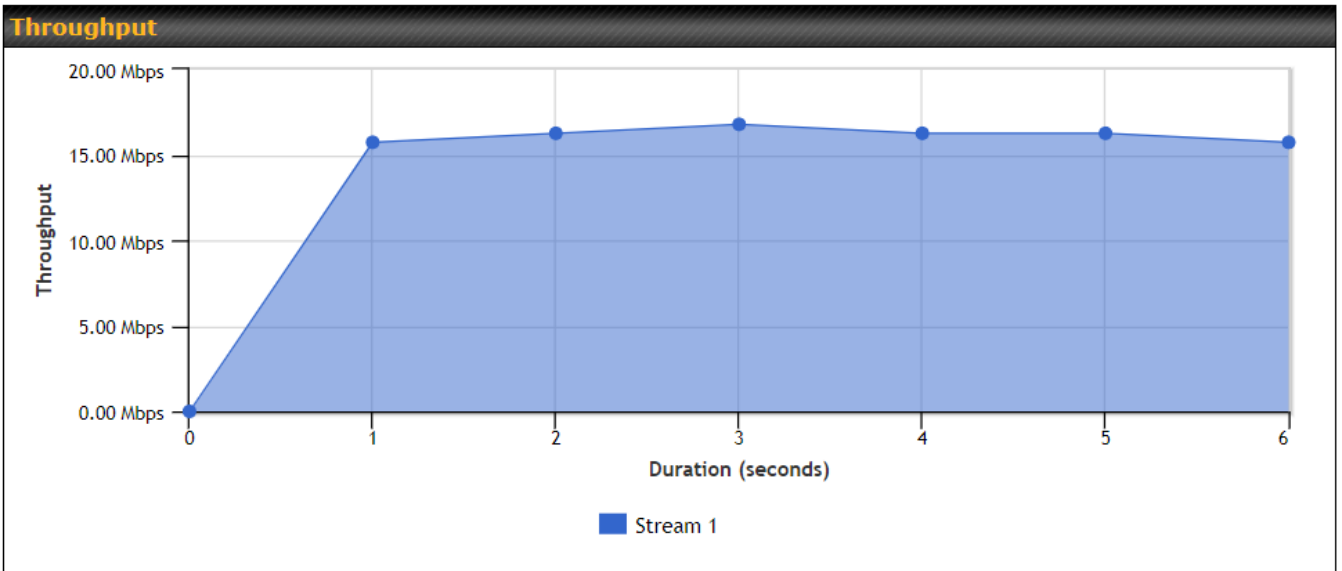
**Data Streams**

Local WAN Connection	Remote IP Address	
1. -- Not Used --		✘
2. -- Not Used --		✘
3. -- Not Used --		✘
4. -- Not Used --		✘
5. -- Not Used --		✘
6. -- Not Used --		✘
7. -- Not Used --		✘
8. -- Not Used --		+

Start Test

The test output will show the **Data Streams Parameters**, the **Throughput** as a graph, and the **Results**.

Data Streams Parameters		
Type	TCP	
Direction	Upload	
Duration	6 seconds	
	Local	Remote
Stream 1	192.168.1.100:80	192.168.1.100:80



### Results

1.0s:	15.7284 Mbps	0 retrans /	146 KB cwnd
2.0s:	16.2527 Mbps	0 retrans /	245 KB cwnd
3.0s:	16.7775 Mbps	0 retrans /	342 KB cwnd
4.0s:	16.2528 Mbps	0 retrans /	451 KB cwnd
5.0s:	16.2530 Mbps	0 retrans /	557 KB cwnd
6.0s:	15.7287 Mbps	0 retrans /	634 KB cwnd
--			
Overall:	16.1172 Mbps	0 retrans /	707 KB cwnd
--			

The test can be run again once it's complete by clicking the **Start** button or you can click **Close** and change the parameters for the test.

# Status

## Device

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

System Information	
Router Name	[REDACTED]
Model	Pepwave Surf SOHO MK3
Product Code	SUS-SOHO
Hardware Revision	1
Serial Number	[REDACTED]
Firmware	[REDACTED]
PepVPN Version	8.0.0
Modem Support Version	1023 ( <a href="#">Modem Support List</a> )
InControl Managed Configurations	Firmware, Scheduled Reboot
Host Name	[REDACTED]
Uptime	6 days 3 hours 30 minutes
System Time	Fri Sep 06 03:00:20 MST 2019
Diagnostic Report	<a href="#">Download</a>
Remote Assistance	<a href="#">Turn On</a>

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

<b>Modem Support Version</b>	This shows the modem support version. For a list of supported modems, click <b>Modem Support List</b> .
<b>InControl Managed Configurations</b>	If the router is (partly) managed by InControl, the options controlled by InControl are listed in this field.
<b>Hostname</b>	The host name assigned to the Pepwave router appears here.
<b>Uptime</b>	This shows the length of time since the device has been rebooted.
<b>System Time</b>	This shows the current system time.
<b>Diagnostic Report</b>	The <b>Download</b> link is for exporting a diagnostic report file required for system investigation.
<b>Remote Assistance</b>	Click <b>Turn on</b> to enable remote assistance.

MAC Address	
LAN	00:1A:DD:68: [blacked out]
WAN	00:1A:DD:68: [blacked out]
Wi-Fi WAN on 5 GHz	00:1A:DD:68: [blacked out]

[Legal](#)

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

**Important Note**

If you encounter issues and would like to contact the Pepwave Support Team, please download the diagnostic report file and attach it along with a description of your issue.

## Active Sessions

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

Overview
Search

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

Service	Inbound Sessions	Outbound Sessions
<a href="#">Amazon</a>	0	1
<a href="#">DNS</a>	0	55
<a href="#">Facebook</a>	0	2
<a href="#">Google</a>	0	19
<a href="#">Google Play Store</a>	0	1
<a href="#">HTTP</a>	0	2
<a href="#">IPsec</a>	0	2
<a href="#">Office 365</a>	0	42
<a href="#">SIP</a>	0	46
<a href="#">SSH</a>	0	1
<a href="#">SSL</a>	3	170
<a href="#">STUN</a>	0	2
<a href="#">Skype</a>	0	5
<a href="#">XMPP</a>	0	1

Interface	Inbound Sessions	Outbound Sessions
eth0	0	308
eth1	2	155
eth2	0	0
eth3	0	0
eth4	0	42
eth5	0	0

**Top Clients**

Client IP Address	Total Sessions
172.16.150.10	174
10.22.1.253	151
10.22.1.166	91
172.16.150.12	75
10.22.1.157	60

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

You can also perform a filtered search for specific sessions. You can filter by subnet, port, protocol, and interface.

To perform a search, navigate to **Status>Active Sessions>Search**.

Overview
Search

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

IP / Subnet	Source or Destination ▾ <input style="width: 150px;" type="text" value="255.255.255.255 (/32)"/>
Port	Source or Destination ▾ <input style="width: 100px;" type="text"/>
Protocol / Service	TCP ▾
Interface	<input type="checkbox"/> <b>1</b> WAN 1 <input type="checkbox"/> <b>2</b> WAN 2 <input type="checkbox"/> WI-FI WAN <input type="checkbox"/> <b>T1</b> Cellular 1 <input type="checkbox"/> <b>T2</b> Cellular 2 <input type="checkbox"/> USB <input type="checkbox"/> VPN
<input type="button" value="Search"/>	

**Outbound**

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

Total searched results: 0

**Inbound**

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

Total searched results: 0


**Transit**

Protocol	Source IP	Destination IP	Service	Interface	Idle Time
No sessions					

Total searched results: 0

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

## Client List

The client list table is located at **Status>Client List**. It lists DHCP and online client IP addresses, names (retrieved from the DHCP reservation table or defined by users), current download and upload rate, and MAC address. Clients can be imported into the DHCP reservation table by clicking the  button on the right. You can update the record after import by going to **Network>LAN**.

Filter		<input checked="" type="checkbox"/> Online Clients Only <input type="checkbox"/> DHCP Clients Only						
Client List								?
IP Address ▲	Name	Download (kbps)	Upload (kbps)	MAC Address	Network Name (SSID)	Signal (dBm)	Import	
10.12.1.1				08:00:27:00:00:00				
10.12.1.2	Wagner Laptop			28:00:00:00:00:00				
10.12.1.3				08:00:27:00:00:00				
10.12.1.100	shasha			08:00:27:00:00:00				
10.12.1.101	shasha			08:00:27:00:00:00				
10.12.1.102	shasha			08:00:27:00:00:00				
10.12.1.103	shasha			08:00:27:00:00:00				
10.12.1.104	shasha			08:00:27:00:00:00				
10.12.1.105	shasha			08:00:27:00:00:00				
10.12.1.106	shasha			08:00:27:00:00:00				
10.12.1.107	shasha			08:00:27:00:00:00				
10.12.1.108	shasha			08:00:27:00:00:00				
10.12.1.109	shasha			08:00:27:00:00:00				
10.12.1.110	shasha			08:00:27:00:00:00				
10.12.1.111	shasha			08:00:27:00:00:00				
10.12.1.112	shasha			08:00:27:00:00:00				
10.12.1.113	shasha			08:00:27:00:00:00				
10.12.1.114	shasha			08:00:27:00:00:00	PEPLINK	-62		
10.12.1.115	shasha			08:00:27:00:00:00				
10.12.1.116	shasha			08:00:27:00:00:00	PEPLINK	-46		
10.12.1.117	shasha			08:00:27:00:00:00				
10.12.1.118	shasha			08:00:27:00:00:00				
10.12.1.119	shasha			08:00:27:00:00:00	PEPLINK	-39		
10.12.1.120	shasha			08:00:27:00:00:00				
10.12.1.121	shasha			08:00:27:00:00:00				
10.12.1.122	shasha			08:00:27:00:00:00				
10.12.1.123	shasha			08:00:27:00:00:00				
10.12.1.124	shasha			08:00:27:00:00:00				
10.12.1.125	shasha			08:00:27:00:00:00				
10.12.1.126	shasha			08:00:27:00:00:00				
10.12.1.127	shasha			08:00:27:00:00:00				
10.12.1.128	shasha			08:00:27:00:00:00				
10.12.1.129	shasha			08:00:27:00:00:00				
10.12.1.130	shasha			08:00:27:00:00:00				
10.12.1.131	shasha			08:00:27:00:00:00				
10.12.1.132	shasha			08:00:27:00:00:00				
10.12.1.133	shasha			08:00:27:00:00:00				
10.12.1.134	shasha			08:00:27:00:00:00				
10.12.1.135	shasha			08:00:27:00:00:00				
10.12.1.136	shasha			08:00:27:00:00:00				
10.12.1.137	shasha			08:00:27:00:00:00				
10.12.1.138	shasha			08:00:27:00:00:00				
10.12.1.139	shasha			08:00:27:00:00:00				
10.12.1.140	shasha			08:00:27:00:00:00				
10.12.1.141	shasha			08:00:27:00:00:00				
10.12.1.142	shasha			08:00:27:00:00:00				
10.12.1.143	shasha			08:00:27:00:00:00				
10.12.1.144	shasha			08:00:27:00:00:00				
10.12.1.145	shasha			08:00:27:00:00:00				
10.12.1.146	shasha			08:00:27:00:00:00				
10.12.1.147	shasha			08:00:27:00:00:00				
10.12.1.148	shasha			08:00:27:00:00:00				
10.12.1.149	shasha			08:00:27:00:00:00				
10.12.1.150	shasha			08:00:27:00:00:00				
10.12.1.151	shasha			08:00:27:00:00:00				
10.12.1.152	shasha			08:00:27:00:00:00				
10.12.1.153	shasha			08:00:27:00:00:00				
10.12.1.154	shasha			08:00:27:00:00:00				
10.12.1.155	shasha			08:00:27:00:00:00				
10.12.1.156	shasha			08:00:27:00:00:00				
10.12.1.157	shasha			08:00:27:00:00:00				
10.12.1.158	shasha			08:00:27:00:00:00				
10.12.1.159	shasha			08:00:27:00:00:00				
10.12.1.160	shasha			08:00:27:00:00:00				
10.12.1.161	shasha			08:00:27:00:00:00				
10.12.1.162	shasha			08:00:27:00:00:00				
10.12.1.163	shasha			08:00:27:00:00:00				
10.12.1.164	shasha			08:00:27:00:00:00				
10.12.1.165	shasha			08:00:27:00:00:00				
10.12.1.166	shasha			08:00:27:00:00:00				
10.12.1.167	shasha			08:00:27:00:00:00				
10.12.1.168	shasha			08:00:27:00:00:00				
10.12.1.169	shasha			08:00:27:00:00:00				
10.12.1.170	shasha			08:00:27:00:00:00				
10.12.1.171	shasha			08:00:27:00:00:00				
10.12.1.172	shasha			08:00:27:00:00:00				
10.12.1.173	shasha			08:00:27:00:00:00				
10.12.1.174	shasha			08:00:27:00:00:00				
10.12.1.175	shasha			08:00:27:00:00:00				
10.12.1.176	shasha			08:00:27:00:00:00				
10.12.1.177	shasha			08:00:27:00:00:00				
10.12.1.178	shasha			08:00:27:00:00:00				
10.12.1.179	shasha			08:00:27:00:00:00				
10.12.1.180	shasha			08:00:27:00:00:00				
10.12.1.181	shasha			08:00:27:00:00:00				
10.12.1.182	shasha			08:00:27:00:00:00				
10.12.1.183	shasha			08:00:27:00:00:00				
10.12.1.184	shasha			08:00:27:00:00:00				
10.12.1.185	shasha			08:00:27:00:00:00				
10.12.1.186	shasha			08:00:27:00:00:00				
10.12.1.187	shasha			08:00:27:00:00:00				
10.12.1.188	shasha			08:00:27:00:00:00				
10.12.1.189	shasha			08:00:27:00:00:00				
10.12.1.190	shasha			08:00:27:00:00:00				
10.12.1.191	shasha			08:00:27:00:00:00				
10.12.1.192	shasha			08:00:27:00:00:00				
10.12.1.193	shasha			08:00:27:00:00:00				
10.12.1.194	shasha			08:00:27:00:00:00				
10.12.1.195	shasha			08:00:27:00:00:00				
10.12.1.196	shasha			08:00:27:00:00:00				
10.12.1.197	shasha			08:00:27:00:00:00				
10.12.1.198	shasha			08:00:27:00:00:00				
10.12.1.199	shasha			08:00:27:00:00:00				
10.12.1.200	shasha			08:00:27:00:00:00				

Scale:  kbps  Mbps

## OSPF & RIPv2a

OSPF & RIPv2	
Area	Remote Networks
▼ 0.0.0.0	
PepVPN	192.168.0.0/24

Information on OSPF and RIPv2 can be found in this section.

## BGP

BGP	
Profile	Neighbor
	No information

Information on BGP can be found in this section.

## PepVPN Status

PepVPN Status shows the current connection status of each connection profile and is displayed at **Status > PepVPN/SpeedFusion**.

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

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



PepVPN with SpeedFusion - Remote Peer

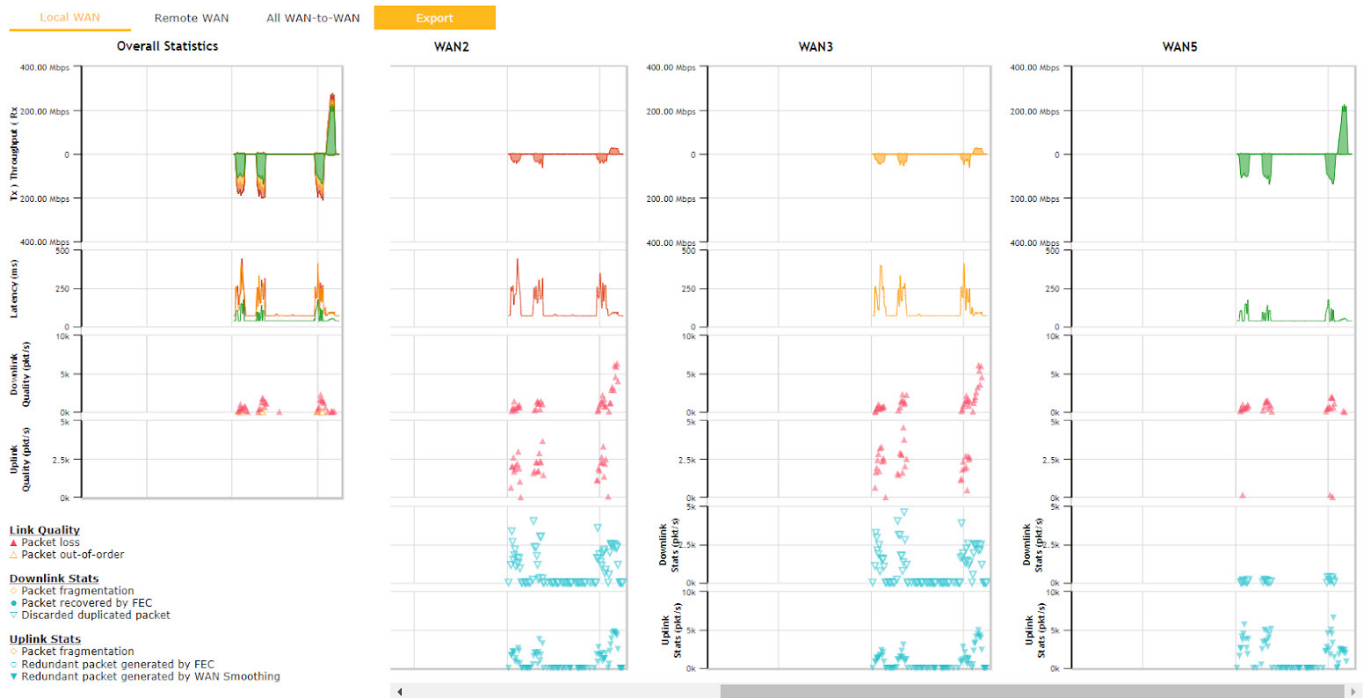
Show all profiles

Search

SFC

Remote Peer ▲	Profile	Information
<ul style="list-style-type: none"> <li>▼ SFC-SIN-001 (SFC-SIN-001)</li> <li>WAN1</li> <li>WAN2</li> <li>WAN3</li> <li>WAN4</li> <li>WAN5</li> <li>Mobile Internet</li> <li>Total</li> </ul>	SFC	<p>SpeedFusion Cloud </p> <p>Not available - WAN disabled</p> <p>Rx: &lt; 1 kbps Tx: &lt; 1 kbps Loss rate: 0.0 pkt/s Latency: 42 ms</p> <p>Rx: &lt; 1 kbps Tx: &lt; 1 kbps Loss rate: 0.0 pkt/s Latency: 42 ms</p> <p>Not available - WAN disabled</p> <p>Rx: &lt; 1 kbps Tx: &lt; 1 kbps Loss rate: 0.0 pkt/s Latency: 10 ms</p> <p>Rx: &lt; 1 kbps Tx: &lt; 1 kbps Loss rate: 0.0 pkt/s Latency: 32 ms</p> <p>Rx: &lt; 1 kbps Tx: 1.1 kbps Loss rate: 0.0 pkt/s</p>

Click button for a chart displaying real-time throughput, latency, and drop-rate information for each WAN connection.



When pressing the  button the following menu will appear:

**PepVPN Details** ✕

**Connection Information** ■ More information

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

**WAN Statistics** 📊

Remote Connections	<input type="checkbox"/> Show remote connections					
WAN Label	<input checked="" type="radio"/> WAN Name <input type="radio"/> IP Address and Port					
WAN1	Not available - WAN disabled					
WAN2	Rx:	< 1 kbps	Tx:	< 1 kbps	Loss rate:	0.0 pkt/s Latency: 43 ms
WAN3	Rx:	< 1 kbps	Tx:	< 1 kbps	Loss rate:	0.0 pkt/s Latency: 44 ms
WAN4	Not available - WAN disabled					
WAN5	Rx:	< 1 kbps	Tx:	< 1 kbps	Loss rate:	0.0 pkt/s Latency: 10 ms
Mobile Internet	Rx:	< 1 kbps	Tx:	< 1 kbps	Loss rate:	0.0 pkt/s Latency: 42 ms
Total	Rx:	< 1 kbps	Tx:	< 1 kbps	Loss rate:	0.0 pkt/s

**PepVPN Test Configuration** ?

Type	<input checked="" type="radio"/> TCP <input type="radio"/> UDP	<b>Start</b>
Streams	4 ▼	
Direction	<input checked="" type="radio"/> Upload <input type="radio"/> Download	
Duration	20 seconds (5 - 600)	

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

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

## Event Log

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

The screenshot shows the PEPWAVE web interface. The top navigation bar includes 'PEPWAVE' and menu items: Dashboard, SpeedFusion Cloud, Network, Advanced, AP, System, Status, and Apply Changes. The left sidebar has a 'Status' section with sub-items: Device, Active Sessions, Client List, OSPF & RIPv2, BGP, Event Log (highlighted), WAN Quality, and Usage Reports (Real-Time, Hourly, Daily, Monthly). A 'Logout' button is also present. The main content area shows two tabs: 'Device Event Log' and 'Firewall Event Log'. The 'Device Event Log' tab is active, displaying a list of events. The events are as follows:

Time	Description
Sep 30 09:23:29	Port: (
Sep 30 09:17:09	System:
Sep 30 09:10:39	Port
Sep 30 09:10:17	WA
Sep 30 09:09:09	Admir
Sep 30 09:08:23	Admir
Sep 30 09:07:53	Admir
Sep 30 09:07:32	Pc
Sep 30 08:56:33	WAN:
Sep 30 08:56:05	WAN:
Sep 30 08:55:52	WAN:
Sep 30 08:55:15	WAN:
Sep 30 08:55:11	WAN:
Sep 30 08:54:42	WAN:
Sep 30 08:54:04	WAN:
Sep 30 08:53:46	WAN:
Sep 30 08:52:51	WAN:
Sep 30 08:52:19	WAN:
Sep 30 08:35:56	WAN:
Sep 30 08:35:36	WAN:
Sep 30 07:24:06	WAN:

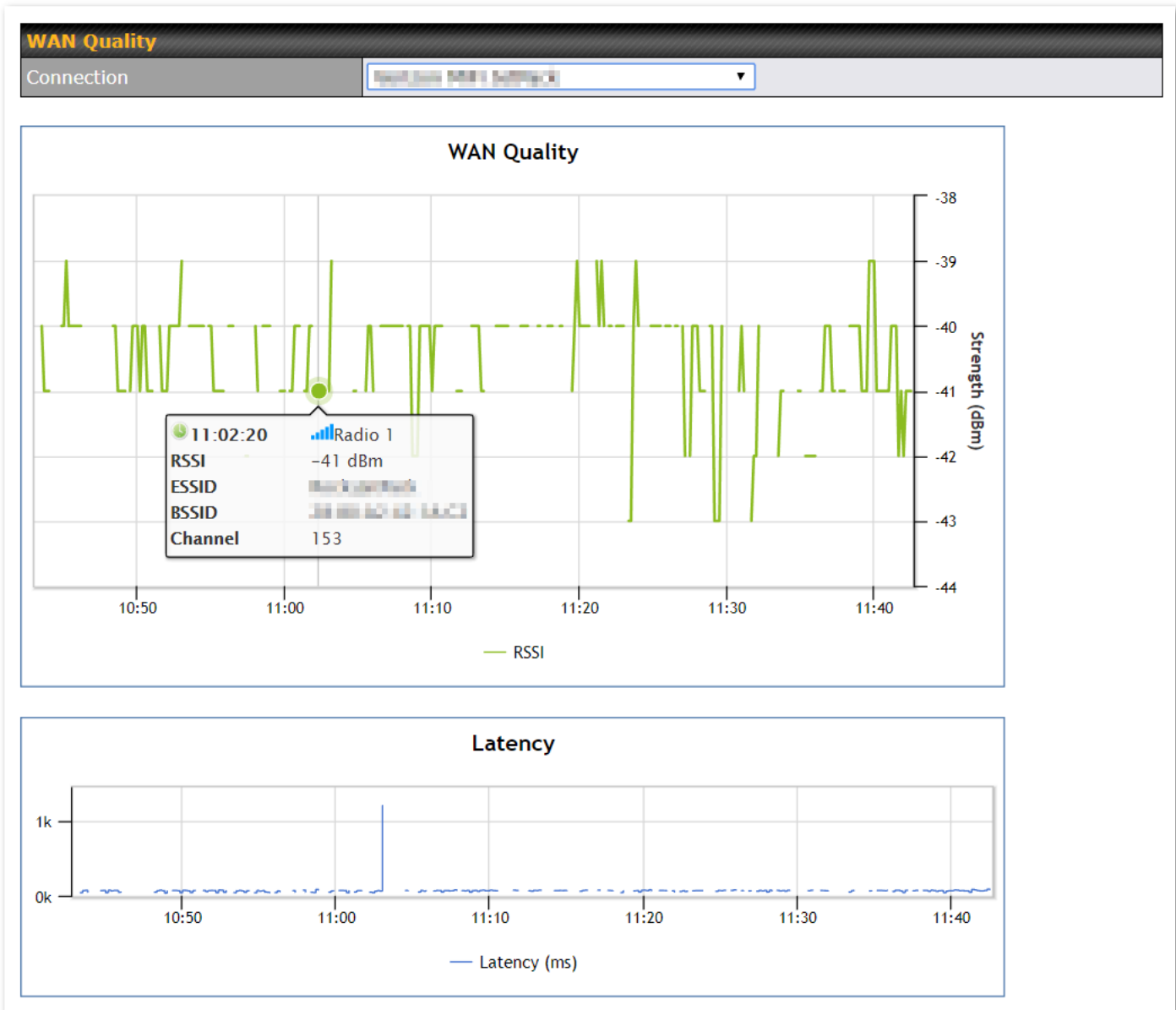
At the bottom of the log list, there is a 'Clear Log' button. An 'Auto Refresh' checkbox is checked in the top right corner of the log section.

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

## WAN Quality

WAN Quality allows you to select each WAN and view current WAN Quality.

Detailed information can be seen when selecting a point on the graph.

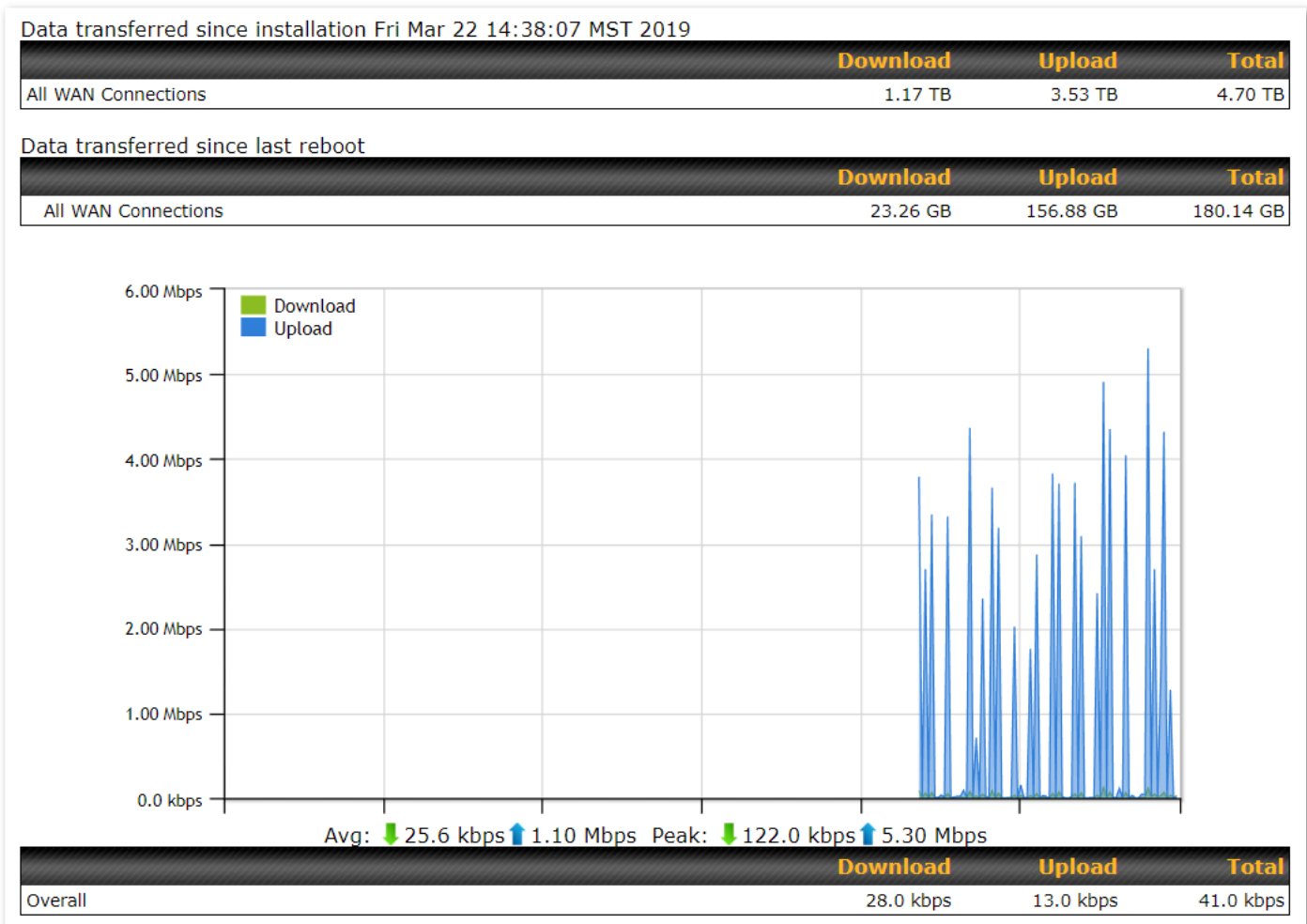


## Usage Reports

This section shows bandwidth usage statistics and is located at **Status>Bandwidth**. Bandwidth usage at the LAN while the device is switched off (e.g., LAN bypass) is neither recorded nor shown.

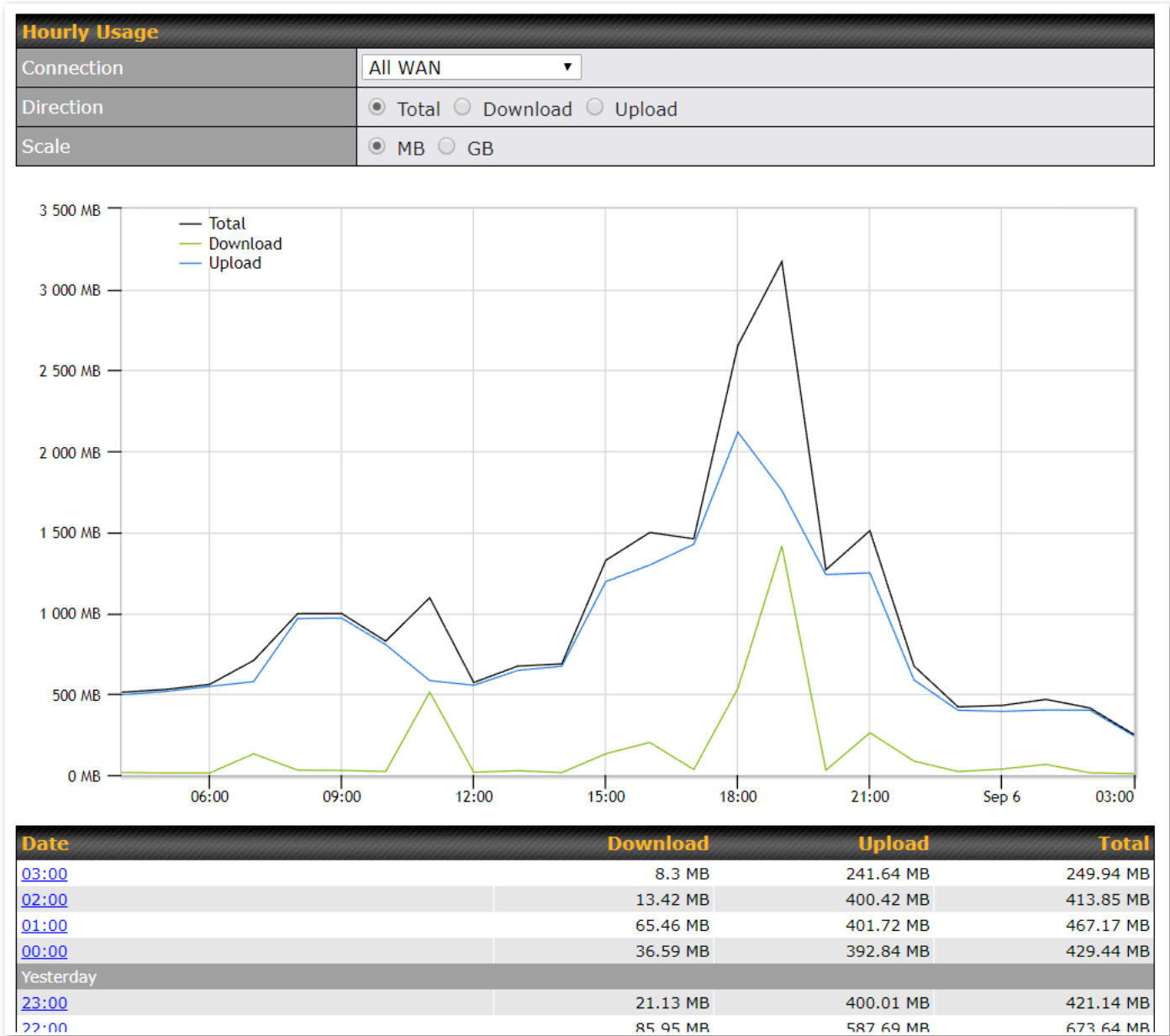
### Real Time

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



## Hourly

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

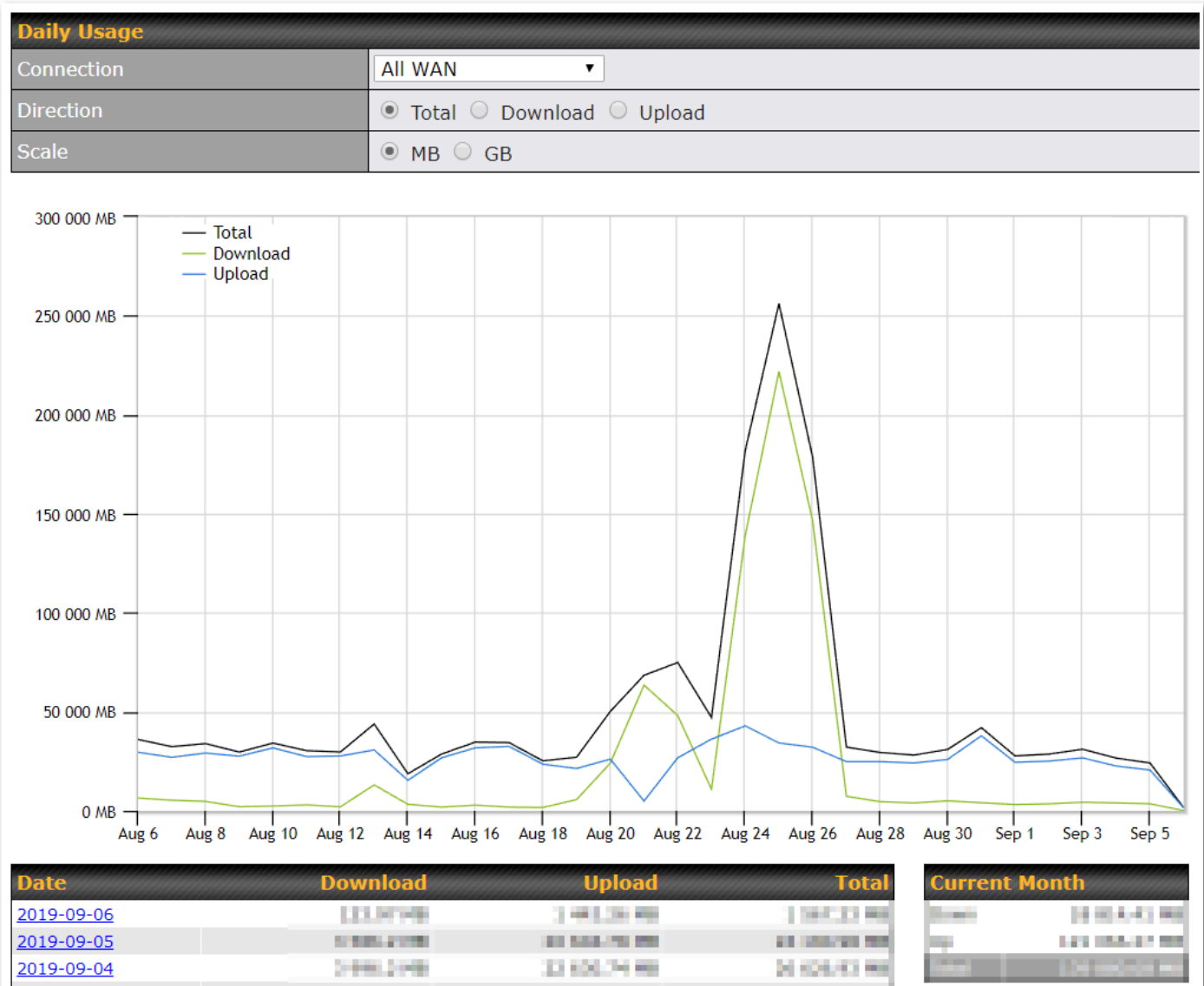


## Daily

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

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

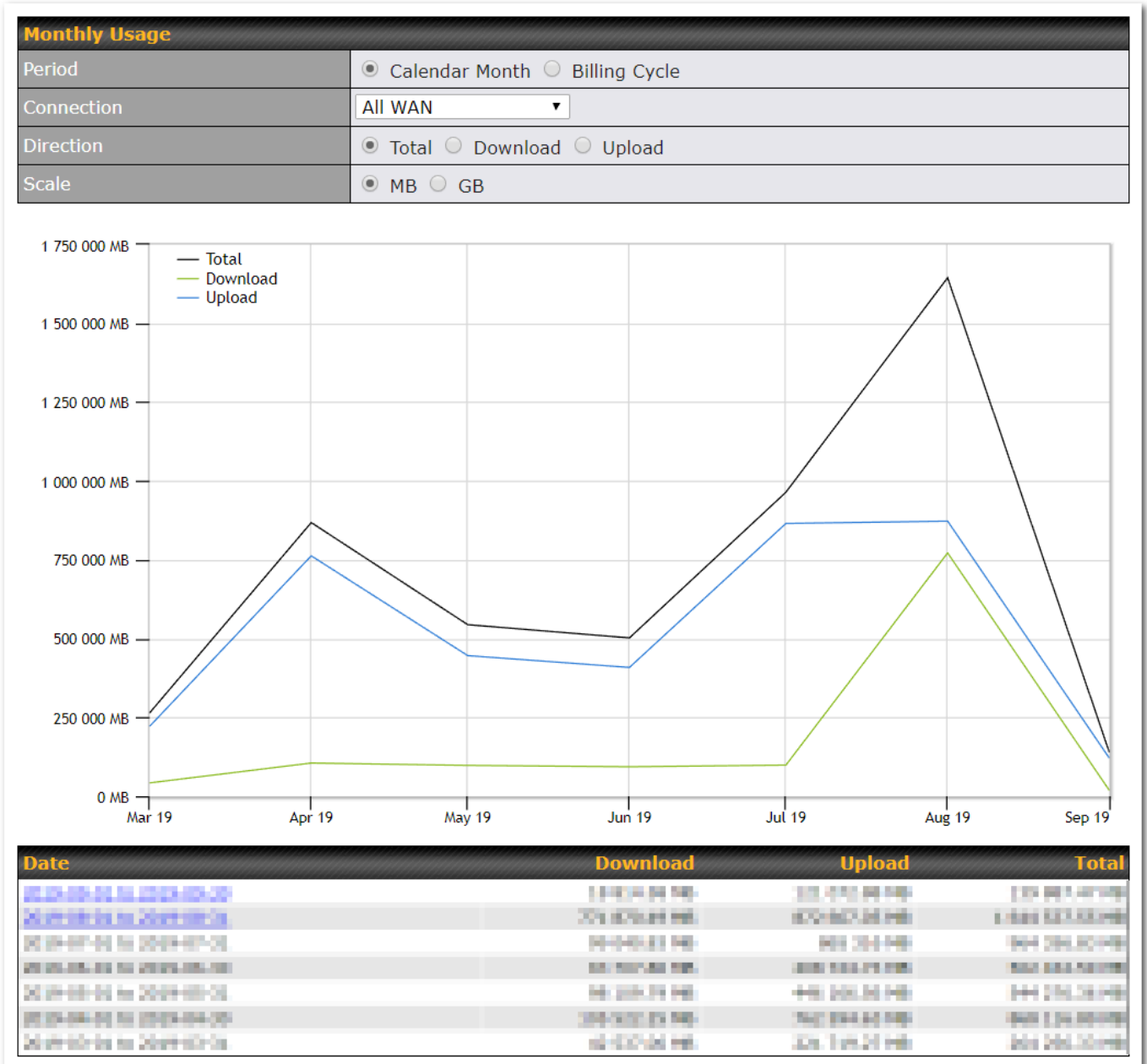
Click on a date to view the client bandwidth usage of that specific date. This feature is not available if you have selected to view the bandwidth usage of only a particular WAN connection. The scale of the graph can be set to display megabytes (**MB**) or gigabytes (**GB**).



## Monthly

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

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





## Appendix A: Restoration of Factory Defaults

To restore the factory default settings on your Pepwave Surf SOHO unit, follow the steps below:

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

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

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

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

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

### Important Note

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

## Appendix B: Overview of ports used by Peplink SD-WAN routers and other Peplink services

Default Port Number	Usage	Service	Inbound/Outbound	Default Status
UDP 5246	Data flow	InControl	Outbound	Enabled
TCP 443	HTTPS service	InControl	Outbound	Enabled
TCP 5246	Optional, used when TCP 443 is not responding	InControl	Outbound	Enabled
TCP 5246	Remote Web Admin	InControl Virtual Appliance	Outbound	Enabled
TCP 4500	VPN Data (TCP Mode)	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
TCP 32015	VPN handshake	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
UDP 4500	VPN Data	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
UDP 32015 <sup>o</sup>	VPN Data (alternative)	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
TCP/UDP 4500+N-1 <sup>^</sup>	VPN Sub-Tunnels Data	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
UDP 32015+N-1 <sup>^</sup>	VPN Sub-Tunnels Data (alternative)	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
UDP 4500	VPN Data	IPsec	Inbound / Outbound*	Disabled
UDP 500	VPN initiation	IPsec	Inbound / Outbound*	Disabled
UDP 500	L2TP	Remote User Access	Inbound	Disabled
UDP 1701	L2TP	Remote User Access	Inbound	Disabled
UDP 4500	L2TP	Remote User Access	Inbound	Disabled
UDP 1194	OpenVPN	Remote User Access	Inbound	Disabled
IP 47	PPTP (GRE)	Remote User Access	Inbound	Disabled
TCP 2222	Remote Assistance Direct connection	Peplink Troubleshooting Assistance	Outbound	Enabled
TCP 80	HTTP traffic	Web Admin Interface access	Inbound	Enabled
TCP 443	HTTPS traffic	Web Admin Interface access (secure)	Inbound	Enabled
TCP 8822	SSH	SSH	Inbound	Disabled
UDP 161	SNMP Get	SNMP monitoring	Inbound	Disabled
UDP 162	SNMP Trap	SNMP monitoring	Outbound	Disabled
TCP, UDP 1812	Radius Authentication	Radius	Outbound	Disabled
TCP, UDP 1813	Radius Accounting	Radius	Outbound	Disabled
UDP 123	Network Time Protocol	NTP	Inbound Outbound	Disabled Enabled
TCP 60660	Real-time location data in	GPS	Outbound	Disabled

	NMEA format		
--	-------------	--	--

**Disclaimer:**

- By default, only TCP 32015 and UDP 4500 are needed for PepVPN / SpeedFusion.
- Inbound / Outbound\* - Inbound = For Server mode; Outbound = For Client mode
- UDP 32015° - If IPsec VPN or L2TP/IPsec RUA is enabled, the UDP 4500 is occupied, so PepVPN / SpeedFusion will automatically switch to UPD 32015 as VPN data port .
- $UDP\ 32015+N-1^{\wedge}$  /  $TCP/UDP\ 4500+N-1^{\wedge}$  - When using Sub-Tunnels, multiple ports are in use (1 for each Sub-Tunnel profile).

The default UDP data ports used when using (N number of Sub-Tunnel profiles) are:  
 4500...4500+N-1, or (when port 4500 is in use by IPsec or L2TP/IPsec) 32015... 32015+N-1".

## Appendix C: Declaration

- **The device supports time division technology**
- **Federal Communication Commission Interference Statement**

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

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

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

### Radiation Exposure Statement

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

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

**CE Statement for Pepwave Routers ( Surf SOHO )**

**DECLARATION OF CONFORMITY**

We affirm the electrical equipment manufactured by us fulfils the requirements of the Radio Equipment Directive 2014/53/EU or R&TTE Directive 1999/5/EC

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

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

EN 301 893 V1.8.1  
EN 300 328 V1.9.1  
EN 62311:2008  
EN 301 489-1 V1.9.2  
EN 301 489-17 V2.2.1  
EN 55032: 2012 + AC:2013  
EN 55024:2010+A1:2015  
EN 61000-3-2: 2014  
EN 61000-3-3: 2013  
EN 60950-1:2006+A11:2009+A1:2010+A12:2011+A2:2013

Yours sincerely,



Antony Chong  
Director of Hardware Engineering  
Peplink International Limited



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

**2.4GHz ( 2412 - 2472 MHz ) : 19.88 dBm**

**5GHz ( 5150 - 5250 MHz ) : 22.57 dBm**

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

This equipment is restricted to indoor use only when operating in the 5150 to 5250 MHz frequency range in above countries.

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

## USB WAN Modem Port Specification

### Surf SOHO Series

	Surf SOHO
Output Rating	5V DC, 2A