



Pepwave Surf SOHO

User Manual

Pepwave Product: Surf SOHO

Pepwave Firmware 8.1.0
September 2020

COPYRIGHT & TRADEMARKS

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

Table of Contents

Introduction and Scope	5
Glossary	6
Product Features	7
WAN	7
LAN	7
VPN	7
Firewall	8
Outbound Policy	8
QoS	8
Other Supported Features	8
Pepwave Surf SOHO Router Overview	9
Panel Appearance	9
LED Indicators	12
Advanced Feature Summary	13
Drop-in Mode and LAN Bypass: Transparent Deployment	13
QoS: Clearer VoIP	13
USB Modem	14
Built-In Remote User VPN Support	14
Installation	15
Preparation	15
Constructing the Network	15
Connecting to the Web Admin Interface	15
SpeedFusion Cloud	18
Activate SpeedFusion Cloud Service	18
Enable SpeedFusion Cloud	20
Connect Clients to Cloud	27
Link Wi-Fi to Cloud	28
Configuring the LAN Interface(s)	30
Network Settings	30
Port Settings	38
Configuring the WAN interface	39
WAN > Quality Monitoring	39

WAN > Ethernet WAN	40
WAN > Physical Interface Settings	41
WAN > Health Check Settings	42
WAN > Bandwidth Allowance Monitor	134
WAN > Additional IP Address Settings	45
WAN > Dynamic DNS Settings	45
Wi-Fi WAN and USB WiFi Network connection	46
WAN > WiFi Connection Profiles	134
WAN > Signal threshold settings	50
Indication of WiFi strength values:	50
PepVPN	50
PepVPN > Send ALL traffic	54
Outbound Policy Management	55
Port Forwarding	58
UPnP / NAT-PMP Settings	60
NAT Mappings	61
QoS	63
Bandwidth Control	63
Application Prioritization	63
Firewall	65
Outbound and Inbound Firewall Rules	65
Intrusion Detection and DoS Prevention	70
Content Blocking	71
ROUTING PROTOCOLS	72
OSPF & RIPv2	72
BGP	74
REMOTE USER ACCESS	78
L2TP with IPsec	78
OpenVPN	78
PPTP	79
Authentication Methods	79
Miscellaneous Settings	81
RADIUS Server	81
Certificate Manager	83
Service Forwarding	83
Service Passthrough	85
Grouped Networks	87
SIM Toolkit	87
AP	90

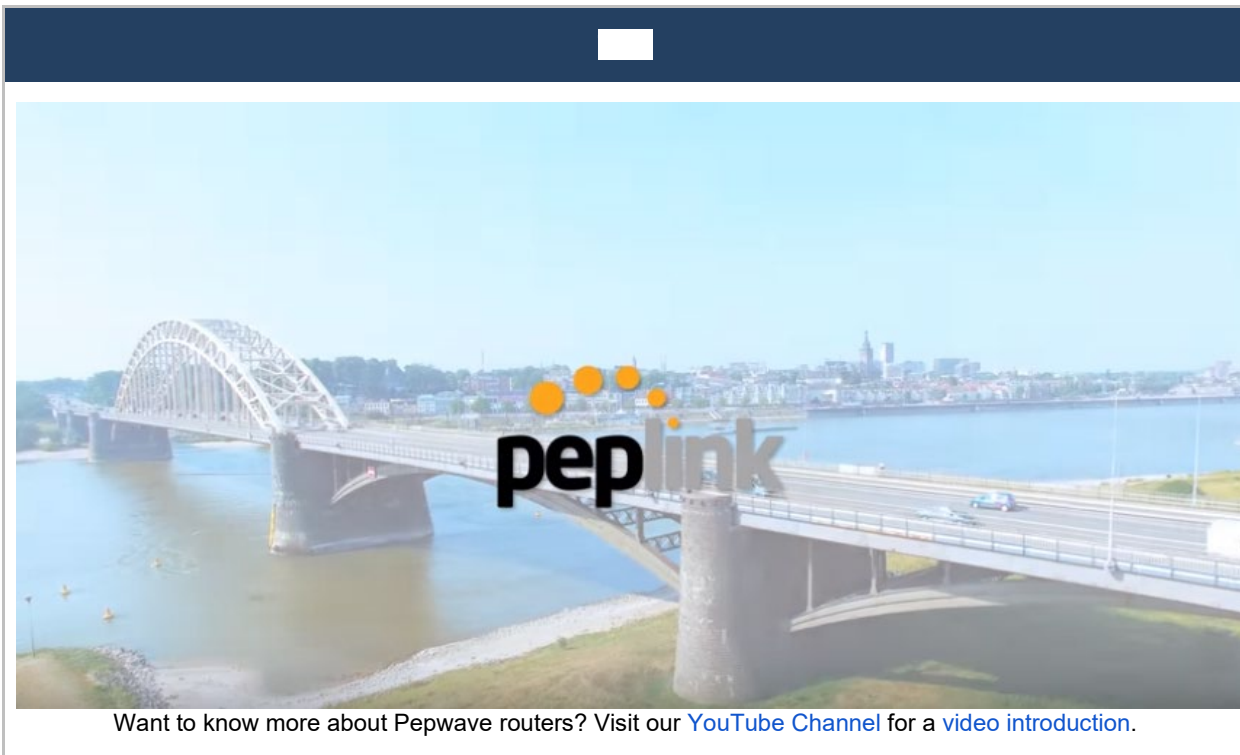
Wireless SSID	90
Settings	95
System Settings	97
Admin Security	97
Firmware	101
Time	102
Schedule	103
Email Notification	104
Event Log	106
SNMP	107
InControl	109
Configuration	109
Feature Add-ons	110
Reboot	111
Tools	111
Ping	111
Traceroute Test	112
Wake-on-LAN	113
WAN Analysis	113
Status	116
Device	116
Active Sessions	118
Client List	119
OSPF & RIPv2	121
BGP	121
PepVPN Status	121
Event Log	124
WAN Quality	125
Usage Reports	126
Appendix A: Restoration of Factory Defaults	130
Appendix B: Declaration	131

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 Surf SOHO router and provides an introduction to their features and usage.



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:

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

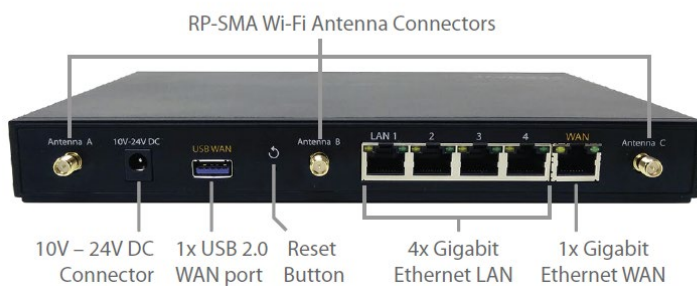
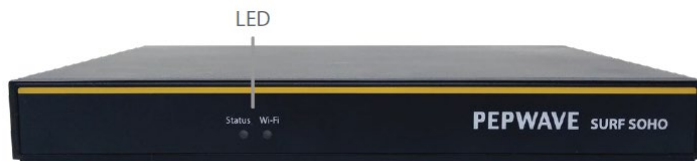
Other Supported Features

- 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



<div style="background-color: white; width: 100px; height: 15px; margin: 0 auto;"></div>	
WAN Interface	1x 100/1000M Ethernet Port 1x USB 2.0 Interface Wi-Fi as WAN
LAN Interface	4x 100/1000M Ethernet Ports Simultaneous Dual-Band 11ac Wi-Fi AP
Wi-Fi AP Operating Frequency	2412 – 2472 MHz and 5180 - 5825 MHz
Wi-Fi Antenna	3x External Wi-Fi Antenna
Recommended Users	1-25
Router Throughput	120Mbps
Number of PPTP VPN Users	3
Number of PPTP VPN Users	2
Power Input	DC Jack: 10V – 24VDC AC Adapter: AC Input 100V – 240V, DC Output 12V, 1.5A
Power Consumption	26W (max) with USB WAN 22W (max) without USB WAN
Dimensions	9.17 x 5.6 x 1.18 inch 233 x 142 x 30 mm
Weight	0.86 pounds 388 grams
Operating Temperature	-14° to 113°F -10° to 45°C
Humidity	15% – 95% (non-condensing)
Certifications	FCC, CE, RoHS
Warranty	1-Year Limited Warranty

LED Indicators

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

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

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

Signal strength	
Off	No connection
Signal strength	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.

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

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 antennas A 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.

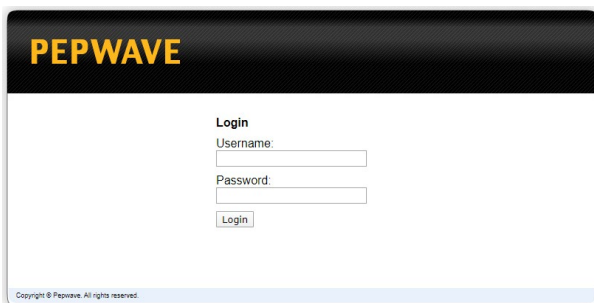
To connect to the web admin of the Pepwave Surf SOHO, enter the following LAN IP address in the address field of the web browser: **https://192.168.50.1**

(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 login.

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

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

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

Logout

WAN Connection Status

Priority 1 (Highest)

WAN	■ Connected	Details
-----	--	----------------

Priority 2

Wi-Fi WAN on 5 GHz	Standby	Wireless Networks Details
--------------------	---------	---

Priority 3

Wi-Fi WAN on 2.4 GHz	Standby	Wireless Networks Details
----------------------	---------	---

Priority 4 (Lowest)

Drag desired (Priority 4) connections here

Disabled

Drag desired (Disabled) connections here

LAN Interface

Router IP Address: 192.168.50.1

Wi-Fi AP ■ ON **Details**

PEPWAVE_8F18	
--------------	--

Device Information

Model:	Pepwave Surf SOHO MK3
Firmware:	8.1.0 build 4941
Uptime:	0 days 18 hours 37 minutes
CPU Load:	40%
Throughput:	↓ 0.0 kbps ↑ 0.0 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.

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 Cloud

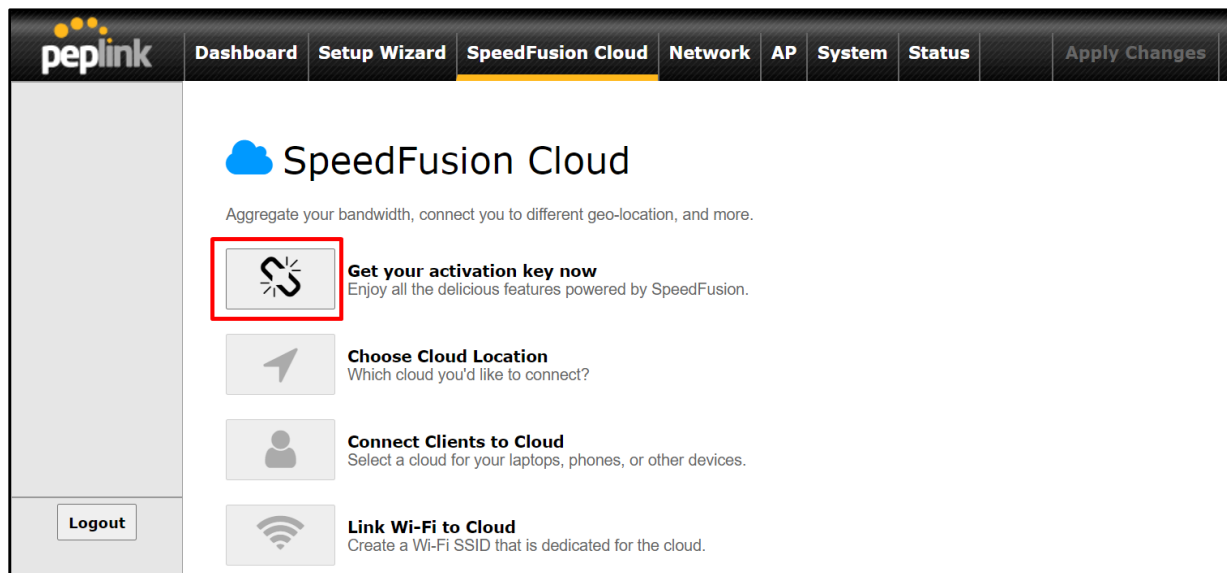
With Peplink products, your device is able to connect to SpeedFusion Cloud without the use of a second endpoint. This service has wide access to a number of SpeedFusion endpoints hosted from around the world, providing your device with unbreakable connectivity wherever you are.*



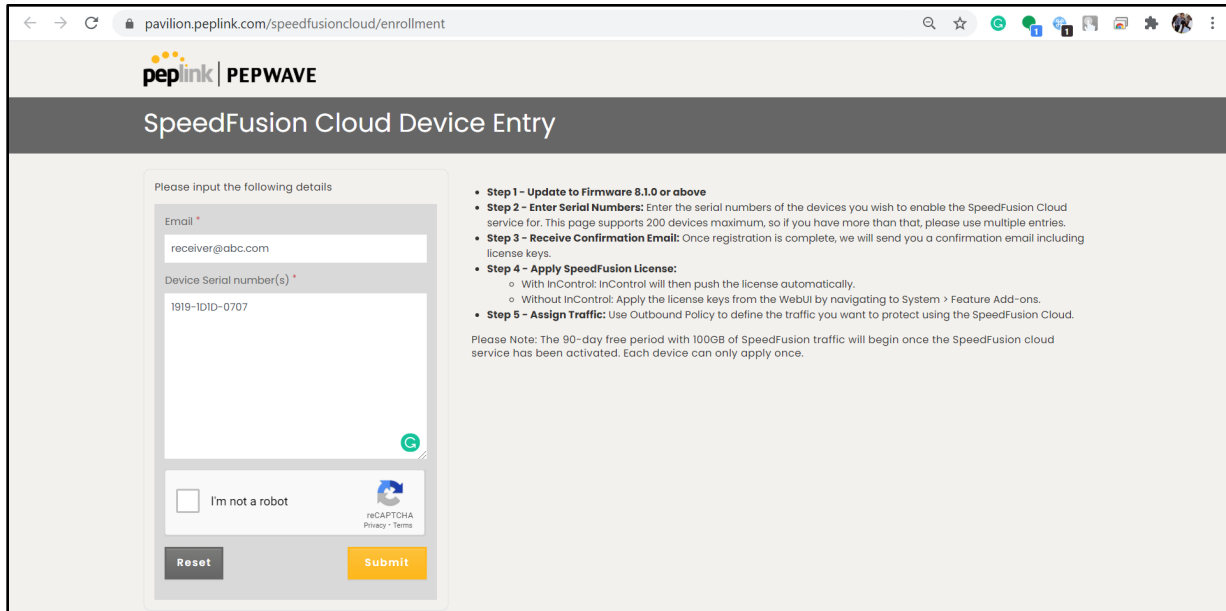
*SpeedFusion Cloud is supported in firmware version 8.1.0 and above. SpeedFusion Cloud is a subscription basis. SpeedFusion Cloud license can be purchased at <https://store.peplink.com/> > Cloud Solutions > SpeedFusion Cloud Service.

Activate SpeedFusion Cloud Service

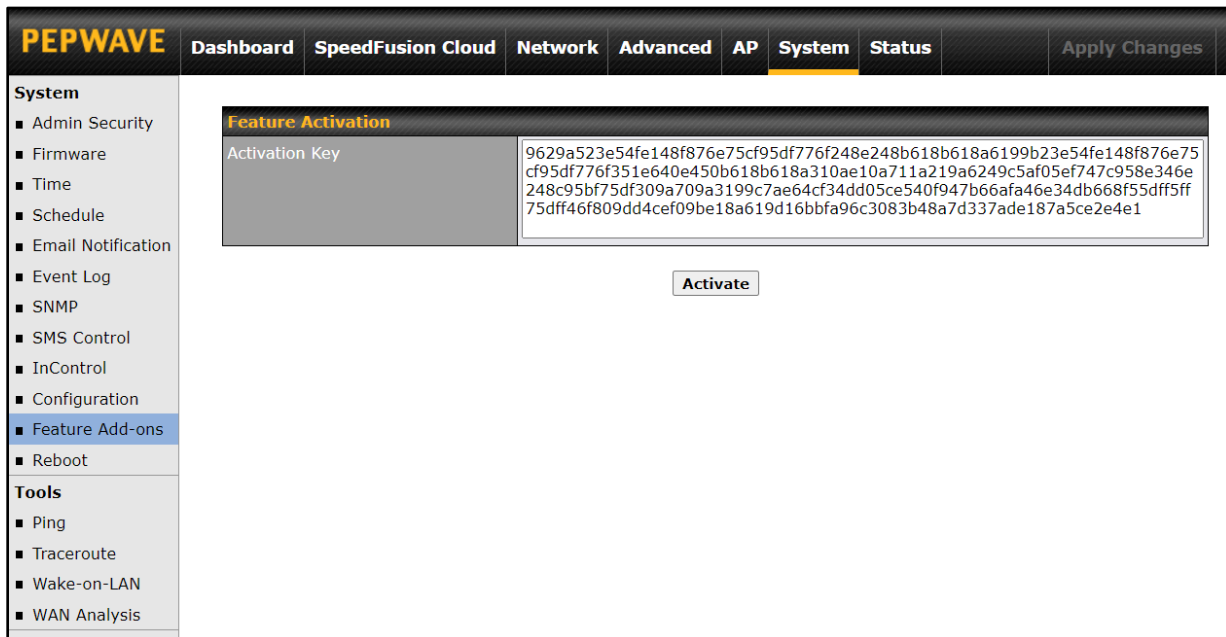
You are entitled to a 90-day free period with 100GB of SpeedFusion traffic upon activation of the SpeedFusion Cloud service. This offer is limited to once per device. To get your activation key please visit SpeedFusion Cloud.



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

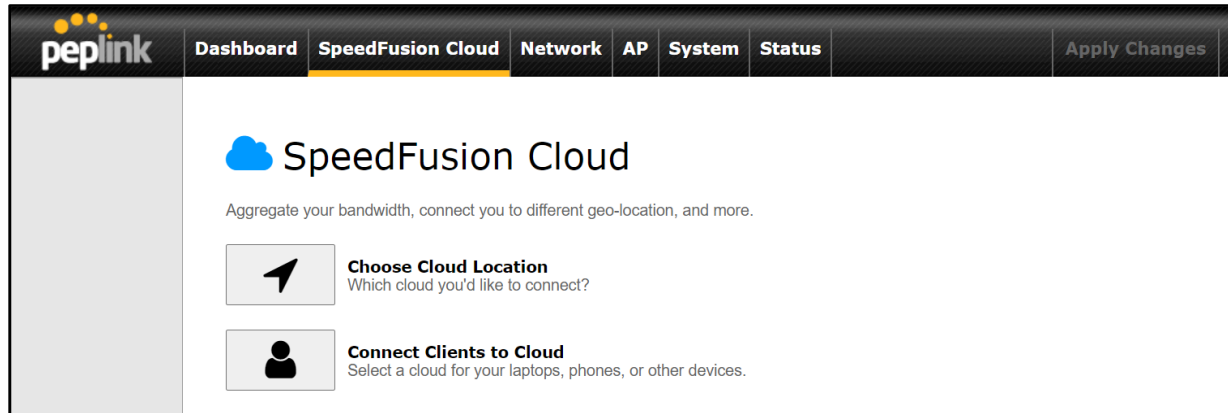


From **System > Features Add-ons**, paste the license key into the window and click on **Activate** once you have received the license key.

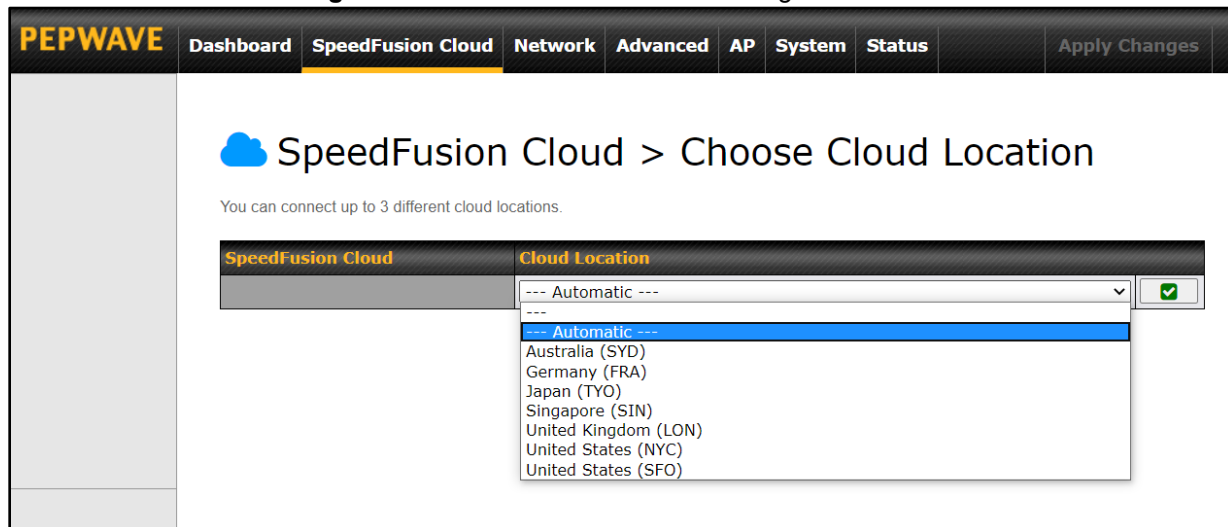


Enable SpeedFusion Cloud

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



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



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

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

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

SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

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

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

Changes applied successfully.

SpeedFusion Cloud > Choose Cloud Location

You can connect up to 3 different cloud locations.

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

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

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

WAN Connection Status ?

Priority 1 (Highest)
 Drag desired (Priority 1) connections here

Priority 2

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

Priority 3
 Drag desired (Priority 3) connections here

Disabled

1	WAN 1	<input type="checkbox"/> Disabled	Details
2	WAN 2	<input type="checkbox"/> Disabled	Details
3	Cellular 3	<input type="checkbox"/> Disabled	Details
4	Cellular 4	<input type="checkbox"/> Disabled	Details
	Wi-Fi WAN	<input type="checkbox"/> Disabled	Details
3	LAN 1 as WAN	<input type="checkbox"/> Disabled	Details
4	LAN 2 as WAN	<input type="checkbox"/> Disabled	Details
5	LAN 3 as WAN	<input type="checkbox"/> Disabled	Details

LAN Interface

Router IP Address: 192.168.50.1

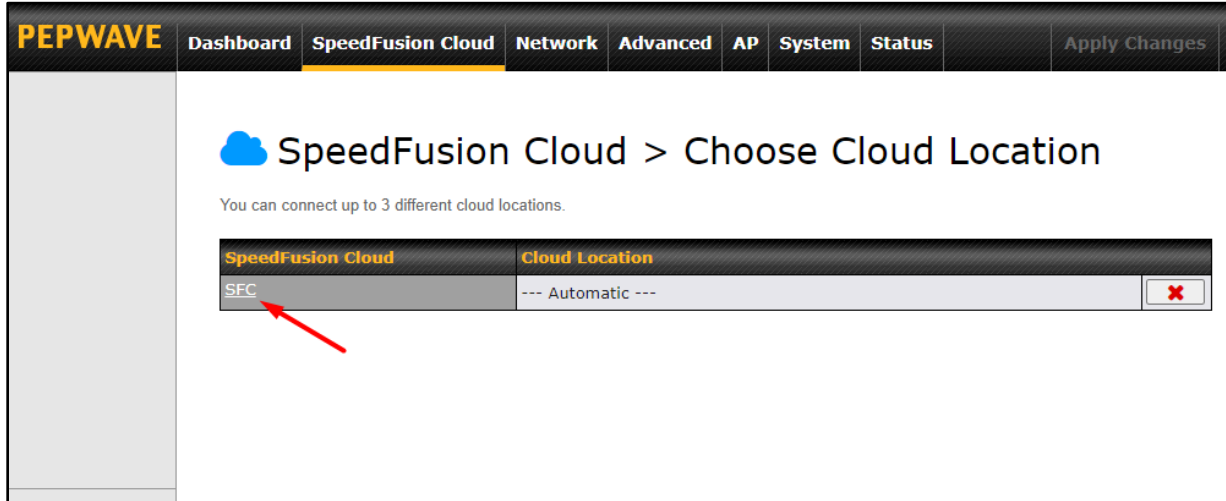
Wi-Fi AP ON [Details](#)

PEPWAVE_EBB4

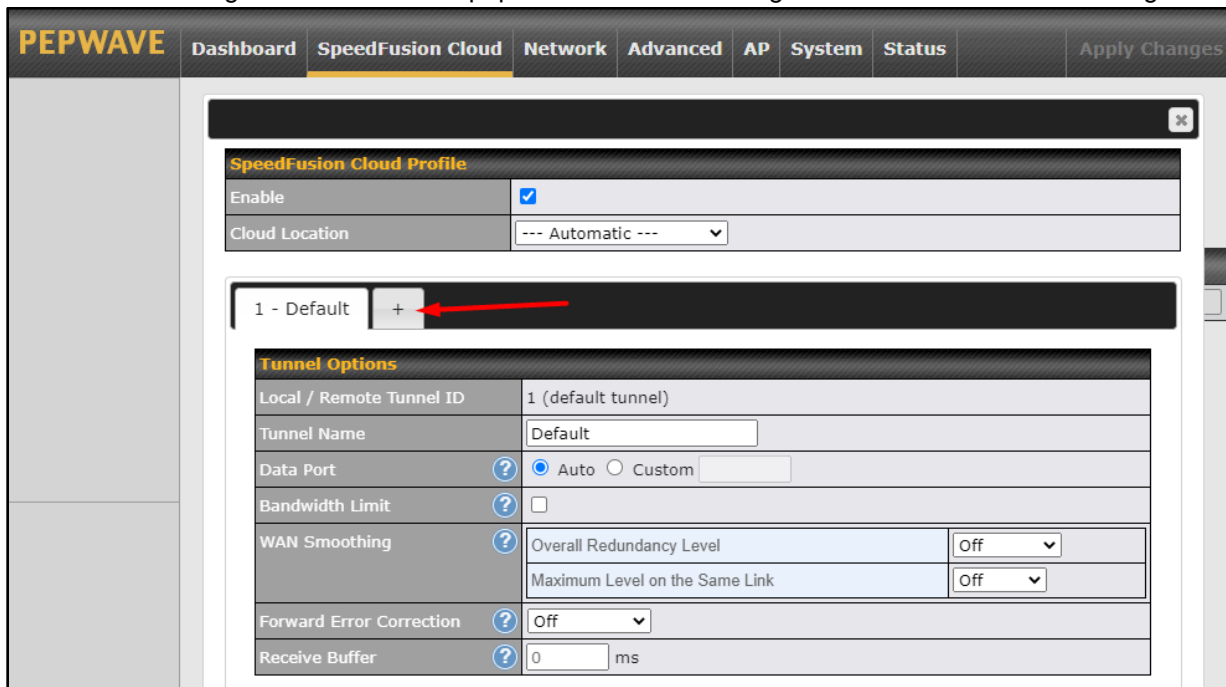
SpeedFusion Cloud

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

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



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



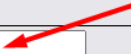
PEPWAVE Dashboard **SpeedFusion Cloud** Network Advanced AP System Status Apply Changes

SpeedFusion Cloud Profile

Enable	<input checked="" type="checkbox"/>
Cloud Location	--- Automatic ---

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

Tunnel Options

Local / Remote Tunnel ID	2	
Tunnel Name	WAN Smoothing 	
Data Port	<input checked="" type="radio"/> Auto <input type="radio"/> Custom <input type="text"/>	
Bandwidth Limit	<input type="checkbox"/>	
WAN Smoothing	Overall Redundancy Level	Normal v
	Maximum Level on the Same Link	Normal v
Forward Error Correction	Off v	
Receive Buffer	0 ms	

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

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

WAN Connection Status

Priority 1 (Highest)
Drag desired (Priority 1) connections here

Priority 2

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

Priority 3
Drag desired (Priority 3) connections here

Disabled

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

LAN Interface
Router IP Address: 192.168.50.1

Wi-Fi AP ■ ON [Details](#)

PEPWAVE_EBB4

SpeedFusion Cloud

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

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

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

The screenshot shows the PEPWAVE web interface with the 'Advanced' tab selected. The 'Outbound Policy' section is active, and a dialog box titled 'Add a New Custom Rule' is open. The dialog box contains the following fields and options:

- Service Name:** to_internet
- Enable:**
- Source:** IP Address (dropdown), 192.168.50.10 (input)
- Destination:** Any (dropdown)
- Protocol:** Any (dropdown), Protocol Selection (dropdown)
- Algorithm:** Priority (dropdown)
- Priority Order:**

Priority Order	Not In Use
Cloud: SFC (1 - Defau...	
Cloud: SFC (2 - WAN ...	
WAN: WAN 1	
WAN: WAN 2	
WAN: Cellular 1	
WAN: Cellular 2	
WAN: Cellular 3	
WAN: Cellular 4	
WAN: USB	
WAN: Wi-Fi WAN	
WAN: LAN 1 as WAN	
WAN: LAN 2 as WAN	
WAN: LAN 3 as WAN	
Lowest Priority	
- When No Connections are Available:** Drop the Traffic (dropdown)
- Terminate Sessions on Connection Recovery:** Enable

Buttons for 'Save' and 'Cancel' are located at the bottom right of the dialog box.

Outbound Policy ?

Custom ✎

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

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


Expert Mode ?

Enabled ✎


Connect Clients to Cloud

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

peplink | Dashboard | **SpeedFusion Cloud** | Network | AP | System | Status | Apply Changes


 **SpeedFusion Cloud**

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



Choose Cloud Location

Which cloud you'd like to connect?



Connect Clients to Cloud

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

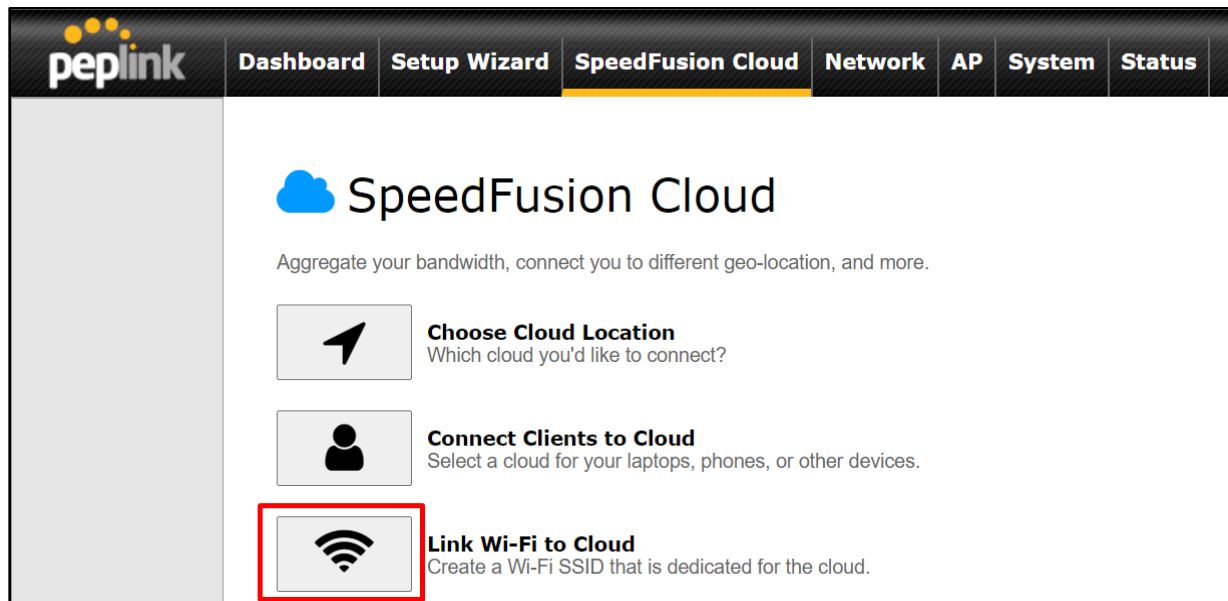
Choose a client from the drop down list > Click + > Save > Apply Changes.

The screenshot shows the Peplink management interface. At the top, there is a navigation bar with the following tabs: Dashboard, SpeedFusion Cloud (highlighted), Network, AP, System, Status, and Apply Changes. A yellow notification bar at the top of the main content area reads: "Saved! Changes will be effective after clicking the 'Apply Changes' button." Below this, the page title is "SpeedFusion Cloud > Connect Clients to Cloud". A sub-header reads: "Traffic from the selected clients will be redirected to the assigned cloud." The main content area features a table titled "SpeedFusion Cloud" with a dropdown menu set to "Automatic". The table has three columns: "Client", "IP Address", and an action column. The first row contains the client name "MY-Room-A-DellPC (40:23:43:26:F7:93)" and the IP address "192.168.52.179", with a red 'X' icon in the action column. The second row shows a dropdown menu with "---" and a blue '+' icon in the action column. A "Save" button is located below the table.

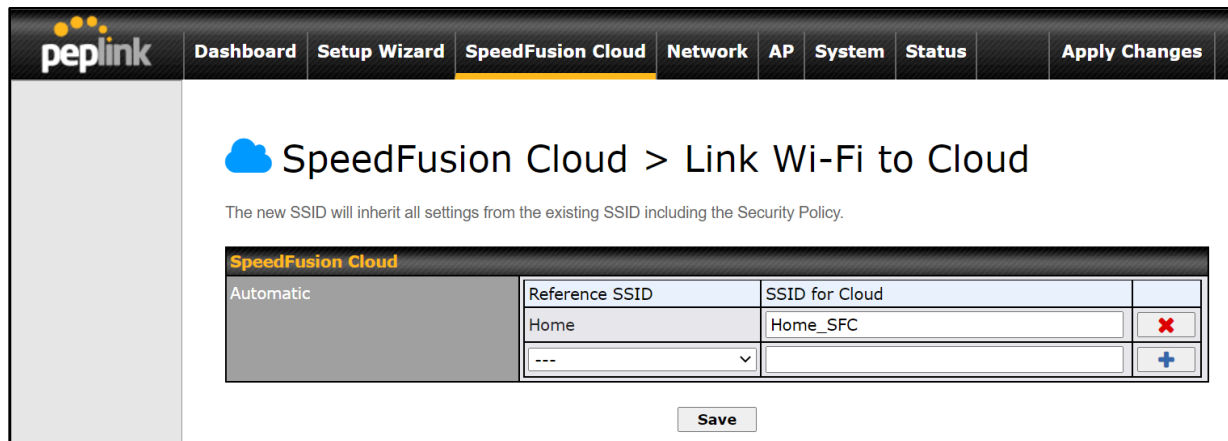
Client	IP Address	
MY-Room-A-DellPC (40:23:43:26:F7:93)	192.168.52.179	X
---		+

Link Wi-Fi to Cloud

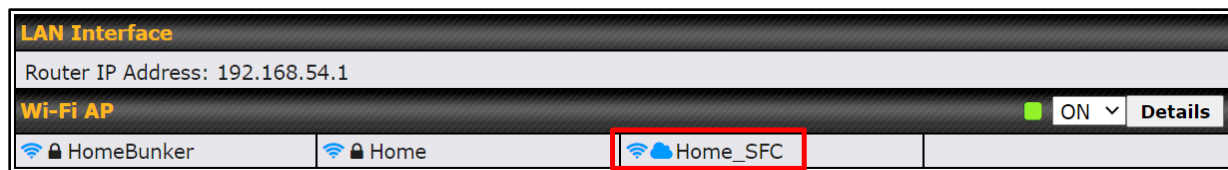
SpeedFusion Cloud provides a convenient way to route the Wi-Fi client to the cloud from **SpeedFusion Cloud > Link Wi-Fi to Cloud**. This option is available for **Balance 20X, Balance 30 Pro, and Balance One**.



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



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



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	<input type="button" value="X"/>
VLAN2	2	3.3.3.3/24	<input type="button" value="X"/>

This represents the LAN interfaces that are active on your router (including VLAN). A grey “X” means that the VLAN is used in other settings and cannot be deleted. You can find which settings are using the VLAN by hovering over the grey “X”.

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

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

IP Settings

IP Address

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

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

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

Layer 2 PepVPN Bridging		?
PepVPN Profiles to Bridge	<input type="text"/> No profile is available	Help Close
Spanning Tree Protocol	<input type="checkbox"/>	If you want to enable DHCP Option 82 Injection, please click here .
Override IP Address when bridge connected	<input checked="" type="radio"/> Do not override <input type="radio"/> Static <input type="radio"/> By DHCP <input type="radio"/> As None	This allow the device to inject Option 82 with Router Name information before forwarding the DHCP Request packet to PepVPN peer, such that the DHCP Server can identify where does this request come from.
DHCP Server		

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

originates from.



DHCP Server									
DHCP Server	<input checked="" type="checkbox"/>	Enable							
DHCP Server Logging	<input type="checkbox"/>								
IP Range		255.255.255.0 (/24)							
Lease Time		0	Mins						
DNS Servers	<input checked="" type="checkbox"/>	Assign DNS server automatically							
BOOTP	<input type="checkbox"/>								
Extended DHCP Option	Option	Value							
	<i>No Extended DHCP Option</i>								
	Add								
DHCP Reservation	<input type="checkbox"/>								
		<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	When this setting is enabled, the DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Pepwave router's DHCP server can prevent IP address collision on the LAN.
DHCP Server Logging	Enable logging of DHCP events in the eventlog by selecting the checkbox.
IP Range & Subnet Mask	These settings allocate a range of IP addresses that will be assigned to LAN computers by the Pepwave router's DHCP server.
Lease Time	This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of the lease time, the assigned IP address will no longer be valid and renewal of the IP address assignment will be required.
DNS Servers	This option allows you to input the DNS server addresses to be offered to DHCP clients. If Assign DNS server automatically is selected, the Pepwave router's built-in DNS server address (i.e., LAN IP address) will be offered.
BOOTP	Check this box to enable BOOTP on older networks that still require it.
Extended DHCP Option	In addition to standard DHCP options (e.g., DNS server address, gateway address, subnet mask), you can specify the value of additional extended DHCP options, as defined in RFC 2132. With these extended options enabled, you can pass additional configuration information to LAN hosts. To define an extended DHCP option, click the Add button, choose the option to define and enter its value. For values that are in IP address list format, you can enter one IP address per line in the provided text area input control. Each option can be defined once only.
DHCP Reservation	This setting reserves the assignment of fixed IP addresses for a list of computers on the LAN. The computers to be assigned fixed IP addresses on the LAN are identified by their MAC addresses. The fixed IP address assignment is displayed as a cross-reference list between the computers' names, MAC

addresses, and fixed IP addresses.

Name (an optional field) allows you to specify a name to represent the device. MAC addresses should be in the format of **00:AA:BB:CC:DD:EE**. Press  to create a new record. Press  to remove a record. Reserved client information can be imported from the **Client List**, located at **Status>Client List**. For more details, please refer to **Section 22.3**.

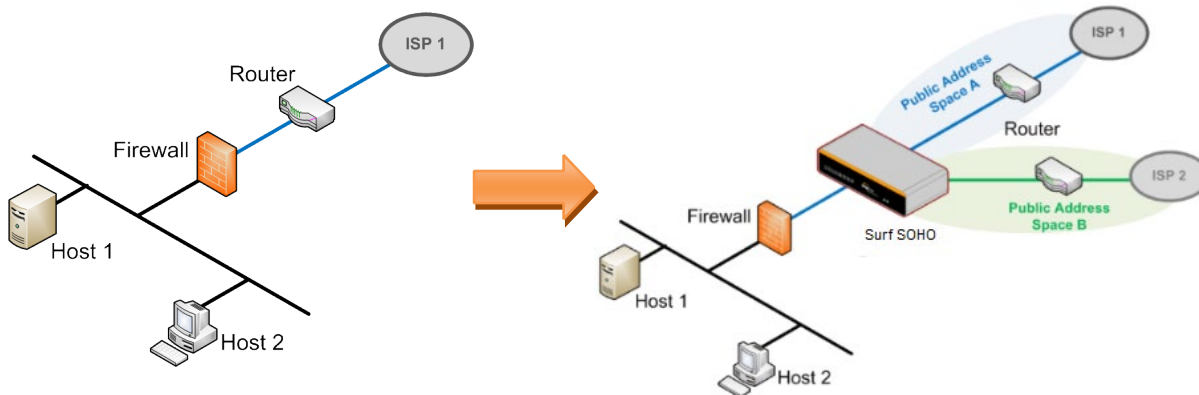
DHCP Relay Settings	
DHCP Relay	 <input checked="" type="checkbox"/> Enable
DHCP Server IP Address	DHCP Server 1: <input type="text"/> DHCP Server 2: <input type="text"/>
DHCP Option 82	 <input type="checkbox"/>
DHCP Relay Logging	<input type="checkbox"/>

DHCP Relay	Enter the address of the DHCP server here. DHCP requests will be relayed to it.
DHCP Server IP Address	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 DHCP Server 1 and DHCP Server 2 fields.
DHCP Option 82	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.
DHCP Relay Logging	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 the WAN for Drop-in mode, various settings including the WAN's connection method and IP address will be automatically updated.


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


After successfully setting up the 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 ?							
Enable	<input checked="" type="checkbox"/>						
WAN for Drop-In Mode ?	WAN ▼ <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 ?	<input checked="" type="checkbox"/>						
Shared IP Address ?	<input type="text"/> 255.255.255.0 (/24) ▼						
Static Route	<table border="1"> <thead> <tr> <th>Destination Network</th> <th>Subnet Mask</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td>255.255.255.0 (/24) ▼</td> <td style="text-align: center;">+</td> </tr> </tbody> </table>	Destination Network	Subnet Mask		<input type="text"/>	255.255.255.0 (/24) ▼	+
	Destination Network	Subnet Mask					
<input type="text"/>	255.255.255.0 (/24) ▼	+					
WAN Default Gateway ?	<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> <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <div style="text-align: right;">✕</div>						
WAN DNS Servers ?	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>							

Enable	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.
WAN for Drop-In Mode	Select the WAN port to be used for drop-in mode. If WAN is selected, the high availability feature will be disabled automatically.
Shared Drop-In IP^A	<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>
Shared IP Address^A	Access to this IP address will be passed through to the LAN port if this device is not serving the service being accessed. The shared IP address will be used in connecting to hosts on the WAN (e.g., email notification, remote syslog, etc.) The device will also listen on the IP address when hosts on the WAN access services served on this device (e.g., web admin accesses from WAN, DNS server, etc.)
WAN Default	Enter the WAN router's IP address in this field. If there are more hosts in addition to the router on the

Gateway	WAN segment, click the  button next to "WAN Default Gateway" and check the other host(s) on the WAN segment box and enter the IP address of the hosts that need to access LAN devices or be accessed by others.
WAN DNS Servers	Enter the selected WAN's corresponding DNS server IP addresses.



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

Static Route Settings 			
Static Route	Destination Network	Subnet Mask	Gateway
	192.168.113.0	255.255.255.0 (/24) ▼	192.168.112.10
		255.255.255.0 (/24) ▼	






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

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

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

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

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

NAT Traffic can only be initiated from local to remote, and these traffic will be NAT'ed and behaves like coming from the same Virtual IP Address.

DNS Proxy Settings ?																			
Enable	<input checked="" type="checkbox"/>																		
DNS Caching ?	<input type="checkbox"/>																		
Include Google Public DNS Servers ?	<input type="checkbox"/>																		
Local DNS Records ?	<table border="1"> <thead> <tr> <th>Host Name</th> <th>IP Address</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td style="text-align: center;">+</td> </tr> </tbody> </table>	Host Name	IP Address		<input type="text"/>	<input type="text"/>	+												
Host Name	IP Address																		
<input type="text"/>	<input type="text"/>	+																	
Domain Lookup Policy ?	<table border="1"> <thead> <tr> <th>Domain</th> <th>Connection</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td style="text-align: center;">+</td> </tr> </tbody> </table>	Domain	Connection		<input type="text"/>	<input type="text"/>	+												
Domain	Connection																		
<input type="text"/>	<input type="text"/>	+																	
DNS Resolvers ?	<table border="1"> <thead> <tr> <th>WAN Connection</th> <th>DNS Servers</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/> WAN 1</td> <td>1.1.1.1 1.0.0.1</td> </tr> <tr> <td><input type="checkbox"/> WAN 2</td> <td></td> </tr> <tr> <td><input type="checkbox"/> WAN 3</td> <td></td> </tr> <tr> <td><input type="checkbox"/> WAN 4</td> <td>8.8.8.8 8.8.4.4</td> </tr> <tr> <td><input type="checkbox"/> WAN 5</td> <td></td> </tr> <tr> <td><input type="checkbox"/> Mobile Internet</td> <td></td> </tr> <tr> <th>LAN Connection</th> <th>DNS Servers</th> </tr> <tr> <td><input type="checkbox"/> Untagged LAN</td> <td><input type="text"/></td> </tr> </tbody> </table> <p>Preferred connections are shown with <input checked="" type="checkbox"/></p>	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	<input type="text"/>
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	<input type="text"/>																		

Enable	<p>To enable the DNS proxy feature, check this box, and then set up the feature at Network>LAN>DNS Proxy Settings.</p> <p>A DNS proxy server can be enabled to serve DNS requests originating from LAN/PPTP/SpeedFusion™ peers. Requests are forwarded to the DNS servers/resolvers defined for each WAN connection.</p>
DNS Caching	<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, DNS Caching is disabled.</p>
Include Google Public DNS Servers	<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>
Local DNS Records	<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 ?. Click + to create a new record. Click ✖ to remove a record.</p>

Domain Lookup Policy

DNS proxy will look up the domain names defined here using only the specified connections.

DNS Resolvers^A

Check the box to enable the WINS server. A list of WINS clients will be displayed at **Network>LAN>DNS Proxy Settings>DNS Resolvers**.

This field specifies which DNS resolvers will receive forwarded DNS requests. If no WAN/VPN/LAN DNS resolver is selected, all of the WAN's DNS resolvers will be selected. If a SpeedFusion™ peer is selected, you may enter the VPN peer's DNS resolver IP address(es). Queries will be forwarded to the selected connections' resolvers. If all of the selected connections are down, queries will be forwarded to all resolvers on healthy WAN connections.

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

Port Settings

To configure port settings, navigate to **Network > LAN > 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"/>	Auto	<input checked="" type="checkbox"/>
4	LAN Port 4	<input checked="" type="checkbox"/>		

Save

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

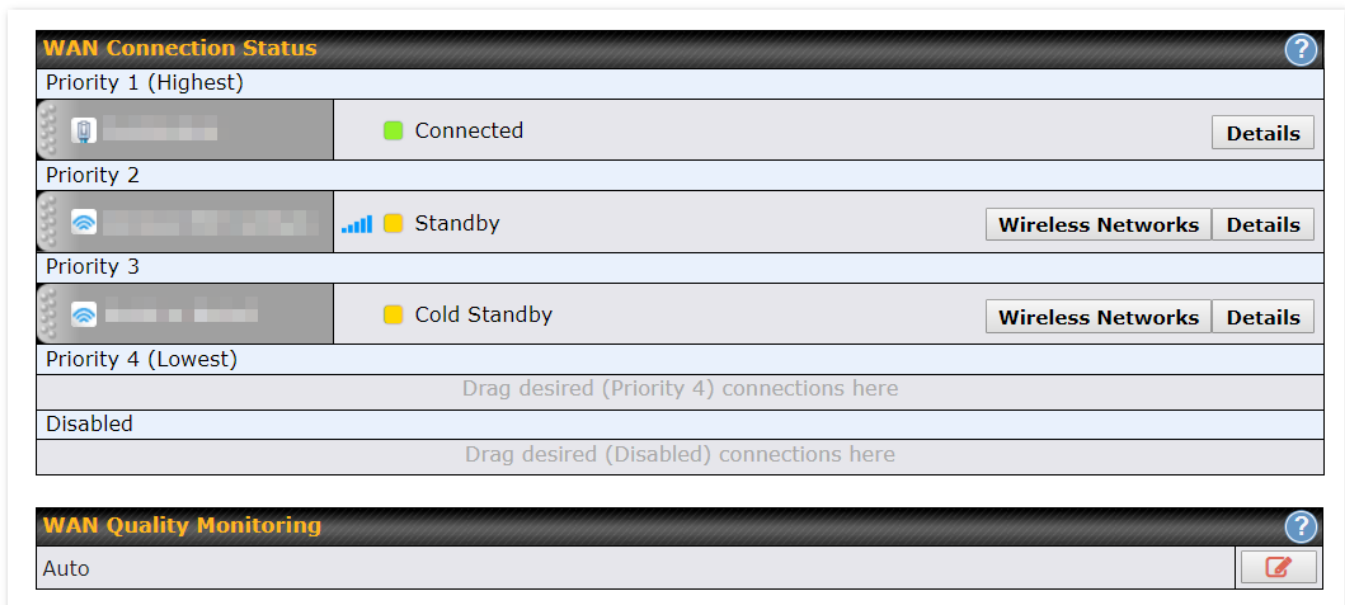
Speed

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

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.

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.

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"/> Default
Connection Method ?	DHCP ▼
Routing Mode ?	<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 ?	<input type="checkbox"/>
Independent from Backup WANs ?	<input type="checkbox"/>
Standby State ?	<input checked="" type="radio"/> Remain connected <input type="radio"/> Disconnect
Reply to ICMP Ping ?	<input checked="" type="radio"/> Yes <input type="radio"/> No
Upload Bandwidth ?	<input type="text" value="10"/> Mbps ▼
Download Bandwidth ?	<input type="text" value="110"/> Mbps ▼

WAN Connection Name	Enter a name to represent this WAN connection.
Schedule	Click the drop-down menu to apply a time schedule to this interface (only visible if Schedules have been created in System > Schedule)
Connection Method	There are five possible connection methods for Ethernet WAN: <ul style="list-style-type: none"> • DHCP • Static IP • PPPoE • L2TP • GRE

The connection method and details are determined by, and can be obtained from the ISP.

Routing Mode	This field shows that NAT (network address translation) will be applied to the traffic routed over this WAN connection. IP Forwarding is available when you click the link in the help text.
Hostname	Provide a hostname for this WAN port if requested by the ISP
DNS Servers	Select a DNS server for this port to use. This port can either be automatically selected or manually designated.
Ip Passthrough	When this IP Passthrough option is active, after the ethernet WAN connection is up, the router's DHCP server will offer the connection's IP address to one LAN client. All incoming or outgoing traffic will be routed without NAT.
Independent from Backup WANs	If this is checked, the connection will be working independent from other Backup WAN connections. Those in Backup Priority will ignore the status of this WAN connection, and will be used when none of the other higher priority connections are available
Standby State	This option allows you to choose whether to remain the connection connected or disconnect it when this WAN connection is no longer in the highest priority and has entered the standby state.
Reply to ICMP Ping	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")
Upload Bandwidth	This field refers to the maximum upload speed. This value is referenced when default weight is chosen for outbound traffic and traffic prioritization. A correct value can result in effective traffic prioritization and efficient use of upstream bandwidth.
Download Bandwidth	This field refers to the maximum download speed. Default weight control for outbound traffic will be adjusted according to this value.

WAN>Physical Interface Settings

Port Speed	This setting specifies port speed and duplex configurations of the WAN port. By default, Auto 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 Advertise Speed checkbox.
MTU	This setting specifies the maximum transmission unit. By default, MTU is set to Custom 1440 . You may adjust the MTU value by editing the text field. Click Default to restore the default MTU value.

Select **Auto** and the appropriate MTU value will be automatically detected. Auto-detection will run each time the WAN connection establishes.

MSS

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 **Auto**, the MSS will also be set automatically. By default, MSS is set to **Auto**.

MAC Address Clone

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 **Default** restores the MAC address to the default value.

VLAN

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

Health Check 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 specifies the number of health check attempts the router will make. Upon reaching this number, the link will be considered as failed.

Recovery Retries: This specifies the number of successful health checks a failed link 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 Email Notification . <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.

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 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

Channel Width	choose between the available options 20 Mhz, 20/40Mhz, 20/40/80 Mhz																														
Channel Selection	Determine whether the channel will be automatically selected. If you select custom, the following table will appear: <div style="border: 1px solid gray; padding: 5px; margin: 10px 0;"> <p style="text-align: center;">Edit auto channel ✕</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 40%;">Scan Channels</th> <th style="width: 10%;">Clear</th> <th style="width: 10%;">All</th> <th colspan="3"></th> </tr> </thead> <tbody> <tr> <td colspan="4">2.4 GHz:</td> <td colspan="2"></td> </tr> <tr> <td><input checked="" type="checkbox"/> 1</td> <td><input checked="" type="checkbox"/> 2</td> <td><input checked="" type="checkbox"/> 3</td> <td><input checked="" type="checkbox"/> 4</td> <td colspan="2"><input checked="" type="checkbox"/> 5</td> </tr> <tr> <td><input checked="" type="checkbox"/> 6</td> <td><input checked="" type="checkbox"/> 7</td> <td><input checked="" type="checkbox"/> 8</td> <td><input checked="" type="checkbox"/> 9</td> <td colspan="2"><input checked="" type="checkbox"/> 10</td> </tr> <tr> <td><input checked="" type="checkbox"/> 11</td> <td colspan="5"></td> </tr> </tbody> </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																															
Output Power	Low, Medium, High, Max (boost options for tickbox).																														

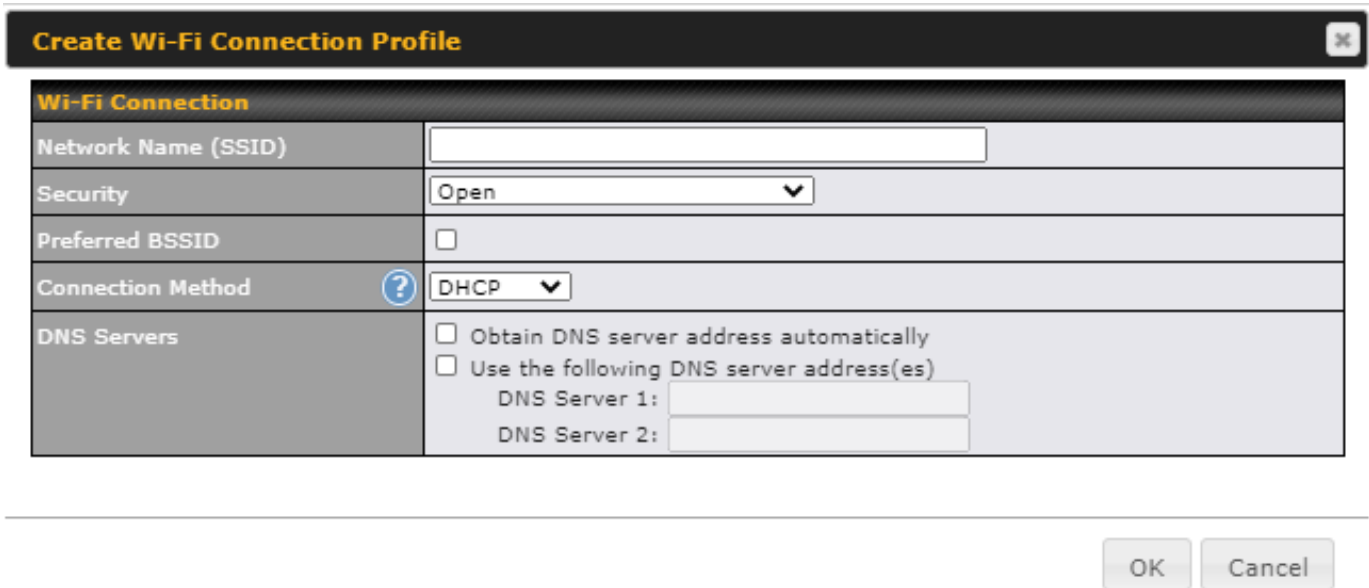
	<p>Max is the Maximum transmit power supported for that country / Maximum power supported of that device (the smaller value). High, Medium, Low is having -3dBm each from the previous level. Transmit power of 2.4Ghz is generally approximately 20dBm.</p>
Data Rate	One of the available advanced options is the ability to configure the Data rate according to the MCS Index (see http://mcsindex.com/)
Roaming	Checking this box will enable Wi-Fi roaming. Click the  icon for additional options.
Roaming Algorithm	select Normal (default) or Advanced (enables Intensive Scan options)
Roaming Signal Level Threshold	Configure the Roaming Signal Level Threshold in dBm
Roaming Signal Level Gain	Configure the Roaming Signal Level Gain in dBm
Roaming Check Interval	Configure the Roaming Check Interval in Seconds
Connect to Any Open Mode AP	This option is to specify whether the Wi-Fi WAN will connect to any open mode access points it finds.
Beacon Miss Counter	Client devices will disconnect from the AP when this amount of beacons is missed
Channel Scan Interval	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.



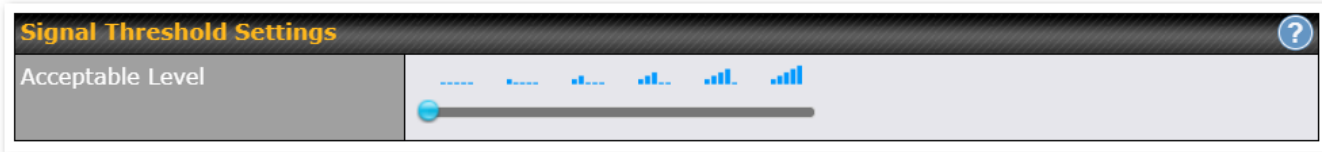
This will open a window similar to the one shown below:



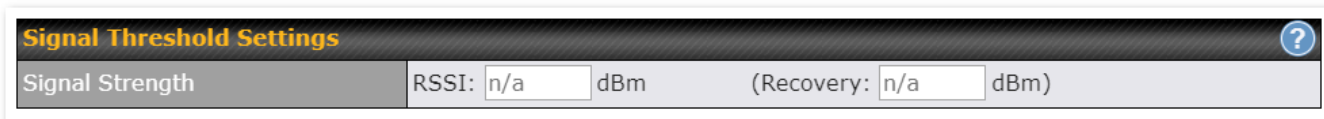
Network Name (SSID)	Enter a name to represent this Wi-Fi connection.
Security	This option allows you to select which security policy is used for this wireless network.

	<p>Available options:</p> <ul style="list-style-type: none"> Open <table border="1" data-bbox="354 359 1114 394"> <tr> <td>Security</td> <td>Open ▾</td> </tr> </table> WEP <table border="1" data-bbox="354 436 1114 533"> <tr> <td>Security</td> <td>WEP ▾</td> </tr> <tr> <td>Encryption Key</td> <td><input type="text"/> <input checked="" type="checkbox"/> Hide Characters</td> </tr> </table> WPA/WPA2 – Personal <table border="1" data-bbox="354 575 1114 672"> <tr> <td>Security</td> <td>WPA/WPA2-Personal ▾</td> </tr> <tr> <td>Shared Key</td> <td><input type="text"/> <input checked="" type="checkbox"/> Hide Characters</td> </tr> </table> WPA/WPA2 – Enterprise <table border="1" data-bbox="354 714 1114 1016"> <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> WPA3 – Personal <table border="1" data-bbox="354 1058 1146 1167"> <tr> <td>Security</td> <td>WPA3-Personal ▾</td> </tr> <tr> <td>Shared Key</td> <td><input type="text"/> <input checked="" type="checkbox"/> Hide Characters</td> </tr> </table> WPA2/WPA3 – Personal <table border="1" data-bbox="354 1209 1138 1318"> <tr> <td>Security</td> <td>WPA2/WPA3-Personal ▾</td> </tr> <tr> <td>Shared Key</td> <td><input type="text"/> <input checked="" type="checkbox"/> Hide Characters</td> </tr> </table> 802.1x with dynamic WEP key <table border="1" data-bbox="354 1360 1138 1684"> <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	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	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	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	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"/>																																														
Preferred BSSID	Configure the BSSID; the BSSID is the MAC address of the wireless access point (WAP)																																														
Connection Method	Choose DHCP or Static IP																																														
DNS servers	Configure the DNS servers that this WAN connection should use																																														

WAN>Signal threshold settings



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)



Indication of WiFi strength values:

Signal Strength (dBm)	Description
-30 dBm	Maximum signal strength
-50 dBm	Excellent signal strength
-60 dBm	Good, reliable signal strength
-67 dBm	Minimum signal strength for applications that require very reliable, timely delivery of data packets.
-70 dBm	Not strong; goof for soet internet browsing and email
-80 dBm	Unreliable
-90 dBm	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 PW

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

Profile	Remote ID	Remote Address(es)	
No VPN Connection Defined			
New Profile			

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)					
Add Rule					

PepVPN Local ID

Local ID [?](#) SURF_SOHO_8F18

PepVPN Settings

Link Failure Detection Time [?](#)

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

Shorter detection time incurs more health checks and higher bandwidth overhead

[Save](#)

To configure PepVPN, navigate to **Advanced > PepVPN** and select **New Profile**.
 The example below had allPepVPN advanced features enabled.


PepVPN Profile ?

Name	<input type="text"/>	
Active	<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	Remote ID <input type="text"/>	Pre-shared Key <input type="text"/>
NAT Mode	<input type="checkbox"/>	
Remote IP Address / Host Names (Optional)	<input type="text"/>	
	If this field is empty, this field on the remote unit must be filled	
Cost	<input type="text" value="10"/>	

1
2
3 ✕
+

Tunnel Options

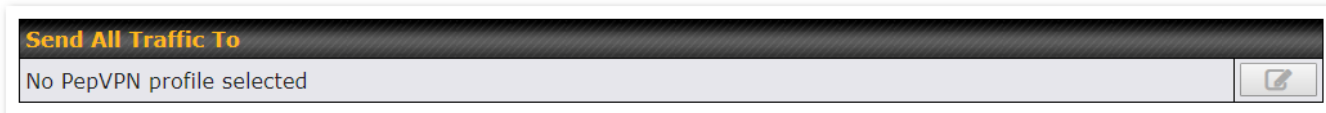
Local / Remote Tunnel ID	1 (default tunnel)	
Tunnel Name	<input type="text"/>	
Data Port	UDP <input type="checkbox"/> Auto <input type="checkbox"/> Custom <input type="text"/>	
Bandwidth Limit	<input checked="" type="checkbox"/> Download: <input type="text"/> kbps (0: Unlimited) <input type="checkbox"/> Upload: <input type="text"/> kbps (0: Unlimited)	
Receive Buffer	<input type="text" value="0"/> ms	
Use IP ToS	<input checked="" type="checkbox"/>	
Latency Difference Cutoff	<input type="text" value="500"/> ms	


<div style="background-color: #cccccc; width: 100px; height: 15px; margin: 0 auto;"></div>	
Name	This field is for specifying a name to represent this profile. The name can be any combination of alphanumeric characters (0-9, A-Z, a-z), underscores (_), dashes (-), and/or non-leading/trailing spaces ().
Active	When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled.
Encryption	By default, VPN traffic is encrypted with 256-bit AES . If Off is selected on both sides of a VPN connection, no encryption will be applied.
Authentication	Select from By Remote ID Only , Preshared Key . When selecting By Remote ID Only , be sure to enter a unique peer ID number in the Remote ID field.
Remote ID / Pre-shared Key	This optional field becomes available when Remote ID / Pre-shared Key is selected as the Pepwave Surf SOHO's VPN Authentication method, as explained above. Pre-shared Key defines the pre-shared key used for this particular VPN connection. The VPN connection's session key will be further protected by the pre-shared key. The connection will be up only if the pre-shared keys on each side match. When the peer is running firmware 5.0+, this setting will be ignored.
NAT Mode	Check this box to allow the local DHCP server to assign an IP address to the remote peer. When NAT Mode is enabled, all remote traffic over the VPN will be tagged with the assigned IP address using network address translation.
Remote IP Address / Host Names (Optional)	<p>If NAT Mode is not enabled, you can enter a remote peer's WAN IP address or hostname(s) here. If the remote uses more than one address, enter only one of them here. Multiple hostnames are allowed and can be separated by a space character or carriage return. Dynamic-DNS host names are also accepted.</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>
Cost	Define path cost for this profile. OSPF will determine the best route through the network using the assigned cost. Default: 10
Data Port	This field is used to specify a UDP or TCP port number for transporting outgoing VPN data. If Default is selected, UDP port 4500 will be used. Port 32015 will be used if port 4500 is unavailable. If Custom is selected, enter an outgoing port number from 1 to 65535.
Bandwidth Limit	Define maximum download and upload speed to each individual peer. This functionality requires the peer to use PepVPN version 4.0.0 or above.
Receive Buffer	Receive Buffer can help to reduce out-of-order packets and jitter, but will introduce extra latency to the tunnel. Default is 0 ms, which disable the buffer, and maximum buffer size is 2000 ms.

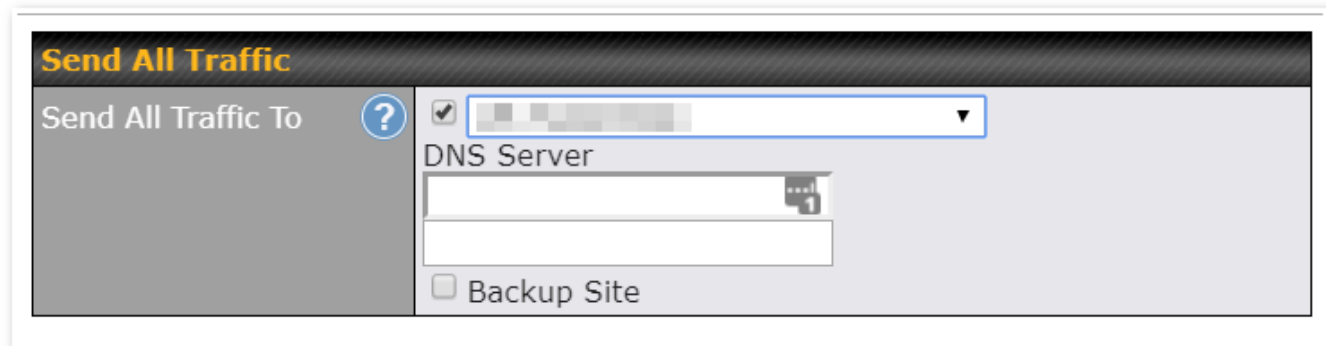
Multiple PepVPN profiles between the same 2 sites

Enable this advanced feature to create up to 5 PepVPN tunnels from your router to the same remote location, each with different behavior.
See: <https://forum.peplink.com/t/outbound-policies-within-a-pepvpn-or-speedfusion-tunnel/>

PepVPN>Send ALL traffic

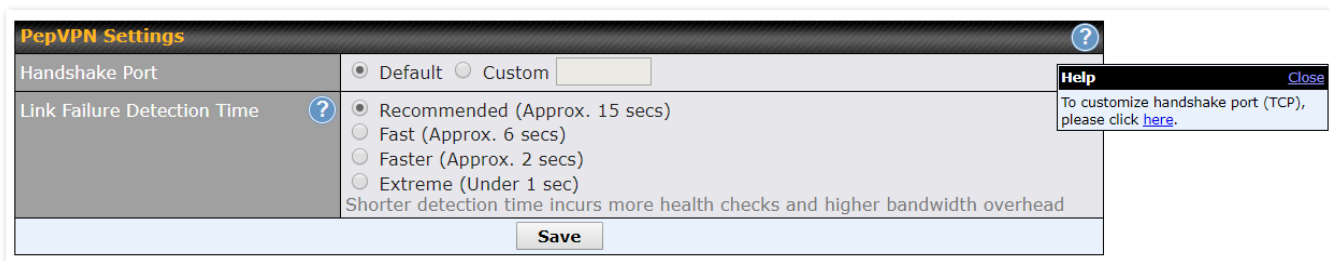


This feature allows you to redirect all traffic to a specified PepVPN connection. Click the  button to select your connection and the following menu will appear:




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.

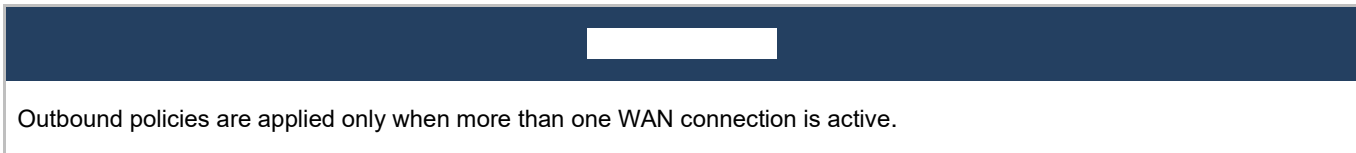
Link Failure Detection Time

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.



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	✖
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
✕

Service Name	<input type="text"/>		
Enable	<input checked="" type="checkbox"/>		
Source	<input type="text" value="Any"/>		
Destination	<input type="text" value="IP Network"/>	<input type="text"/>	Mask: <input type="text" value="255.255.255.0 (/24)"/>
Protocol	<input type="text" value="Any"/>	<input type="text" value=":: Protocol Selection ::"/>	
Algorithm	<input type="text" value="Enforced"/>		
Enforced Connection	<input type="text"/>		

[Title Bar]	
Service Name	This field is for specifying a name to represent this profile. The name can be any combination of alphanumeric characters (0-9, A-Z, a-z), underscores (_), dashes (-), and/or non-leading/trailing spaces ().
Enable	When this box is checked, this outbound policy will be enabled. Otherwise, it will be disabled.
Source	This setting specifies the source IP address, IP network, or MAC address for traffic that matches the rule.
Destination	This setting specifies the destination IP address, IP network, or domain name for traffic that matches the rule.
Protocol	This setting specifies the IP protocol and port of traffic that matches this rule.
Algorithm	This setting specifies the behavior of the Pepwave router for the custom rule. One of the following values can be selected: <ul style="list-style-type: none"> Enforced : Enforce traffic matching this rule through a selected WAN or VPN connection. Priority: Prioritise traffic matching this rule through selected WAN or VPN connection(s)
Enforced Connection	Specify the WAN or VPN connection to be used for routing traffic regardless of the connection's health status.

<p>When No Connections are Available</p>	<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"> • Drop the Traffic - Traffic will be discarded. • Use Any Available Connections - Traffic will be routed to any available Connection, even it is not selected in the list. • Fall-through to Next Rule - Traffic will continue to match next Outbound Policy rule just like this rule is inactive.
<p>Terminate Sessions on Connection Recovery</p>	<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) ?	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="background-color: #333; color: white;">Connection / IP Address(es)</th> <th style="background-color: #333; color: white;">All</th> <th style="background-color: #333; color: white;">Clear</th> </tr> </thead> <tbody> <tr><td><input type="checkbox"/> [blurred]</td></tr> <tr><td><input type="checkbox"/> [blurred]</td></tr> <tr><td><input type="checkbox"/> [blurred]</td></tr> <tr><td><input type="checkbox"/> [blurred]</td></tr> <tr><td><input type="checkbox"/> [blurred]</td></tr> </tbody> </table>	Connection / IP Address(es)	All	Clear	<input type="checkbox"/> [blurred]	<input type="checkbox"/> [blurred]	<input type="checkbox"/> [blurred]	<input type="checkbox"/> [blurred]	<input type="checkbox"/> [blurred]
Connection / IP Address(es)	All	Clear							
<input type="checkbox"/> [blurred]									
<input type="checkbox"/> [blurred]									
<input type="checkbox"/> [blurred]									
<input type="checkbox"/> [blurred]									
<input type="checkbox"/> [blurred]									
Server IP Address ?	<input type="text"/>								

Enable This setting specifies whether the inbound service takes effect. When **Enable** is checked, the inbound service takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When this setting is disabled, the inbound service does not take effect: the Pepwave router disregards the other parameters of the rule.

Service Name This setting identifies the service to the system administrator. Valid values for this setting consist of only alphanumeric and underscore “_” characters.


Protocol

The **Protocol** setting, along with the **Port** setting, specifies the protocol of the service as TCP, UDP, ICMP, or IP. Traffic that is received by the Pepwave router via the specified protocol at the specified port(s) is forwarded to the LAN hosts specified by the **Servers** setting. Please see below for details on the **Port** and **Servers** settings. Alternatively, the **Protocol Selection Tool** drop-down menu can be used to automatically fill in the protocol and a single port number of common Internet services (e.g. HTTP, HTTPS, etc.). After selecting an item from the **Protocol Selection Tool** drop-down menu, the protocol and port number remain manually modifiable.

Port

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


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

Port	 Any Port
------	--

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

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

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

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

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

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

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

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

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

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

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

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	
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	Connection / Inbound IP Address(es) <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 <input type="checkbox"/> USB												
Outbound Mappings	Connection / Outbound IP Address <table border="1"> <tr> <td>WAN 1</td> <td>10.88.3.158 (Interface IP) ▾</td> </tr> <tr> <td>WAN 2</td> <td>Interface IP ▾</td> </tr> <tr> <td>Wi-Fi WAN</td> <td>Interface IP ▾</td> </tr> <tr> <td>Cellular 1</td> <td>Interface IP ▾</td> </tr> <tr> <td>Cellular 2</td> <td>Interface IP ▾</td> </tr> <tr> <td>USB</td> <td>Interface IP ▾</td> </tr> </table>	WAN 1	10.88.3.158 (Interface IP) ▾	WAN 2	Interface IP ▾	Wi-Fi WAN	Interface IP ▾	Cellular 1	Interface IP ▾	Cellular 2	Interface IP ▾	USB	Interface IP ▾
WAN 1	10.88.3.158 (Interface IP) ▾												
WAN 2	Interface IP ▾												
Wi-Fi WAN	Interface IP ▾												
Cellular 1	Interface IP ▾												
Cellular 2	Interface IP ▾												
USB	Interface IP ▾												

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

these addresses to a number of public IP addresses (specified below) to facilitate outbound traffic. This option is only available when **IP Network** is selected.

Inbound Mappings

This setting specifies the WAN connections and corresponding WAN-specific Internet IP addresses on which the system should bind. Any access to the specified WAN connection(s) and IP address(es) will be forwarded to the LAN host. This option is only available when **IP Address** is selected in the **LAN Client(s)** field.

Note that inbound mapping is not needed for WAN connections in drop-in mode or IP forwarding mode. Also note that each WAN IP address can be associated to one NAT mapping only.

Outbound Mappings

This setting specifies the WAN IP addresses that should be used when an IP connection is made from a LAN host to the Internet. Each LAN host in an IP range or IP network will be evenly mapped to one of each selected WAN's IP addresses (for better IP address utilization) in a persistent manner (for better application compatibility).

Note that if you do not want to use a specific WAN for outgoing accesses, you should still choose default here, then customize the outbound access rule in the **Outbound Policy** section. Also note that WAN connections in drop-in mode or IP forwarding mode are not shown here.

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

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

QoS

Bandwidth Control

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
	0 <input type="text"/> Mbps <input type="button" value="v"/>	0 <input type="text"/> Mbps <input type="button" value="v"/> (0: Unlimited)

Application Prioritization

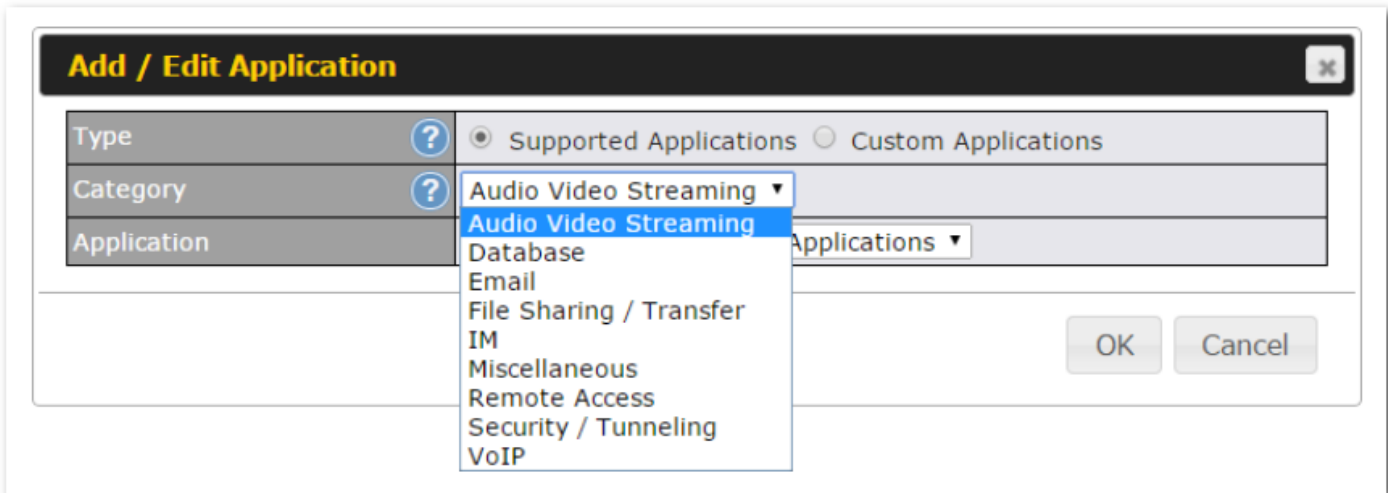
Three application priority levels can be set: **↑ High**, **– Normal**, and **↓ Low**. Pepwave routers can detect various application traffic types by inspecting the packet content. Select an application by choosing a supported application, or by defining a custom application manually. The priority preference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

Application	Priority	Action
	↑ 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

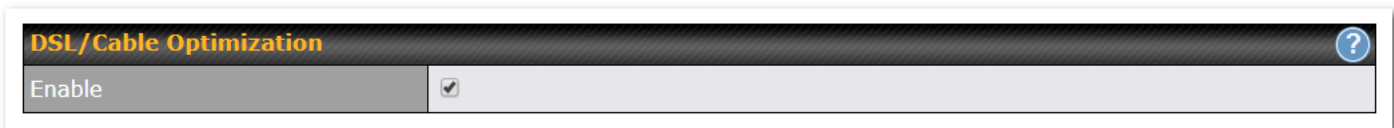
Click the **Add** button to define a custom application. Click the button in the **Action** column to delete the custom application in the corresponding row.

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.



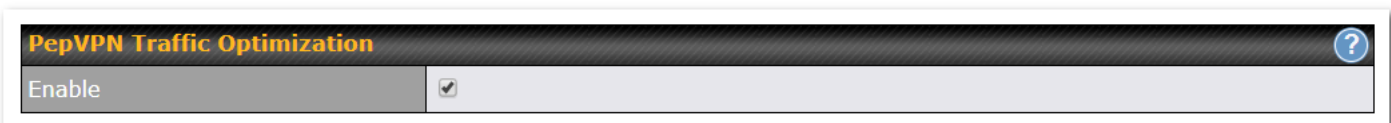
DSL/ Cable Optimization

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.



PepVPN Traffic Optimization

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



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	✓

Add Rule

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

Rule	Protocol	WAN	Source	Destination	Action
Default	Any	Any	Any	Any	✓

Add Rule

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

Rule	Protocol	Source	Destination	Action
Default	Any	Any	Any	✓

Add Rule

Intrusion Detection and DoS Prevention

Disabled

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

Rule	Service	WAN	Source	Action
Default	Any	Any	Any	✓

Add Rule

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	Any ▾ ← :: Protocol Selection :: ▾
Source	Any Address ▾
Destination	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

Save Cancel

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	
test	Any	Any	Any		
Default	Any	Any	Any		
<input type="button" value="Add Rule"/>					

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

Save Cancel

New Firewall Rule	
Rule Name	This setting specifies a name for the firewall rule.
Enable	<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>
WAN Connection (Inbound)	Select the WAN connection that this firewall rule should apply to.
Protocol	<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"> • TCP • UDP • ICMP • IP <p>Alternatively, the Protocol Selection Tool drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.)</p> <p>After selecting an item from the Protocol Selection Tool drop-down menu, the protocol and port number remains manually modifiable.</p>
Source IP & Port	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 Source setting.

Destination IP & Port	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 Destination setting.
Action	This option allows you to define whether to allow or deny an IP session matching this Firewall Rule
Event Logging	<p>This setting specifies whether or not to log matched firewall events. The logged messages are shown on the page Status>Event Log. A sample message is as follows: Aug 13 23:47:44 Denied CONN=Ethernet WAN SRC=20.3.2.1 DST=192.168.1.20 LEN=48 PROTO=TCP SPT=2260 DPT=80</p> <ul style="list-style-type: none"> • CONN: The connection where the log entry refers to • SRC: Source IP address • DST: Destination IP address • LEN: Packet length • PROTO: Protocol • SPT: Source port • DPT: Destination port

Click **Save** to store your changes. To create an additional firewall rule, click 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.

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

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

Add Rule

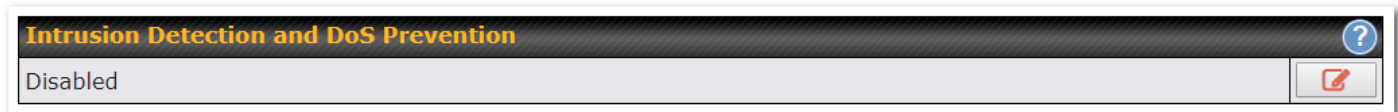
To remove a rule, click the button.


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

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 Adware Audio-Video File Hosting
 Moderate P2P/File sharing Pornography Update Sites
 Low
 Custom

Content Filtering Database Auto Update ?

Customized Domains ?
 +

Exempted Domains from Web Blocking ?
 +

Exempted Subnets ?

Network	Subnet Mask	
<input type="text"/>	255.255.255.0 (/24)	+

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	
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 style="border-bottom: 1px solid #ccc; padding-bottom: 2px;">---</div> <div style="text-align: right; padding-right: 5px;">▼</div> <div style="font-size: 0.8em; padding-top: 2px;">All LAN/VLAN networks will be advertised when no network advertising is chosen.</div> </div> <div style="text-align: right;"></div>						
Static Route Advertising		<input checked="" type="checkbox"/> Enable <table border="1" style="width: 100%; margin-top: 5px;"> <thead> <tr> <th>Excluded Networks</th> <th>Subnet Mask</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td>255.255.255.0 (/24) ▼</td> <td></td> </tr> </tbody> </table>	Excluded Networks	Subnet Mask		<input type="text"/>	255.255.255.0 (/24) ▼	
Excluded Networks	Subnet Mask							
<input type="text"/>	255.255.255.0 (/24) ▼							
Save								

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

OSPF settings ✕

Area ID	<input type="text"/>
Link Type	<input checked="" type="radio"/> Broadcast <input type="radio"/> Point-to-Point
Authentication	None ▾
Interfaces	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

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

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

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

OSPF & RIPv2 Route Advertisement	
PepVPN Route Isolation	<input type="checkbox"/> Enable
Network Advertising	<input type="text" value="---"/> <input type="button" value="+"/>
All LAN/VLAN networks will be advertised when no network advertising is chosen.	
Static Route Advertising	<input type="checkbox"/> Enable
<input type="button" value="Save"/>	

PepVPN Route Isolation	<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>
Network Advertising	<p>Selected networks will be advertised over OSPF & 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>
Static Route Advertising	<p>Enable this option to advertise LAN static routes over OSPF & 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 ▼					
Router ID	<input checked="" type="radio"/> LAN IP Address <input type="radio"/> Custom: <input type="text"/>					
Autonomous System	<input type="text"/>					
Neighbor ?	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="text" value="240"/>					
Next Hop Self ?	<input type="checkbox"/>					
iBGP Local Preference ?	<input type="text" value="100"/>					
BFD ?	<input type="checkbox"/> Enable					

Name	This field is for specifying a name to represent this profile.
Enable	When this box is checked, this BGP profile will be enabled. Otherwise, it will be disabled.
Interface	The interface where BGP neighbor is located
Autonomous System	The Autonomous System Number (ASN) of this profile
Neighbor	BGP Neighbor's details
IP address	Neighbor's IP address
Autonomous System	Neighbor's ASN
Multihop/TTL	Time-to-live (TTL) of BGP packet. Leave it blank if BGP neighbor is directly connected, otherwise you must specify a TTL value. Accurately, this option should be used if the configured neighbor IP address does not match the selected Interface's network subnets. TTL value must be between 2 to 255.
Password	Optional password for MD5 authentication of BGP sessions.
AS-Path Prepending:	AS path to be prepended to the routes received from this neighbor. The value must be a comma separated ASN. For example "64530,64531" will prepend "64530, 64531" to received routes.
Hold Time	Time in seconds to wait for a keepalive message from the neighbor before considering the BGP connection is staled. This value must be either 0 (infinite hold time) or between 3 and 65535 inclusively.

Next Hop Self	Enable this option to advertise own source address as next hop when propagate routes.
iBGP Local Preference	Metric advertised to iBGP neighbors to indicate the preference for external routes. Value must between 0 to 4294967295 inclusively. Default: 100
BFD	Enable this option to add Bidirectional Forwarding Detection for path failure detection. All direct connected neighbors use the same physical interface share same BFD settings. All multi hop neighbors share 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		Networks	Subnet Mask
			255.255.255.0 (/24)
Advertise OSPF Route		<input type="checkbox"/>	
Set Community		Community	Route Prefix

Network Advertising	Networks to be advertised to BGP neighbor.
Static Route Advertising	Enable this option to advertise LAN static routes. Static routes that match the Excluded Networks table will not be advertised.
Custom Route Advertising	Additional routes advertise to BGP neighbor.
Advertise OSPF Route	When this box is checked, all learnt OSPF routes will be advertised.
Set Community	Assign Community to matched prefixes. Community: Two numbers in new-format. e.g. 65000:21344 Well-known communities: no-export 65535:65281 no-advertise 65535:65282 no-export-subconfed 65535:65283 no-peer 65535:65284

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

Filter Mode	<p>This option selects the route import filter mode.</p> <p>None: all BGP routes will be accepted.</p> <p>Accept: Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected.</p> <p>Reject: Routes in "Blocked Networks" will be rejected, routes not in the list will be accepted.</p>
Restricted / Blocked Networks	<p>This specifies the network in the "route import" entry</p> <p>Exact Match: When this box is checked, only routes with the same Networks and Subnet Mask will be filtered.</p> <p>Otherwise, routes within the Networks and Subnet will be filtered.</p>

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

Filter Mode	<p>This option selects the route export filter mode.</p> <p>None: all BGP routes will be accepted.</p> <p>Accept: Routes in "Restricted Networks" will be accepted, routes not in the list will be rejected.</p> <p>Reject: Routes in "Blocked Networks" will be rejected, routes not in the list will be accepted.</p>
Restricted / Blocked Networks	<p>This specifies the network in the "route export" entry</p> <p>Exact Match: When this box is checked, only routes with the same Networks and Subnet Mask will be filtered.</p> <p>Otherwise, routes within the Networks and Subnet will be filtered.</p>
Export to other BGP Profile	When this box is checked, routes learnt from this BGP profile will export to other BGP profiles.
Export to OSPF	When this box is checked, routes learnt from this BGP profile will export to the OSPF routing protocol.

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

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

Continue to configure the authentication method.

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 You can obtain the OpenVPN client profile from the status page .

Select OpenVPN and continue to configure the authentication method.

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

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

You have a choice between 2 different OpenVPN Client profiles.

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

and VLAN segment through the OpenVPN tunnel.

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	<input type="text" value="Untagged LAN"/>						
Authentication	<input type="text" value="Local User Accounts"/>						
User Accounts	<table border="1"> <thead> <tr> <th>Username</th> <th>Password</th> <th></th> </tr> </thead> <tbody> <tr> <td><input type="text"/></td> <td><input type="password"/></td> <td><input type="button" value="+"/></td> </tr> </tbody> </table>	Username	Password		<input type="text"/>	<input type="password"/>	<input type="button" value="+"/>
Username	Password						
<input type="text"/>	<input type="password"/>	<input type="button" value="+"/>					

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

User accounts:

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

Note:

The username must contain lowercase letters, numerics, underscores(_), dash(-), at sign(@), and period(.) only. The password must be between 8 and 12 characters long.

LDAP Server:

Connect to Network	<input type="text" value="Untagged LAN"/>
Authentication	<input type="text" value="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 1812	Default
Auth Server Secret	<input type="text"/>	<input checked="" type="checkbox"/> Hide Characters	
Accounting Server	<input type="text"/>	Port 1813	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 style="float: left; margin-right: 5px;" 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		
New Profile		

Accounting Server	Host	Port
No server profiles defined		
New Profile		

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="password"/>

Hide Characters

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

Accounting Server
✕

Name	<input style="width: 95%;" type="text"/>
Host	<input style="width: 95%;" type="text"/>
Port	<input style="width: 95%;" type="text" value="1813"/>
Secret	<input style="width: 95%;" type="text"/> <input checked="" type="checkbox"/> Hide Characters

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

SMIP 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		<input checked="" type="checkbox"/> 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		<input checked="" type="checkbox"/> Enable	
Web Proxy Interception Settings			
Proxy Server		IP Address <input type="text"/>	Port <input type="text"/>
<small>(Current settings in users' browser)</small>			
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	<input type="checkbox"/> 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	<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="+"/>

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

Service Passthrough

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

Service Passthrough Support ?	
SIP ?	<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 ?	<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 ?	<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.

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

Grouped Networks

Grouped Networks		
Name	Networks	
Add Group		

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.

Grouped Networks		
Name	Networks	
Accounting		
	Network	Subnet Mask
	192.168.50.192	255.255.255.224 (/27) ✖
		255.255.255.255 (/32) +

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

PEPWAVE		Dashboard	SpeedFusion Cloud	Network	Advanced	AP	System
Advanced <ul style="list-style-type: none"> PeppVPN GRE Tunnel Port Forwarding 							
NAT Mappings							
QoS <ul style="list-style-type: none"> Bandwidth Control Application 							
Firewall <ul style="list-style-type: none"> Access Rules 							
Add a New Outbound Firewall Rule							
New Firewall Rule							
Rule Name							
Enable	<input checked="" type="checkbox"/>						
Protocol	Any ? ← :: Protocol Selection ::						
Source	Grouped Network ? Accounting ?						
Destination	Any Address ?						
Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny						

SIM Toolkit

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

SIM Status
No SIM information

USSD

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

SIM Status	
WAN Connection	Cellular
SIM Card	1
IMSI	[REDACTED]
Tool	USSD

USSD	
USSD Code	<input type="text"/> <input type="button" value="Submit"/>

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

SIM Status	
WAN Connection	Cellular
SIM Card	1
IMSI	856195002108538
USSD Code	*138# <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>PCX As of May 27th Account Balance: \$ 0.00 Amount Unbilled Voice Calls: 0 minutes Video Calls: 0 minutes SMS (Roaming): 0 SMS (Within Network): 0 MMS (Roaming): 0 MMS (Within Network): 0 Data Usage: 7384KB (For reference only, please refer to bill)</p> <input type="button" value="✘"/>
Aug 8 , 2013 14:51	<p>PCX iPhone & Android users need to make sure "PCX" is entered as the APN under "Settings" > "Mobile network setting" for web browsing and mobile data service. Other handset models will receive handset settings via SMS shortly (PIN: 1234) (Consumer Service Hotline: 1000 / Business Customer Hotline 10088)</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	214021 100000000
Tool	SMS

SMS		Refresh
Jun 21, 2017 18:00	<p>Hi!</p> <p>Thank you, your anti-phishing/virus/ids - you can change this when you first login at thru.com.au</p>	
May 06, 2017 12:23	<p>Hi!</p> <p>Your new bill is ready to view. Go to your My3 account on your desktop or on a mobile phone click here http://mobile.thru.com.au/bills</p>	
Mar 15, 2017 10:03	<p>Hi!</p> <p>There is planned maintenance in the Southern Cross 3G/4G service area. If your service is affected, you can get updates here http://3g.thru.com.au</p>	
Mar 06, 2017 14:50	<p>Hi!</p> <p>Your new bill is ready to view. Go to your My3 account on your desktop or on a mobile phone click here http://mobile.thru.com.au/bills</p>	
Dec 28, 2016 09:53	<p>Hi!</p> <p>We are happy you've agreed to our monthly half-price offer and to remind you, this offer applied to your first 6 bills, your monthly recurring charge will revert to full price on your next 6th bill.</p>	
Dec 06, 2016 13:09	<p>Hi!</p> <p>Your new bill is ready to view. Go to your My3 account on your desktop or on a mobile phone click here http://mobile.thru.com.au/bills</p>	
Nov 08, 2016 11:29	<p>Hi!</p> <p>There is planned maintenance in the Southern Cross 3G/4G service area. If your service is affected, you can get updates here http://3g.thru.com.au</p>	
Sep 07, 2016 17:05	<p>Hi!</p> <p>Need more details regarding your choice of upgrading equipment? You can call us on 1800 400 01 or email your details to 180040001@thru.com.au</p>	

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.

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

AP

- Wireless SSID
- Settings

Status

- Access Point
- Wireless SSID
- Wireless Client
- Nearby Device
- Event Log

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

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 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"/> 5 GHz: <input type="text"/> (0: Unlimited)
Band Steering	<input type="checkbox"/> Disable ▼

SSID

This setting specifies the Router SSID that Wi-Fi clients will see when scanning.

Enable	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.
VLAN	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.
Broadcast SSID	This setting specifies whether or not Wi-Fi clients can scan the SSID of this wireless network. Broadcast SSID is enabled by default.
Data Rate	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.
Multicast Filter	This setting enables the filtering of multicast network traffic to the wireless SSID.
Multicast Rate	This setting specifies the transmit rate to be used for sending multicast network traffic.
IGMP Snooping	To allow your access point to convert multicast traffic to unicast traffic for associated clients, select this option.
Layer 2 Isolation	<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 (https://forum.peplink.com/t/lan-isolation-with-balance30-and-ap-one-ac-mini-help-needed/3914/4) for visual illustration of the feature. By default, the setting is disabled.</p>
Maximum number of Clients	Enter the maximum number of clients that can simultaneously connect to your SSID, or enter 0 to allow unlimited Wi-Fi clients.
Band Steering	<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>Force - Clients capable of 5 GHz operation are only offered with 5 GHz frequency.</p> <p>Prefer - 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: Disable</p>

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

Security Policy

This setting configures the wireless authentication and encryption methods. Available options :

- Open (No Encryption)
- WPA3 -Personal (AES:CCMP)
- WPA2/WPA3 -Personal (AES:CCMP)
- WPA2 -Personal (AES:CCMP)
- WPA2 – Enterprise
- WPA/WPA2 - Personal (TKIP/AES: CCMP)
- WPA/WPA2 – Enterprise

When WPA/WPA2 - Enterprise is 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.

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.

NOTE:

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

Management Frame Protection

This feature protects stations against forged management frames spoofed from other devices. Frames that are protected include Disassociation, Deauthentication and QoS Action.

Fast Transition

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 ?	<input type="text"/>

Restricted Mode	The settings allow administrators to control access using Mac address filtering. Available options are None , Deny all except listed , Accept all except and RADIUS MAC Authentication .
MAC Address List	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 here to define RADIUS Server Authentication profile, or you may go to RADIUS Server 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 here to define RADIUS Server Accounting profile, or you may go to RADIUS Server 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 ▾	

Host	Specifies the IP address or hostname of the RADIUS server host.
Secret	This field is for entering the secret key for communicating to the RADIUS server.
Authentication Port	This setting specifies the UDP destination port for authentication requests. By default, the port number is 1812.

Accounting Port	This setting specifies the UDP destination port for accounting requests. By default, the port number is 1813.
NAS-Identifier	The setting allows administrators to identify the client to the RADIUS server. Available options are Device Name , LAN Mac Address , Device Serial Number and Custom Value .

Firewall Settings

Firewall Mode	Lockdown - Block all except... ▼	
Firewall Exceptions	Disable Flexible - Allow all except... Lockdown - Block all except...	Item New Rule

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

Settings

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

Wi-Fi Radio Settings																
Operating Country	United States															
SSID	<table border="0"> <tr> <td>2.4GHz</td> <td>5GHz</td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td></td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> <td></td> </tr> </table>	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"/>	
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"/>	Auto <input type="button" value="Edit"/>
	Channels: 1 2 3 4 5 6 7 8 9 10 11	Channels: 36 40 44 48 149 153 157 161
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	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	Max <input type="checkbox"/> Boost
Client Signal Strength Threshold	0 -95 dBm (0: Unlimited)	0 -95 dBm (0: Unlimited)
Maximum number of clients	0 (0: Unlimited)	0 (0: Unlimited)
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	<input type="button" value="0"/> <input type="button" value="Default"/>	
Fragmentation Threshold	<input type="button" value="0"/> (0: Disable) <input type="button" value="Default"/>	
Distance / Time Converter	<input type="text" value="4050"/> m Note: Input distance for recommended values	
Slot Time	<input type="radio"/> Auto <input checked="" type="radio"/> Custom <input type="text" value="9"/> μ s <input type="button" value="Default"/>	
ACK Timeout	<input type="button" value="48"/> μ s <input type="button" value="Default"/>	
Frame Aggregation	<input type="checkbox"/>	

Operating Country	
Operating Country	This option sets the country whose regulations the PEPwave router follows.
SSID	Select if an SSID is broadcasting on 2.4 Ghz, 5 Ghz or both bands

Protocol	
Protocol	This option allows you to specify which client association requests will be accepted. By default, 802.11ng is selected.
Channel Width	Settings for 2.4 GHz AP and 5GHz AP can be configured here: 2.4 GHz: 40 MHz, 20/40 MHz and 20 MHz are available. The default setting is 20/40 MHz , which allows both widths to be used simultaneously. 80 MHz , 40 Mhz, 20 Mhz, and(20/40 MH) are available. The default setting is 80 MHz . 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).
Channel	This option allows you to select which 802.11 RF channel will be used.
Auto Channel Update	Indicate the time of day for updating the automatic channel selection.
Output Power	This option is for specifying the transmission output power for the Wi-Fi AP. There are 4 relative power levels available – Max, High, Mid, and Low . The actual output power will be bound by the regulatory limits of the selected country.
Client Signal Strength Threshold^A	This field determines that maximum signal strength each individual client will receive. The measurement unit is dBm.
Maximum number of clients	Enter the maximum number of clients that can simultaneously connect to the wireless network or enter 0 to allow an unlimited number of connections.
Beacon Rate^A	This option is for setting the transmit bit rate for sending a beacon. By default, 1Mbps is selected.
Beacon Interval^A	This option is for setting the time interval between each beacon. By default, 100ms is selected.
DTIM^A	This field allows you to set the frequency for the beacon to include a delivery traffic indication message. The interval is measured in milliseconds. The default value is set to 1 ms .
RTS Threshold	Set the minimum packet size for your access point to send an RTS using the RTS/CTS handshake. Setting 0 disables this feature.

Fragmentation Threshold^A	Determines the maximum size (in bytes) that each packet fragment will be broken down into. Set 0 to disable fragmentation.
Distance/Time Converter^A	Select the distance you want your Wi-Fi to cover in order to adjust the below parameters. Default values are recommended.
Slot Time^A	This field is for specifying the wait time before the Surf SOHO transmits a packet. By default, this field is set to 9 μs .
ACK Timeout^A	This field is for setting the wait time to receive an acknowledgement packet before performing a retransmission. By default, this field is set to 48 μs .
Frame Aggregation^A	This option allows you to enable frame aggregation to increase transmission throughput.

System Settings

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

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

Admin Settings

Device Name: [] hostname: surf-soho- []

Admin User Name: [admin]

Admin Password: []

Confirm Admin Password: []

Read-only User Name: [user]

User Password: []

Confirm User Password: []

Web Session Timeout: [4] Hours [0] Minutes

Authentication Method: [?] Local Account RADIUS TACACS+

CLI SSH & Console: [?] Enable

Security: [HTTPS]

Web Admin Access: [LAN Only]

Web Admin Port: [443]

Logout Save

Admin Security

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

Device Name	This field allows you to define a name for this Pepwave router. By default, Router Name is set as surf-soho-XXXX , where XXXX refers to the last 4 digits of the unit's serial number.																						
Admin User Name	Admin User Name is set as <i>admin</i> by default, but can be changed, if desired.																						
Admin Password	This field allows you to specify a new administrator password.																						
Confirm Admin Password	This field allows you to verify and confirm the new administrator password.																						
[REDACTED]																							
Read-only User Name	Read-only User Name is set as <i>user</i> by default, but can be changed, if desired.																						
User Password	This field allows you to specify a new user password. Once the user password is set, the read-only user feature will be enabled.																						
Confirm User Password	This field allows you to verify and confirm the new user password.																						
Web Session Timeout	This field specifies the number of hours and minutes that a web session can remain idle before the Pepwave router terminates its access to the web admin interface. By default, it is set to 4 hours .																						
<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"> • Local Account • RADIUS 																							
Authentication Method	<table border="1"> <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></td> <td>You may click here to define RADIUS Server Authentication profile, or you may go to RADIUS Server 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></td> <td>You may click here to define RADIUS Server Accounting profile, or you may go to RADIUS Server 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 here to define RADIUS Server Authentication profile, or you may go to RADIUS Server 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 here to define RADIUS Server Accounting profile, or you may go to RADIUS Server 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 here to define RADIUS Server Authentication profile, or you may go to RADIUS Server 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 here to define RADIUS Server Accounting profile, or you may go to RADIUS Server 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 Protocol	This specifies the authentication protocol used. Available options are MS-CHAP v2 and PAP .																						

Authentication Host	This specifies the IP address or hostname of the RADIUS server host.
Authentication Port	This setting specifies the UDP destination port for authentication requests.
Authentication Secret	This field is for entering the secret key for accessing the RADIUS server.
Accounting Host	This specifies the IP address or hostname of the RADIUS server host.
Accounting Port	This setting specifies the UDP destination port for accounting requests.
Accounting Secret	This field is for entering the secret key for accessing the accounting server.
Authentication Timeout	This option specifies the time value for authentication timeout

- TACACS+

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

TACACS+ Server	This specifies the access address of the external TACACS+ server.
TACACS+ Server Secret	This field is for entering the secret key for accessing the RADIUS server.
TACACS+ Server Timeout	This option specifies the time value for TACACS+ timeout

CLI SSH & Console	The CLI (command line interface) can be accessed via SSH. This field enables CLI support. For additional information regarding CLI, please refer to Section 30.5 .
CLI SSH Access	This menu allows you to choose between granting access to LAN and WAN clients, or to LAN clients only.
CLI SSH Port	This field determines the port on which clients can access CLI SSH.
Security	<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"> • HTTP • HTTPS • HTTP/HTTPS <p>HTTP to HTTPS redirection is enabled by default to force HTTPS access to the web admin interface.</p>
Web Admin Access	<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"> • LAN only • LAN/WAN

If LAN/WAN is chosen, the **WAN Connection Access Settings** form will be displayed.

Web Admin Port This field is for specifying the port number on which the web admin interface can be accessed.

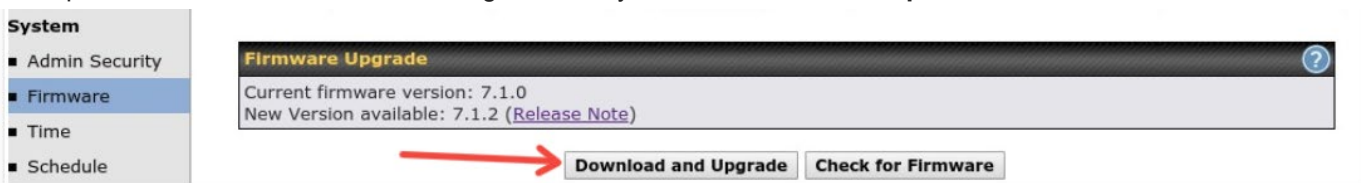
Firmware

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**.

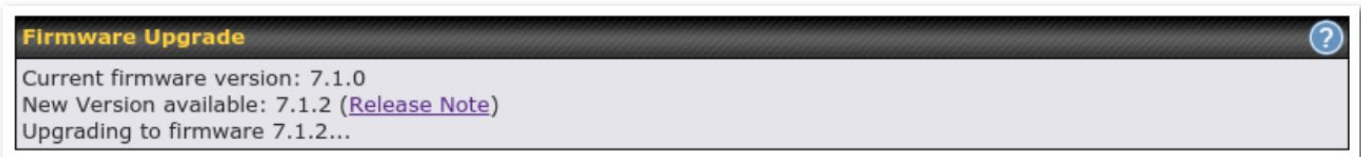


If an update is found the buttons will change to allow you to **Download and Update** the firmware.



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

Balance

Product

Search:

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

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

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

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

Manual Firmware Upgrade ?

Firmware Image No file chosen

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

***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

 Show all

Time Server

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

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		
New Schedule		

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	<input type="text"/>	


Schedule Map

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

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

Email Notification

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

Email Notification Setup ?	
Email Notification	<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	smtuser
SMTP Password	••••
Confirm SMTP Password	••••
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com 

Email Notification	This setting specifies whether or not to enable email notification. If Enable is checked, the Pepwave router will send email messages to system administrators when the WAN status changes or when new firmware is available. If Enable is not checked, email notification is disabled and the Pepwave router will not send email messages.
SMTP Server	This setting specifies the SMTP server to be used for sending email. If the server requires authentication, check Require authentication .

Connection Security	<p>This setting specifies via a drop-down menu one of the following valid connection security:</p> <ul style="list-style-type: none"> • None • STARTTLS • SSL/TTS <p>When connection security is selected, SMTP Port will set a default port number automatically.</p>
SMTP Port	<p>This field is for specifying the SMTP port number. By default, this is set to 25; when STARTTLS is selected, the default port number will be set to 587. When SSL/TTS is selected, the default port number will be set to 465. You may customize the port number by editing this field.</p>
SMTP User Name / Password	<p>This setting specifies the SMTP username and password while sending email. These options are shown only if Require authentication is checked in the SMTP Server setting.</p>
Confirm SMTP Password	<p>This field allows you to verify and confirm the new administrator password.</p>
Sender's Email Address	<p>This setting specifies the email address the Pepwave router will use to send reports.</p>
Recipient's Email Address	<p>This setting specifies the email address(es) to which the Pepwave router will send email notifications. For multiple recipients, separate each email addresses using the enter key.</p>

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. Email notification settings are not saved, it will be saved after clicked the 'Save' button.

Test Result

```
[INFO] Try email through connection #3
[<-] 220 ESMTP
[->] EHLO balance
[<-] 250-smtp Hello balance [210.210.210.210]
250-SIZE 100000000
250-8BITMIME
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
```

Event Log

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

Send Events to Remote Syslog Server ?

Remote Syslog	<input type="checkbox"/>
Remote Syslog Host	<input style="width: 90%;" type="text"/> Port: <input style="width: 50px;" type="text" value="514"/>

Push Events to Mobile Devices ?

Push Events	<input type="checkbox"/>
-------------	--------------------------

Remote Syslog	This setting specifies whether or not to log events at the specified remote syslog server.
Remote Syslog Host	This setting specifies the IP address or hostname of the remote syslog server and port that is used.
Push Events	The Pepwave router can also send push notifications to mobile devices that have our Mobile Router Utility installed. Check the box to activate this feature. For more information on the Router Utility, go to: www.peplink.com/products/router-utility

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	<input type="text"/>
Location ?	<input type="text"/>
SNMP Port	<input type="text" value="161"/> <input type="button" value="Default"/>
SNMPv1	<input type="checkbox"/> Enable
SNMPv2c	<input type="checkbox"/> Enable
SNMPv3	<input type="checkbox"/> Enable
SNMP Trap	<input type="checkbox"/> Enable
<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"/>		

[Redacted]	
SNMP Device Name	This field shows the router name defined at System>Admin Security .
SNMP Port	This option specifies the port which SNMP will use. The default port is 161 .
SNMPv1	This option allows you to enable SNMP version 1.
SNMPv2	This option allows you to enable SNMP version 2.
SNMPv3	This option allows you to enable SNMP version 3.
SNMP Trap	This option allows you to enable SNMP Trap

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: 30%;" type="text"/> / 255.255.255.0 (/24) ▼

Community Name This setting specifies the SNMP community name.

Allowed Source Subnet Address This setting specifies a subnet from which access to the SNMP server is allowed. Enter subnet address here (e.g., 192.168.1.0) and select the appropriate subnet mask.

To define a 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: 60%;" type="text"/>
Privacy	DES ▼ <input style="width: 60%;" type="text"/>

User Name This setting specifies a user name to be used in SNMPv3.

Authentication Protocol This setting specifies via a drop-down menu one of the following valid authentication protocols:

- NONE
- MD5
- SHA

When MD5 or SHA is selected, an entry field will appear for the password.

Privacy Protocol This setting specifies via a drop-down menu one of the following valid privacy protocols:

- None
- DES
- AES

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

InControl

Controller Management Settings	
Controller	? InControl <input type="checkbox"/> Restricted to Status Reporting Only
Privately Host InControl	<input checked="" type="checkbox"/>
InControl Host	<input type="text"/> <input 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 box beside the "Privately Host InControl" open, and enter the IP Address of your InControl Host.

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

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.

Restore Configuration to Factory Settings ?

Download Active Configurations ?

Upload Configurations ?

Configuration File No file chosen

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

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**.

Feature Activation

Activation Key

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.

Reboot System ?

Select the firmware you want to use to start up this device:

Firmware 1: 8.0.1b01 build 2658 (Running)

Firmware 2: 8.0.0 build 2636

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 Clear Log

```

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
    
```

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 byte packets
 0 100.86.137.254 (100.86.137.254) 0.708 ms 0.472 ms 0.267 ms
 1 100.86.89.254 (100.86.89.254) 0.813 ms 0.292 ms 0.498 ms
 2 100.86.89.1 (100.86.89.1) 0.875 ms 0.823 ms 0.968 ms
 3 100.86.9.2 (100.86.9.2) 0.182 ms 0.203 ms 0.296 ms
 4 100.86.89.254 (100.86.89.254) 0.294 ms 1.09.175.240.22 (1.09.175.240.22) 0.707 ms 1.08.143.89.254 (1.08.143.89.254) 0.472 ms
 5 192.75.46.128 (192.75.46.128) 0.689 ms 198.95.229.46 (198.95.229.46) 0.293 ms 0.293 ms
 6 208.128.1.158 (208.128.1.158) 0.301 ms 7.499 ms 7.499 ms
 7 109.175.89.254 (109.175.89.254) 4.811 ms 208.128.9.1 (208.128.9.1) 4.872 ms 192.75.109.148 (192.75.109.148) 4.241 ms
 8 208.128.9.229 (208.128.9.229) 0.238 ms 72.14.194.246 (72.14.194.246) 0.491 ms 208.128.9.229 (208.128.9.229) 4.878 ms
 9 72.14.209.20 (72.14.209.20) 0.842 ms 74.125.49.108 (74.125.49.108) 4.877 ms 72.14.209.20 (72.14.209.20) 0.984 ms
10 72.14.209.20 (72.14.209.20) 0.984 ms 209.85.292.161 (209.85.292.161) 7.213 ms 209.85.243.30 (209.85.243.30) 6.484 ms
11 209.85.292.117 (209.85.292.117) 4.872 ms 209.85.242.163 (209.85.242.163) 6.809 ms 0.989 ms
12 216.239.92.47 (216.239.92.47) 0.892 ms * 7.392 ms
13 64.233.189.99 (64.233.189.99) 0.179 ms 0.144 ms 0.822 ms
                    
```

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**.

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.

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"/>
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**

WAN Performance Analysis

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

Client Settings

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

Data Streams

Local WAN Connection	Remote IP Address	
1. -- Not Used --	<input type="text"/>	<input checked="" type="checkbox"/>
2. -- Not Used --	<input type="text"/>	<input checked="" type="checkbox"/>
3. -- Not Used --	<input type="text"/>	<input checked="" type="checkbox"/>
4. -- Not Used --	<input type="text"/>	<input checked="" type="checkbox"/>
5. -- Not Used --	<input type="text"/>	<input checked="" type="checkbox"/>
6. -- Not Used --	<input type="text"/>	<input checked="" type="checkbox"/>
7. -- Not Used --	<input type="text"/>	<input checked="" type="checkbox"/>
8. -- Not Used --	<input type="text"/>	<input type="checkbox"/>

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

Throughput

Duration (seconds)	Throughput (Mbps)
0	0.00
1	15.7284
2	16.2527
3	16.7775
4	16.2528
5	16.2530
6	15.7287

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 (Modem Support List)
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	Download
Remote Assistance	Turn On

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

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

MAC Address

LAN	00:1A:DD:68: [blurred]
WAN	00:1A:DD:68: [blurred]
Wi-Fi WAN on 5 GHz	00:1A:DD:68: [blurred]

[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**

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
Amazon	0	1
DNS	0	55
Facebook	0	2
Google	0	19
Google Play Store	0	1
HTTP	0	2
IPsec	0	2
Office 365	0	42
SIP	0	46
SSH	0	1
SSL	3	170
STUN	0	2
Skype	0	5
XMPP	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"/> / 255.255.255.255 (/32) ▾
Port	Source or Destination ▾ <input style="width: 150px;" type="text"/>
Protocol / Service	TCP ▾
Interface	<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 <input type="checkbox"/> USB <input type="checkbox"/> VPN
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 Online Clients Only DHCP Clients Only

Client List ?

IP Address ▲	Name	Download (kbps)	Upload (kbps)	MAC Address	Network Name (SSID)	Signal (dBm)	Import
10.10.1.1				08:00:27:00:00:00			
10.10.1.2	Wagner Laptop			08:00:27:00:00:00			
10.10.1.3				08:00:27:00:00:00			
10.10.1.100	elena			08:00:27:00:00:00			
10.10.1.101	elena			08:00:27:00:00:00			
10.10.1.102	elena			08:00:27:00:00:00			
10.10.1.103	elena			08:00:27:00:00:00			
10.10.1.104	elena			08:00:27:00:00:00			
10.10.1.105	elena			08:00:27:00:00:00			
10.10.1.106	elena			08:00:27:00:00:00			
10.10.1.107	elena			08:00:27:00:00:00			
10.10.1.108	elena			08:00:27:00:00:00			
10.10.1.109	elena			08:00:27:00:00:00			
10.10.1.110	elena			08:00:27:00:00:00			
10.10.1.111	elena			08:00:27:00:00:00			
10.10.1.112	elena			08:00:27:00:00:00			
10.10.1.113	elena			08:00:27:00:00:00			
10.10.1.114	elena			08:00:27:00:00:00	PERFWAVE	-62	
10.10.1.115				08:00:27:00:00:00			
10.10.1.116	elena			08:00:27:00:00:00	PERFWAVE	-46	
10.10.1.117	elena			08:00:27:00:00:00			
10.10.1.118	elena			08:00:27:00:00:00			
10.10.1.119	elena			08:00:27:00:00:00	PERFWAVE	-39	
10.10.1.120	elena			08:00:27:00:00:00			
10.10.1.121				08:00:27:00:00:00			
10.10.1.122				08:00:27:00:00:00			
10.10.1.123				08:00:27:00:00:00			
10.10.1.124				08:00:27:00:00:00			
10.10.1.125				08:00:27:00:00:00			
10.10.1.126				08:00:27:00:00:00			
10.10.1.127				08:00:27:00:00:00			
10.10.1.128				08:00:27:00:00:00			
10.10.1.129				08:00:27:00:00:00			
10.10.1.130				08:00:27:00:00:00			
10.10.1.131				08:00:27:00:00:00			
10.10.1.132				08:00:27:00:00:00			
10.10.1.133				08:00:27:00:00:00			
10.10.1.134				08:00:27:00:00:00			
10.10.1.135				08:00:27:00:00:00			
10.10.1.136				08:00:27:00:00:00			
10.10.1.137				08:00:27:00:00:00			
10.10.1.138				08:00:27:00:00:00			
10.10.1.139				08:00:27:00:00:00			
10.10.1.140				08:00:27:00:00:00			
10.10.1.141				08:00:27:00:00:00			
10.10.1.142				08:00:27:00:00:00			
10.10.1.143				08:00:27:00:00:00			
10.10.1.144				08:00:27:00:00:00			
10.10.1.145				08:00:27:00:00:00			
10.10.1.146				08:00:27:00:00:00			
10.10.1.147				08:00:27:00:00:00			
10.10.1.148				08:00:27:00:00:00			
10.10.1.149				08:00:27:00:00:00			
10.10.1.150				08:00:27:00:00:00			
10.10.1.151				08:00:27:00:00:00			
10.10.1.152				08:00:27:00:00:00			
10.10.1.153				08:00:27:00:00:00			
10.10.1.154				08:00:27:00:00:00			
10.10.1.155				08:00:27:00:00:00			
10.10.1.156				08:00:27:00:00:00			
10.10.1.157				08:00:27:00:00:00			
10.10.1.158				08:00:27:00:00:00			
10.10.1.159				08:00:27:00:00:00			
10.10.1.160				08:00:27:00:00:00			
10.10.1.161				08:00:27:00:00:00			
10.10.1.162				08:00:27:00:00:00			
10.10.1.163				08:00:27:00:00:00			
10.10.1.164				08:00:27:00:00:00			
10.10.1.165				08:00:27:00:00:00			
10.10.1.166				08:00:27:00:00:00			
10.10.1.167				08:00:27:00:00:00			
10.10.1.168				08:00:27:00:00:00			
10.10.1.169				08:00:27:00:00:00			
10.10.1.170				08:00:27:00:00:00			
10.10.1.171				08:00:27:00:00:00			
10.10.1.172				08:00:27:00:00:00			
10.10.1.173				08:00:27:00:00:00			
10.10.1.174				08:00:27:00:00:00			
10.10.1.175				08:00:27:00:00:00			
10.10.1.176				08:00:27:00:00:00			
10.10.1.177				08:00:27:00:00:00			
10.10.1.178				08:00:27:00:00:00			
10.10.1.179				08:00:27:00:00:00			
10.10.1.180				08:00:27:00:00:00			
10.10.1.181				08:00:27:00:00:00			
10.10.1.182				08:00:27:00:00:00			
10.10.1.183				08:00:27:00:00:00			
10.10.1.184				08:00:27:00:00:00			
10.10.1.185				08:00:27:00:00:00			
10.10.1.186				08:00:27:00:00:00			
10.10.1.187				08:00:27:00:00:00			
10.10.1.188				08:00:27:00:00:00			
10.10.1.189				08:00:27:00:00:00			
10.10.1.190				08:00:27:00:00:00			
10.10.1.191				08:00:27:00:00:00			
10.10.1.192				08:00:27:00:00:00			
10.10.1.193				08:00:27:00:00:00			
10.10.1.194				08:00:27:00:00:00			
10.10.1.195				08:00:27:00:00:00			
10.10.1.196				08:00:27:00:00:00			
10.10.1.197				08:00:27:00:00:00			
10.10.1.198				08:00:27:00:00:00			
10.10.1.199				08:00:27:00:00:00			
10.10.1.200				08:00:27:00:00:00			

Scale: kbps Mbps

OSPF & RIPv2

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.

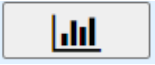
PepVPN Status

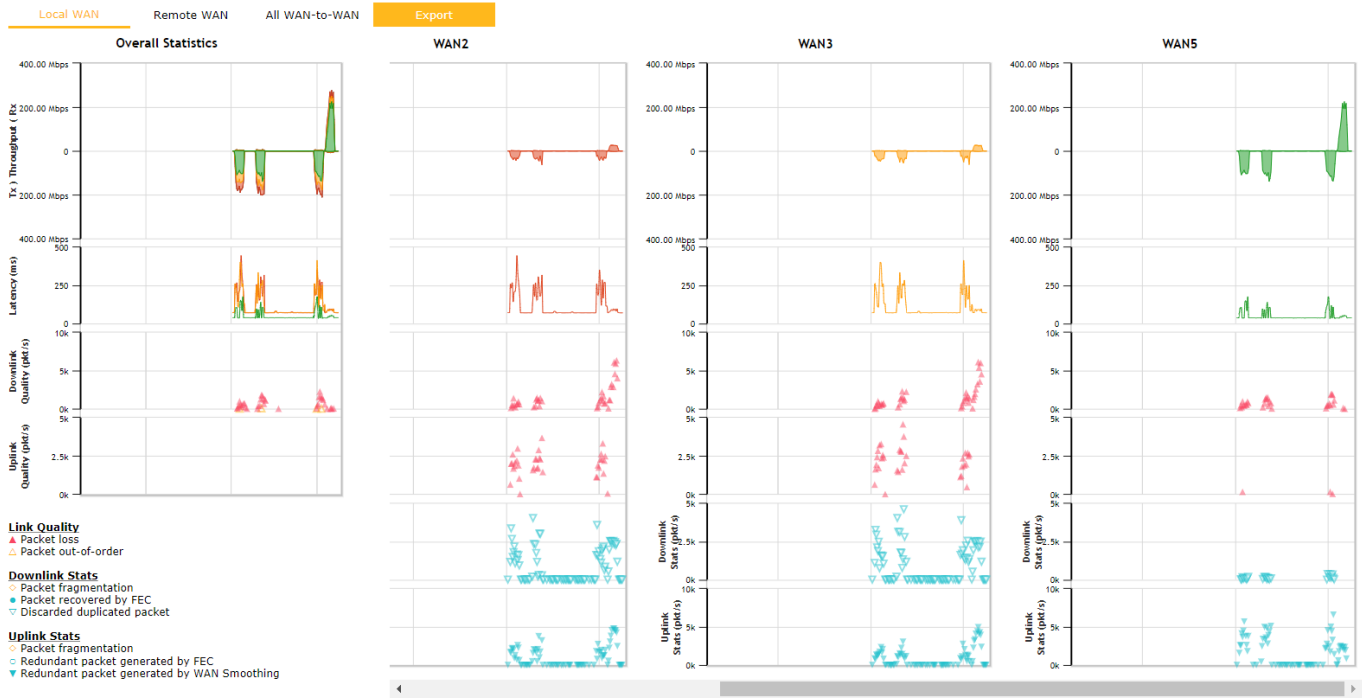
PepVPN Status shows the current connection status of each connection profile and is displayed at **Status> PepVPN/SpeedFusion**.

PepVPN with SpeedFusion - Remote Peer Details			<input type="checkbox"/> Show disconnected profiles
Search			
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			<input type="checkbox"/> Show all profiles
Search			
Remote Peer	Profile	Information	
SFC-SIN-001 (SFC-SIN-001)	SFC	SpeedFusion Cloud	
WAN1		Not available - WAN disabled	
WAN2	Rx: < 1 kbps Tx: < 1 kbps	Loss rate: 0.0 pkt/s Latency: 42 ms	
WAN3	Rx: < 1 kbps Tx: < 1 kbps	Loss rate: 0.0 pkt/s Latency: 42 ms	
WAN4		Not available - WAN disabled	
WAN5	Rx: < 1 kbps Tx: < 1 kbps	Loss rate: 0.0 pkt/s Latency: 10 ms	
Mobile Internet	Rx: < 1 kbps Tx: < 1 kbps	Loss rate: 0.0 pkt/s Latency: 32 ms	
Total	Rx: < 1 kbps Tx: 1.1 kbps	Loss rate: 0.0 pkt/s	

Click  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	<div style="border: 1px solid gray; padding: 5px; width: 50px; margin: auto;">Start</div>
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 displays the 'Device Event Log' tab, which contains a table of events. The table has two columns: 'Time' and 'Description'. The events listed are as follows:

Time	Description
Sep 30 09:23:29	Port: f ()
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:

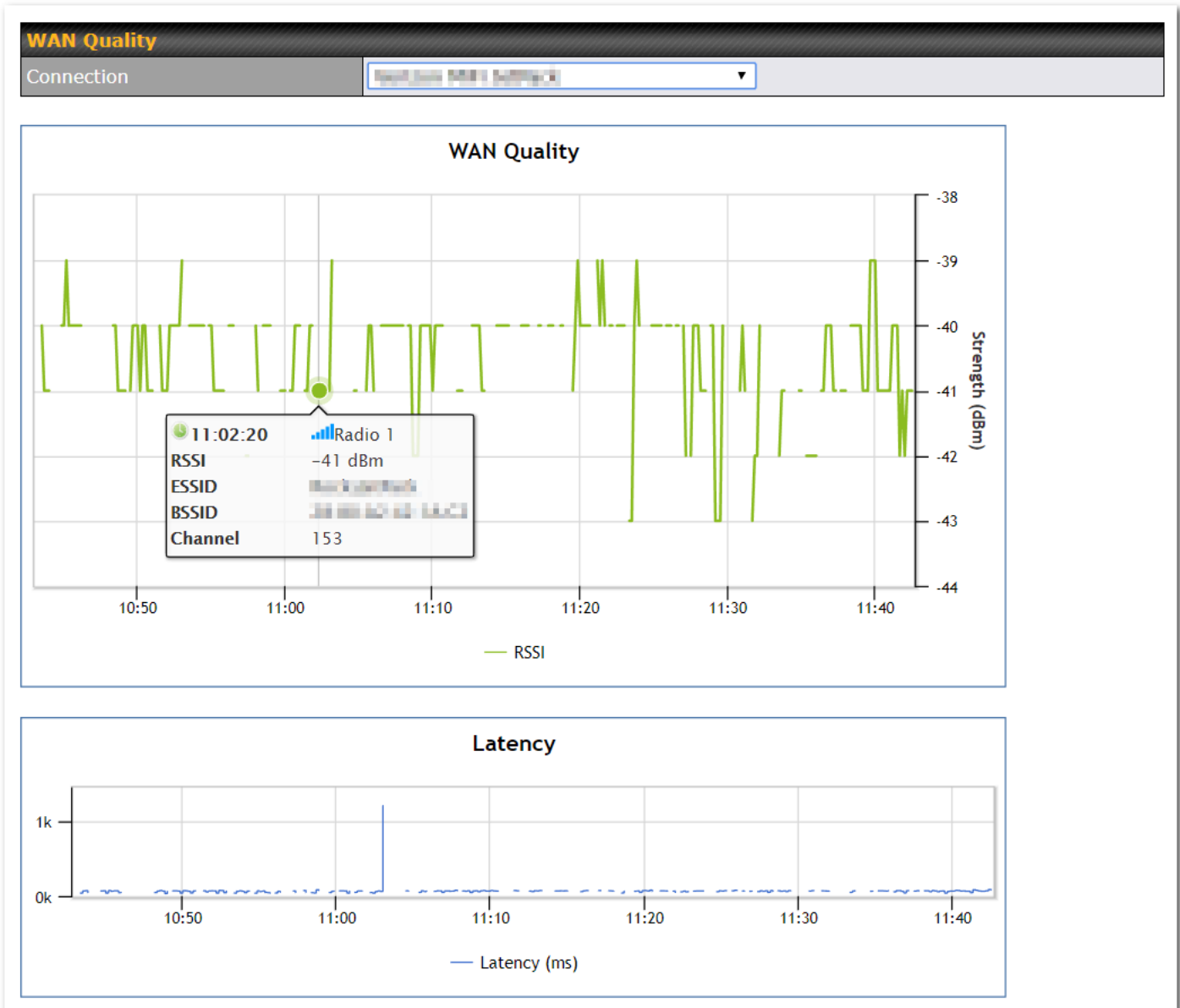
At the bottom of the log section, there is a 'Clear Log' button. An 'Auto Refresh' checkbox is checked in the top right corner of the log area.

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.

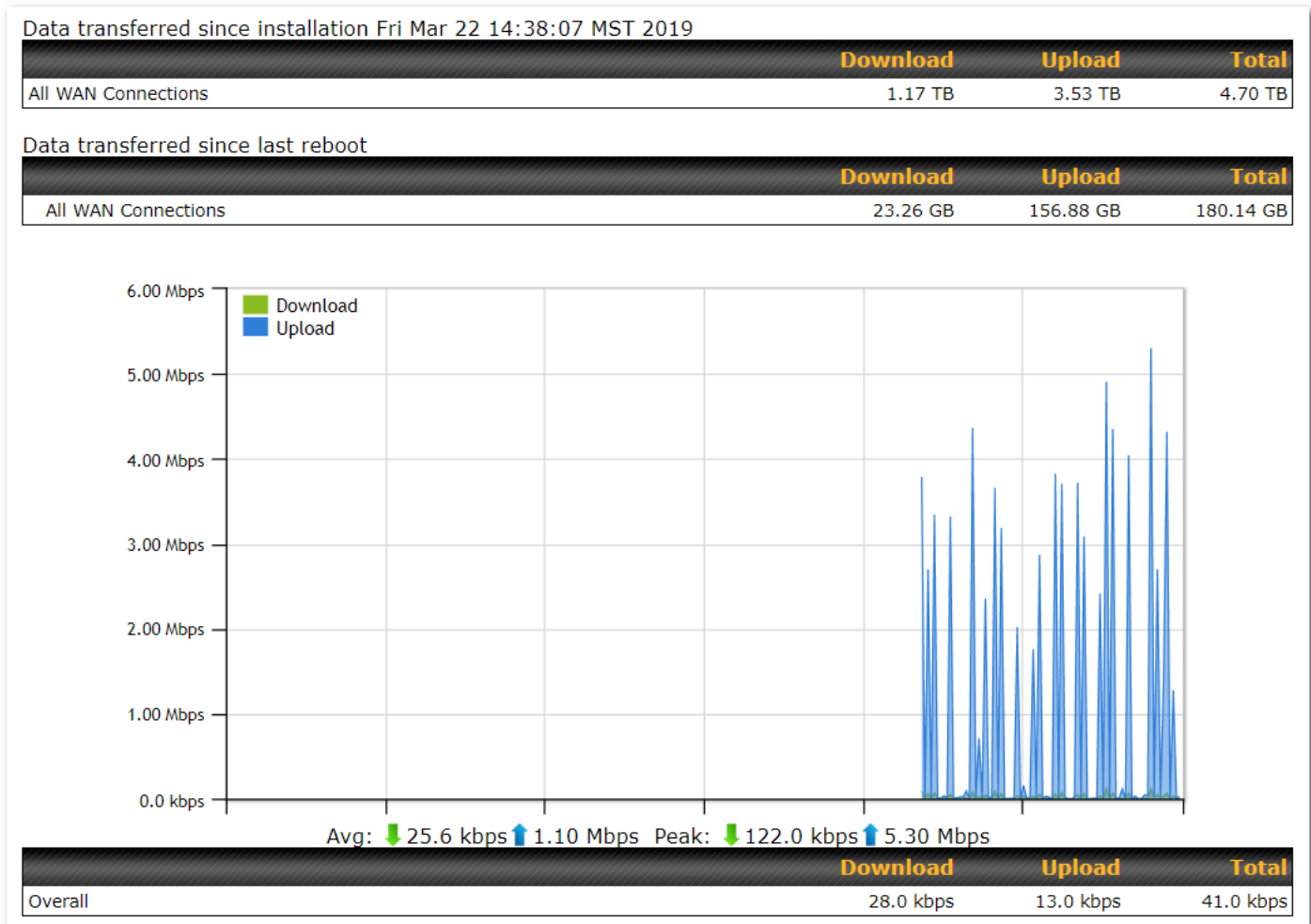


Usage Reports

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.

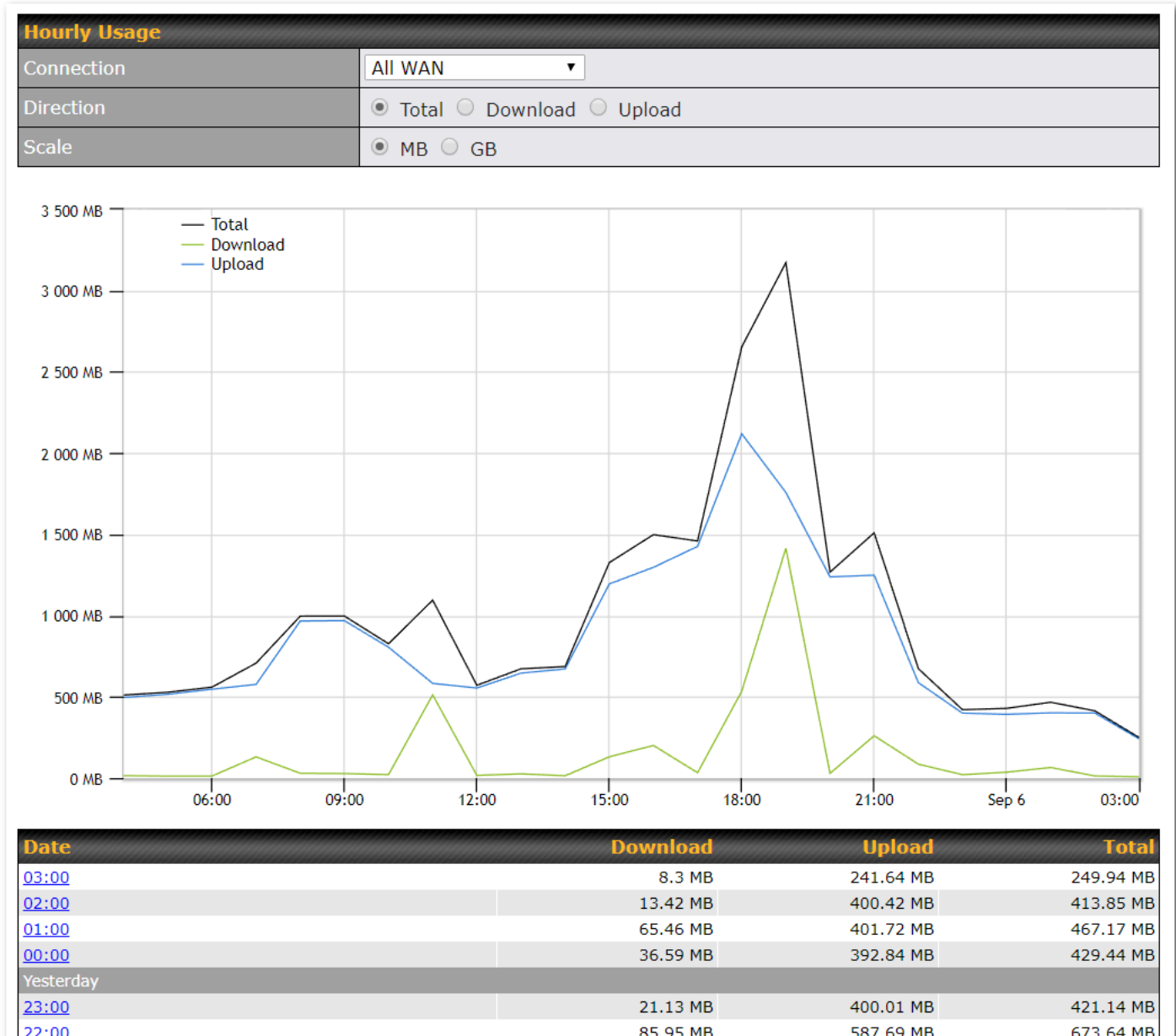
Real Time

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.

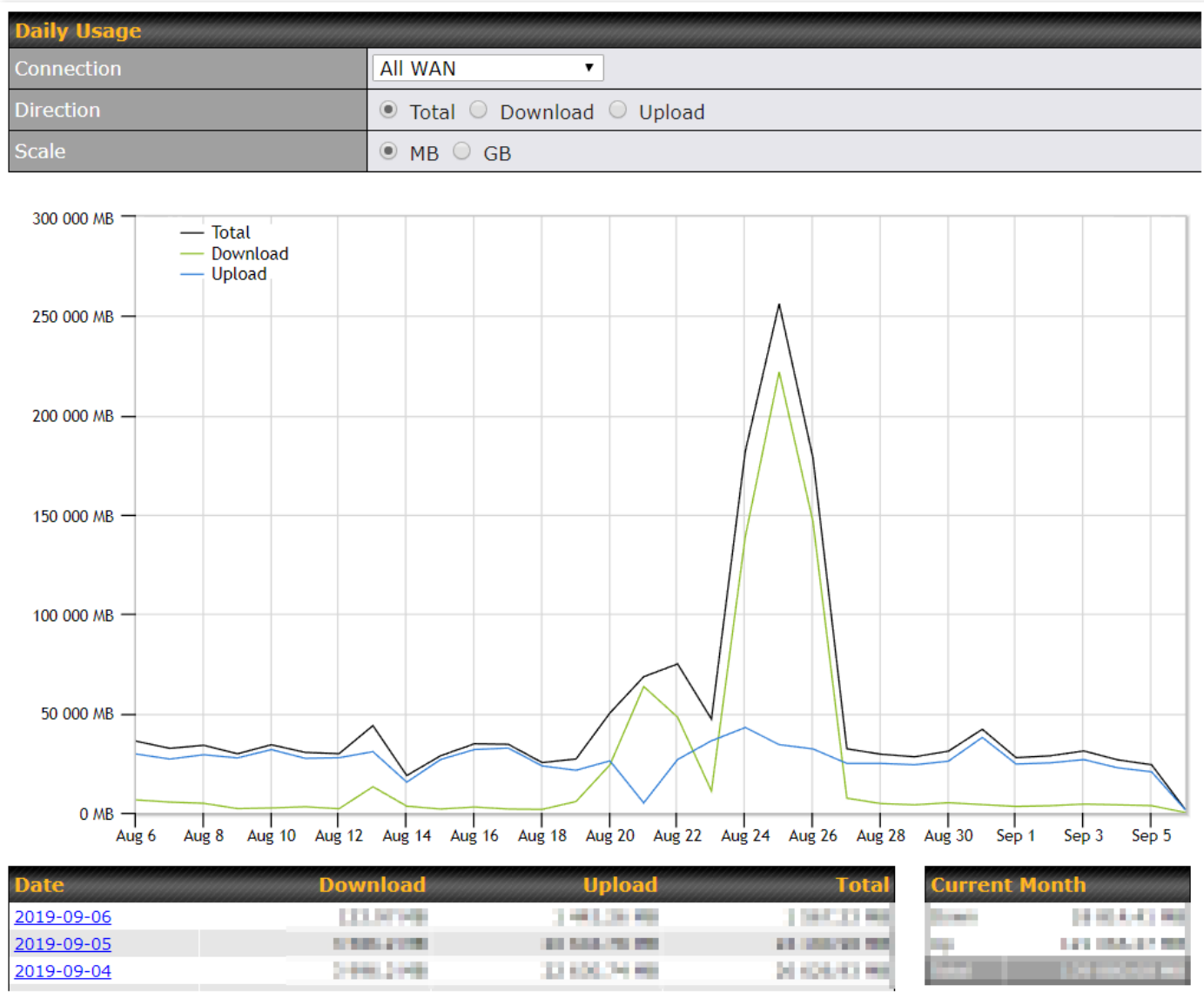


Daily

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.

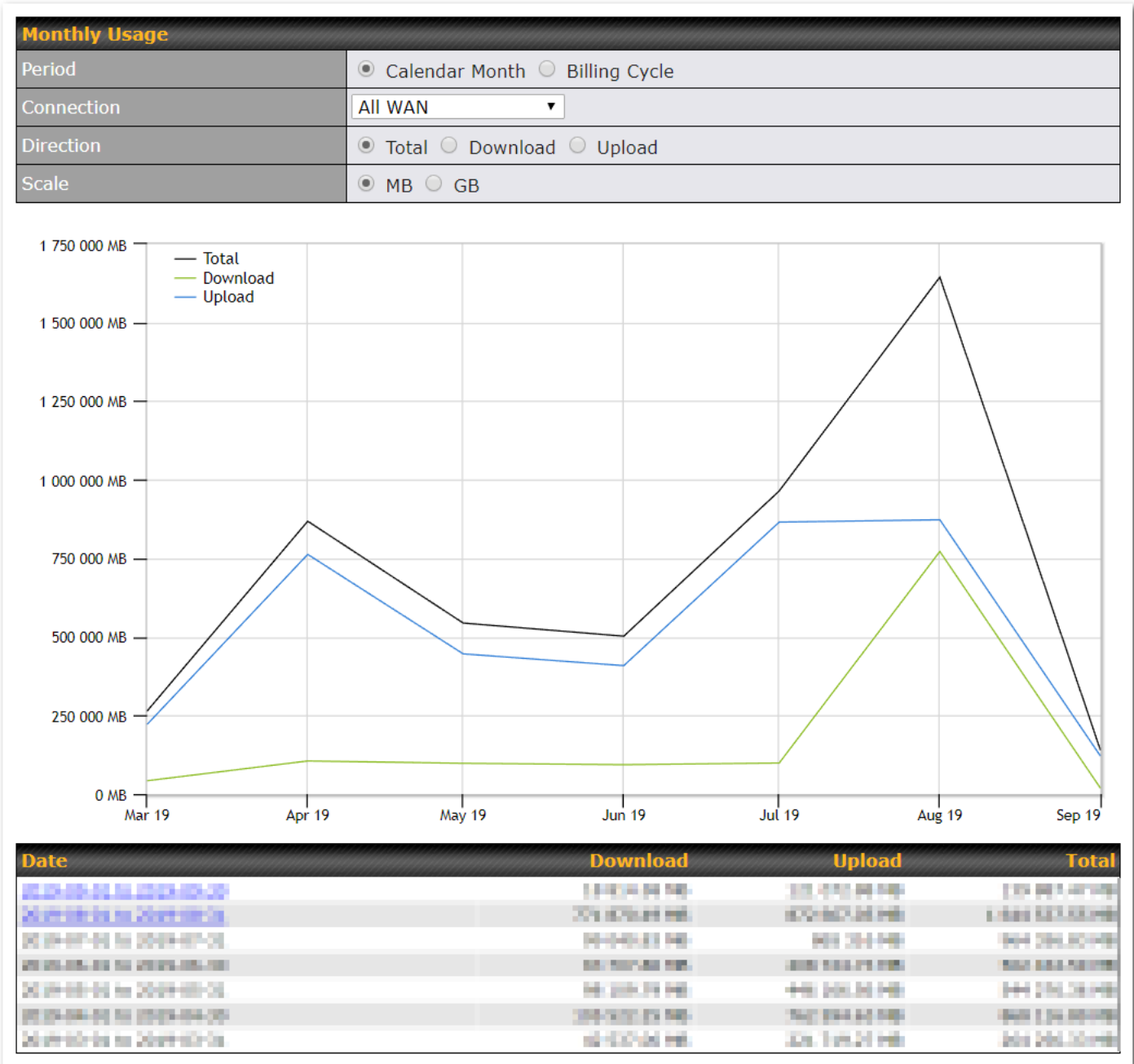
Click on a date to view the client bandwidth usage of that specific date. This feature is not available if you have selected to view the bandwidth usage of only a particular WAN connection. The scale of the graph can be set to display megabytes (**MB**) or gigabytes (**GB**).



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.

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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

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**

Europe – EU Declaration of Conformity
 This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

EN 60950-1: 2006 + A11 : 2009+A1 : 2010+ A12: 2011
 Safety of Information Technology Equipment

EN50385 : 2002 / Article 3(1)(a)
 Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110MHz - 40 GHz) - General public

EN 300 328 V1.7.1: 2006
 Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

EN 301 908-1 V5.2.1: 2011
 Electromagnetic compatibility and Radio spectrum Matters (ERM); Base Stations (BS), Repeaters and User Equipment (UE) for IMT-2000 Third-Generation cellular networks; Part 1: Harmonized EN for IMT-2000, introduction and common requirements, covering essential requirements of article 3.2 of the R&TTE Directive

EN 301 511 V9.0.2: 2003
 Global System for Mobile communications (GSM); Harmonized standard for mobile stations in the GSM 900 and DCS 1800 bands covering essential requirements under article 3.2 of the R&TTE directive (1999/5/EC)



EN 301 489-1 V1.9.2: 2008
 Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements









EN 301 489-7 V1.3.1: 2005
 ElectroMagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment ad services; Part 7: Specific conditions for mobile and portable radio and ancillary equipment of digital cellular radio telecommunications systems (GSM and DCS)

EN 301 489-17 V2.2.1: 2012
 Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

EN 301 489-24 V1.5.1: 2010
 Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 24: Specific conditions for IMT-2000 CDMA Direct Spread (UTRA) for Mobile and portable (UE) radio and ancillary equipment



 Český [Czech]	<p><i>[Jméno výrobce]</i> tímto prohlašuje, že tento <i>[typ zařízení]</i> je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.</p>
 Dansk [Danish]	<p>Undertegnede <i>[fabrikantens navn]</i> erklærer herved, at følgende udstyr <i>[udstyrets typebetegnelse]</i> overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.</p>
 Deutsch [German]	<p>Hiermit erkläre <i>[Name des Herstellers]</i>, dass sich das Gerät <i>[Gerätetyp]</i> in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.</p>
 Eesti [Estonian]	<p>Käesolevaga kinnitab <i>[tootja nimi = name of manufacturer]</i> seadme <i>[seadme tüüp = type of equipment]</i> vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.</p>
 English	<p>Hereby, <i>[name of manufacturer]</i>, declares that this <i>[type of equipment]</i> is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.</p>
 Español [Spanish]	<p>Por medio de la presente <i>[nombre del fabricante]</i> declara que el <i>[clase de equipo]</i> cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.</p>
 Ελληνική [Greek]	<p>ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ <i>[name of manufacturer]</i> ΔΗΛΩΝΕΙ ΟΤΙ <i>[type of equipment]</i> ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.</p>
 Français [French]	<p>Par la présente <i>[nom du fabricant]</i> déclare que l'appareil <i>[type d'appareil]</i> est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.</p>
 Italiano [Italian]	<p>Con la presente <i>[nome del costruttore]</i> dichiara che questo <i>[tipo di apparecchio]</i> è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.</p>
 Latviski [Latvian]	<p>Ar šo <i>[name of manufacturer / izgatavotāja nosaukums]</i> deklarē, ka <i>[type of equipment / iekārtas tips]</i> atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.</p>
 Lietuvių [Lithuanian]	<p>Šiuo <i>[manufacturer name]</i> deklaruoją, kad šis <i>[equipment type]</i> atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.</p>
 Nederlands [Dutch]	<p>Hierbij verklaart <i>[naam van de fabrikant]</i> dat het toestel <i>[type van toestel]</i> in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.</p>

 Malti [Maltese]	<p>Hawnhekk, <i>[isem tal-manifattur]</i>, jiddikjara li dan <i>[il-mudel tal-prodott]</i> jikkonforma mal- nġigijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.</p>
 Magyar [Hungarian]	<p>Alulírott, <i>[gyártó neve]</i> nyilatkozom, hogy a <i>[... típus]</i> megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.</p>
 Polski [Polish]	<p>Niniejszym <i>[nazwa producenta]</i> oświadczam, że <i>[nazwa wyrobu]</i> jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.</p>
 Português [Portuguese]	<p><i>[Nome do fabricante]</i> declara que este <i>[tipo de equipamento]</i> está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.</p>
 Slovensko [Slovenian]	<p><i>[Ime proizvajalca]</i> izjavlja, da je ta <i>[tip opreme]</i> v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.</p>
 Slovensky [Slovak]	<p><i>[Meno výrobcu]</i> týmto vyhlasuje, že <i>[typ zariadenia]</i> spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.</p>
 Suomi [Finnish]	<p><i>[Valmistaja = manufacturer]</i> vakuuttaa täten että <i>[type of equipment = laitteen tyyppimerkintä]</i> tyypinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.</p>
 Svenska [Swedish]	<p>Härmed intygar <i>[företag]</i> att denna <i>[utrustningstyp]</i> står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.</p>