

Pepwave Surf SOHO

User Manual

Peplink Products: Surf SOHO

Pepwave Firmware 8.2.0 March 2022

COPYRIGHT & TRADEMARKS Specifications are subject to change without notice.

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

Table of Contents

Introduction and Scope	6
Glossary	7
Product Features LAN VPN Firewall Outbound Policy QoS Other Supported Features Pepwave Surf SOHO Router Overview	8 8 9 9 9 9 9
Panel Appearance LED Indicators	10 12
Advanced Feature Summary Drop-in Mode and LAN Bypass: Transparent Deployment QoS: Clearer VoIP USB Modem Built-In Remote User VPN Support DPI Engine Wi-Fi Air Monitoring SP Default Configuration SpeedFusion Cloud Relay DNS over HTTPS (DoH) Installation	 13 13 14 14 14 15 16
Preparation Constructing the Network	16 16
Connecting to the Web Admin Interface	16
SpeedFusion Cloud Activate SpeedFusion Cloud Service Enable SpeedFusion Cloud Connect Clients to Cloud Link Wi-Fi to Cloud Optimize Cloud Application	19 19 21 30 31 33
Configuring the LAN Interface(s) Network Settings	34 34

Port Settings	42
Configuring the WAN interface	43
WAN > WAN Quality Monitoring	44
WAN > Ethernet WAN	45
WAN > Physical Interface Settings	46
WAN > Health Check Settings	47
WAN > Bandwidth Allowance Monitor	48
WAN > Additional IP Address Settings	49
WAN > Dynamic DNS Settings	49
Wi-Fi WAN and USB WiFi Network connection	50
WAN > WiFi Connection Profiles	52
WAN > Signal threshold settings	54
PepVPN	56
PepVPN > Send ALL traffic	61
Outbound Policy Management	63
Port Forwarding	66
UPnP / NAT-PMP Settings	68
NAT Mappings	69
QoS	71
User Group	71
Bandwidth Control	71
Application Prioritization	72
Firewall	76
Outbound and Inbound Firewall Rules	75 76
Intrusion Detection and DoS Prevention	78
Content Blocking	80
	00
Routing Protocols	81
OSPF & RIPv2	81
BGP	84
Remote User Access	88
L2TP with IPsec	88
OpenVPN	89
PPTP	89
Authentication Methods	90
Miscellaneous Settings	92
RADIUS Server	92
Certificate Manager	94

Service Forwarding Service Passthrough	94 97
Grouped Networks	98
SIM Toolkit	99
AP	102
Wireless SSID	102
Settings	108
AP > Status	111
Access Point	111
Wireless SSID	114
Wireless Client	115
Mesh / WDS	117
Nearby Device	118
Event Log	119
System Settings	120
Admin Security	120
Firmware	123
Time	124
Schedule	125
Email Notification	126
Event Log	130
SNMP	131
InControl	133
Configuration	134
Feature Add-ons	135
Reboot	135
Tools	135
Ping	136
Traceroute Test	137
Wake-on-LAN	137
WAN Analysis	138
Status	141
Device	142
Active Sessions	144
Client List	146
OSPF & RIPv2	147
BGP	147
PepVPN Status	147

Event Log	150
WAN Quality	151
Usage Reports	152
Appendix A: Restoration of Factory Defaults	156
Appendix B: Overview of ports used by Peplink SD-WAN routers and other Peplink services	157
Appendix C: Declaration	159

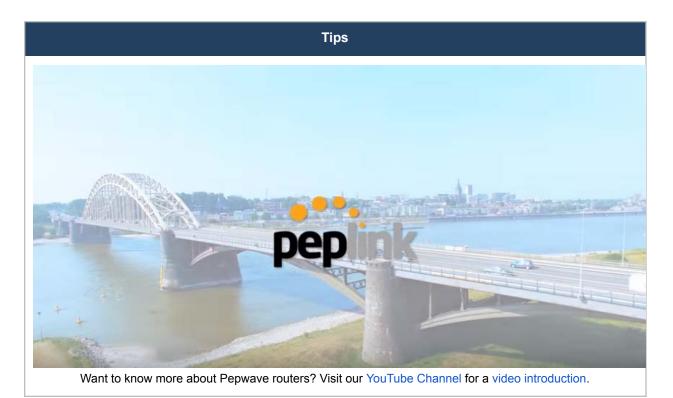


Introduction and Scope

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

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

This manual covers setting up a Surf SOHO router and provides an introduction to their features and usage.





Glossary

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

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

Product Features

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

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

Below is a list of supported features on Pepwave routers. Features vary by model. For more information, please visit <u>our website</u>.

WAN

- Ethernet WAN connection in full/half duplex
- Static IP support for PPPoE
- USB mobile connection(s)
- Wi-Fi WAN connection
- Network address translation (NAT)/port address translation (PAT)
- Inbound and outbound NAT mapping
- IPsec NAT-T and PPTP packet pass through
- Intelligent Failover
- MAC address clone and passthrough
- Customizable MTU and MSS values
- WAN connection health check
- Dynamic DNS
- Ping, DNS lookup, and HTTP-based health check

LAN

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

VPN

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

Firewall

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

Outbound Policy

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

QoS

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

Other Supported Features

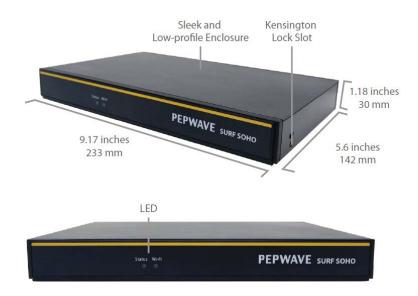
- User-friendly web-based administration interface
- HTTP and HTTPS support for web admin interface
- Configurable web administration port and administrator password
- Firmware upgrades, configuration backups, ping, and traceroute via web admin interface
- Remote web-based configuration (via WAN and LAN interfaces)
- Time server synchronization
- SNMP
- Email notification
- Read-only user for web admin
- Shared IP drop-in mode
- Authentication and accounting by RADIUS server for web admin
- Syslog
- SIP passthrough
- PPTP packet pass through
- Event log
- Active sessions

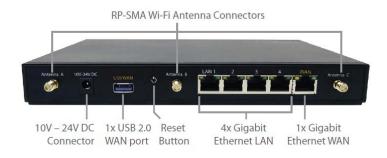


- Client list
- UPnP / NAT-PMP
- Real-time, hourly, daily, and monthly bandwidth usage reports and charts

Pepwave Surf SOHO Router Overview

Panel Appearance





	Specifications
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 and Status Indicators				
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				

		LAN and Ethernet WAN Ports
0	ON	1000 Mbps
Green LED	OFF	10 Mbps / 100 Mbps or port is not connected
	ON	Port is being connected
Orange LED	Blinking	Data is being transferred
	OFF	No data is being transferred or port is not connected
Port type	Auto MDI/MDI-2	X ports

	Wi-Fi Signal
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 looses 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 <u>250 modem types</u>.

Built-In Remote User VPN Support



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

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

DPI Engine

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

SSCS

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



Wi-Fi Air Monitoring

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

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

```
    Wi-Fi Air Monitoring
    Enable Save
    WARNING: Any supported Wi-Fi / AP features will cease to function when Wi-Fi Air Monitoring is turned on.
```

SP Default Configuration

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

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

SpeedFusion Cloud Relay

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

https://forum.peplink.com/t/configure-speedfusion-cloud-relay-server-and-client/6215ca9b017e48e0f3ff24 79/

DNS over HTTPS (DoH)

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



Installation

The following section details connecting Pepwave routers to your network.

Preparation

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

- At least one Internet/WAN access account and/or Wi-Fi access information
- Depending on network connection type(s), one or more of the following:
- Ethernet WAN: An ethernet cable with RJ45 connector
- USB: A USB modem

• **Wi-Fi WAN**: Wi-Fi antennasA computer with the TCP/IP network protocol and a web browser installed. Supported browsers include Microsoft Internet Explorer 11 or above, Mozilla Firefox 24 or above, Apple Safari 7 or above, and Google Chrome 18 or above.

Constructing the Network

Construct the network according to the following steps:

1: With an Ethernet cable, connect a computer to one of the LAN ports on the Pepwave router. Repeat with different cables for up to 4 computers to be connected.

2: With another Ethernet cable or a USB modem/Wi-Fi antenna/, connect to one of the WAN ports on the Pepwave router. Repeat the same procedure for other WAN ports.

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

Connecting to the Web Admin Interface

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

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

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

PEPWAVE	
	Login Username:
	Password:
	Legin
logyrght & Pepviswe. All rights reserved.	

admin interface.

Username: admin Password: admin

(This is the default admin user login of the Pepwave



Surf SOHO.)

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

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

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

PEPWAVE	Dashboard	SpeedFusion Cloud	Network	Advanced	AP	System	Status	Apply Changes
		st change your default	password n	ow to procee	d			
	Change Current P	Password						
	New Pass		1		0			
	C		Require at	least 10 chara	icters,	lower and	upper case, with	numbers.
	Connirm	New Password						
				Save an	d app	Y		

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

PEPWAVE	Dashboard	SpeedFusion (Cloud Netwo	rk Advanced	AP S	system	Status	Apply	Changes
		nnection Status							?
	Priority 1	(Highest)							
	📄 💿 Wi-	Fi WAN on 2.4	📶 📒 Connect	ed to				Wireless Networks	Details
	💿 wi-	Fi WAN on 5 GHz	📶 📒 Connect	ed to				Wireless Networks	Details
	Priority 2								
			Drag	g desired (Priority	/ 2) conne	ections he	re		
	Disabled								
	🗿 🔲 wat	N	🗌 Disabled						Details
	🕜 Оре	nVPN WAN 1	🔲 Disabled						Details
	LAN Inte	rface							
		Address: 192.168	8.50.1						
	Wi-Fi AP							OFF 🗸	Details
	Wi-Fi AP	has been disabled							
				(No Wi	i-Fi AP)				
	Device I	nformation							
	Model: Firmware: Uptime: CPU Load Throughp	:	Pepwave Surf SC 8.2.0b01 build 5 0 days 1 hour 51 4 52.0 kbps † 6	054 minutes] 31%					

The Dashboard shows current WAN, LAN, and Wi-Fi AP statuses. Here, you can change WAN

connection priority and switch on/off the Wi-Fi AP.

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

Important Note

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



SpeedFusion Cloud

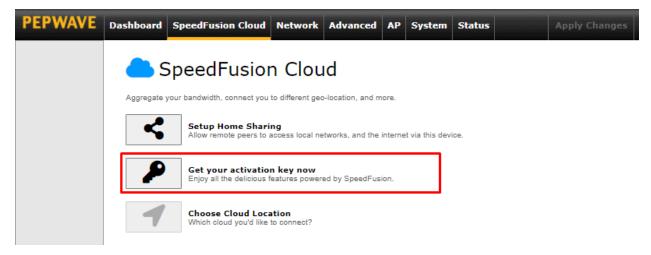
With Peplink products, your device is able to connect to SpeedFusion Cloud without the use of a second endpoint. This service has wide access to a number of SpeedFusion endpoints hosted from around the world, providing your device with unbreakable connectivity wherever you are.*



*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 <u>https://store.peplink.com/</u> > Cloud Solutions > SpeedFusion Cloud Service.

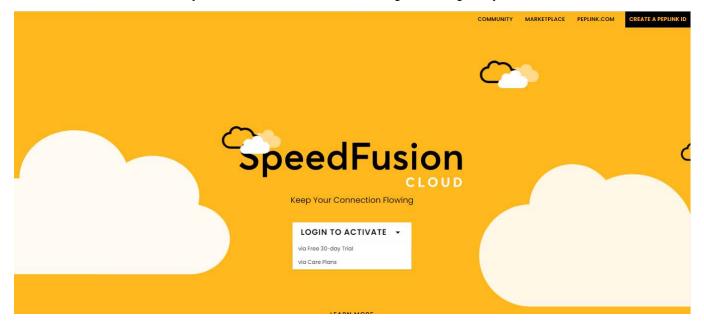
Activate SpeedFusion Cloud Service

You are entitled to a 30-days free period with 100GB of SpeedFusion usage upon activation of the SpeedFusion Cloud service. This offer is limited to once per device. To get your activation key please visit SpeedFusion Cloud.





Go to activate.speedfusion.com and select the type of SpeedFusion Cloud service, "Via Free 30-days Trial" or "Via Care Plans", that you would like to activate. Next, register or login to your account.



Select the devices that you wish to activate SpeedFusion Cloud on and Click ACTIVATE.

Activate SFC via	Free 30-Day Trial			
Please select the devices to activate.	Only eligible devices will be displayed.			
Groups All	Model All	Device Name. V Please Enter	Serial Number Please Enter	
Total: 2 eligible device(s)				Grid 📕 List
 ✓ 				1 device(s) selected
Inactive MAX BRI MK2 LTEA (INT/APAC)	MAX Hotspot LTE (Europe/int'l			
atl MAX	GSM)			
Firmware 8.1.0 Plan: null	Firmwore 7.0.2 Pierc SFC-DP-TRIAL			
Devices Per Page 25 💙				
				ACTIVATE



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

PEPWAVE	Dashboard	SpeedFusion Cloud	Network	Advanced	AP	System	Status		Apply Changes
System									
 Admin Security 	Feature	Activation		ana	hhhh			handahan	
 Firmware 	Activation	Кеу							23e54fe148f876e75
Time									05ef747c958e346e e34db668f55dff5ff
 Schedule 			75dff46f8	09dd4cef09be1	8a61	9d16bbfa96	c3083b48a	a7d337ade18	7a5ce2e4e1
 Email Notification 									
Event Log				Activ	ate				
SNMP									
 SMS Control 									
 InControl 									
 Configuration 									
 Feature Add-ons 									
 Reboot 									

Enable SpeedFusion Cloud

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





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

SpeedFusion Cloud > Setup Home Sharing									
SpeedFusion Cloud									

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

SpeedFusion Cloud > Setup Home Sharing							
Allow remote peers to access loca	al networks, and the internet via this device.						
SpeedFusion Cloud	Cloud Location	?					
SFH-SHARE-SIN	Home Sharing Code:	×					

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

SpeedFusion Cloud > Choose Cloud Location								
You can connect up to 3 different cloud locations.								
SpeedFusion Cloud	Cloud Location	\bigcirc						
apeedrasion Cloud		•						
SDWC SFC-HKG	Hong Kong (HKG)	×						



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

PEPWAVE	Dashboard	SpeedFusion Cloud	Network	Advanced	АР	System	Status		Apply Changes
		peedFusion		d > Cł	100	ose C	loud	Locati	on
	SpeedFu	sion Cloud	United Sta	atic atic (SYD) (FRA) O)					

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

SpeedFusion Cloud > Choose Cloud Location								
You can connect up to 3 different closes	You can connect up to 3 different cloud locations. SpeedFusion Cloud Cloud Location							
	[Home Sharing] ✓ [e.g. 1234-5678-1234-5678							

Click on Apply Changes to save the change.

PEPWAVE	Dashboard	SpeedFusion Cloud	Network	Advanced	AP System	Status	Apply Changes
	Saved! (Changes will be effectiv	ve after click	ting the 'Apply	y Changes' bu	tton.	
	a S	peedFusior	n Clou	d > Ch	oose (Cloud Loc	ation
		nnect up to 3 different cloud					
	SpeedFu SFC	ision Cloud	Cloud Loc				×
PEPWAVE	Dashboard	d SpeedFusion Clou	ud Netwo	rk Advance	ed AP Sys	stem Status	Apply Changes
PEPWAVE				rk Advance	ed AP Sys	stem Status	Apply Changes
PEPWAVE	Change	es applied successful	ly.				
PEPWAVE	Chang	es applied successfull SpeedFusic	_{ly.} on Clo				
PEPWAVE	Chang Chang You can c	es applied successful	ly. On Clo ud locations.				
PEPWAVE	Chang Chang You can c	es applied successfull SpeedFusic connect up to 3 different clo	ly. On Clo uud locations. Cloud 1	ud > (
PEPWAVE	Chang Chang Speedf	es applied successfull SpeedFusic connect up to 3 different clo	ly. On Clo uud locations. Cloud 1	ud > (Location			ocation



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)	5	()
		Drag desired (Priority 1) connections here	
	Priority 2		
	1 Cellular 1	Connected to MY MAXIS LITEA	Details
	T2 Cellular 2	📶 🧧 Connected to MY MAXIS 💵	Details
	Priority 3	Drag desired (Priority 3) connections here	
	Disabled	Drag desired (Fronzy 5) connections here	
	1 WAN 1	Disabled	Details
	2 WAN 2	Disabled	Details
	T3 Cellular 3	Disabled	Details
	🚹 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: 192.1	68.50.1	
	Wi-Fi AP		ON 🗸 Details
	SpeedFusion Cloud	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**.

PEPWAVE	Dashboard	SpeedFusion Cloud	Network	Advanced	АР	System	Status		Apply Changes
		peedFusior		d > Cł	100	ose C	loud	Locati	on
	SpeedFu SFC	sion Cloud	Cloud Loc						×

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 Ch	anges
		×
	SpeedFusion Cloud Profile	
	Cloud Location Automatic	
	1 - Default +	
	Tunnel Options	
	Local / Remote Tunnel ID 1 (default tunnel)	
	Tunnel Name Default	
	Data Port O Auto O Custom	
	Bandwidth Limit 🕐 🗆	
	WAN Smoothing Overall Redundancy Level Off	
	Maximum Level on the Same Link Off 🗸	
	Forward Error Correction 🕐 Off 🗸	
	Receive Buffer 🕐 🛛 ms	

PEPWAVE	Dashboard	SpeedFusion Cloud	Network	Advanced	AP Syst	em Status		Apply Changes
								×
	SpeedFu	sion Cloud Profile						
	Enable		>					
	Cloud Loo	cation	Automa	tic 🗸				
				_				
	1 - De	efault 2 - WAN Smo	o × +					
	Tunn	el Options						
		/ Remote Tunnel ID	2					
	Tunne	l Name	WAN Smo	othing 🖌				
	Data	Port 🥐	O Auto	Custom				
	Bandy	vidth Limit 🛛 🤶						1
	WAN	Smoothing	Overall Rec	lundancy Level			Normal 🗸	
			Maximum L	evel on the Sam	e Link		Normal 🗸	
	Forwa	rd Error Correction (Off	~		L		
	Receiv	ve Buffer 🤶	0	ms				



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

Priority 1 (Highest)	us	
	Drag desired (Priority 1) connections here	
Priority 2		
1 Cellular 1	Connected to MY MAXIS LTEA	Detai
T2 Cellular 2	📶 🧧 Connected to MY MAXIS 💴	Detai
Priority 3	Drag desired (Priority 3) connections here	
Disabled	bray desired (Phoney 5) connections here	
1 WAN 1	Disabled	Detai
2 WAN 2	Disabled	Detai
 T3 Cellular 3	Disabled	Detai
诸 Cellular 4	Disabled	Detai
🗟 Wi-Fi WAN	Disabled	Detai
3 LAN 1 as WAN	Disabled	Detai
4 LAN 2 as WAN	Disabled	Detai
5 LAN 3 as WAN	Disabled	Detai
LAN Interface		
Router IP Address: 192.	.168.50.1	
Wi-Fi AP		🔵 ON 🗸 Detai



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

PEPWAVE	Dashboard SpeedFusion Cloud Network Advanced AP System Status Ap	
Advanced		
 SpeedFusion 	Outbound Policy	
IPsec VPN	Custom	
GRE Tunnel		
 Outbound Policy 	Add a New Custom Rule	× (
Port Forwarding		
NAT Mappings	Service Name to_internet	
QoS	Enable 🗹	
 User Groups 	Source (?) IP Address V 192.168.50.10	×
 Bandwidth 	Destination (?) Any V	
Control	Protocol (2) Any V C:: Protocol Selection :: V	1
Application	Algorithm (?) Priority	
Firewall	Priority Order (?) Highest Priority Not In Use	ī (
 Access Rules 	Cloud: SFC (1 - Defau	
Content Blocking	Cloud: SFC (2 - WAN	
Routing Protocols	WAN: WAN 1	
OSPF & RIPv2	WAN: WAN 2	
BGP	WAN: Cellular 1 WAN: Cellular 2	
Remote User	WAN: Cellular 3	
Access	WAN: Cellular 4	
Misc. Settings	WAN: USB	
 High Availability 	WAN: Wi-Fi WAN	
 RADIUS Server 	WAN: LAN 2 as WAN	
Certificate	WAN: LAN 3 as WAN	
Manager	Lowest Priority	
 Service Forwarding 	When No Connections are O Drop the Traffic	
 Service Passthrough 	Terminate Sessions on Connection Recovery	
 GPS Forwarding 		
NTP Server	Save Cancel	
 Grouped Networks 		

Outbound Policy Custom					?
Rules (¹ /Drag and drop Service	rows by the left to chan Algorithm	ge rule order) Source	Destination	Protocol / Port	?
)SPF / BGP / RIPv2 F IFusion Cloud Routes			
<u>to internet</u>	Priority VPN: SFC (1 - Def	IP Address 192.168.50.10	Any	Any	×
HTTPS Persistence	Persistence (Src) (Auto)	Any	Any	TCP 443	×
<u>Default</u>			(Auto)	•	
		Add Rule			
Expert Mode Enabled					2

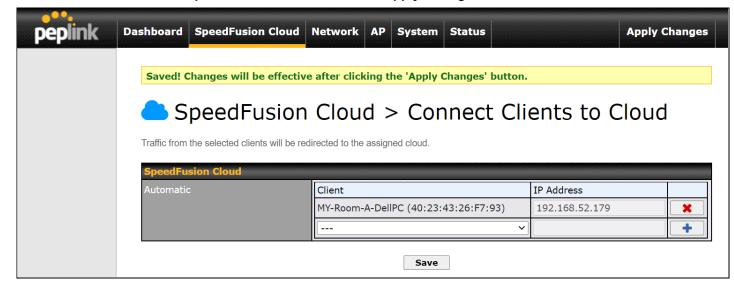
Connect Clients to Cloud

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

SpeedFusion Cloud				
Aggregate your bandwidth, connect you to different geo-location, and more.				
Setup Home Sharing Allow remote peers to access local networks, and the internet via this device.				
Choose Cloud Location Which cloud you'd like to connect?				
Traffic Steering Priority				
Connect Clients to Cloud Select a cloud for your laptops, phones, or other devices.				

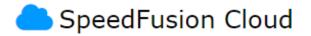


Choose a client from the drop down list > Click + > Save > Apply Changes.



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**.



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



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



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



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





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** followed by **Apply Changes**.

peplink	Dashboard	Setup Wizard	SpeedFusion Cloud	Network	AP	System	Status		Apply Ch	anges	
	b S	peedFus	ion Cloud >	> Link	W	'i-Fi t	o Clo	ud			
	The new SS	BID will inherit all setti	ings from the existing SSID ir	cluding the Se	curity F	Policy.					
	SpeedFu	sion Cloud		hinnin		hhhhhh		hinnin	hinnin		6
	Automatio		Reference SSID		SSID	for Cloud					
			Home		Hom	ne_SFC				×	
				~						+	
				Save							

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

LAN Interface			
Router IP Address: 192.168.5	54.1		
Wi-Fi AP			🗧 ON 🗡 Detail
奈 🔒 HomeBunker	🛜 🔒 Home	🛜 🌥 Home_SFC	



Optimize Cloud Application

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

📥 Sp	SpeedFusion Cloud				
Aggregate your	bandwidth, connect you to different geo-location, and more.				
۷	Setup Home Sharing Allow remote peers to access local networks, and the internet via this device.				
4	Choose Cloud Location Which cloud you'd like to connect?				
—— Traff	ic Steering Priority				
	Connect Clients to Cloud Select a cloud for your laptops, phones, or other devices.				
≡	Create a Wi-Fi SSID that is dedicated for the cloud.				
≡	Optimize Cloud Application Connect to Google, Microsoft, Zoom and others using the Cloud.				

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

SpeedFusion Cloud.

SpeedFusion Cloud > Optimize Cloud Application				
Traffic of the selected cloud application	on will be redirected to the assigned cloud.			
Singapore (SIN)				
SFC-SIN	Cloud Application			
	Zoom			
	···· · · · · · · · · · · · · · · · · ·			
	Google Workspace Microsoft Office 365 Lifesize Salesforce			

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	
<u>VLAN1</u>	1	2.2.2/24	×
VLAN2	2	3.3.3/24	×
Ne	w LAN		

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

You can find which settings are using the VLAN by hovering over the grey "X".

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

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

IP Settings	
IP Address	255.255.0 (/24) 🔻

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

Network Settings		?
Name	Нер	Close
VLAN ID	To define a layer-2 b PepVPN, please click	ridging based <u>here</u> .
Inter-VLAN routing		

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

Layer 2 PepVPN Bridging	2
PepVPN Profiles to Bridge 🔹 🕐	No profile is available
Remote Network Isolation 🛛 📀	
Spanning Tree Protocol	
DHCP Option 82 Injection	
Override IP Address when ?	$lace$ Do not override \bigcirc Static \bigcirc By DHCP \bigcirc As None

Layer 2 PepVPN Bridging

PepVPN Profiles to Bridge	The remote network of the selected PepVPN profiles will be bridged with this local LAN, creating a Layer 2 PepVPN, they will be connected and operate like a single LAN, and any broadcast or multicast packets will be sent over the VPN.
Remote Network Isolation	Enable this option if you want to block network traffic between the remote networks, this will not affect the connectivity between them and this local LAN.
Spanning Tree Protocol	Click the box will enable STP for this layer 2 profile bridge.
DHCP Option 82	Click on the question Mark if you want to enable DHCP Option 82. This allows the device to inject Option 82 with Router Name information before forwarding the DHCP Request packet to a PepVPN peer, such that the DHCP Server can identify where the request originates from.
Override IP Address when bridge connected	Select "Do not override" if the LAN IP address and local DHCP server should remain unchanged after the Layer 2 PepVPN is up. If you choose to override IP address when the VPN is connected, the device will not act as a router, and most Layer 3 routing functions will cease to work.

DHCP Server	iiiiii						
DHCP Server	?	✓ Enable					
DHCP Server Logging	Help		2				
IP Range	built-	k the Enable box to enable the in DHCP server which serves		2	55.255.255.0 (/24)	T	
Lease Time	If you	P requests on the LAN. u want to enable DHCP relay er, click <u>here</u> .	0 Min	IS			
DNS Servers	Assign DNS server automatically						
воотр							
Extended DHCP Option		Option	Value				
			No Extended DHCP Option				
		Add					
DHCP Reservation	(?)	Name	MAC Addres	S	Static IP		
			00:00:00:00	0:00:00		+	

	DHCP Server Settings	
DHCP Server	When this setting is enabled, the DHCP server automatically assigns an IP address to each computer that is connected via LAN and configured to obtain an IP address via DHCP. The Pepwave router's DHCP server can prevent IP address collision on the LAN.	
DHCP Server Logging	Enable logging of DHCP events in the eventlog by selecting the checkbox.	
IP Range & Subnet Mask	These settings allocate a range of IP addresses that will be assigned to LAN computers by the Pepwave router's DHCP server.	
Lease Time	This setting specifies the length of time throughout which an IP address of a DHCP client remains valid. Upon expiration of the lease time, the assigned IP address will no longer be valid and renewal of the IP address assignment will be required.	
DNS Servers	This option allows you to input the DNS server addresses to be offered to DHCP clients. If Assign DNS server automatically is selected, the Pepwave router's built-in DNS server address (i.e., LAN IP address) will be offered.	
BOOTP	Check this box to enable BOOTP on older networks that still require it.	
Extended DHCP Option		
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	



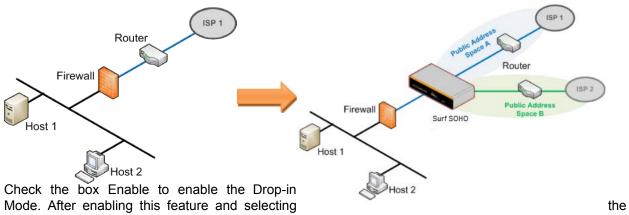
remove a record. Reserved client information can be imported from the **Client List**, located at **Status>Client List**. For more details, please refer to **Section 22.3**.

DHCP Relay Settings	
DHCP Relay 🥐	✓ Enable
DHCP Server IP Address	DHCP Server 1: DHCP Server 2:
DHCP Option 82	
DHCP Relay Logging	

DHCP Relay Settings			
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:



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	2			
WAN for Drop-In Mode	WAN V WAN V Apply NAT on VLAN networks outgoing Internet traffic VLAN network(s) may route their outgoing Internet traffic to this unit. When this checkbox is checked their traffic will be NAT'd before forwarding out of this WAN. Leave this checkbox checked if you are not sure.			
Share Drop-In IP 🔹 🕐				
Shared IP Address ?	255.255.255.	0 (/24) 🗸		
Static Route	Destination Network	Subnet Mask		
		255.255.255.0 (/24)		
WAN Default Gateway	✓ I have other host(s) on WAN segment IP Address -			
WAN DNS Servers 🤶	DNS server 1: DNS server 2:			
NOTE: The DHCP Server Settings will be overwritten.				
Dynamic DNS Settings.	overwritten: Connection Method, MTU,	Health Check, Additional Public IP, and		
The PPTP Server will be disabled.				
Tip: please review the DNS Forward	ding setting under the Service Forwardi	ing section.		

Drop-in Mode Settings 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	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.).
	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.).
Shared IP Address ^A	Access to this IP address will be passed through to the LAN port if this device is not serving the service being accessed. The shared IP address will be used in connecting to hosts on the WAN (e.g., email notification, remote syslog, etc.) The device will also listen on the IP address when hosts on the WAN access services served on this device (e.g., web admin accesses from WAN, DNS server, etc.)
WAN Default Gateway	Enter the WAN router's IP address in this field. If there are more hosts in addition to the router on the WAN segment, click the 🞯 button next to "WAN Default Gateway" and check the other host(s) on the WAN segment box and enter the IP address of the hosts that need to access LAN devices or be accessed by others.
WAN DNS Servers	Enter the selected WAN's corresponding DNS server IP addresses.

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

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 Settings
Static Route	This table is for defining static routing rules for the LAN segment. A static route consists of the network address, subnet mask, and gateway address. The address and subnet mask values are in <i>w.x.y.z</i> 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			
<u> </u>	· · · · · · · · · · · · · · · · · · ·		+		
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: <u>https://youtu.be/C1FMdZCn3Z8</u>

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

DNS Proxy Settings			mininter		?	
Enable						
DNS Caching	?					
Include Google Public DNS Servers	?					
Local DNS Records	?	Host Name		IP Address		
					+	
Domain Lookup Policy	?	Domain	Connectior)		
					• +	
DNS Resolvers	?	WAN Connection			DNS Servers	
		WAN 1			1.1.1.1 1.0.0.1	
		WAN 2				
		WAN 3				
		WAN 4			8.8.8.8 8.8.4.4	
		WAN 5				
		Mobile Internet				
		LAN Connection			DNS Servers	
		Untagged LAN				
		Preferred connections are show	n with 🗹			

	DNS Proxy Settings
Enable	To enable the DNS proxy feature, check this box, and then set up the feature at Network>LAN>DNS Proxy Settings . A DNS proxy server can be enabled to serve DNS requests originating from LAN/PPTP/SpeedFusion [™] peers. Requests are forwarded to the DNS servers/resolvers defined for each WAN connection.
DNS Caching	This field is to enable DNS caching on the built-in DNS proxy server. When the option is enabled, queried DNS replies will be cached until the records' TTL has been reached. This feature can 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.
Include Google Public DNS Servers	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.
Local DNS Records	This table is for defining custom local DNS records. A static local DNS record consists of a host name and IP address. When looking up the host name from the LAN to LAN IP of the Pepwave Surf SOHO, the corresponding IP address will be returned. To display the option to set TTL manually, click 2. Click to create a new record. Click to remove a record.
Domain Lookup Policy	DNS proxy will look up the domain names defined here using only the specified connections.



	Check the box to enable the WINS server. A list of WINS clients will be displayed at Network>LAN>DNS Proxy Settings>DNS Resolvers .
DNS Resolvers ^a	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 Ø button on the top right-hand corner to activate.

Port Settings

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

Port	Name	Enable	Speed	Advertise Speed
1	LAN Port 1			
2	LAN Port 2		Auto 🔻	
3	LAN Port 3		Auto	Yes
4	LAN Port 4		1 Gbps Full Duplex 100 Mbps Full Duplex	
	Save		100 Mbps Half Duplex 10 Mbps Full Duplex 10 Mbps Half Duplex	

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

	LAN Physical Settings
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.

PEPWAVE	Dashboard	SpeedFusion C	loud Network	Advanced	AP System	Status	Apply	Changes
LAN								
 Network Settings 	WAN Cor	nection Status						?
Port Settings	Priority 1	(Highest)						
WAN	🖉 💿 Wi-l	Fi WAN on 2.4	.111 📒 Connected	to			Wireless Networks	Details
	💿 Wi-l	Fi WAN on 5 GHz	📶 🧧 Connected	to			Wireless Networks	Details
	Priority 2							
			Drag (desired (Priority	2) connections	here		
	Disabled							
	🗐 💷 wat	N	🔲 Disabled					Details
	💮 Ope	nVPN WAN 1	🗌 Disabled					Details
	DNS ove	UTTOS						
	Disabled							
	WAN Qua	ality Monitoring						?
	Auto							

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

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

DNS over HTTPS (DoH)



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

DNS over HTTPS			
Enable 🕐	2		
Server	Cloudflare Cloudflare Quad9 Google DNS		
	OpenDNS Custom URL: Save Cano	el	

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

WAN > WAN Quality Monitoring

This setting advice how WAN Quality information is being gathered.

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

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

Important Note

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



WAN > Ethernet WAN

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

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

WAN Connection Settings		
WAN Connection Name		Default
Connection Method	?	DHCP V
Routing Mode	?	• NAT
Hostname (Optional)		Use custom hostname
DNS Servers		 Obtain DNS server address automatically Use the following DNS server address(es) DNS Server 1: DNS Server 2:
IP Passthrough	?	
Independent from Backup WANs	?	
Standby State	?	Remain connected O Disconnect
Reply to ICMP Ping	?	● Yes ○ No
Upload Bandwidth	?	10 Mbps •
Download Bandwidth	?	110 Mbps •

WAN Connection Settings				
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: 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 (Optional)	Provide a hostname for this WAN port if requested by the ISP
Management IP Address	Management IP Address is available for configuration when you click the link in the help icon via the Hostname.
	This option allows you to configure the management IP address for the DHCP WAN connection.
DNS Servers	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 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 traffi 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

	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 .

	Physical Interface Settings
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 defaut MAC address is a unique value assigned at the factory. In most cases, the default value 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 enab multiple broadcast domains. Once you enable VLAN, you will be able to enter a name for you 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:
	Host 2:
	Use first two DNS servers as PING Hosts
Timeout	5 v second(s)
Health Check Interval	5 v 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 specified the number of health check attempts the router will make. Upon reaching this number, the link will be considered as failed

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

WAN > Bandwidth Allowance Monitor

The Bandwidth Allowance Monitor helps to keep track of your network usage. To enable this function, connect to the Web Admin Interface and go to **Network > WAN**. Check the box **Enable** next to Bandwidth Allowance Monitor and you can see the following:

Bandwidth Allowance Moni	tor	
Bandwidth Allowance Monitor	?	Enable
Action	?	 Email notification is currently disabled. You can get notified when usage hits 75%/95% of monthly allowance by enabling <u>Email Notification</u>. Reserve for management traffic when usage hits 100% of monthly allowance Disconnect when usage hits 100% of monthly allowance
Start Day	?	On 1st • of each month at 00:00 midnight
Monthly Allowance	?	GB ▼

Action: If the feature **Email Notification** *i*s 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.

Additional IP Address Settings	
Additional IP Address	IP Address
	Subnet Mask 255.255.255.255 (/32) 🔻
	•
	A
	× X

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

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

WAN > Dynamic DNS Settings

Pepwave Surf SOHO routers allow registering domain name relationships to dynamic DNS service providers. Through registration with dynamic DNS service provider(s), the default public Internet IP address of each WAN connection can be associated with a hostname.

With dynamic DNS service enabled for a WAN connection, you can connect to your WAN's IP address externally even if its IP address is dynamic.

You must register for an account from the listed dynamic DNS service providers before enabling this option.

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

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

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

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

Wi-Fi WAN and USB WiFi Network connection

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

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

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

Wi-Fi WAN Settings	······································		
Channel Width	20/40 MHz •		
Channel	○ Auto ● Custom Edit Channels:		
Output Power	Max Boost		
Data Rate	● Auto ○ Fixed		
Roaming	✓ Enable		
Roaming Algorithm	Normal O Advanced		
Roaming Signal Level Threshold	-75 dBm		
Roaming Signal Level Gain	5 dBm		
Roaming Check Interval	30 seconds		
Connect to Any Open Mode AP ?	○ Yes ● No		
Beacon Miss Counter	5		
Channel Scan Interval	50 ms		

	Wi-Fi WAN Settings		
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:		
Output Power	Low, Medium, High, Max (boost options for tickbox). Max is the Maximum transmit power supported for that country / Maximum power supported of that device (the smaller value). High, Medium, Low is having -3dBm each from the previous level. Transmit power of 2.4Ghz is generally approximately 20dBm.		
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) pr 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.

Wi-Fi Connection Profiles		?
Network Name (SSID)	Security	
		×
	Open	×
	Open	×
	■ WPA/WPA2-Personal	×
	Open	×
Create Profile		

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

Create Wi-Fi Connection Profile				
Wi-Fi Connection				
Network Name (SSID)				
Security	Open 🗸			
Preferred BSSID				
Connection Method	DHCP V			
DNS Servers	 Obtain DNS server address automatically Use the following DNS server address(es) DNS Server 1: DNS Server 2: 			

OK	Cancel
U.L.	Calicei

Wi-Fi Connection Profile Settings				
Network Name (SSID)	Enter a name to represent this Wi-Fi connection.			
Security	This option allows yo Available options: • Open	ou to selec	ct which security policy is used for this wireless network.	
	Security	Open	T	
	• WEP			
	Security	WEP	T	
	Encryption Key		Characters	
	• WPA/WPA2 – F			
	Security	WPA/WPA	PA2-Personal	
	Shared Key			
			Characters	
	• WPA/WPA2 – E	-		
	Security	WPA/WPA	PA2-Enterprise 🔻	
	Login ID Password			
	Confirm Password			
	EAP Method	PEAP •]	
	EAP Phase 2 Method	EAP/CHA	AP T	
	EAP outer authentication	Anony		
	authentication User Credentials			
	WPA3 – Personal			
	Security		WPA3-Personal V	
	Shared Key			
	✓ Hide Characters			
	WPA2/WPA3 – Personal			
	Security		WPA2/WPA3-Personal	
	Shared Key		✓ Hide Characters	
• 802.1x with dynamic WEP key				

	Security	802.1x with dynamic WEP key 🗸	
	EAP Method	PEAP V	
	EAP Phase 2 Method	EAP/CHAP V	
	Login ID		
	Password		
	Confirm Password		
	EAP outer authentication identity	Anonymous User Credentials Other:	
Preferred BSSID	Configure the BSSID; the BSS	ID 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

Signal Threshold Settings	
Acceptable Level	a at. atl. atl

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

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

Signal Threshold Settings			hini	?
Signal Strength	RSSI: n/a	dBm	(Recovery: n/a	dBm)

Indication of WiFi strength values:

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



-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 Spee	dFusion Clo	ud Network	Advanced	AP System	m Status	Appl	y Changes
Advanced								
PepVPN								
 GRE Tunnel 	PepVPN	N						ES 😶
Port Forwarding	•							
NAT Mappings	O InControl ma	nagement ena	bled. Settings ca	an now be config	gured on <u>InCo</u>	ntrol.		
QoS	Profile	Remo		Remote Addr	vass(es)			
 Bandwidth Control 				No VPN Connec	tion Defined			
 Application 				New Pr	ofile			
Firewall								
 Access Rules 	Send All Traffic	: To						
Content Blocking	No PepVPN profil	e selected						
Routing Protocols								
OSPF & RIPv2	Rules (Drag	and drop rov	vs by the left to	o change rule o	order)			?
BGP	Service		Algorithm	Source	•	Destination	Protocol	
Remote User Access				(Auto			/ Port	
Misc. Settings				Add R	ule			
RADIUS Server								
 Certificate Manager 	PepVPN Local 1 Local ID	D	() SURF_SOF	HO_8F18				
 Service Forwarding 				_				
 Service Passthrough 	PepVPN Setting		Recom	mended (Appro	v 15 secs)			?
 Grouped Networks 			O Fast (A	Approx. 6 secs) (Approx. 2 secs				
 SIM Toolkit 				ne (Under 1 sec etection time inc		Ith checks and	d higher bandwidth o	verhead
Logout				Sav	e			

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

The example below had allPepVPN advanced features enabled.

PepVPN Profile				
Name 🤅				
Enable				
Encryption) 💿 🚔 256-bit AES 🔿 🖴 OFF			
Authentication	Remote ID / Pre-shared Key			
Remote ID / Pre-shared Key	Remote ID Pre-shared Key			
NAT Mode				
Remote IP Address / Host ? Names (Optional)				
	If this field is empty, this field on the remote unit must be filled			
Cost	10			
Data Port 🤅	UDP 🗸 🖲 Auto 🔿 Custom			
Bandwidth Limit 🤇				
Receive Buffer	0ms			
Packet Fragmentation	● Always ○ Use DF Flag			
Use IP ToS				
Latency Difference Cutoff	500 ms			

	PepVPN Profile Settings
Name	This field is for specifying a name to represent this profile. The name can be any combination of alphanumeric characters (0-9, A-Z, a-z), underscores (_), dashes (-), and/or non-leading/trailing spaces ().
Active	When this box is checked, this VPN connection profile will be enabled. Otherwise, it will be disabled.
Encryption	By default, VPN traffic is encrypted with 256-bit AES . If Off is selected on both sides of a VPN connection, no encryption will be applied.
Authentication	Select from By Remote ID Only , Preshared Key . 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)	If NAT Mode is not enabled, you can enter a remote peer's WAN IP address or hostname(s) here. If the remote uses more than one address, enter only one of them here. Multiple hostnames are allowed and can be separated by a space character or carriage return. Dynamic-DNS host names are also accepted.
	This field is optional. With this field filled, the Pepwave 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.
	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.
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.
Packet Fragmentation	If the packet size is larger than the tunnel's MTU, it will be fragmented inside the tunnel in order to pass through.
	Select Always to fragment any packets that are too large to send, or Use DF Flag to only fragment packets with Don't Fragment bit cleared. This can be useful if your application does Path MTU Discovery, usually sending large packets with DF bit set, if allowing them to go through by fragmentation, the MTU will not be detected correctly.
Use IP ToS ^A	If Use IP ToS is enabled, the ToS value of the data packets will be copied to the PepVPN header during encapsulation.
Latency Difference Cutoff ^A	Traffic will be stopped for links that exceed the specified millisecond value with respect to the lowest latency link. (e.g. Lowest latency is 100ms, a value of 500ms means links with latency 600ms or more will not be used)
Multiple PepVPN profiles between the same 2 sites ^A	Enable this advanced feature to create up to 5 PepVPN tunnels from your router to the same remote location, each with different behavior. See: <u>https://forum.peplink.com/t/outbound-policies-within-a-pepvpn-or-speedfusion-tunnel/</u>

^A - Advanced feature, please click the 2 button on the top right-hand corner to activate.

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

Traffic Distribution	
Policy ?	Bonding

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

	Traffic Distribution
Policy	This option allows you to select the desired out-bound traffic distribution policy:
Foncy	Bonding - Aggregate multiple WAN-to-WAN links into a single higher



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

PepVPN > Send ALL traffic

Send All Traffic To	
No PepVPN profile selected	
	- 81

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

Backup Site

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

PepVPN Settings		?
Handshake Port	• Default O Custom	Help <u>Close</u>
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 	To customize handshake port (TCP), please click <u>here</u> .
	Save	

Handshake Port

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

Link Failure Detection Time

The bonded VPN can detect routing failures on the path between two sites over each WAN connection. Failed WAN connections will not be used to route VPN traffic. Health check packets are sent to the remote unit to detect any failure. The more frequently checks are sent, the shorter the detection time, although more bandwidth will be consumed.

- When Recommended (default) is selected, a health check packet is sent every five seconds, and the expected detection time is 15 seconds.
- When Fast is selected, a health check packet is sent every three seconds, and the expected detection time is six seconds.
- When Faster is selected, a health check packet is sent every second, and the expected detection time is two seconds.
- When Extreme is selected, a health check packet is sent every 0.1 second, and the expected detection time is less than one second.

Outbound Policy Management

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

Important Note

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

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

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

Rules (\"Drag and drop rows by the left to change rule order)							
Service	Algorithm	Source	Destination	Protocol / Port			
	PepVPN	/ OSPF / BGP / RI	Pv2 Routes				
HTTPS Persistence Enforced WAN: WAN Any Any TCP 443							
		Add Rule					

The bottom-most rule HTPS_Peristence 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 I	Rule	
Service Name		
Enable		
Source		Any 🔻
Destination	?	IP Network Mask: 255.255.0 (/24)
Protocol	?	Any
Algorithm	?	Enforced •
Enforced Connection	?	
		Save Cancel

	Default Outbound Policy Settings				
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, MAC address or Client's Associated SSID for traffic that matches the rule.				
Destination	This setting specifies the destination IP address, IP network, Domain name, SpeedFusion Cloud, PepVPN Profile or Grouped network for traffic that matches the rule.				
Protocol	This setting specifies the IP protocol and port of traffic that matches this rule. Via a drop-down menu, the following protocols can be specified:				

	 Any TCP UDP IP DSCP Alternatively, the Protocol Selection Tool drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.) After selecting an item from the Protocol Selection Tool drop-down menu, the protocol and port number remains manually modifiable.
Algorithm	 This setting specifies the behavior of the Pepwave router for the custom rule. One of the following values can be selected: 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.
When No Connections are Available	 This field allows you to configure the default action when all the selected Connections are not available. Drop the Traffic - Traffic will be discarded. Use Any Available Connections - Traffic will be routed to any available Connection, even it is not selected in the list. Fall-through to Next Rule - Traffic will continue to match next Outbound Policy rule just like this rule is inactive.
Terminate Sessions on Connection Recovery	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. When Source is a MAC address, this option will be disabled automatically. Default: Disable



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 Servic	es Defined		
	Add S	ervice		

To define a new service, click Add Service.

Port Forwarding	
Enable	
Service Name	
Protocol	TCP ▼ ← :: Protocol Selection :: ▼
Port	Any Port
Inbound IP Address(es) (Require at least one IP address)	Connection / IP Address(es) All Clear
Server IP Address	
	Save Cancel

	Port Forwarding Settings
Enable	This setting specifies whether the inbound service takes effect. When Enable is checked, the inbound service takes effect: traffic is matched and actions are taken by the Pepwave router based on the other parameters of the rule. When this setting is disabled, the inbound service does not take effect: the Pepwave router disregards the other parameters of the rule.
Service Name	This setting identifies the service to the system administrator. Valid values for this setting consist of only alphanumeric and underscore "_" characters.
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 automatica fill in the protocol and a single port number of common Internet services (e.g. HTTP, HTTPS, etc.). As selecting an item from the Protocol Selection Tool drop-down menu, the protocol and port number rem manually modifiable.
Port	The Port setting specifies the port(s) that correspond to the service, and can be configured to behave in or 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 servers specified by the Servers setting. For example, with IP Protocol set to TCP , and Port set to Port , all TCP traffic is forwarded to the configured servers.
	Port ? Single Port Service Port: 80
	set to TCP , and Port set to Single Port and Service Port 80, TCP traffic received on port 80 is forwarded 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 prange is forwarded via the same respective ports to the LAN hosts specified by the Servers setting. Example, with IP Protocol set to TCP , and Port set to Port Range and Service Ports 80-88, TCP transfer 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
	Map to Port: 88 Port Mapping: traffic that is received by Pepwave router via the specified protocol at the specified por
	Map to Port: 88 Port Mapping: traffic that is received by Pepwave router via the specified protocol at the specified por 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 P



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	Enable					
NAT-PMP	Enable					
Save						

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

peplink	Dashboard	Setup Wiza	rd Network	AP	System	Status		Apply Changes
Status								
 Device 	Forward	ed Ports	assistentiation	and the second				
Ethernet Ports	External 🔺	Internal II	nternal Address	UPnP	/ NAT-PMP	Protocol	Description	
 Active Sessions 	8080	8080 1	92.168.1.10	UPnF	0	ТСР	Test8080	*
 Client List 								Delete All
 OSPF & RIPv2 								
 BGP 								
UPnP / NAT-PMP								
Event Log								

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			
<u>192.168.1.23</u>	(WAN 1):10.88.3.158 (Interface IP)	Use Interface IP only			
	Add NAT Rule				

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

LAN Client(s)	IP Address 🔻			
Address 🕜				
Inbound Mappings	Connection / Inbound IP Address(es) WAN 1 WAN 2 Wi-Fi WAN Cellular 1 Cellular 2 USB			
Outbound Mappings	Connection / Outbound IP Address			
	WAN 1	10.88.3.158 (Interface IP)		
	WAN 2 Interface IP			
	WI-FI WAN Interface IP			
	Cellular 1	Interface IP		
	Cellular 2	Interface IP		
	USB	Interface IP		

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

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

Important Note

Inbound firewall rules override the Inbound Mappings settings.



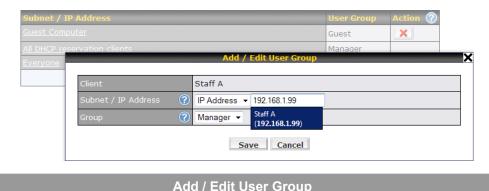
QoS

User Group

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

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

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



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

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

Bandwidth Control

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

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

Group Bandwidth Reservation					
Enable					
0 0					
-	Manager	Staff	Guest		
Bandwidth %	50%	30%	20%		
USB	500.00 Mbps 500.00 Mbps	300.00 Mbps 300.00 Mbps	200.00 Mbps 200.00 Mbps		
Wi-Fi WAN on 2.4 GHz	10.00 Mbps 10.00 Mbps	6.00 Mbps 6.00 Mbps	4.00 Mbps 4.00 Mbps		
Wi-Fi WAN on 5 GHz	10.00 Mbps 10.00 Mbps	6.00 Mbps 6.00 Mbps	4.00 Mbps 4.00 Mbps		

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

Individual Bandwidth Limit				?
Enable				
User Bandwidth Limit		Download	Upload	
	Manager	Unlimited	Unlimited	
	Manager Staff	0 Mbps 🗸	0 Mbps 🗸 (0: Unlimited)	
	Guest	0 Mbps 🗸	0 Mbps 🗸 (0: Unlimited)	

Application Prioritization

Three application priority levels can be set: \uparrow **High**,— **Normal**, and \downarrow **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.

Priority	
↑ High ▼	×
Add	
	 ↑ High ↑ High ↑ High ↑ High ↑ High

Prioritization for Custom Applications

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

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

Add / Edit Application	×.
Туре 📀	Supported Applications O Custom Applications
Category 🥐	Audio Video Streaming 🗸
Application	1Kxun V

		?	Гуре
		• [Application Name
	TCP V	[Scope / Protocol
	Single Port 🗸	[Port
	Single Port 🗸		Port

DSL/Cable Optimization

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

DSL/Cable Optimization	?
Enable	

peplink PEPWAVE

OK

Cancel



PepVPN Traffic Optimization

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

PepVPN Traffic Optimization	
Enable	



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 Clou	d Net	twork	Advanced	AP	System	Status	Apply Change
Advanced									
PepVPN	Outboun	d Firewall Rules (👋	Orag and	d drop ro	ws by the lef	t to cha	ange rule (order)	
GRE Tunnel	Rule		otocol	Source			Des	tination	Action
Port Forwarding	Default	An	у	Any			Any		O
NAT Mappings					Add I	Rule			
)oS									
Bandwidth		Firewall Rules (VD)				to chan	ige rule or		
Control	Rule		otocol	WAN	Source			Destination	Action
Application	<u>Default</u>	An	у	Any	Any			Any	v
irewall					Add I	Rule			
Access Rules		Network Firewall Ru	1 ()44	D			0.1.		
Content Blocking	Rule		otocol	Source		y the le		tination	Action
Routing Protocols	Default	An		Any			Any	tination	Action
OSPF & RIPv2	<u>berden</u>		,	7	Add I	Rule			
BGP									
Remote User Access		Detection and DoS	Preven	tion					
lisc. Settings	Disabled								
RADIUS Server	Local Ser	vice Firewall Rules	Drag	and drop	rows by the	left to	change r	ule order)	
Certificate	Rule		rvice			VAN		Source	Action
Manager	Default	An	у		A	Any		Any	O
Service Forwarding		· · · · ·			Add	Rule		·	· ·
Service Passthrough									
Grouped Networks									
SIM Toolkit									

Outbound and Inbound Firewall Rules

The outbound and inbound firewall settings are located at Advanced>Firewall>Access Rules.

Outbound Firewall Rules	(\"Drag and	I drop rows by the left to change	rule order)		?	
Rule	Protocol	Source	Destination	Action		
<u>test</u>	Any	Any	Any	Q,	×	
<u>Default</u>	Any	Any	Any	0		
	Add Rule					

Click Add Rule to display the following screen:

New Firewall Rule		
Rule Name		
Enable		Always on V
Protocol	?	Any V CIProtocol Selection :: V
Source	?	Any Address 🗸
Destination	?	Any Address 🗸
Action	?	● Allow ○ Deny
Event Logging	?	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	
<u>test</u>	Any	Any	Any	Any	0	×
<u>Default</u>	Any	Any	Any	Any	0	
	Add Rule					

Click Add Rule to display the following screen:

Add a New Inbound Firewall Rule					
New Firewall Rule					
Rule Name					
Enable	Always on V				
WAN Connection	Any 🗸				
Protocol 🤅	Any V Contraction Contraction Contraction				
Source 🤇	Any Address 🗸				
Destination	Any Address				
Action	● Allow ○ Deny				
Event Logging	Enable				
	Save Cancel				

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

Internal Network Firewall Rules (^{WD} rag and drop rows by the left to change rule order)						
Rule	Protocol	Source	Destination	Action		
<u>test</u>	Any	Any	Any	Q	×	
<u>Default</u>	Any	Any	Any	0		
	Add Rule					

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

Add a New Internal Network Firewall Rule				
New Firewall Rule				
Rule Name				
Enable	Always on V			
Protocol 🤶	Any V C:: Protocol Selection :: V			
Source 🤶	Any Address 🗸			
Destination 🤶	Any Address 🗸			
Action 🤶	● Allow ○ Deny			
Event Logging	Enable			

Save Cancel

	Inbound / Outbound / Internal Network Firewall Settings
Rule Name	This setting specifies a name for the firewall rule.
Enable	This setting specifies whether the firewall rule should take effect. If the box is checked, the firewall rule takes effect. If the traffic matches the specified protocol/IP/port, actions will be taken by the Pepwave router based on the other parameters of the rule. If the box is not checked, the firewall rule does not take effect. The Pepwave router will disregard the other parameters of the rule.
	Click the dropdown menu next to the checkbox to place this firewall rule on a time schedule.
WAN Connection (Inbound)	Select the WAN connection that this firewall rule should apply to.
Protocol	This setting specifies the protocol to be matched. Via a drop-down menu, the following protocols can be specified: Any TCP UDP ICMP DSCP IP Alternatively, the Protocol Selection Tool drop-down menu can be used to automatically fill in the protocol and port number of common Internet services (e.g., HTTP, HTTPS, etc.) After selecting an item from the Protocol Selection Tool drop-down menu, the protocol and port number remains manually modifiable.
Source IP & Port	This specifies the source IP address(es) and port number(s) to be matched for the firewall rule. A single address, 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	This setting specifies whether or not to log matched firewall events. The logged messages are shown on the page Status>Event Log . A sample message is as follows: Aug 13 23:47:44 Denied CONN=Ethernet WAN SRC=20.3.2.1 DST=192.168.1.20 LEN=48 PROTO=TCP SPT=2260 DPT=80 • CONN : The connection where the log entry refers to • SRC : Source IP address • DST : Destination IP address • LEN : Packet length • PROTO : Protocol • SPT : Source port • DPT : Destination port



Click **Save** to store your changes. To create an additional firewall rule, click 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 Firewal	l Rules (Drag and drop rows to change	rule order)	2
Rule	Protocol	Source IP Port	Destination IP Port	Policy
No web access	тср	Any Any	Any 80	Deny 🗙
No FTP access	¶ [®] ≱	Any Any	Any 21	Deny 🔀
<u>Default</u>	Any	Any	Any	Allow
Add Rule				

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.

Тір
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

Intrusion Detection and DoS Prevention	?
Disabled	
Disabled	

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

To turn on this feature, click **I**, 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

To remove a rule, click the **to** button.

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

Content Blocking

Application Blockin Please Select Applic				?
Web Blocking				?
Preset Category High Moderate Low Custom 	 Adware P2P/File sharing 	Audio-VideoPornography	 File Hosting Update Sites 	
Content Filtering Dat Update	tabase Auto (🗍 🗌			
Customized Domains	5			?
Exempted Domains f	from Web Blocking			+ ? +
Exempted Subnets			Subnet Mask 255.255.255.0 (/24)	? • •
URL Logging				
Enable Log Server Host		Ē P	ort: 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	
<u>0.0.0.0</u>	No interface is selected	×
	Add	

RIPv2 No RIPv2 Defined.

OSPF & RIPv2 Route Advertisement				
PepVPN Route Isolation	?	🗌 Enable		
Network Advertising	?		~	+
		All LAN/VLAN networks will be adve	ertised when no network advertising is chosen.	
Static Route Advertising	?	2 Enable		
	\sim	Excluded Networks	Subnet Mask	
			255.255.255.0 (/24) 🗸	+
		Save		

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

OSPF settings		×
Area ID		
Link Type	Isoadcast O Point-to-Point	
Authentication	None 🔻	
Interfaces	Help Close Click here to customize interface cost	
	Save	Cancel

	OSPF Settings	
Area ID	Determine the name of your Area ID to apply to this group. Machines linked to this group will send and receive related OSPF packets, while unlinked machines will ignore it.	
Link Type	Choose the network type that this area will use.	
Authentication	Choose an authentication method, if one is used, from this drop-down menu. Available options are MD5 and Text . Enter the authentication key next to the drop-down menu.	
Interfaces	Determine which interfaces this area will use to listen to and deliver OSPF packets	
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	E
Authentication	None 🔻
Interfaces	
	Save Cancel

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

OSPF & RIPv2 Route Advertisement		
PepVPN Route Isolation	Enable	
Network Advertising	All LAN/VLAN networks will be advertised when no network advertising is chosen.	
Static Route Advertising	Enable	
	Save	

	OSPF & RIPv2 Route Advertisement
PepVPN Route	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.
Isolation	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.
Network	Selected networks will be advertised over OSPF & RIPv2. If no network is selected, all LAN / VLAN networks will be advertised by default.
Advertising	All the networks belonging to interfaces that have OSPF or RIPv2 enabled will be advertised even if they are not selected in this table.
Static Route Advertising	Enable this option to advertise LAN static routes over OSPF & RIPv2. Static routes that match the Excluded Networks table will not be advertised.



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.	
		Add	

Click "x" to delete a BGP profile

Click "Add" to add a new BGP profile

BGP Profile	
Profile Name	
Enable	
Interface	Untagged LAN 🗸
Router ID	LAN IP Address Custom:
Autonomous System	
Neighbor ?	IP Address Autonomous Multihop Password AS-Path System / TTL Password Prepending
	disable +
Hold Time 📀	240
Next Hop Self 📀	
iBGP Local Preference 📀	100
BFD ?	Enable

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

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

Route Advertisement						
Network Advertising	?				~	+
Static Route Advertising	?	🗌 Enable				
Custom Route Advertising	?	Networks		Subnet Mask		
	\sim			255.255.255.0 (/24)	~	+
Advertise OSPF Route	?					
Set Community	?	Community R	oute Prefix			
	Ŭ					+

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



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

Route Import				
Filter Mode	? Reject ▼			
Blocked Networks	Network	Subnet Mask	Exact Match	
		255.255.255.0 (/24)	▼ □	+

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

Route Export						
Filter Mode (? 🖪	Accept 🗸				
Restricted Networks	N	letwork	Subnet Mask		Exact Match	
			255.255.255.0 (/24)	~		+
Export to other BGP Profile (?					
Export to OSPF	?					

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

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	\checkmark	
VPN Type	● L2TP with IPsec ○ PPTP ○ OpenVPN	
Preshared Key	✓ Hide Characters	

L2TP with IPsec Remote User Access Settings		
Pre-shared Key	Enter your pre shared key in the text field. Please note that remote devices will need this preshared key to access the Balance.	



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

Continue to configure the authentication method.

OpenVPN

Remote User Access Settings		
Enable		
VPN Type	○ L2TP with IPsec ○ PPTP ● OpenVPN You can obtain the OpenVPN client profile from the <u>status page</u> .	

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	
VPN Type	○ L2TP with IPsec ● PPTP ○ OpenVPN

No additional configuration required.

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

Continue to configure authentication methods.

Authentication Methods

Connect to Network ?	Untagged LAN V	
Authentication	Local User Accounts	
User Accounts ?	Username	Password

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

User accounts:

This setting allows you to define the Remote User Accounts.

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

Note:

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

The password must be between 8 and 12 characters long.

LDAP Server:

Connect to Network 🛛 🕐	Untagged LAN V
Authentication	LDAP Server
LDAP Server	Port 389 Default
	Use DN/Password to bind to LDAP Server
Base DN	
Base Filter	

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

Radius Server:

Authentication	RADIUS Server	
Auth Protocol	MS-CHAP v2 V	
Auth Server	Port 1812 Default	
Auth Server Secret	🕑 Hide Characters	
Accounting Server	Port 1813 _ Default	
Accounting Server Secret	📃 🗹 Hide Characters	

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

Active Directory:

Connect to Network 📀	Untagged LAN 🔻
Authentication	Active Directory
Server Hostname	
Domain	
Admin Username	
Admin Password	✓ Hide Characters

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



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		
Host		
Port	1812	
Secret	Hide Characters	
		Save Cancel

	Authentication Server
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		
Host		
Port	1813	
Secret		
	Hide Characters	

	Accounting Server
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 Add Certificate				
Wi-Fi WAN CA Certificate No Certificates defined				
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	Enable
Web Proxy Forwarding Setup Web Proxy Forwarding	Enable
DNS Forwarding Setup Forward Outgoing DNS Requests to Local DNS Proxy	Enable
Custom Service Forwarding Setu Custom Service Forwarding Settings	P
	· · · · · · · · · · · · · · · · · · ·



SMTP Forwarding

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

SMTP Forwarding	Enable			
Connection		Enable Forwarding?	SMTP Server	SMTP Port
WAN 1				
WAN 2				
WI-FI WAN				
Cellular 1				
Cellular 2				
USB				

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

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

Web Proxy Forwarding

Web Proxy Forwarding Setup				
Web Proxy Forwarding	Enable			
Web Proxy Interception Se	ttings			
Proxy Server	IP Address (Current settings	Por in users' browser)	t	
Connection		Enable Forwarding?	Proxy Server IP Address : Port	
WAN 1				
WAN 2				
Wi-Fi WAN				
Cellular 1			:	
Cellular 2			:	
USB				

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

DNS Forwarding

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

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

Custom Service Forwarding

Custom Service Forwarding Se	tup				
Custom Service Forwarding	Enable				
Settings	Source Network	TCP Port	Server IP Address	Server Port	
	▼				+

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



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

Service Passthrough

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

Service Passthrough Support	
SIP 🥐	 Standard Mode ● Compatibility Mode ✓ Define custom signal ports 1. 2. 3.
H.323	✓ Enable
FTP 🕐	 Enable Define custom control ports 1. 2. 3.
ТЕТР	Enable
IPsec NAT-T	 Enable Define custom ports 2. 3. Route IPsec Site-to-Site VPN via
(Registered trademarks are copyrighted by thei	r respective owner)

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

	Service Passthrough Support
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	Accounting	Accounting			
Networks	Network	Subnet Mask			
	192.168.50.192	255.255.255.224 (/27) 🔻 🗶			
		255.255.255 (/32) 🔹 🕂			

PEPWAVE Dashboard SpeedFusion Cloud Network Advanced AP System Advanced PepVPN Add a New Outbound Firewall Rule GRE Tunnel Port Forwarding **New Firewall Rule** NAT Mappings Rule Name QoS ~ Bandwidth Protocol (?) Any 🗙 🗲 :: Protocol Selection :: ~ Control Application (?)Grouped Network V Accounting V Firewall ? ~ Any Address Access Rules (?)● Allow ○ Deny

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



SIM Toolkit

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

	SIM Status	
No SIM information	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	294287963063004
Tool	USSD
USSD	
USSD Code	Submit

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

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

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

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

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

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

SMS

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

SIM Status	
WAN Connection	Cellular
SIM Card	1
IMSI	234207302582581
Tool	SMS •

SMS		Refresh
Jun 21, 2017 18:00	eter Thank you, your arti-parametrik/vitik/dir - you are sharperide-adar you first topic at them.as.ak	×
May 06, 2017 12:23	3.4644 where is him over will is weak in size. So is your Phylic second on your desires or a weakle place whether here http://www.example.com/example.com/ here.com/	×
Mar 15, 2017 10:03	From Herry Sector New a planned membraneous a final sector time stop and the week. If your sectors attained, you use physicise from \$2.9, 199-199.	×
Mar 06, 2017 14:50	(MAGP) "Processing theory and the methy increases. On the paper PhySic measurement providentings on on a maintent phonon which have interpreterminate drawn an analytic state of a	×
Dec 28, 2016 09:53	From Here: rs, as here pulse approximation to mention half-prove offer test to control you, the affer applied to your fract take, they matches including charge wit research influence investor next (or, from	×
Dec 06, 2016 13:09	Minet Affects 2: Your new sold is made to come. On to pour Phy? account on your displays or or is making phone city. Instructing of walking them as any formality of	
Nov 08, 2016 11:29	Proper Blance Profile. Dense is planned materiansame in the distribution film MrQ annu Neurands. If your section is affected, you can party provide interaction of the Article	×
Sep 07, 2016 17:05	Press literar Read more deductor temportubility over modes of describing backgroups of the car buy is tells with or to meet your residuingers bit in Contemp Operating 1	×



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	АР	System	Status	Apply Changes
АР								
Wireless SSID	O InCon	trol management enabled	l. Wireless SS	SID can now b	e conf	igured on <u>Ir</u>	Control.	
Settings	SSID			Security Pol	icv			
Status				WPA2 - Perso	1.11			×
Access Point				New	SID			
Wireless SSID						R.		0
Wireless Client								
Nearby Device								
Event Log								

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

SSID Settings				
SSID				
Enable	Always on V			
VLAN	Untagged LAN 🗸			
Broadcast SSID				
Data Rate	● Auto ○ Fixed			
Multicast Filter				
Multicast Rate	MCS16/MCS8/MCS0/6M			
IGMP Snooping				
Layer 2 Isolation				
Maximum number of clients	2.4 GHz: 0 5 GHz: 0 (0: Unlimited)			
Band Steering	Disable 🗸			

	SSID Settings
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	Layer 2 refers to the second layer in the ISO Open System Interconnect model.			
	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.			
	Do refer to this link (https://forum.peplink.com/t/lan-isolation-with-balance30-and-ap-one-ac-mini-help-needed/3914/3) for visual illustration of the feature. By default, the setting is disabled.			
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	To reduce 2.4 GHz band overcrowding, AP with band steering steers clients capable of 5 GHz operation to 5 GHz frequency.			
	Force - Clients capable of 5 GHz operation are only offered with 5 GHz frequency.			
	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.			

Security Settings		
Security Policy	WPA2 - Personal	
Encryption	AES:CCMP	
Shared Key		
	✓ Hide Characters	
Management Frame Protection	Default (Disabled) V	
Fast Transition 🤶		

Security Settings		
Security Policy	WPA2 - Enterprise V	
Encryption	AES:CCMP	
802.1X Version	• V1 O V2	
Management Frame Protection	Default (Disabled) 🗸	
Fast Transition 🤶		

	Security Settings
Security Policy	 This setting configures the wireless authentication and encryption methods. Available options: : Open (No Encryption) WPA3 -Personal (AES:CCMP) WPA2/WPA3 -Personal (AES:CCMP) WPA2 -Personal (AES:CCMP) WPA2 - Enterprise WPA/WPA2 - Personal (TKIP/AES: CCMP) WPA/WPA2 - Enterprise
	When WPA/WPA2 - Enterprise is 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.

Restricted Mode	Deny	all except listed	T	
MAC Address List	?			

	Access Control
Restricted Mode	The settings allow administrators to control access using Mac address filtering. Available options are None, Deny all except liste d, 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 <u>here</u> to define RADIUS Server Authentication profile, or you may go to <u>RADIUS Server</u> page to define multiple profiles		
Authentication Host			
Authentication Port	1812	1812	
Authentication Secret	Hide Characters	Hide Characters	
	You may click <u>here</u> to define RADIUS Server Accounting profile, or you may go to <u>RADIUS Server</u> page to define multiple profiles		
Accounting Host			
Accounting Port	1813	1813	
Accounting Secret			
	Hide Characters	Hide Characters	
NAS-Identifier	Device Name 🗸		

	RADIUS Server
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.

Guest Protect				
Block All Private IP				
Custom Subnet	Network	Subnet Mask		
		255.255.255.0 (/24) +		
Block Exception	Network	Subnet Mask		
		255.255.255.0 (/24)		

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

Firewall Mode	Lockdown - Block all except 🔻		
	Disable		
Firewall Exceptions	Flexible - Allow all except	Item	
	Lockdown - Block all except		

Firewall Settings		
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	2.4GHz 5GHz C C C C C C C C C C C C C C C C C C C		
Wi-Fi AP Settings		(2)	
Protocol	802.11ng •	802.11ac •	
Channel Width	20/40 MHz 🔻	80 MHz •	
Channel	Auto	Auto Edit Channels: 36 40 44 48 149 153 157 161	
Auto Channel Update	Daily at Clear All 00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 Wait until no active client associated 100 100	Daily at Clear All 00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00 23:00 Wait until no active client associated 100 100	
Output Power	Max V Boost	Max 🔻 🕒 Boost	
Client Signal Strength Threshold	0 -95 dBm (0: Unlimited)	0 -95 dBm (0: Unlimited)	
Maximum number of clients	0 (0: Unlimited)	0 (0: Unlimited)	
Beacon Rate ?	1 Mbps 🔻		
Beacon Interval 🔹 🕐	100 ms •		
DTIM ?	1 Default		
RTS Threshold	0 Default		
Fragmentation Threshold	0 (0: Disable) Default		
Distance / Time Converter	4050 m Note: Input distance for recommended values		
Slot Time ?	O Auto Custom 9 µs Default		
ACK Timeout ?	48 μs Default		
Frame Aggregation			

	Wi-Fi Radio Settings
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

	Wi-Fi AP Settings
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 [▲]	This field is for specifying the wait time before the Surf SOHO transmits a packet. By default, this field is set to $9 \ \mu s$.
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 $48 \ \mu s$.
Frame Aggregation ^A	This option allows you to enable frame aggregation to increase transmission throughput.

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

AP > Status

Access Point

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



AP Status		
Name	IP Address	G Ø
2	(Local)	👑 🕼 🔝

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

Client List						
MAC Address	IP Address	Туре	Signal	SSID	Upload	Download
80:56:f2:98:75:ff	10.9.2.7	802.11ng	Excellent (37)	Balance	66.26 MB	36.26 MB
c4:6a:b7:bf:d7:15	10.9.2.123	802.11ng	Excellent (42)	Balance	6.65 MB	2.26 MB
70:56:81:1d:87:f3	10.9.2.102	802.11ng	Good (23)	Balance	1.86 MB	606.63 KE
e0:63:e5:83:45:c8	10.9.2.101	802.11ng	Excellent (39)	Balance	3.42 MB	474.52 KE
18:00:2d:3d:4e:7f	10.9.2.66	802.11ng	Excellent (25)	Balance	640.29 KB	443.57 KE
14:5a:05:80:4f:40	10.9.2.76	802.11ng	Excellent (29)	Balance	2.24 KB	3.67 KB
00:1a:dd:c5:4e:24	10.8.9.84	802.11ng	Excellent (29)	Wireless	9.86 MB	9,76 MB
00:1a:dd:bb:29:ec	10.8.9.73	802.11ng	Excellent (25)	Wireless	9.36 MB	11.14 MB
40:b0:fa:c3:26:2c	10.8.9.18	802.11ng	Good (23)	Wireless	118.05 MB	7.92 MB
e4:25:e7:8a:d3:12	10.10.11.23	802.11ng	Excellent (35)	Marketing	74.78 MB	4.58 MB
04:f7:e4:ef:68:05	10.10.11.71	802.11ng	Poor (12)	Marketing	84.84 KB	119.32 KE

Close

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

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

Close

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

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



Click on any point in the graphs to display detailed usage and client information for that device, using that SSID, at that point in time. On the **Data Usage by** menu, you can display the information by SSID or by AP send/receive rate.

Event Log		🗹 Auto re	fresh
Aug 18 13:54:41	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with	0 (2.4 GHz)	
Aug 18 13:54:41	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) disassociated from	(2.4 GHz)	
Aug 18 13:52:14	Client Gliminian (B2:AD:FF:A4:3F:FF) associated with Research (2.4 GHz)	
Aug 18 13:48:58	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with	6669 (2.4 GHz)	
Aug 18 12:12:33	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with	(5 GHz)	
Aug 18 11:25:32	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) disassociated from	(2.4 GHz)	
Aug 17 15:14:28	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with	(5 GHz)	
Aug 17 15:14:27	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) disassociated from P	9 (5 GHz)	
Aug 17 15:14:11	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with	(5 GHz)	
Aug 17 15:13:35	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) disassociated from	(5 GHz)	
Aug 17 11:51:13	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with	(5 GHz)	
Aug 17 11:51:13	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) disassociated from	(2.4 GHz)	
Aug 17 09:00:05	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with	(2.4 GHz)	
Aug 17 09:00:04	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) disassociated from	(2.4 GHz)	
Aug 17 09:00:04	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with	(2.4 GHz)	
Aug 16 09:42:15	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with	(2.4 GHz)	
Aug 16 09:42:15	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) disassociated from	(5 GHz)	
Aug 16 09:07:18	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with	(5 GHz)	
Aug 13 09:03:53	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) associated with	(5 GHz)	
Aug 12 18:28:44	Client LAPTOP-TIRBRFPU (C8:B2:9B:63:C2:CA) disassociated from	(5 GHz)	

Click the Event tab next to Wireless Usage to view a detailed event log for that particular device.

Wireless SSID

SID Received(kbps) Sent(kbps) APs WPA2 - Personal 1 695.62 561.00 1 🗹 2.4 GHz 🗹 5 GHz Usage Total Send Total Recv 28.61 MB 19.07 MB -Usage 9.54 MB -0 B · 08:10 08:20 07:40 07:50 08:00 08:30 No. of Clients Total 2 Clients 1 0 07:40 07:50 08:10 08:20 08:00 08:30

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

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



Wireless Client

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

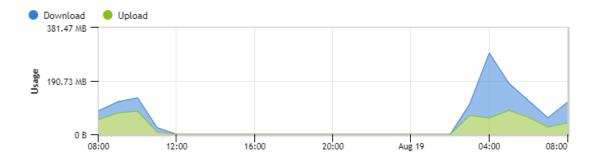
Search Filter								
Search Key		Client MAC	Address	s / SSID				
Maximum Result (1-256	5)	50						
Show Associated Clients	s Only							
Search Result								
			ſ	Search				
				Search				
			l	Search				
Wireless Clients				Search				
	IP Address	<u>Type</u>	RSSI (dBm)	SSID	AP		Duration	
	<u>(P Address</u>		<u>(dBm)</u>		AP		<u>Duration</u> 02:26:42	☆ Lu
Name / MAC Address A I			(<u>dBm)</u> -54		AP			☆ ☆ ₩
Name / MAC Address A I	-	802.11ac 802.11ng	<u>(dBm)</u> -54 -	SSID	<u>AP</u> -		02:26:42	
<u>Name / MAC Address</u> ▲ I	-	802.11ac 802.11ng	<u>(dBm)</u> -54 -	SSID	AP - Upload	Downle	02:26:42	

Here, you will be able to see your network's heaviest users as well as search for specific users. Clicking on the $\frac{1}{2}$ icon bookmarks the specific user, and clicking on the $\frac{1}{2}$ icon displays additional details about the user.

x

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

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



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

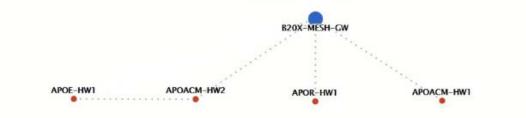
Close

Mesh / WDS

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

		Peer MAC	Protocol	Rate (Send)	Rate (Receive)	Signal (<u>dBm)</u>	Duration
•	APOACM-HW1						
	Mesh (memilik)		802.11ac	325M	650M	-56	19:13:35
	APOACM-HW2/						
	Mesh (Internet)	(802.11ac	650M	351M	ant -63	00:49:20
	Mesh (Contraction of the local division of the loc	802.11ac	390M	325M	 -67	01:35:09
•	APOE-HW1/						
	Mesh (Contraction of the local division of the	802.11ac	58.5M	130M	att -69	00:45:22
٠	APOR-HW1/						
	Mesh (Mesh)		802.11ac	325M	866.7M	 -53	19:14:44
•	B20X-MESH-GW/						
	Mesh (802.11ac	433M	650M	att -69	19:14:44
	Mesh (802.11ac	325M	390M	att -66	01:35:42
	Mesh (802.11ac	351M	650M	-70	19:13:45
	Mesh (802.11ac	130M	117M	-88	00:45:52







Nearby Device

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

Search Filter			
Search Key	MAC Address / SSID		
Туре			
Maximum Result (1-999)	200		
Time	From hh:mm to hh:mm		
Search			

Nearb	y Devices							
<u>Mark</u>	Type	MAC Address	<u>SSID</u>	<u>Channel</u>	Encryption	Last Seen	Mar	rk as
	Station Probe	54:27:1E:71:24:3D	-	6		2 minutes ago	0	8
	Station Probe	F8:A7:63:99:1A:4B	-	6		2 minutes ago	0	-
	Station Probe	B4:69:21:67:77:E9	-	6		3 minutes ago	0	8
	Station Probe	F4:D1:08:C4:49:B0	-	36		3 minutes ago	0	8
	Station Probe	08:F8:BC:63:B4:28	-	6		4 minutes ago	0	8
	Station Probe	44:1C:A8:9C:2E:3B	-	6		5 minutes ago	0	8
	Station Probe	E8:5A:8B:F7:EF:9D	-	36		5 minutes ago	0	8
	Station Probe	C4:FE:5B:AC:44:9B	-	6		6 minutes ago	0	8
	Station Probe	80:30:49:3E:35:A1	-	36		7 minutes ago	0	8
	Station Probe	40:EC:99:5E:83:1E	-	6		8 minutes ago	0	8
	Station Probe	50:3D:C6:8C:2C:DA	-	36		9 minutes ago	0	8
	Station Probe	E4:F0:42:2E:FE:7A	-	36		10 minutes ago	0	8
	Station Probe	38:F9:D3:99:BE:5D	-	6		13 minutes ago	0	8
	Station Probe	94:90:34:FE:9E:61	-	6		16 minutes ago	\bigcirc	8
	Station Probe	88:46:04:51:9B:31	-	6		17 minutes ago	0	8
	Station Probe	F4:60:E2:D8:B1:14	-	6		20 minutes ago	0	8
	Station Probe	B0:89:00:24:93:ED		6		23 minutes ago	0	8
	Station Probe	C8:F6:50:E2:03:00	-	6		26 minutes ago	0	8
	Station Probe	A4:77:33:57:A6:E2		6		30 minutes ago	0	8
	Station Probe	68:3E:26:FC:F9:B3	-	6		32 minutes ago	0	8

Prev 1-20 V (79) <u>Next</u>

Suspected Rogue Devices

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



Event Log

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

Filter	
Search key	Client MAC Address / Wireless SSID / AP Serial Number / AP Profile Name
Time	From hh:mm to hh:mm
Alerts only	
	Search

Event Log		🗹 Auto re	fresh
Aug 23 11:24:23	Client LAPTOP-) associated with	
Aug 23 10:16:08	Client LAPTOP-	disassociated from ()	
Aug 23 09:40:33	Client LAPTOP-	associated with (
Aug 20 17:23:07	Client LAPTOP	associated with	
Aug 20 17:23:07	Client LAPTOP-T	uncontraction () disassociated from ()	
Aug 20 09:02:40	Client LAPTOP-T	associated with income (and the second se	
Aug 19 18:38:02	Client LAPTOP-1	associated with (
Aug 19 18:37:44	Client LAPTOP-	disassociated from (
Aug 19 18:19:46	Client LAPTOP-T	associated with	
Aug 19 17:52:37	Client LAPTOP-) disassociated from the second second second	
Aug 19 17:51:35	Client LAPTOP	···) associated with	
Aug 19 17:43:05	Client LAPTOP	disassociated from	
Aug 19 17:42:30	Client LAPTOP-1	associated with	
Aug 19 17:37:41	Client LAPTOP-) disassociated from	
Aug 19 17:36:37	Client LAPTOP-	associated with (
Aug 19 17:19:10	Client LAPTOP-1	.) disassociated from (
Aug 19 17:15:21	Client LAPTOP-1) associated with	
Aug 19 17:13:16	Client LAPTOP-1	 disassociated from k 	
Aug 19 13:13:53	Client LAPTOP-7) associated with	
Aug 19 13:13:53	Client LAPTOP-1	disassociated from	
			More

Events

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



System Settings

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

PEPWAVE	Dashboard	SpeedFusion Cloud	Network	Advanced	AP S	ystem	Status		Apply Changes
System									
 Admin Security 	Admin Se	ettings							(2
Firmware	Device Na	ame	[HO_SHIS		hos	stname: su	urf-soho-	
Time	Admin Us	er Name	admin						
Schedule	Admin Pas	ssword		•		_			
Email Notification	Confirm A	Admin Password		•		=			
Event Log		y User Name	user			=			
SNMP	User Pass					=			
 InControl 						=			
 Configuration 		Jser Password							
Feature Add-ons	Web Sess	ion Timeout		urs 0 Minu	ites				
Reboot	Authentic	ation Method	🔵 💿 Local A	Account \odot RA	DIUS O	TACACS	+		
Tools	CLI SSH 8	& Console 🤇	🕽 🗆 Enable						
Ping	Security		HTTPS	~					
Traceroute	Web Admi	in Access	LAN Only	~					
Wake-on-LAN	Web Admi	in Port	443						
 WAN Analysis 									
Logout				Sar	ve				

Admin Security

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

	Admin Settings
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 <i>XXXX</i> refers to the last 4 digits of the unit's serial number.
Admin User Name	Admin User Name is set as admin 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.
Read-only User Name	Read-only User Name is set as user 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		ber of hours and minutes that a web session can remain idle before the saccess to the web admin interface. By default, it is set to 4 hours .			
	external server. Authenticate with read-only access. Local	ation is selected, the web admin will authenticate using the corresponding ed users are treated as either "admin" with full read-write permission or "user I admin and user accounts will be disabled. However, when the device is no ne external server, local accounts are enabled to allow emergency access. By unt.			
	Authentication Method	O Local Account RADIUS O TACACS+			
	Authentication Protocol	MS-CHAP v2 V			
		You may click <u>here</u> to define RADIUS Server Authentication profile, or you may go to <u>RADIUS Server</u> page to define multiple profiles			
	Authentication Host				
	Authentication Port	1812			
	Authentication Secret				
		Hide Characters			
		You may click <u>here</u> to define RADIUS Server Accounting profile, or you may go to <u>RADIUS Server</u> page to define multiple profiles			
	Accounting Host				
	Accounting Port	1813			
Authentication Method	Accounting Secret	Z Hide Characters			
Wethou	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.			

	Timeout		
	• TACACS+		
	Authentication Method O Local Account O RADIUS TACACS+		
	TACACS+ Server		
	TACACS+ Server Secret		
	TACACS+ Server Timeout 3 seconds		
	TACACS+ Server This specifies the access address of the external TACACS+ server.		
	TACACS+ Server SecretThis field is for entering the secret key for accessing the RADIUS server.		
	TACACS+ Server This option specifies the time value for TACACS+ timeout Timeout 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.		
CLI SSH Access Public Key	This field is for entering the Public Key for Admin Users and Read-only Users to access CLI SSH.		
Security	 This option is for specifying the protocol(s) through which the web admin interface can be accessed: HTTP HTTPS HTTP/HTTPS HTTP to HTTPS redirection is enabled by default to force HTTPS access to the web admin interface. 		
Web Admin Access	 This option is for specifying the network interfaces through which the web admin interface can be accessed: 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**.

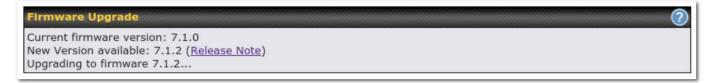
Firmware Upgrade	?
Current firmware version: 8.0.0 Firmware check pending	
	Check for Firmware

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

System	
Admin Security	Firmware Upgrade
Firmware	Current firmware version: 7.1.0
Time	New Version available: 7.1.2 (<u>Release Note</u>)
Schedule	Download and Upgrade Check for Firmware

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

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



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

Firmware Upgrade

It may take up to 8 minutes.

*Upgrading the firmware will cause the router to reboot.

Web admin interface : install updates manually

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



recommended or required for a couple of reasons.

All of the Peplink/Pepwave GA firmware can be found <u>here</u> 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	T			_	
				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	Choose File No file chosen
	Manual Upgrade

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**.

ъ

Time Settings					
Time Zone		(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, Lon ▼ □ Show all			
Time Server	0.pepwave.pool.ntp.org Default				
Save					
		Time Settings			
Time Zone	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	e profile	
Schedule Sett	ings	
Enable		The schedule function of those associated features will be lost if profile is disabled.
Name		
Schedule		Always on
Used by		
Schedule Map		
	Midnight	4am 8am Noon 4pm 8pm
Sunday	~ ~ ~ ~ ~ ~ ~ ~ ~	
Monday	· · · · · · · · ·	· · · · · · · · · · · · · · · · · · ·
Tuesday	~ ~ ~ ~ ~ ~ ~ ~ ~	
Wednesday	· · · · · · · · ·	
Thursday	· · · · · · · · ·	
Friday	· · · · · · · · ·	
Saturday	· · · · · · · · ·	
		Save Cancel

	Edit Schedule Profile
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	0
Email Notification	Z Enable
SMTP Server	smtp.mycompany.com Require authentication
Connection Security	None V
SMTP Port	25
SMTP User Name	smtpuser
SMTP Password	••••
Confirm SMTP Password	••••
Sender's Email Address	admin@mycompany.com
Recipient's Email Address	system@mycompany.com staff@mycompany.com

	Email Notification Settings
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	 This setting specifies via a drop-down menu one of the following valid connection security: None STARTTLS SSL/TTS When connection security is selected, SMTP Port will set a default port number automatically.
SMTP Port	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.
SMTP User Name / Password	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.
Confirm SMTP Password	This field allows you to verify and confirm the new administrator password.
Sender's Email Address	This setting specifies the email address the Pepwave router will use to send reports.



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

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

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

Send Test Notification Cancel

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

.....

÷

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

Email Notification Setup		
Email Notification	Enable	
SMTP Server	Require authentication	
Connection Security	SSL/TLS (Note: any server certificate will be accepted)	
SMTP Port	465	
SMTP User Name		
SMTP Password	•••••	
Confirm SMTP Password	•••••	
Sender's Email Address		
Recipient's Email Address	©	

Test Email Notification Save

Test Result

- [INFO] Try email through auto detected connection [INFO] SMTP through SSL connected
- [<-] 220 smtp.gmail.com ESMTP h11sm3907691pjg.46 gsmtp [->] EHLO balance.peplink.com

- [->] EELO balance.pepinik.com
 [<-] 250-smtp.gmail.com at your service, [14.192.209.255]
 [<-] 250-SIZE 35882577
 [<-] 250-8BITMIME
 [<-] 250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN OAUTHBEARER XOAUTH
- [<-] 250-ENHANCEDSTATUSCODES
 [<-] 250-PIPELINING</pre>
- [<-] 250-CHUNKING</p>
- 250 SMTPUTF8 [<-]
- [->] AUTH PLAIN AGdwc2dhbjk0QGdtYWlsLmNvbQBwdnJ6bWF6cGhtYXJpanpp



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	
Remote Syslog Host	Port: 514

Push Events to Mobile Devices	2
Push Events	

URL Logging		
Enable		
Log Server Host		
	Port: 514	

Session Logging		
Enable		
Log Server Host		
	Port: 514	

Save

	Event Log Settings
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
URL Logging	This setting is to enable event logging at the specified log server.
URL Logging Host	This setting specifies the IP address or hostname of the URL log server.
Session Logging	This setting is to enable event logging at the specified log server.



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

SNMP

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

SNMP Settings		
SNMP Device Name	SURF_SOHO_8439	
Location 🥐		
SNMP Port	161 Default	
SNMPv1	Enable	
SNMPv2c	Enable	
SNMPv3	Enable	
SNMP Trap	C Enable	
SNMP Trap Community		
SNMP Trap Server		
SNMP Trap Port	162	
SNMP Trap Server Heartbeat		
	Save	

Community Name	Allowed Source Network Access Mode	
No SNMPv1 / SNMPv2c Communities Defined		
Add SNMP Community		

SNMPv3 User Name	Authentication / Privacy	Access Mode
	No SNMPv3 Users Defined	
	Add SNMP User	

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

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

SNMP Community		×
Community Name Allowed Network	/ 255.255.0 (/24) ▼	
		Save Cancel

	SNMP Community Settings
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., <i>192.168.1.0</i>) 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	
Authentication	SHA V
Privacy	DES T
	Save Cancel

	SNMPv3 User Settings
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 🔻 🗖 Restricted to Status Reporting Only	
Privately Host InControl		
InControl Host		
	Fail over to InControl in the cloud.	
Save		

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

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



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

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

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

You can sign up for an InControl account at <u>https://incontrol2.peplink.com/</u>. 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	?
	Restore Factory Settings	
Ball I A Ball Ball Ball		
Download Active Configurations		
	Download	
Upload Configurations		(2)
Configuration File	Choose File No file chosen	
	Upload	

	Configuration
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	
	Activate

Reboot

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

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

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	
Reboot	



Tools

Ping

The ping test tool sends pings through a specific Ethernet interface or a SpeedFusionTM 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
	Start Stop
Results	
	Clear Log
PING 8.8.8.8 (8.8.8.8) from 10.22.1.182 5	
64 bytes from 8.8.8.8: icmp_req=1 ttl=12:	
64 bytes from 8.8.8.8: icmp_req=2 ttl=12:	
64 bytes from 8.8.8.8: icmp_req=3 ttl=12:	
64 bytes from 8.8.8.8: icmp_req=4 ttl=12:	
64 bytes from 8.8.8.8: icmp_req=5 ttl=12:	1 time=11.4 ms
8.8.8.8 ping statistics	
5 packets transmitted, 5 received, 0% pack	ket loss, time 4006ms
rtt min/avg/max/mdev = 11.427/11.680/1	1 000/0 100

Тір

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	
	Start Stop	
Results	Clea	ar Log
Frequenciate to 64,222,128.3	(34.222.285.98), 20 hope max, 60 byte packate	
1 10.01.137.254 (00.41.13	254) 3.708 ma 4.472 ma 9.207 ma	
2 10.00.00.254 (10.00.00.	M) 0.010 mg 1.000 mg 1.446 mg	
1.0.00.00.1	275 ma 1.525 ma 1.968 ma	
+ 10.003.2 (10.00.3.2) & I	2 ma 0.202 ma 0.200 ma	
1 COR. (403-886, 254 (COR. 140	88.204(3.304 mg 128.175.240.22 (128.175.240.22) 5.707 mg 128.383.88.204 (128.383.88.204) 3.472 mg	6
100.72.46.129 (100.72.4	1290 5.488 mg 188.85.229.46 (188.95.229.46) 3.292 mg 3.292 mg	
7 228-128-1.198 (228-128)	2002 4.301 mg 7.696 mg 7.496 mg	
1 138 175 86 184 1186 17	RE-1940 4-811 YM 200-128 R-1 (228-128 R-1) 4-872 YM 290-70-108-118 (240-70-180-118) 4-341 YM	
1 200 120 A 200 (200 120	2201) 3-238 mg 73.14.284.346 (72.14.284.346) 4.451 mg 228.128.8.229 (228.128.8.229) 4.678 mg	
10 15 14 205 20 (15 14 20	201 9.842 Htt 74.125.48.158 (74.125.48.158) 4.877 Ht 75.14.255.20 (72.14.255.20) 9.584 Ht	
12 12 24 205 20 175 24 20	201 & NEW ma 2016-88, 2011 1811 (2016-88, 2011 1611) 7 July ma 2016-88, 2413-30 (2016-85, 2413-30) 4, 484 ma	
12 1094-00.2502.213 (2004-0)	201.211) 6.873 ma 209.85.241.242 (209.85.241.241) 6.859 ma 6.589 ma	
1 214-228-86-47 (214-228	50.47) 8.892 ma * 7.390 ma	
or the little pass for these little	88. 881 R. (75) ma R. (48. ma R. 820 ma	

Tip

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

Wake-on-LAN

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

Wake-on-LAN Target Custom MAC Address V 00:00:00:00:00:00 Send
ke-on-LAN larget Custom MAC Address • 00:00:00:00:00 Send

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

WAN Analysis

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

PEPWAVE	Dashboard	SpeedFusion Cloud	Network	Advanced	AP	System	Status
System							
Admin Security	WAN	Performar	ce Ar	alvsis			
Firmware		point-to-point WAN performa					
Time							
Schedule		As a server	111 - 1257/10	8 8	92		
Email Notification		For the peer who has p	ublic IP addres	sses to accept c	onnecti	on.	
Event Log							
SNMP	>>	As a client For the peer to initiate	connection				
InControl		Por the peer to initiate	connection.				
 Configuration 							
Feature Add-ons							
Reboot							
Tools	1						
Ping							
Traceroute							
Wake-on-LAN							
WAN Analysis							

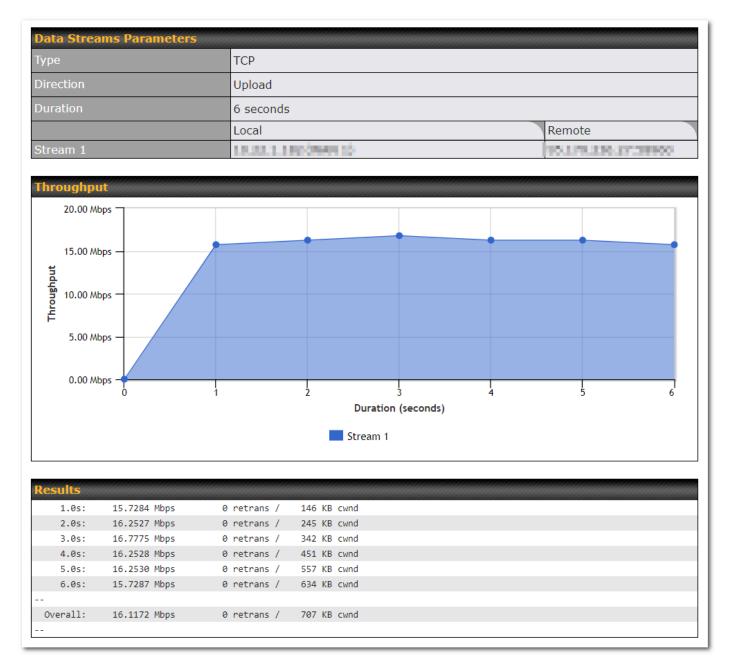
The default port is 6000 and can be changed if required. The IP address of the WAN interface will be shown in the **WAN Connection Status** section.

PEPWAVE	Dashboard	SpeedFusion Cloud	Network	Advanced	АР	System	Status	Apply Changes
System								
Admin Security	ΜΑΝ	l Performar	ice Ar	alvsis				
Firmware		point-to-point WAN performs						
Time				-				
Schedule	Server S	ettings			-			
Email Notification	Status		📒 Listenin	ng (Control Por	t: 600	0)		
Event Log	Control P	ort	6000					
SNMP				Apply	Stop	>		
 InControl 								
 Configuration 	WAN Co	nnection Status			in the second			
Feature Add-ons	📳 WAN							
Reboot	🔮 USB		No Devi	ice Detected				
Tools	💿 Wi-Fi 🗤	WAN on 2.4 GHz	🗌 Disable	д				
Ping	💿 Wi-Fi 🗤	WAN on 5 GHz	🗌 Disable	d				
Traceroute								
Wake-on-LAN								
WAN Analysis								

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 Statu	Apply Changes
System			
Admin Security	WAN Performa	nce Analysis	
Firmware	Check your point-to-point WAN perform		
Time		-	
Schedule	Client Settings		
Email Notification	Control Port	6000	
Event Log	Data Port	45232 - 45239	
SNMP	Туре	● TCP ○ UDP	
 InControl 	Direction	Upload O Download	
 Configuration 	Duration	20 seconds (5 - 600)	
Feature Add-ons			
 Reboot 	Data Streams		
Tools	Local WAN Connection		Remote IP Address
Ping	1 Not Used	~	
Traceroute	2 Not Used	v	×
Wake-on-LAN	3 Not Used	~	×
 WAN Analysis 	4 Not Used	~	
Logout	5 Not Used	~	×
	6 Not Used	~	×
	7 Not Used	~	×
	8 Not Used	~	+
		Start Test	

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



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	And
Model	Pepwave Surf SOHO MK3
Product Code	SUS-SOHO
Hardware Revision	1
Serial Number	The second se
Firmware	
PepVPN Version	8.0.0
Modem Support Version	1023 (<u>Modem Support List</u>)
InControl Managed Configurations	Firmware, Scheduled Reboot
Host Name	ALC: UNK TABLE
Uptime	6 days 3 hours 30 minutes
System Time	Fri Sep 06 03:00:20 MST 2019
Diagnostic Report	Download
Remote Assistance	Turn On

	System Information
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.

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

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

Important Note

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



Active Sessions

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

Session data captured within one		
0 !		
Service	Inbound Sessions	Outbound Sessions
Amazon	0	1
<u>DNS</u>	0	2
Facebook	0	
<u>Google</u>	0	19
Google Play Store	0	1
HTTP	0	2
IPsec	0	-
Office 365	0	42 46
<u>SIP</u>	0	
<u>SSH</u>	0	1
<u>SSL</u>	3	170
STUN	0	2 5
<u>Skype</u>	0	
XMPP	0	1
Interface	Inbound Sessions	Outbound Sessions
	0	308
	2	155
	0	0
	0	0
and the second se	0	42
	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**.

IP / Subnet	Source or Destination •	/ 255	5.255.255.255 (/32) 🔻	
Port	Source or Destination 🔻			
Protocol / Service	ТСР	•		
Interface	I WAN 1 If Cellular 1 Cellular 1 Pon	2 WAN 2 12 Cellular 2	🗆 😞 WI-FI WAN 💷 🐓 USB	
Search				
Outbound Protocol Source IP	Destination IP	Service Interfa	ace Idle Ti	ime
Total searched res	ults: 0			
Inhound				
Inbound Protocol Source IP	Destination IP	Service Interfa	ace Idle Ti	ime
			ace Idle Ti	ime
Protocol Source IP Fotal searched rest			ace Idle Ti	ime
Protocol Source IP				100000

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**.

te	r		Clients Only Clients Only					
e	nt List							
1	IP Address 🔺	Name	Download U (kbps) (l	pload (bps)	MAC Address	Network Name (SSID)	Signal (dBm)	Impo
	10.				NUCLEAR AND A			•
	10.	INCOME TRADES		1	(BOB-ROBORDA)			
	10.				2012/01/01/02/02			•
	10.	situation (1997)			10-0031-04-01-38			•
	10.	1 Acres and			10.1014/00146-05			
	10.	ay 100 0400			10.1A.00.7518A.36			•
	10.	M. Charge water		H	DOM: NOTIFICATION OF THE PARTY			•
	10.		1		104012101210			•
	10.	ANTE 100		1	1010A004040340			
	10.	COLORADO IN	25	14	HARDARDON NO.			•
	10.	mine and			10 1.5 10 1.5 10 PC			•
	10.	James Beaking		10	18-63-007Y-00453			•
	10.	with D-Max			10-14-00-54-80-03			•
	10.				AND DECADERAD			•
	10.	providence -			NUMBER OF STREET, STRE	PER. 250.1	 -62	•
	10.				In state of the second second			•
	10.	Sector 42			10-21-01-01-02-05	PER-201_1	 1 -46	•
	10.	Store Desiring	2		0.01046404040			•
	10.	19450-30-007			IO NOTICE THE			•
	10.	MARKING MARKING			NUMBER OF STREET, STRE	PER. (%) 1		•
	10.	dana.			10-0029-07-08-08			
	10.				DATE NOTICE TO			•
	10.				LUNCH STREET			•
	10.	(1-0603)			0.0.0000.0000			
	10.	be complete		14	LENGTH DURING			•
	10	an ter	1.1	1	No. 10 (Control of Control of Con			•
	10.				0.0101030-00.01			•
	171				In the party of the last			
	17.	and and			NUMBER OF STREET, STRE			
	17:	and the second sec		1	0.0000000000000			•

OSPF & RIPv2

OSPF & RIPv2		
Агеа	Remote Networks	
▼0.0.0.0		
PepVPN	192.168 /24	

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

BGP

Profile	Neighbor	
	No information	

Information on BGP can be found in this section.

PepVPN Status

🔒 🕨 3ED2-8F63-1824

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

PepVPN with SpeedFusion -	Sho	w disconnected profiles	
Search			
	·		
Remote Peer 🔺	Profile	Information	
ADA0-FFFC-11F8	FH	192.168.77.0/24	

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.

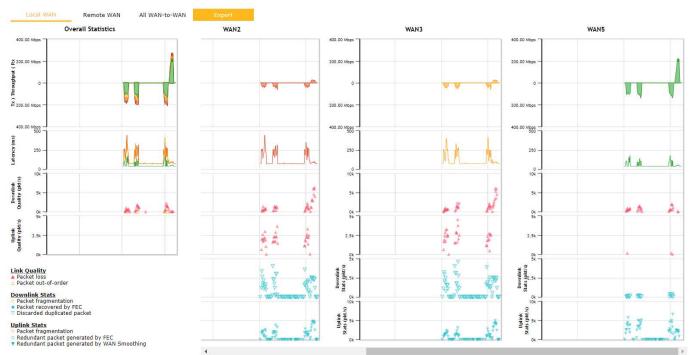
380-5 - NO NAT

....

68

Pe	oVPN with SpeedFusion - Rei	note Peer			hhhhh	Show al	l profiles
Sea	arch	SFC					
	Remote Peer 🔺	Profile		Information			
	SFC-SIN-001 (SFC-SIN-001)	SFC		SpeedFusion Cloud			
	WAN1			Not available - WAN disat	oled		
	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 disat	oled		
	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.



х

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	🗆 sł	Show remote connections						
WAN Label	● WAN Name ○ IP Address and Port							
WAN1			Not available - WAN disat	oled				
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 disab	oled				
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		?
Туре	● TCP ○ UDP	
Streams	4 🗸	Chart
Direction	● Upload ○ Download	Start
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

itatus					
Device		1			
Active Sessions	Device Event L	Firewall Event Log)		
Client List					
OSPE & RIPv2	Device Event L				Auto Refres
	Sep 30 09:23:29	Port: F		:)	
BGP	Sep 30 09:17:09	System:			
Event Log	Sep 30 09:10:39	Port			
	Sep 30 09:10:17	WA			
VAN Quality	Sep 30 09:09:09	Admir			
sage Reports	Sep 30 09:08:23	Admir			
Real-Time	Sep 30 09:07:53	Admir			
	Sep 30 09:07:32	Pc			
Hourly	Sep 30 08:56:33	WAN:			
Daily	Sep 30 08:56:05	WAN:			
Monthly	Sep 30 08:55:52	WAN:			
	Sep 30 08:55:15	WAN:			
Logout	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:			

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.



151

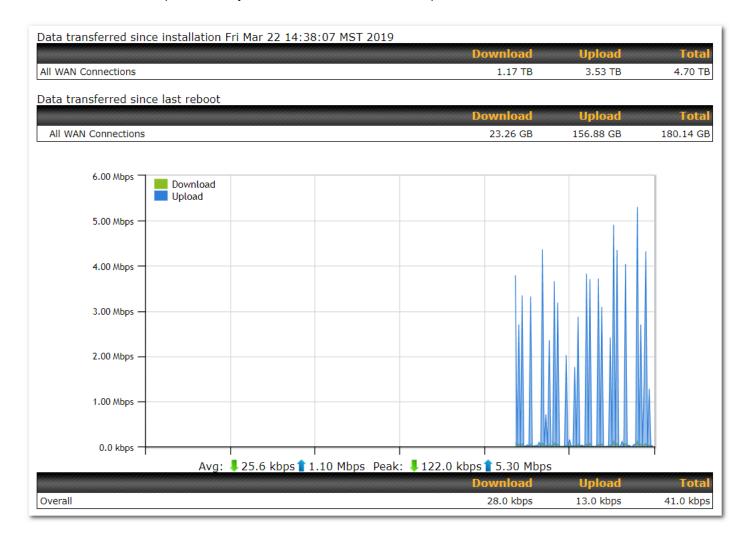


Usage Reports

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

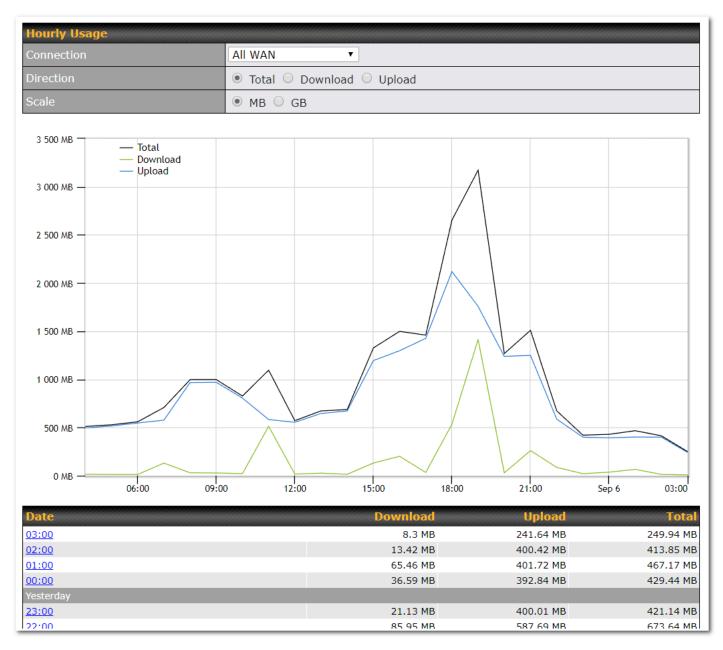
The **Data transferred since installation** table indicates how much network traffic has been processed by the device since the first bootup. The **Data transferred since last reboot** table indicates how much network traffic has been processed by the device since the last boot up.





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.



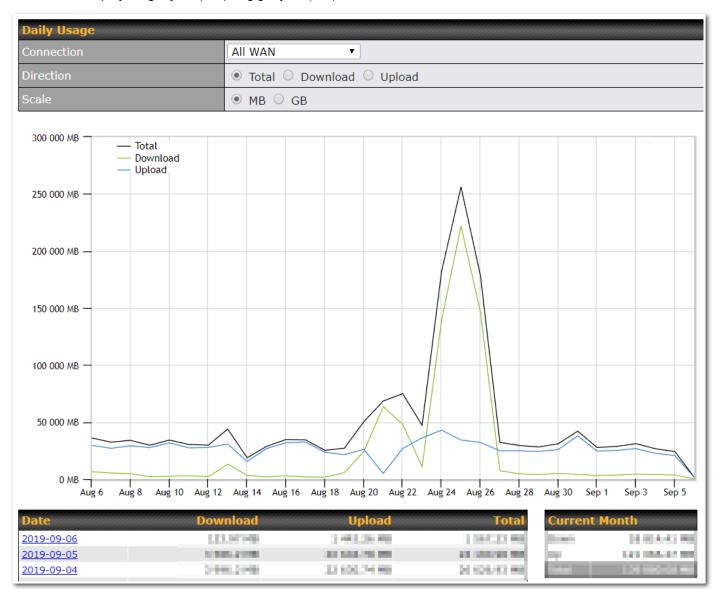


Daily

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**).

Monthly Usage		iiii
Period	● Calendar Month ○ Billing Cycle	
Connection	All WAN 🔻	
Direction	● Total ○ Download ○ Upload	
Scale	● MB ○ GB	
1 750 000 MB — Total — Total — Download — Upload		
1 500 000 MB -		-
1 250 000 MB -		-
1 000 000 MB		-
750 000 MB		
500 000 MB		+
0 MB Apr 19 Apr 19	May 19 Jun 19 Jul 19 Aug 19 Sep	19
Date	Download Upload To	otal
0.01010-0111-00010-00-00	1940A3196 30.050976 100.054	
2014 OF 18 19 19 2014 OF 18 20	251.029.0198. 029.02.0198. 1.601.02.03	1
2010-07-01 to 2010-07-01	14-040-83 Mill 20140 844 281.82	-
2010-05-05-01 10 2010-05-00	to the All All and the Part of the All All All All All All All All All Al	
2010-08-01 to 2009-08-01.	14.316.79 HE +HL06.36 HE 144.29L38	
20125-04-00 No 2015-04-05	2013/22/23 56 562 294,61100 068 124,65	_
2019-00-01 to 2019-00-01.	645246 HB 334,104,21 HB 264,261,20	240



Appendix A: Restoration of Factory Defaults

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

1. Locate the reset button on the back panel of the Pepwave Surf SOHO.

2. With a paperclip, press and keep the reset button pressed.

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

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

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

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

Important Note

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



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

Usage	Service	Inbound/Outbound	Default Status
Data flow	InControl	Outbound	Enabled
HTTPS service	InControl	Outbound	Enabled
Optional, used when TCP 443 is not responding	InControl	Outbound	Enabled
Remote Web Admin	Appliance	Outbound	Enabled
VPN Data (TCP Mode)	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
VPN handshake	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
VPN Data	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
VPN Data (alternative)	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
VPN Sub-Tunnels Data	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
VPN Sub-Tunnels Data (alternative)	PepVPN / SpeedFusion	Inbound / Outbound*	Disabled
VPN Data	IPsec	Inbound / Outbound*	Disabled
VPN initiation	IPsec	Inbound / Outbound*	Disabled
L2TP	Remote User Access	Inbound	Disabled
L2TP	Remote User Access	Inbound	Disabled
L2TP	Remote User Access	Inbound	Disabled
OpenVPN	Remote User Access	Inbound	Disabled
PPTP (GRE)	Remote User Access	Inbound	Disabled
Remote Assistance Direct connection	Peplink Troubleshooting Assistance	Outbound	Enabled
HTTP traffic	Web Admin Interface access	Inbound	Enabled
HTTPS traffic	Web Admin Interface access (secure)	Inbound	Enabled
SSH	SSH	Inbound	Disabled
SNMP Get	SNMP monitoring	Inbound	Disabled
SNMP Trap	SNMP monitoring	Outbound	Disabled
Radius Authentication	Radius	Outbound	Disabled
Radius Accounting	Radius	Outbound	Disabled
Network Time Protocol	NTP	Inbound Outbound	Disabled Enabled
			Disabled
	Data flow HTTPS service Optional, used when TCP 443 is not responding Remote Web Admin VPN Data (TCP Mode) VPN handshake VPN Data (Alternative) VPN Data (alternative) VPN Sub-Tunnels Data (alternative) VPN Sub-Tunnels Data (alternative) VPN Data VPN initiation L2TP L2TP L2TP L2TP DopenVPN PPTP (GRE) Remote Assistance Direct connection HTTP traffic SSH SNMP Get SNMP Trap Radius Authentication	Data flowInControlHTTPS serviceInControlOptional, used when TCPInControl443 is not respondingInControl VirtualRemote Web AdminApplianceVPN Data (TCP Mode)PepVPN / SpeedFusionVPN bata (TCP Mode)PepVPN / SpeedFusionVPN Data (TCP Mode)PepVPN / SpeedFusionVPN Data (alternative)PepVPN / SpeedFusionVPN Data (alternative)PepVPN / SpeedFusionVPN Sub-Tunnels DataPepVPN / SpeedFusion(alternative)PepVPN / SpeedFusionVPN DataPescVPN DataPescL2TPRemote User AccessL2TPRemote User AccessL2TPRemote User AccessOpenVPNRemote User AccessPPTP (GRE)Remote User AccessRemote Assistance DirectPeplink Troubleshooting AssistanceHTTP trafficSSHSNMP GetSNMP monitoringSNMP GetSNMP monitoringRadius ActountingRadiusRedius AccountingRadiusNetwork Time ProtocolNTP	Data flowInControlOutboundHTTPS serviceInControlOutboundOptional, used when TCPInControlOutbound443 is not respondingInControlOutboundRemote Web AdminApplianceOutboundVPN Data (TCP Mode)PepVPN / SpeedFusionInbound / Outbound*VPN Data (TCP Mode)PepVPN / SpeedFusionInbound / Outbound*VPN Data (TCP Mode)PepVPN / SpeedFusionInbound / Outbound*VPN Data (alternative)PepVPN / SpeedFusionInbound / Outbound*VPN Data (alternative)PepVPN / SpeedFusionInbound / Outbound*VPN Sub-Tunnels Data (alternative)PepVPN / SpeedFusionInbound / Outbound*VPN DataPepVPN / SpeedFusionInbound / Outbound*VPN DataPepVPN / SpeedFusionInbound / Outbound*VPN Sub-Tunnels Data (alternative)PepVPN / SpeedFusionInbound / Outbound*VPN DataIPsecInbound / Outbound*VPN pataIPsecInboundL2TPRemote User AccessInboundL2TPRemote User AccessInboundQpenVPNRemote User AccessInboundQpenVPNRemote User AccessInboundPTP (GRE)Remote User AccessInboundRemote Assistance Direct connectionPeplink Troubleshooting AssistanceInboundHTTP trafficaccess (secure)InboundSNMP GetSNMP monitoringInboundSNMP TrapSNMP monitoringOutboundSNMP TrapSNMP

NMEA format

Disclaimer:

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

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



Appendix C: Declaration

- <u>The device supports time division technology</u>
- Federal Communication Commission Interference Statement

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

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

-Reorient or relocate the receiving antenna.

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

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

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

Radiation Exposure Statement

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

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



CE Statement for Pepwave Routers (Surf SOHO)

DECLARATION OF CONFORMITY

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

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



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

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

Yours sincerely,

Antony Chong Director of Hardware Engineering Peplink International Limited





<u>2.4GHz (2412 - 2472 MHz) : 19.88 dBm</u> <u>5GHz (5150 - 5250 MHz) : 22.57 dBm</u>

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

contact as: https://www.peplink.com/

USB WAN Modem Port Specification

Surf SOHO Series

	Surf SOHO
Output Rating	5V DC, 2A